Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TUULI MARJOMAA

NIS2-direktiivin tarpeellisuus kyber-uhkien torjunnassa Euroopassa

TIETOJENKÄSITTELYN TUTKINTO-OHJELMA
2025

TIIVISTELMÄ

Marjomaa, Tuuli: NIS2-direktiivin tarpeellisuus kyberuhkien torjunnassa Euroopassa
Opinnäytetyö, AMK
Tietojenkäsittelyn tutkinto-ohjelma
Toukokuu 2025
Sivumäärä: 22

Tässä opinnäytetyössä tutkittiin Euroopan Unionin uudistettua kyberturvallisuusdirektiiviä eli NIS2-direktiiviä, joka tuli voimaan vuonna 2023 ja oli asetettava osaksi jäsenmaiden kansallista lainsäädäntöä lokakuuhun 2024 mennessä. Tämän direktiivin uudistamisen tarkoituksena oli lisätä Euroopan Unionin turvallisuutta. Opinnäytetyössä huomioitiin myös uudistetun direktiivin edeltäjä, vuonna 2016 voimaatullut NIS-tietoturvadirektiivi ja vertailtiin näiden direktiivien eroja sekä kerrottiin syitä direktiivin uudistamisen tarpeellisuuteen.

Työssä esiteltiin toimialat, joita NIS2-direktiivi koskee ja kerrottiin mitä vaatimuksia direktiivi näillä toimialoilla toimiville yrityksille ja organisaatioille asettaa. Kerrottiin myös, miten direktiivin noudattamista valvotaan sekä kiinnitettiin huomiota myös noudattamatta jättämisestä koituviin sanktioihin.

Työssä todettiin NIS2-direktiivin tarkoituksen olevan helpottaa organisaatioiden ja yritysten valmistautumista kyberuhkiin sekä parantaa näiden sietokykyä kyberuhkia vastaan. Kyberuhkia työssä käsitellessä tarkasteltiin fyysisiä, taloudellisia ja digitaalisia kyberuhkia ja esiteltiin erilaisia kyberuhan muotoja.

Tarkastelun tuloksena päästiin johtopäätökseen, että tietoturvariskien kasvaessa ja kyberuhkien lisääntyessä EU:n yhteisen NIS2-direktiivin merkitys on äärettömän suuri ja yhteiset pelisäännöt raportointiin ja valvontaan ovat enemmän kuin tarpeellisia. Uudistunut direktiivi on vaativampi, laajempi ja valvotumpi, joten sen myötä tietoturvariskien määrä vähenee sekä tietoisuus hyökkäyksistä on julkisempaa. Julkisuus tuo tietoa myös muille jäsenvaltioille ja näin ollen he osaavat myös varautua esimerkiksi mahdollisiin iskuihin ja kalasteluihin tehokkaammin.

Avainsanat: kyberturvallisuus, NIS2-direktiivi, Euroopan Unioni, kyberuhka, tietoturvadirektiivi

ABSTRACT

Marjomaa, Tuuli: The necessity of the NIS2 directive in defense against cyber threats
Bachelor's thesis
Bachelor of Business Administration, Business Information Systems
May 2025
Number of pages: 22

This thesis examined the European Union's revised cybersecurity directive, known as the NIS2 Directive, which came into force in 2023 and was required to be incorporated into the national legislation of EU member states by October 2024. The purpose of the revision was to enhance the security of the European Union. This thesis also took into account the predecessor of the revised directive, the NIS Directive, which was entered into force in 2016. It compared the differences between these directives and discussed the reasons for the need to update the directive.

This thesis presented the sectors affected by the NIS2 Directive and described the requirements the directive sets for companies and organizations operating within these sectors. It also explained how compliance with the directive is monitored and drew attention to the sanctions resulting from non-compliance.

This thesis concluded that the purpose of the NIS2 Directive is to help organizations and companies prepare for cyber threats and improve their resilience against such threats. In discussing cyber threats, this thesis presented and examined physical, financial, and digital cyber threats.

As a result of the analysis, the conclusion was drawn that as information security risks grow and cyber threats increase, the significance of the EU's common NIS2 Directive is extremely high, and common rules for reporting and monitoring are more than necessary. The revised directive is more demanding, broader in scope, and more closely monitored, and as a result, the number of information security risks will decrease and awareness of attacks will become more public. This publicity also provides information to other member states, allowing them to better prepare for example potential attacks and phishing attempts.

Keywords: cybersecurity, NIS2 Directive, European Union, cyber threat, cybersecurity directive

SISÄLLYS

1 JOHDANTO

Nopeasti muuttuvassa ja kehittyvässä maailmassa on päivä päivältä tärkeämpää pysyä muutoksien mukana, tai paremminkin niiden edellä. Samaan aikaan kun teknologia kehittyy äärimmäisen nopeaa vauhtia, myös uhat sen ympärillä kasvavat suuremmiksi. Organisaatiot ja yritykset siirtyvät yhä riippuvaisemmiksi toimivista sekä turvallisista digitaalisista palveluista ja sen vuoksi niiden tulee olla entistäkin valmistautuneempia mahdollisiin kyberuhkiin.

Helpottaakseen organisaatioiden ja yritysten valmistautumista on Euroopan Unioni säätänyt kyberturvallisuusdirektiivin, joka kulkee tuttavallisemmin nimellä NIS2-direktiivi. Tämä direktiivi on päivitetty versio aiemmasta NIS-direktiivistä, joka on astunut voimaan vuonna 2016 (Insta, n.d., kohta Keitä direktiivi koskee?).

Työssä tullaan käsittelemään NIS2-direktiiviä ja pohtimaan sen tarpeellisuutta kyberuhkien torjunnassa Euroopan Unionin alueella. Aluksi tutustutaan lähemmin direktiiviin, pohditaan vanhan ja uuden direktiivin eroavaisuuksia sekä selvitetään direktiivin vaatimuksia. Keskellä käsitellään kyberturvallisuutta ja -uhkia sekä miten NIS2-direktiivin auttaa tässä kaikessa. Lopuksi pohditaan vielä Euroopan Unionin merkitystä kyberuhkien torjunnassa ja muita tapoja, joilla se vahvistaa kyberturvallisuutta. Työn tavoitteena on antaa lukijalleen käsitys NIS2-direktiiviin tarpeellisuudesta ja siitä miten iso rooli sillä on kyberuhkien torjunnassa.

2 NIS2-DIREKTIIVI

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 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 eli lyhyesti sanottuna NIS2-direktiivi on hyväksytty Euroopan Unionissa 14. joulukuuta 2022 ja se astui voimaan 16. tammikuuta 2023. Euroopan Unionin jäsenmaiden siirtymäaika alkoi voimaan astumisesta ja kestää 21 kuukautta. Tämä tarkoittaa, että direktiivin vaatimat säädökset tuli olla kirjattuna jäsenmaiden kansalliseen lakiin 17. lokakuuta 2024 mennessä. Täten täytäntöönpanoa koskevien säännösten soveltaminen alkoi 18. lokakuuta 2024. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, s. 1; Insta, n.d.) Tällöin aiemmin voimassa ollut direktiivi (EU) 2016/1148 eli NIS-direktiivi kumoutui korvaantuessaan uudella direktiivillä.

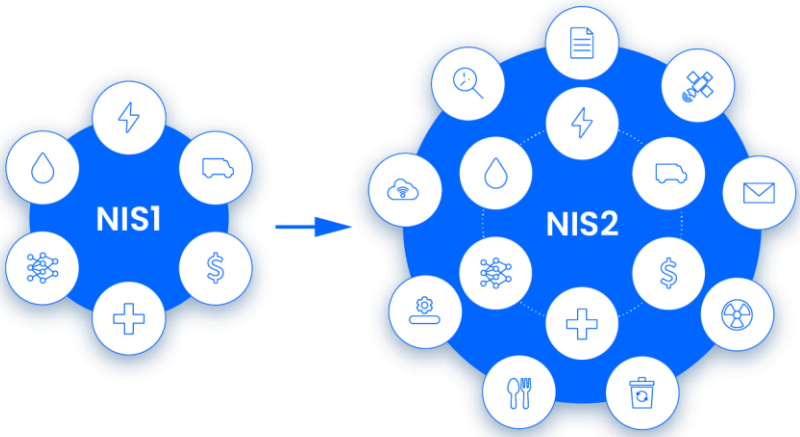
2.1 Aiempi tietoturvadirektiivi lyhyesti

NIS-direktiivi astui voimaan Euroopan Unionissa vuonna 2016 ja Suomen lainsäädäntöön se on lisätty vuonna 2018. Direktiivin tavoitteena oli asettaa yhteinen kyberturvallisuuden vähimmäistaso kriittisille toimialoille Euroopan Unionissa. (Kaihovaara, 2023.)

2.2 Direktiivin merkittävimmät uudistukset

Uudistettu NIS2-direktiivi on monessa suhteessa laajempi kuin edeltäjänsä (Insta, n.d., kohta Keitä direktiivi koskee?). Velvoitettujen toimialojen määrää on kasvatettu huomattavasti, kuten kuva 1 osoittaa. Myös turvatoimia on laajennettu merkittävästi verrattuna aiempaan direktiiviin. Yksi merkittävimmistä uudistuksista on raportointivelvollisuus eli viranomaisille tulee toimittaa raportti vuorokauden sisällä tietoturvapoikkeaman havaitsemisesta. (Netnordic, 2024.) Lisäksi NIS2-direktiivin avulla pyritään korjaamaan aiemman direktiivin

puutteet säännöissä ja tarpeissa, jolloin myös tavoitteet kasvavat kyberturvallisuuden vähimmäistasosta selkeästi korkeammalle tasolle (Deloitte, n.d.).



Kuva 1. Velvoitettujen toimialojen määrä kasvoi huomattavasti NIS2-direktiivin myötä (Uniqkey A/S, n.d.-a).

2.3 Direktiivin muutoksen syyt

Euroopan uhkaympäristö muuttui suuresti maailmanlaajuisen koronapandemian aikana. Pandemia lisäsi digitaalisten palveluiden käyttöä sekä etätyöskentelyä kotona, mahdollisesti suojaamattomissa kotiverkoissa. Jo pelkästään Suomessa pandemia-aika kasvatti suuresti erilaisiin huijausyrityksiin liittyneiden yhteydenottojen määrää. (Traficom, 2023 -b). Pandemian laannuttua Venäjä aloitti vuonna 2022 hyökkäyssodan Ukrainassa, jonka myötä useat hakkeriaktivistit, kyberrikolliset ja valtioiden tukemat ryhmät ovat aktivoituneet. Tämänkaltaisen toiminnan lisääntyminen on tuonut uuden maailmanlaajuisen uhan, eritoten Euroopan alueelle. (Eurooppa-neuvosto, 2023.) Myös teknologia ja sen ymmärrys kehittyvät jatkuvasti, jonka myötä rikolliset keksivät yhä uusia keinoja kyberturvallisuuden horjuttamiseksi.

2.4 NIS2-direktiivin tavoitteet

NIS2-direktiivi on luotu parantamaan organisaatioiden sietokykyä kyberuhkia vastaan. Direktiivin tavoitteena on varmistaa yhteinen korkea kyberturvallisuustaso koko Euroopan Unionin alueella. Kyberuhalla tarkoitetaan muun muassa tilanteita, joissa voisi aiheutua häiriötä ja vahinkoa verkko- ja tietojärjestelmille. (Insta, n.d., kohta EU:n NIS2-direktiivi parantaa organisaatioiden sietokykyä kyberuhkia vastaan.)

2.5 Toimialat

Kyberturvallisuusdirektiivi koskee toimialoja, joille kyberhyökkäykset olisivat äärimmäisen tuhoisia. Toimialat on jaettu erittäin kriittisiin ja muihin kriittisiin toimialoihin. (Insta, n.d., kohta Kriittiset toimialat.) Näiden toimialojen sisällä on direktiivin soveltamisalaan kuuluvia tahoja rajattu kokokynnyksellä, jolloin velvoite ei koske automaattisesti kaikkein pienimpiä mikroyrityksiä (Euroopan komissio, 2023 -a, kohta ”What elements of the previous…”). Yritykset ja organisaatiot, jotka joko työllistävät vähintään 50 työntekijää tai joiden vuosittainen liikevaihto tai taseen loppusumma on vähintään 10 miljoonaa euroa ovat velvoitettuja toimimaan direktiivin mukaisesti. Myös ne toimijat, jotka työllistävät yli 250 työntekijää kuuluvat direktiiviin vaikutuksen piiriin riippumatta niiden liikevaihdosta. (Pro Kyberturva, n.d.) Kokokynnystä sovelletaan myös tiettyjen pienempien toimijoiden kohdalla. Tällainen toimija voi olla muun muassa jäsenvaltion ainoa kriittistä toimintoa tarjoava yritys tai tärkeän ICT-palvelun tarjoaja. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 2 art.)

2.5.1 Erittäin kriittiset toimialat

Erittäin kriittisillä toimialoilla toimivat organisaatiot ovat suurin riski valtion kyberturvallisuuden kannalta. Niihin kohdistuvat hyökkäykset aiheuttaisivat laajaa tuhoa. Erittäin kriittisiä toimialoja kutsutaan joissain yhteyksissä myös keskeisiksi toimialoiksi.

Erittäin kriittisiin toimialoihin lukeutuvat: energia, kuljetus, pankki- ja finanssiala sekä niiden infrastruktuuri, terveydenhuolto, julkishallinto, avaruus, juoma- ja jätevesi, digitaalinen infrastruktuuri ja TVT-palveluiden hallinta (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, Liite I).

2.5.2 Muut kriittiset toimialat

Kuten aiemmin on mainittu, vuonna 2016 voimaan tulleesta NIS-direktiivistä poiketen NIS2-direktiiviä sovelletaan laajemmin eri toimialoille. Näin ollen direktiiviin on lisätty mukaan myös muut kriittiset toimialat.

Muihin kriittisiin toimialoihin kuuluvat: posti- ja kuriiripalvelut, jätehuolto, kemikaaliteollisuus ja -jakelu, elintarviketeollisuus, -jalostus ja -jakelu, digitaalisen palvelun tarjoajat ja tutkimustoiminta. Lisäksi lääkinnällisten laitteiden, tietokoneiden tai muiden elektronisten tai sähköisten laitteiden, moottoriajoneuvojen sekä muiden kulkuneuvojen valmistajat ovat direktiiviin kuuluvia toimialoja. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, Liite II.) Digitaalisen palvelun tarjoajilla tarkoitetaan verkkoyhteisöalustoja, hakukoneita ja verkossa toimivia markkinapaikkoja (Uniqkey A/S, n.d. -b).

2.6 NIS2-direktiivin vaatimukset organisaatioille ja yrityksille

NIS2-direktiivi tuo organisaatioille ja yrityksille uusia vaatimuksia verrattuna aiemmin voimassa olleeseen direktiiviin. Velvoitteet on jaettu neljään pääalueeseen: riskienhallinta, yritysvastuu, raportointivelvoitteet ja liiketoiminnan jatkuvuus (Uniqkey A/S, n.d. -c). Direktiivi vaatii organisaatioita ja yrityksiä valvomaan jatkuvasti digitaalista infrastruktuuriaan ja varautumaan poikkeustilanteisiin jatkuvuussuunnitelmalla sekä dokumentoidulla kyberturvallisuusstrategialla (Maijala, 2023).

Haasteita voi tulla, jos organisaatiolla tai yrityksellä on toimintaa useassa eri Euroopan Unionin maassa. Eri jäsenmaat voivat soveltaa omassa

lainsäädännössään direktiiviä toisistaan poikkeavilla tavoilla, jotka tulee ottaa huomioon toimintasuunnitelmaa luodessa. (Maijala, 2023.)

2.6.1 Riskienhallinta

Riskienhallinnan haasteeksi muodostuu arviointi siitä, onko riskienhallintasuunnitelma riittävän kattava organisaation toiminnan kriittisyyteen verrattuna. Organisaation tulee toteuttaa riskiarvio, jossa arvioidaan jatkuvasti toteutettavien toimenpiteiden riittävyyttä erilaisia uhkia kohtaan. Arvion tulee ulottua toimitusketjuun, joka on usein organisaation heikoin kohta. Toimitusketjun riskiarvioinnissa tulee huomioida myös kumppanien tietoturvan heikot kohdat, jotta riskienhallinta saadaan oikealle tasolle. (Asikainen, 2024.) Kumppaneita voivat olla esimerkiksi alihankkijat, jotka toimittavat palveluita kriittisellä alalla toimivalle organisaatiolle. Tällöin mahdollisesti pieni kriittisten toimialojen ulkopuolelle jäävä alihankkijayritys on myös velvollinen huolehtimaan NIS2-direktiivin velvoitteista. (Second Nature Security, n.d.)

2.6.2 Yritysvastuu

NIS2-direktiivi vaatii toimijoilta dokumentit kyberhygieniakäytännöistä sekä henkilöstön ja kumppaneiden perustason kyberturvallisuuskoulutuksen (Secapp, n.d.). Kyberhygieniakäytännöillä tarkoitetaan toimia, joilla organisaatio tai yritys voi parantaa laitteidensa verkkoturvaa ja ylläpitää järjestelmän kuntoa. Käytäntöjen tulisi olla osa käyttäjien jokapäiväistä rutiinia, jolloin se toimii ennaltaehkäisevänä prosessina uhkien torjunnassa. Jokapäiväinen toiminta auttaa pitämään myös laitteet ajantasaisesti päivitettyinä. Yrityksen tai organisaation kyberhygieniakäytäntöihin voivat kuulua esimerkiksi salasanojen vaihtaminen säännöllisesti, monivaiheisen tunnistautumisen käyttö kirjautuessa, tiedostojen säännöllinen varmuuskopiointi, palomuurien käyttö ja laadukkaan virusturvan varmistaminen. (Kaspersky, n.d.)

2.6.3 Raportointivelvollisuus

Aiemmin mainittu (kohta 2.2) raportointivelvollisuus tuo haasteita yrityksille. Organisaatiolla tulee olla ennalta luotu suunnitelma nopeaa raportointia varten, sillä ennakkoilmoitus huomatusta kyberuhasta tulee tehdä 24 tunnin sisällä ja poikkeamailmoitus 72 tunnin sisällä havainnosta. Ilmoitus tehdään CSIRT-yksikölle sekä yrityksen tai organisaation palveluiden vastaanottajille, jos mahdollinen kyberuhka saattaisi vaikuttaa heidän toimintoihinsa. Valvovista viranomaisista ja CSIRT-yksiköstä lisää kohdassa 2.7. Uhasta ilmoittaminen ei vähennä ilmoittajan vastuuta tapauksen käsittelyssä. Ilmoittajan tulee viranomaisen pyynnöstä toimittaa väliraportti mahdollisista tilannepäivityksistä sekä kuukauden kuluttua ilmoituksen jättämisestä lopullinen raportti, joka sisältää muun muassa yksityiskohtaisen kuvauksen poikkeamasta. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 23 art.)

2.6.4 Liiketoiminnan jatkuvuus

Liiketoiminnan jatkuvuuden kannalta on tärkeää, että organisaatio on huolehtinut riittävästä varmuuskopioinnista. Jos kyberhyökkäyksen myötä tiedot katoavat, turvallinen ja kattava varmuuskopiointi voi pelastaa organisaation suuremmalta vahingolta. Lisäksi hyvin luotu palautumissuunnitelma, etukäteen suunnitellut kriisinhallintatoimenpiteet ja prosessit tietoturvapoikkeaman käsittelyyn luovat turvaa liiketoiminnan jatkuvuudelle. NIS2-direktiivi velvoittaa organisaatiota huolehtimaan näiden edellä mainittujen toimintojen toteuttamisesta jatkuvuuden turvaamiseksi. (Secapp, n.d.)

2.6.5 Sanktio

Jos yritys tai organisaatio ei noudata direktiiviä, velvoittaa se jäsenmaata määräämään kyseiselle yritykselle tai organisaatiolle sakkoja. Erittäin kriittisillä toimialoilla sakko on pienimmillään joko 10 miljoonaa euroa tai 2 prosenttia liikevaihdosta, muilla kriittisillä toimijoilla joko 7 miljoonaa euroa tai 1,4 prosenttia liikevaihdosta. Sakon summaksi valikoituu vaihtoehdoista suurempi summa.

(Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 34 art.) Rahallisen sanktion lisäksi organisaation tai yrityksen liiketoiminta voidaan väliaikaisesti keskeyttää ja yrityksen vastuuhenkilö voidaan asettaa johtotehtäväkieltoon. Vastuuhenkilö voi olla toimitusjohtaja tai muu vastaava yrityksen tai organisaation laillinen edustaja. (Loistetrust, n.d.)

2.7 Direktiivin valvonta

Jokainen Euroopan Unionin jäsenmaa on määrittänyt tahon, joka toimii direktiivin toteutumista valvovana viranomaisena. Kyseinen viranomaistaho on näin ollen vastuussa myös raporttien vastaanottamisesta ja niihin puuttumisesta. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 23 art.) Erittäin kriittisiä toimialoja valvotaan viranomaisten taholta aktiivisesti etukäteen ja muita kriittisiä toimialoja passiivisesti jälkikäteen (Loihdetrust, n.d.). Valvontaa tehostaakseen jäsenvaltioissa tulee toimia myös valvova CSIRT-yksikkö.

2.7.1 CSIRT-yksiköt

NIS2-direktiivi velvoittaa jokaista jäsenmaata perustamaan yhden tai useamman tietoturvaloukkauksiin reagoivan ja niitä tutkivan yksikön. Tätä yksikkö kutsutaan CSIRT-yksiköksi. On tärkeää, että yksiköt varmistavat viestintäkanaviensa saatavuuden ja tiedottavat niistä selkeästi kohderyhmilleen. Toimintatilat ja niitä tukeva teknologia tulee suojata ja sijoittaa paikkoihin, joissa ne ovat turvassa. Jäsenmaiden tulee varmistaa, että CSIRT-yksiköiden käytössä oleva viestintä- ja tietoinfrastruktuuri on häiriönsietokykyistä. Jatkuvuuden varmistamiseksi resursseja tulee olla riittävästi ja varajärjestelmien tulee olla hyvin suunniteltuja sekä luotettavia. CSIRT-yksiköiden tärkeimpiä tehtäviä ovat kyberuhkien seuranta ja analysointi, niistä varoittaminen ja poikkeamiin reagoiminen. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555, 10–11 art.) Suomessa CSIRT-yksikön toiminnasta vastaa Traficom Kyberturvallisuuskeskus (Traficom, 2023 -a, kohta Koordinointi).

2.7.2 NIS2-soveltaminen Suomessa

Suomessa NIS2-direktiivin valvomisesta vastaa korkeimmalla tasolla Traficom Kyberturvallisuuskeskus. Valvonta on jaettu eri vastuusektoreille ja sektorien valvonnasta vastaavat eri viranomaiset (taulukko 1). Viranomaiset valvovat oman sektorinsa toimijoiden osalta lain ja direktiivin nojalla annettuja määräyksiä sekä säädöksiä. He pitävät kirjaa toimijoista toimijaluettelossa, joihin toimijoiden tulee itse ilmoittaa tietonsa, kuten nimensä, yhteystietonsa, IP-osoitealueensa, toimialatietoja sekä EU:n jäsenvaltiot, joissa sillä on toimintaa. Lisäksi, jos toimijoiden tietoihin tulee muutoksia, tulee ne ilmoittaa enintään kahden viikon kuluessa valvovalle viranomaiselle. Lisäksi viranomaisilla tulee olla ilmoituskanava, jota kautta toimialoilla toimivat yritykset voivat ilmoittaa NIS2-direktiivin vaatimuksien mukaisesti kyberuhista. Myös muut direktiivin ulkopuoliset toimijat ja yksityishenkilöt voivat tehdä ilmoituksen mahdollisista kyberuhista joko Traficomin Kyberturvallisuuskeskukseen tai poliisiin. Poliisi toimii Suomessa tietoverkkorikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa. (Kyberturvallisuuskeskus, 2025.)

Taulukko 1. NIS2-direktiivin valvovat viranomaiset Suomessa toimialoittain (Kyberturvallisuuskeskus, 2025, kohta ”Mitkä viranomaiset vastaavat toimialojen valvonnasta ja ohjeistuksesta?”).

Toimiala	Vastuuviranomainen
Energia	Energiavirasto ja Tukes
Liikenne (ilma-, raide-, vesi- ja tie-)	Traficom
Pankkitoiminta	Finanssivalvonta
Finanssimarkkinoiden infrastruktuurit	Finanssivalvonta
Terveys (terveydenhuollon tarjoajat ja EU:n vertailulaboratoriot)	Valvira
Terveys (lääkkeiden jakelu, valmistus ja tutkimus, lääkinnälliset laitteet, veripalvelut, apteekit)	Fimea

Juomavesi	Etelä-Savon ELY-keskus
Jätevesi	Etelä-Savon ELY-keskus
Digitaalinen infrastruktuuri	Traficom
TVT-palveluiden hallinta (yritysten välinen)	Traficom
Julkishallinto	Traficom
Avaruus	Traficom
Posti- ja kuriiripalvelut	Traficom
Jätehuolto	Etelä-Savon ELY-keskus
Kemikaalien valmistus, tuotanto ja jakelu	Tukes
Elintarvikkeiden tuotanto, jalostus ja jakelu	Ruokavirasto
Valmistus (Lääkinnällisten laitteiden ja in vitro -diagnostiikkaan tarkoitettujen lääkinnällisten laitteiden valmistus)	Fimea
Valmistus (Moottoriajoneuvot, perävaunut, puoliperävaunut ja muut ajoneuvot)	Traficom
Valmistus (tietotekniikka, sähkölaitteet, muut laitteet ja koneet)	Tukes
Digitaalisen palvelun tarjoajat	Traficom
Tutkimustoiminta	Traficom

3 KYBERTURVALLISUUS

Kyberturvallisuudella tarkoitetaan järjestelmien ja niiden käyttäjien kyberuhilta suojaamiseen tarvittavia toimia. Euroopan Unionin alueella tästä pidetään huolta EU:n kyberturvallisuusvirastossa. Unionin sisällä on paljon erilaisia toimintamalleja kyberturvallisuuden ylläpitämiseksi. Kyberturvallisuusdirektiivin lisäksi laadittuna on muun muassa kyberturvallisuusstrategia ja -asetus. Myös jäsenmaita velvoitetaan kantamaan oma vastuunsa kyberturvallisuudesta. (Eurooppa-neuvosto, 2024.) Suomessa tämä toimija on liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus, jonka tärkeimpänä tehtävänä on kehittää ja valvoa verkkojen ja palveluiden toimintavarmuutta sekä turvallisuutta. Keskuksen tehtävänä on myös ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. (Traficom, 2020.)

3.1 Yleisimmät kyberuhat

Kyberuhkia ovat kaikki uhat, jotka kohdistuvat tieto- ja viestintäverkkoihin tai muihin vastaavin tärkeisiin digitaalisiin laitteisiin. Uhkia voi ilmentyä eri muodoissa, esimerkiksi hyökkäys tai tietojen kalastelu ovat kyberuhkia. Hyökkäyksien yksi mahdollisesti tunnetuimmista muodoista on palvelunestohyökkäys, jolloin joku tai jokin pyrkii kuormittamaan palvelua tai tietojärjestelmää, kunnes järjestelmä jumiutuu. Myös hakkerointi on yleisesti tunnettu hyökkäysmuoto. Silloin tunkeudutaan väkisin tietojärjestelmiin ja päästään mahdollisesti käsiksi arkaluonteiseen tietoon tai päästään käyttämään ohjelmaa, palvelua tai muuta resurssia, jonka avulla saadaan aiheutettua haittaa järjestelmän haltijalle. (Traficom, 2020.)

Yhdeksi suurimmista kyberuhista Euroopan Unionin alueella lähivuosina on noussut kiristysohjelmahyökkäykset. Näiden hyökkäysten avulla varastetaan Euroopan Unionin alueelta yli 10 teratavua dataa kuukausittain. (Eurooppa-neuvosto, 2023.) Hyökkäyksessä kiristyshaittaohjelma tunkeutuu laitteelle ja lukitsee käyttäjän pääsyn tiedostoihin tai mahdollisesti koko tietokoneelle tai -järjestelmään. Tämän jälkeen uhri saa lunnasvaatimuksen, yleensä

bitcoineina, ja ainoa tapa saada pääsy takaisin koneelle on maksaa vaadittu rahasumma. Bitcoineja käytetään, koska niiden jäljittäminen on vaikeampaa kuin muiden maksutapojen. Ohjelmat pääsevät yleensä laitteelle vahingossa jonkun muun ohjelman kautta, esimerkiksi sähköpostin liitteestä tietojenkalasteluyrityksen yhteydessä, saastuneilta verkkosivuilta tai suojaamattomasta Wi-Fi-verkosta. (F-secure, n.d.)

3.2 Kyberuhkien jaottelu

Pääsääntöisesti kyberuhat voidaan jakaa kolmeen pääalueeseen: fyysiset, taloudelliset ja digitaalisen maailman uhat. Uhka voi esiintyä kuitenkin myös näissä kaikissa kolmessa alueessa samanaikaisesti. Kyberuhka voi olla rikollisen hyökkäyksen aiheuttamaa tai ihmisestä johtumaton uhka, kuten laaja ja pitkäaikainen sähkökatkos. Kyberuhkia on eritasoisia ja ne voidaan jakaa viiteen eri tasoon, joista yleisin ja vähiten vaarallisin on kybervandalismi ja harvinaisin, mutta vaarallisin, on kybersodankäynti. (Peda.net, n.d, kohta Kyberuhat ja niiden aiheuttajat.) Ei ole kuitenkaan täysin yksiselitteistä, mihin mikäkin kyberuhka luetellaan ja tasoilla onkin paljon yhteistä.

3.2.1 Kybervandalismi

Yleisin, mutta vaarattomin kyberuhan taso on kybervandalismi. Kybervandalismilla saavutetaan usein paljon huomiota, mutta niiden kesto on lyhytaikaista. (Peda.net, n.d., kohta Kyberuhat ja niiden aiheuttajat.) Tarkoituksena on usein tahallinen digitaalisen omaisuuden vahingoittaminen, häiritseminen tai turmeleminen, mutta kybervandalismin keinoja voidaan käyttää myös laillisiin tarkoituksiin. Digitaalisella omaisuudella tarkoitetaan esimerkiksi verkkosivustoja tai tietokantoja. Kybervandalismi voi aiheuttaa merkittävää haittaa sen uhriksi joutuneelle yritykselle, järjestölle tai yksityishenkilölle. (VPN unlimited, n.d.)

Kybervandalismiksi luetaan muun muassa hakkerointi ja haktivismi (Peda.net, n.d., kohta Kyberuhat ja niiden aiheuttajat). Haktivismi on verkossa tapahtuvaa aktivismia eli toimintaa, jolla pyritään paljastamaan

epäoikeudenmukaisuuksia. Tämä yleisesti hyvää tarkoittava toiminta voi kuitenkin saada suurta tuhoa aikaan paljastamalla arkaluontoisia tietoja, kuten ihmisten osoitetietoja. (Norton, 2011.)

3.2.2 Kyberrikollisuus

Kyberrikollisuudella tarkoitetaan tietotekniikkaan tai -verkkoihin kohdistuvaa rikollisuutta tai niitä hyväksikäyttäen tehtäviä rikoksia. Yleisimpiä rikostyyppejä ovat erilaiset omaisuusrikokset, kuten petokset, rahanpesu, kiristysrikokset ja maksuvälinepetokset. Myös lapsiin ja nuoriin verkon kautta tehty seksuaalinen hyväksikäyttö voidaan lukea kyberrikollisuudeksi. Terrorismin suunnittelu ja kaikki siihen liittyvä toiminta, rekrytoiminen, materiaalien levittäminen ja lietsonta on myös osa kyberrikollisuutta. (Sisäministeriö, n.d.)

Kyberrikollisuus voidaan jakaa kahteen ryhmään: tietoverkkosidonnaiset rikokset ja tietoverkkoavusteiset rikokset. Tietoverkkosidonnainen rikos kohdistuu suoraan tietoverkkoon tai -järjestelmään. Tämän kaltaista rikosta ei voi tehdä muuten kuin tietokonetta tai tietoverkkoa käyttäen. Näitä ovat esimerkiksi palvelunestohyökkäykset ja tietomurrot. Tietoverkkoavusteinen rikos sen sijaan hyödyntää tietoverkkoja tai tietojärjestelmiä yhtenä osana isompaa, verkon ulkopuolella tapahtuvaa, rikosta. Tämän kaltaisia rikoksia ovat esimerkiksi petokset ja huumausainerikokset. Näissä rikoksissa tietoverkko mahdollistaa rikokset, mutta nämä rikokset eivät suoraan kohdistu tietoverkkoon tai -järjestelmään. (Poliisi, n.d.)

3.2.3 Kybersodankäynti

Kybersodankäynti pitää sisällään erilaisia kyberrikoksia ja -vandalismia. Sodankäyntiä siitä tulee, kun toiminta sisältää yksittäisten hyökkäysten lisäksi myös vastahyökkäyksiä valtioiden välillä. Toinen selkeä eroavaisuus kybersodankäynnin ja -rikosten välillä on osapuolten pääasialliset tavoitteet. Sodankäynnin tarkoitus on tuottaa kansallista uhkaa muun muassa infrastruktuurille,

kriittisille toimijoille sekä rikkoa siviilien turvallisuuden tunne. Hyökkäystavat ovat usein samoja kuin kyberrikollisuudessa. (Cybersecurity Guide, 2024.)

4 EUROOPAN UNIONI JA KYBERTURVALLISUUS

4.1 EU:n kyberturvallisyysstrategia

Euroopan komissio ja Euroopan ulkosuhdehallinto ovat yhdessä esitelleet joulukuussa 2020 koko Euroopan Unionin yhteisen kyberturvallisuusstrategian. Eurooppa-neuvosto hyväksyi tämän strategian 22. maaliskuuta 2021. Strategian tavoitteena on luoda vahvempi vastus Eurooppaan kohdistuvia kyberuhkia vastaan. Kyberturvallisuuden koetaan olevan tärkeää, jotta saadaan rakennettua selviytymiskykyinen, vihreä ja turvallisesti digitaalinen Eurooppa. (Eurooppa-neuvosto, 2024, kohta EU:n kyberturvallisuusstrategia.) Vaikka strategian tavoitteena on mahdollistaa Euroopan teknologinen itsemääräämisoikeus, se pyrkii myös tehostamaan Euroopan Unionin yhteistyötä maailmanlaajuisesti demokraattisten oikeusvaltioiden kanssa. Tämän yhteistyön tavoitteena on luoda kansainvälistä turvallisuutta ja vakautta kyberavaruudessa. (Euroopan komissio, 2022.)

4.2 EU:n kyberturvallisuusasetus

Kyberturvallisuusasetus on tullut voimaan kesäkuussa 2019 (Eurooppa-neuvosto, 2024, kohta EU:n kyberturvallisuusasetus). Se toi mukanaan uuden Euroopan Unionin laajuisen sertifiontijärjestelmän tietoteknisille tuotteille, prosesseille ja palveluille. Asetus on toimeksianto EU:n kyberturvallisuusvirasto ENISAlle, jonka rooli on huolehtia sertifiontijärjestelmän toimivuudesta. ENISA toimii yhteistyössä CSIRT-yksiköiden kanssa. (Euroopan komissio, 2023 -b.)

5 PÄÄTELMÄ: NIS2-DIREKTIIVIN MERKITYS KYBERUHKIEN TORJUNNASSA

Kyberuhkien ja Venäjän hyökkäyssodan varjostamassa Euroopassa on tärkeää, että Euroopan Unionin jäsenmaat vetävät yhtä köyttä ja ovat samalla linjalla vastuksen edessä. Nykyaikainen sodankäynti tapahtuu yhä useammin verkossa ja kansallinen uhka on suuri, ellei kriittisiä tietoja ole suojattu parhaalla mahdollisella tavalla. Tietoturvadirektiivin uudistaminen on siis äärettömän tärkeää ja uudistetun direktiivin noudattaminen vielä tärkeämpää.

Vanhentunut NIS-direktiivi oli hyvin suppea eikä se ajanut asiaansa toivotulla tavalla. Sen noudattamatta jättäminen oli helppoa ja mahdollisti suurten tietoturvariskien kasvun. Uudistunut direktiivi on vaativampi, laajempi ja valvotumpi, joten sen myötä tietoturvariskien määrä vähenee sekä tietoisuus hyökkäyksistä on julkisempaa. Julkisuus tuo tietoa myös muille jäsenvaltioille ja näin ollen he osaavat myös varautua mahdollisiin iskuihin ja kalasteluihin tehokkaammin.

Näin ollen mielestäni direktiivin uusiminen ja uusitun direktiivin käyttöönottaminen oli hyvin tarpeellista koko Euroopan Unionin kannalta. Sen merkitys on suuri, mutta toki kaikella on varjopuolensa. Jotta direktiivi hoitaa työnsä, sitä pitää myös noudattaa. Säädetty sanktio toki tuo toimijoille paineen huolehtia osuudestaan, mutta jos jäsenvaltiot jättävät valvonnan hoitamatta, niin ajaako pelkkä sanktion luoma pelote silloin asiansa.

Uusittu direktiivi on otettu käyttöön kuitenkin vasta niin vähän aikaa sitten, ettei sen vaikutuksia tulevaisuuden kannalta vielä pystytä varmuudella ennustamaan.

LÄHTEET

Asikainen, M. (9.1.2024). NIS2-direktiivi ja laki kyberturvallisuuden riskienhallinnasta – mistä on kyse? https://gofore.com/nis2-direktiivi-ja-laki-kyberturvallisuuden-riskienhallinnasta-mista-onkaan-kyse/

Cybersecurity Guide. (2024). Cyberwarfare: The new frontlines. Haettu 26.4.2025 osoitteesta https://cybersecurityguide.org/resources/cyberwarfare/

Deloitte. (n.d.). NIS2-direktiivi – Tavoitteena kyberturvallisempi tulevaisuus. Haettu 29.2.2024 osoitteesta https://www2.deloitte.com/fi/fi/pages/risk/articles/nis2-direktiivi-tavoitteena-kyberturvallisempi-tulevaisuus.html

Euroopan komissio. (7.6.2022). The Cybersecurity Strategy. Haettu 6.3.2024 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Euroopan komissio. (29.6.2023 -a). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Euroopan komissio. (18.8.2023 -b). The EU Cybersecurity Act. Haettu 6.3.2024 osoitteesta https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Eurooppa-neuvosto. (2.2.2023). Infografiikka – Suurimmat kyberuhat EU:ssa. Haettu 4.3.2024 osoitteesta https://www.consilium.europa.eu/fi/infographics/cyber-threats-eu/

Eurooppa-neuvosto. (15.2.2024). Kyberturvallisuus: miten EU torjuu kyberuhkia? Haettu 6.3.2024 osoitteesta https://www.consilium.europa.eu/fi/policies/cybersecurity/

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. EUVL L 333/80, 27.12.2022, s. 1–73. https://eur-lex.europa.eu/eli/dir/2022/2555

F-Secure. (n.d.), MiKä on ransomware? Haettu 4.3.2024 osoitteesta https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack

Insta. (n.d.) NIS2-Direktiivi. Haettu 26.2.2024 osoitteesta https://www.insta.fi/nis2

Kaihovaara, A. (27.2.2023). EU hyväksyi NIS2-direktiivin kyberturvallisuuden kriittisyyden kasvaessa - Gartner ennustaa 30 % kasvua tietoturvaloukkauksiin. https://csit.fi/2023/02/27/nis2-direktiivi/

Kaspersky. (n.d.). Top Tips for Cyber Hygiene to Keep Yourself Safe Online. Haettu 5.3.2024 osoitteesta https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

Kyberturvallisuuskeskus. (10.04.2025). Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2). Haettu 23.4.2025 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa

Loistetrust. (n.d.). NIS2-direktiivi. Haettu 5.3.2024 osoitteesta https://www.loihdetrust.com/nis2-direktiivi/

Maijala, J. (30.10.2023). EU:n uusi tietoturvadirektiivi NIS2 tulee, oletko valmis? https://www.cinia.fi/blogi/mika-on-eun-uusi-tietoturvadirektiivi-nis2

Netnordic. (23.2.2024). NIS2-direktiivi velvoittaa lokakuusta alkaen – ollaanko siihen valmiita? Moni yritys ei ole, sanovat asiantuntijat. https://netnordic.fi/insights/tietoturva/nis2-direktiivi-velvoittaa-lokakuusta-alkaen/

Norton. (11.9.2023). Hacktivism: Definition, types, + newsworthy attacks. https://us.norton.com/blog/emerging-threats/hacktivism

Peda.net. (2016). ITKP0002 Johdatus kyberturvallisuuteen. Haettu 6.2.2025 osoitteesta https://peda.net/jyu/it/do/kkv

Poliisi. (n.d.). Kyberrikokset. Haettu 6.2.2025 osoitteesta https://poliisi.fi/kyberrikokset

Pro Kyberturva. (n.d.). Useimpien pk-yritysten on parannettava tietoturvan tasoa vuonna 2024 – NIS2 Kyberturvallisuusdirektiivi. Haettu 5.3.2024 osoitteesta https://www.kyberturvallisuus.eu/nis2-kyberturvallisuusdirektiivi/

Secapp. (n.d.). Oletko valmis tulevan NIS2-direktiivin vaatimuksiin? Haettu 5.3.2024 osoitteesta https://www.secapp.fi/fi/nis2-direktiivi-ja-varautuminen/

Second Nature Security. (n.d.). Toimitusketjun tietoturva haltuun – vastaaminen NIS2:n esittämiin haasteisiin. Haettu 5.3.2024 osoitteesta https://www.2ns.fi/toimitusketjun-tietoturva-haltuun-vastaaminen-nis2n-esittamiin-haasteisiin/

Sisäministeriö. (n.d.). Kyberrikollisuus ylittää rajat tietoverkoissa. Haettu 6.2.2025 osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Traficom. (30.11.2020). Kyberturvallisuuden perussanasto. Haettu 4.3.2024 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto

Traficom. (31.3.2021). Traficomin vuosi 2020: varmistimme koronavuonna ihmisten, datan ja tavaroiden sujuvan ja turvallisen liikkumisen. https://www.traficom.fi/fi/ajankohtaista/traficomin-vuosi-2020-varmistimme-koronavuonna-ihmisten-datan-ja-tavaroiden-sujuvan

Traficom. (13.7.2023 -a). NIS-koordinointi ja viranomaisyhteistyö. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkosto-johtaminen/nis-koordinointi-ja-viranomaisyhteistyo

Traficom. (21.12.2023 -b). Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä. https://efti.fi/fi/ajankohtaista/traficom-laatii-suositusta-nis2-direktiivin-kyberturvallisuuden-riskienhallinnan

Uniqkey A/S. (n.d. -a). The NIS2 Directive Explained. Haettu 28.2.2024 osoitteesta https://nis2directive.eu/

Uniqkey A/S. (n.d. -b). Who Does NIS2 Apply To? Haettu 5.3.2024 osoitteesta https://nis2directive.eu/who-are-affected-by-nis2/

Uniqkey A/S. (n.d. -c). NIS2 Requirements Haettu 5.3.2024 osoitteesta https://nis2directive.eu/nis2-requirements/

VPN unlimited. (n.d.) Cyber Vandalism. Haettu 20.2.2025 osoitteesta https://www.vpnunlimited.com/help/cybersecurity/cyber-vandalism