

Alexi Mutka

KYBERHARJOITTELU OSANA ORGANISAATION RISKIENHALLINTAA

Informaatioteknologian ja viestinnän tiedekunta

Kandidaattitutkielma

Maaliskuu 2026

TIIVISTELMÄ

Aleksi Mutka: Kyberharjoittelu osana organisaation riskienhallintaa
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Maaliskuu 2026

Digitalisaation kehittymisen myötä kyberturvallisuuden merkitys on kasvanut merkittävästi eri toimialoilla. Vastauksena digitalisaation tuomiin haasteisiin Euroopan unioni on laatinut NIS2-direktiivin, jonka tavoitteena on vahvistaa kyberturvallisuuden tasoa jäsenvaltioissa. Direktiivi velvoittaa yhteiskunnallisesti merkittäviä toimijoita ylläpitämään sekä kehittämään kyberturvallisuuteen liittyvää riskienhallintaa, jatkuvuuden varmistamista sekä henkilöstön osaamisen kehittämistä toimintaympäristössään.

Tässä tutkielmassa tarkastellaan kyberturvallisuuteen liittyvien harjoitusten tarjoamia mahdollisuuksia organisaatioiden kyberturvallisuuden kehittämisessä sekä niiden merkitystä NIS2-direktiivin asettamien velvoitteiden täyttämässä. Tutkielmassa kyberturvallisuuden harjoitukset on jaoteltu kolmeen harjoitusmuotoon: teknisiin harjoituksiin, keskustelupohjaisiin harjoituksiin sekä näitä yhdistäviin yhdistelmämuotoisiin harjoituksiin. Teknisiin harjoituksiin lukeutuvat esimerkiksi CDX-harjoitukset, joissa osallistujat torjuvat simuloituja kyberuhkia ja harjoittavat teknisiä kyberturvallisuuteen liittyviä taitojaan. Keskustelupohjaiset harjoitukset, kuten Tabletop-harjoitukset keskittyvät puolestaan päätöksentekoon, roolien koordinointiin ja organisaation toimintaprosessien testaamiseen simuloituissa häiriötilanteissa. Yhdistelmämuotoiset harjoitukset yhdistävät teknisten ja keskustelupohjaisten harjoitusten elementtejä. Tästä esimerkkinä kyberturvallisuutta testaava stressitesti.

Kyberturvallisuutta kehittävät harjoitukset auttavat työntekijöitä tunnistamaan riskien syy- ja seuraussuhteita sekä hahmottamaan oman roolinsa merkitystä häiriötilanteissa. Näiden harjoitusten avulla organisaatiot voivat kehittää teknisten valmiuksien lisäksi henkilöstön sitoutumista turvallisuuskäytäntöihin sekä vähentää inhimillisiä virheitä. Säännölliset ja kohdennetut harjoitukset muodostavat lähestymistavan, jolla organisaatiot voivat parantaa kyberturvallisuuttaan jatkuvasti kehittyvässä digitaalisessa ympäristössä.

Avainsanat: NIS2, kyberharjoittelu, riskienhallinta, stressitestausta, jatkuvuuden varmistaminen

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

Ei

Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaproessin aikana seuraavia tekoälysovelluksia:

ScopusAI

ChatGPT

Tekoälysovellusten nimet ja versiot:

ScopusAI

OpenAI, ChatGPT (GPT-5 mini)

Käyttötarkoitus:

ScopusAI:ta on käytetty lähteiden löytämiseen sekä hakusanojen avulla aiheen tarkentamiseen. ChatGPT:tä on hyödynnetty oikeinkirjoituksen tarkistamisessa sekä englanninkielisten sanojen kääntämisessä, jotta tieteellisten lähteiden sisältö tulisi ymmärretyksi oikein. Näiden lisäksi tekoälyä on hyödynnetty tekstin luonnostelussa.

Osiot, joissa tekoälyä on käytetty:

Tekoälyä on hyödynnetty satunnaisesti koko tutkielmassa.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

1	JOHDANTO	1
2	TUTKIMUSMENETELMÄ	3
3	NIS2-DIREKTIIVI OSANA ORGANISAATION RISKIENHALLINTAA	5
3.1	NIS2-DIREKTIIVI	5
3.2	NIS2-DIREKTIIVI OSANA ORGANISAATION JATKUVUUDEN SUUNNITTELUA.....	6
4	KYBERHARJOITTELU	9
4.1	CYBER DEFENCE-HARJOITUS (CDX)	10
4.2	TABLETOP-HARJOITUS (TTX/TTE).....	11
4.3	KYBERSTRESSITESTAUS	12
5	HARJOITUSTEN MAHDOLLISUUDET ORGANISAATIOLLE.....	14
6	YHTEENVETO	17
	LÄHTEET	19

Lyhenteet ja merkinnät

CDX	Simuloitu kyberuhka tai häiriötilanne todellista toimintoympäristöä muistuttavissa skenaarioissa
CSIRT	CSIRT vastaanottaa ja käsittelee kyberturvallisuuden liittyviä häiriöitä ja poikkeamia. CSIRT tukee lisäksi kansallista kyberturvallisuutta seuraamalla tilannetta sekä jakamalla ajankohtaista tietoa kyberturvallisuuteen liittyen.
ENISA	Euroopan unionin asiantuntijavirasto, jonka rooli on vahvistaa EU:n kyberturvallisuuden tasoa.
NIS2	EU:n direktiivi, joka on määritetty yksityisille sekä julkisille toimijoille verkko- ja tietojärjestelmien kohdistuvien riskien hallitsemiseksi
TTX/TTE	Tabletop-harjoitus (TTX/TTE) on keskustelupohjainen harjoitus, jossa osallistujat käyvät yhdessä läpi ennalta määritetyn poikkeama- tai häiriötilanteeseen perustuvan skenaarion

1 Johdanto

Digitalisaation myötä kyberturvallisuuden merkitys on kasvanut merkittävästi ja kehitys on vaikuttanut myös siihen, että kyberturvallisuuden uhkat ovat muuttuneet monimutkaisemmiksi. NIS2 (Network and Information Systems) on Euroopan unionin laatima direktiivi, joka korostaa organisaatioiden vastuuta riskienhallinnassa, jatkuvuuden varmistamisessa ja kyberturvallisuuteen liittyvän osaamisen kehittämisessä toimintaympäristösään. [1]

Tässä tutkielmassa tarkastellaan NIS2-direktiivin vaatimuksia sekä kyberharjoittelun ja kyberturvallisuuteen liittyvän stressitestauksen roolia osana organisaation riskienhallintaa, jatkuvuuden suunnittelua sekä toiminnan jatkuvuuden varmistamista häiriötilanteissa. Tutkielma keskittyy arvioimaan, miten stressitestaaminen ja kyberharjoitukset voivat tukea organisaatioiden kykyä mukautua poikkeuksellisiin häiriötilanteisiin ja varmistaa kriittisten toimintojen jatkuvuus myös vakavissa kyberhäiriöissä NIS2-direktiivin viitekehysessä.

Tutkimuskysymykset ovat:

- 1) Miksi kyberharjoittelu tukee organisaation riskienhallintaa?
- 2) Miten kyberharjoittelu tukee NIS2-direktiivien vaatimusten täyttämistä?

Stressitestaaminen ja kyberharjoitukset tarjoavat keinoja arvioida organisaation kyvykkyyksiä, prosesseja sekä teknisiä ja organisatorisia valmiuksia toimia kuormittavissa ja poikkeuksellisissa tilanteissa. Tässä tutkielmassa ei tarkastella NIS2-direktiivin vaatimuksia julkiselle sektorille tai valtiollisia toimijoita koskevia vaatimuksia, vaan painopiste on stressitestauksen roolissa organisaation toiminnan laadun kehittämisessä sekä henkilöstön osaamisen ja valmiuksien vahvistamisessa. Kyberharjoitusten ja stressitestien avulla organisaatiot voivat tunnistaa puutteita jatkuvuuteen liittyvissä suunnitelmissaan, testata päätöksentekoa ja kehittää yhteistyötä häiriötilanteissa. Näin kyberharjoitukset ja stressitestit tukevat riskienhallintaa sekä NIS2-direktiivin edellyttämien hallinnollisten ja teknisten toimenpiteiden toteuttamista.

Kyberturvallisuuteen liittyvät harjoitukset voidaan luokitella kolmeen erilliseen muotoon: keskustelupohjaisiin harjoituksiin, teknisiin harjoituksiin sekä harjoituksiin, joissa yhdistetään molempien muotojen ominaisuuksia. Keskustelupohjaisissa harjoituksissa

osallistujat tarkastelevat yhdessä skenaariopohjaisesti erilaisia kyberturvallisuuden liittyviä häiriö- ja poikkeamatilanteita sekä niihin liittyviä toimintamalleja. Tekniset harjoitukset ovat käytännönläheisiä ja sisältävät usein realistisia simulaatioita. Ne voivat sisältää esimerkiksi tietojärjestelmien haavoittuvuuksien tunnistamista tai järjestelmien suojaamista ylimääräiseltä kuormitukselta. Keskustelupohjaisten ja teknisten harjoitusten yhdistäminen mahdollistaa kokemuksen, jossa yhdistyy teknisten taitojen harjoittelu sekä toimintamallien tarkastelu osana kyberturvallisuutta. [2] Tutkielmassa esitellään esimerkit keskustelupohjaisesta harjoituksesta, teknisestä harjoituksesta sekä harjoitusmuodosta, jossa on elementtejä molemmista harjoitusmuodoista.

Kyberharjoitukset ja stressitestit voivat toimia tehokkaina välineinä NIS2-direktiivin velvoitteiden toteutumisen arvioinnissa. Tässä tutkielmassa tarkastellaan harjoitusten ja koulutusten merkitystä organisaatioiden kyberturvallisuuden kehittämisessä sekä analysoidaan niiden vaikutuksia henkilöstön osaamiseen, toimintavalmiuksiin ja organisaation resilienssiin. Erityistä huomiota kiinnitetään siihen, miten harjoitukset tukevat riskienhallintaa ja jatkuvuuden suunnitelmia osana NIS2-direktiivin edellyttämiä hallinnollisia ja teknisiä toimenpiteitä.

2 Tutkimusmenetelmä

Tämä tutkielma on toteutettu kirjallisuuskatsauksena. Kirjallisuuskatsausta varten lähteitä etsittiin erilaisten hakusanojen avulla pääosin Andoria, Scopusta sekä ACM:n tietokantoja hyödyntäen. Hakusanoissa hyödynnettiin pääosin englanninkielisiä termejä, joista käytetyimpiä olivat ”Cyber stress test”, ”NIS2”, ”Organizations continuity plan”, ”Tabletop exercises”, ”Cyber exercises”. Hakusanoja kehitettiin ja täsmennettiin systemaattisesti tutkimuksen tavoitteiden mukaisesti. Lisäksi ScopusAI:n tarjoamaa generatiivista tekoälyä käytettiin hakusanojen optimointiin sekä aiheeseen olennaisten lähteiden tunnistamiseen.

Aineiston valintaan vaikutti lähteiden ajankohtaisuus sekä julkaisuajankohta. Etenkin NIS2-direktiivin voimaan astumisen ajankohta vaikutti osaltaan viitekehukseen lähteiden valinnassa. Yli viisi vuotta vanhoissa lähteissä oli löydettävissä yhteyksiä NIS2 edeltävään NIS1-direktiiviin, jonka vaatimukset eroavat nykyisestä kyberturvallisuudirektiivistä.

Tiedonhakua toteutettiin neljässä eri vaiheessa. Ensimmäisessä vaiheessa haettiin tietoa NIS2-direktiivistä sekä etsittiin mahdollisia lähteitä, joissa oli koottuna direktiivin keskeisiä asioita liittyen kyberturvallisuuteen sekä henkilöstön kouluttamiseen.

Toisessa vaiheessa haettiin tietoa kyberturvallisuuden kouluttamisesta sekä erilaisista harjoituksista. Samalla löytyi viitekehys, jonka avulla oli mahdollista luokitella harjoituksia osakokonaisuuksiin, kuten keskustelupohjaisiin harjoituksiin ja teknisiin harjoituksiin.

Kolmannessa vaiheessa haettiin tietoa kyberturvallisuusharjoitusten toteutuksesta sekä NIS2-direktiivin vaikutuksista organisaation toimintaan. Tämän vaiheen aikana aineistosta muodostui viitekehys, jonka avulla harjoitukset voitiin luokitella esimerkiksi keskustelupohjaisiin ja teknisiin harjoituksiin. Samalla vaihe tuotti aineistoa, joka mahdollisti harjoitusten yhteyden ja vaikutusten ymmärtämisen osana organisaation kyberturvallisuuden kokonaisuutta.

Neljännessä vaiheessa keskityttiin henkilöstön kouluttamisen hyötyihin organisaation näkökulmasta, kuten osaamisen kehittymiseen, sitoutumiseen turvallisuuskäytäntöihin ja

ihimillisten virheiden vähentämiseen. Tämän vaiheen aineisto täydensi aikaisempia vaiheita ja mahdollisti kattavan kuvan muodostamisen kyberturvallisuuteen liittyvän koulutuksen merkityksestä.

Lähteet ovat vertaisarvioituja, poikkeuksena verkkolähteet, kuten esimerkiksi Traficomin verkkosivuilta haettu aineisto, jossa esitellään Traficomin viranomaisrooli NIS2-direktiivin toteuttamisessa.

3 NIS2-direktiivi osana organisaation riskienhallintaa

Digitaalisen kehittymisen myötä järjestelmiin kohdistuvat tietomurrot ovat lisääntyneet ja niiden vakavuus sekä laajuus ovat kasvaneet merkittävästi. Kriittisten järjestelmien ja infrastruktuurin automatisointi on osaltaan lisännyt haavoittuvuuksia sekä mahdollistanut myös ulkoisten toimijoiden, kuten rikollisryhmien ja aktivistien kohdistamat hyökkäykset. Puutteet kyberturvallisuudessa voivat aiheuttaa organisaatioille taloudellisia tappioita, jotka voivat vaihdella mittasuhteiltaan vähäisistä jopa katastrofaalisiin seurauksiin. Tämä korostaa organisaatioiden tarvetta kyberriskien hallintaan organisaatioissa. [3] Kriittisten järjestelmien ja infrastruktuurin automatisointi lisää usein keskinäisiä riippuvuuksia sekä monimutkaisuutta. Riippuvuudet kasvattavat samalla riskiä yksittäisten häiriöiden kohdalla, mitkä voivat aiheuttaa laajamittaisia ja ennakoimattomia tapahtumia ja vaikutuksia. Tämä korostaa tarvetta tarkastella kyberturvallisuutta kokonaisuutena eikä ainoastaan yksittäisten järjestelmien tai infrastruktuurin osa-alueiden näkökulmasta.

Useat organisaatiot ovat investoineet kyberturvallisuuteen tunnistaakseen, arvioidakseen sekä hallitakseen riskejä. Panostuksistaan huolimatta monilta organisaatioilta puuttuu riittävä tilannetietoisuus mahdollisista uhkista sekä toimijoista. Kasvavat riskienhallintaan varattavat menot kasvavat usein budjetoitua suuremmaksi mahdollisten tietoturvaan liittyvien loukkausten ja mahdollisten sanktioiden myötä. [3] Puutteellinen tilannetietoisuus heikentää organisaatioiden kykyä ennakoida uhkia ja reagoida niihin ajoissa. Tällöin riskienhallinta painottuu korjaaviin toimenpiteisiin, jotka voivat olla kustannuksiltaan huomattavasti suurempia verrattuna ennaltaehkäiseviin toimenpiteisiin.

3.1 NIS2-direktiivi

NIS2 on vuonna 2022 hyväksytty kyberturvallisuudsdirektiivi, jonka tarkoituksena on parantaa kyberturvallisuuden tasoa Euroopan unionin jäsenmaissa. NIS2-direktiivi (2022/2555) on EU:n toinen verkko- ja tietojärjestelmiä koskeva direktiivi, joka korvaa ja laajentaa NIS1-direktiivin (2016/1148) soveltamisalaa. Se hyväksyttiin vastauksena digitalisaation kiihtymiseen ja teknologiseen riippuvuuteen. NIS2 kattaa yksityisiä sekä julkisia toimijoita tavoitteenaan luoda turvallinen EU:n laajuinen digitaalinen ympäristö. [1]

NIS2-direktiivin tarkoituksena on vähentää kyberturvallisuuteen liittyviä eroja sääntelypiirissä olevien toimijoiden välillä. Kyberturvallisuuden tason yhtenäistäminen mahdollistaa toimintaedellytykset siihen, että kriittisten sektoreiden toimijat ylläpitävät korkeita

tietoturvastandardeja, mikä osaltaan parantaa koko EU:n kyberturvallisuutta. NIS2-direktiivi tukee myös tietojenvaihtoa Euroopan unionin lakien mukaisesti. [1] NIS2-direktiivin tarkoituksena on vähentää kyberturvallisuuteen liittyviä eroja sääntelypiirissä olevien toimijoiden välillä sekä yhdenmukaistaa kyberturvallisuuden tasoa EU:ssa. Käytännön vaikutukset riippuvat pitkälti siitä, miten direktiivin vaatimukset toimeenpannaan sääntelyn piiriin kuuluvissa organisaatioissa sekä siitä, kuinka tehokkaasti vaatimusten noudattamista valvotaan.

NIS2-direktiivin soveltamisalaan kuuluvat direktiivissä määritetyt keskeiset sekä tärkeät toimijat. Keskeisiksi toimijoiksi on määritetty taloudellisesti ja yhteiskunnallisesti kriittiset toimijat. Sen sijaan tärkeiksi toimijoiksi on määritetty toimijat, joilla on vastuu tukea yhteiskunnallisesti ja taloudellisesti tärkeitä järjestelmiä, mutta jotka eivät vaikuta suoraan kriittisten palveluiden saatavuuteen. NIS2-direktiivin mukaisesti keskeiset toimijat ovat tiukempien turvallisuusvaatimusten alaisia verrattuna tärkeisiin toimijoihin. [1] Organisaatioiden näkökulmasta NIS2-direktiivi ohjaa kyberturvallisuuden kehittämistä aiempaa systemaattisemmaksi ja korostaa ennakoivia ja jatkuvasti kehitettäviä toimenpiteitä.

Suomessa valvovaksi viranomaiseksi on määritetty kyberturvallisuuslain myötä Traficom. Traficomien kyberturvallisuuskeskus toimintaan sisältyy lisäksi valvovien viranomaisten koordinoinnin ja yhteistyön kehittäminen. CSIRT (Computer Security Incident Response Team) toimii kyberturvallisuuskeskuksen yhteydessä, minkä tarkoituksena on reagoida poikkeamailmoituksiin sekä tarvittaessa avustaa ilmoituksen tehnyttä toimijaa tai tahoa poikkeaman käsittelyssä. Lisäksi CSIRT tukee kansallista kyberturvallisuutta seuraamalla tilannetta sekä jakamalla ajankohtaista tietoa kyberturvallisuuteen liittyen. [4] Viranomaisen tarjoamasta tuesta huolimatta direktiivin piirissä olevilla organisaatioilla on vastuunsa kyberturvallisuuden kehittämisestä osana niiden riskienhallintaa.

3.2 NIS2-direktiivi osana organisaation jatkuvuuden suunnittelua

NIS2-direktiivissä on määritelty vaatimuksia keskeisille sekä tärkeille toimijoille kolmella eri tasolla, jotka liittyvät organisaatioiden hallintoon, teknisiin järjestelmiin sekä riskeihin liittyviin arviointeihin. Organisaatioiden on määritettävä selkeästi kyberturvallisuuteen liittyvät vastuut, laadittava suunnitelmat häiriötilanteiden varalta sekä järjestet-

tävä henkilöstölle koulutuksia. Teknisten järjestelmien osalta pääsynvalvonta sekä järjestelmien monitorointi ovat tärkeässä roolissa. Lisäksi organisaatioiden on tehtävä säännöllistä riskien arviointia sekä laadittava toimintamalli liiketoiminnan jatkuvuuden varmistamiseksi. [1] Säännöllinen riskien arviointi ja raportointivelvollisuus ei ainoastaan täytä direktiivin vaatimuksia, vaan tarjoaa myös organisaatiolle mahdollisuuden tunnistaa uusia uhkia ja heikkouksia. Tämä mahdollistaa proaktiivisen varautumisen, jolloin toimenpiteitä voidaan kohdentaa ennen kuin poikkeamat tai häiriöt aiheuttavat merkittäviä vaikutuksia.

Suomessa organisaation tehtävänä on selvittää, että kuuluvatko ne NIS2-direktiivin sääntelyyn alaiseiksi ja mahdollisesti ilmoitauduttava omalle valvovalle viranomaiselleen. Traficom on laatinut suosituksen valvoville viranomaisille, joka tukee lisäksi NIS2-toimijoiden riskienhallinnan suunnittelua. [4]

NIS2-direktiivin alaisten toimijoiden on ylläpidettävä ajantasaista kyberturvallisuuden riskienhallinnan toimintamallia, joka pitää sisällään viestintäverkkojen ja tietojärjestelmien suojaaminen poikkeamilta ja niiden vaikutuksilta. Toimintamalli pitää sisällään lisäksi fyysisen ympäristön suojaamisen. Seuraava luettelo perustuu Traficomien koontiin kyberturvallisuuden riskienhallinnan toimintamalliin, mikä toimijoiden tulee huomioida:

1. Toimintaperiaatteet kyberturvallisuusriskien hallintaan sekä hallintatoimenpiteiden vaikuttavuuden arviointi
2. Toimintaperiaatteet, jotka koskevat tietojärjestelmiä ja viestintäverkkoja
3. Viestintäverkkojen ja tietojärjestelmien elinkaaren turvallisuus, mikä pitää sisällään hankinnat, kehittämisen ja ylläpidon sekä tarvittavat toimet haavoittuvuuksien käsittelyä ja julkistamista varten
4. Välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen laatu ja häiriönsietokyky sekä niihin liittyvät kyberturvallisuuskäytännöt.
5. Omaisuudenhallintaa koskevat menettelyt sekä omaisuuden turvallisuuden kannalta merkittävien toimintojen tunnistaminen.
6. Henkilöstön turvallisuus ja kyberturvallisuuteen liittyvä koulutus
7. Toimintatavat pääsynvalvontaan ja todentamiseen
8. Toimenpiteet salausmenetelmien käytölle ja suojatun sähköisen viestinnän menettelyt

9. Poikkeamien tunnistaminen ja käsittely sekä toimenpiteet turvallisuuden ja toimintavarmuuden ylläpitämiseksi
10. Menettelyt toiminnan jatkuvuuden varmistamiseksi, mikä pitää sisällään varmuuskopioinnin, palautumissuunnittelun, kriisinhallinnan ja tarvittaessa suojatun viestinnän
11. Menettelyt perustason tietoturvan varmistamiseksi toiminnassa, tietoliikenteessä, laitteistoissa, ohjelmistoissa ja tietoaineistoissa
12. Fyysisen ympäristön, tilojen turvallisuuden ja kriittisten resurssien hallinta viestintäverkkojen ja tietojärjestelmien osalta. [5]

Toimenpiteet suhteutetaan toiminnan laajuuteen, mahdollisiin välittömiin vaikutuksiin, toimijan tietojärjestelmien ja viestintäverkkojen haavoittuvuuksiin. Lisäksi arvioidaan poikkeamien toteutumisen todennäköisyyksiä, seurausten vakavuuksia sekä mahdollisia poikkeamista johtuvia kustannuksia. Näiden lisäksi tulee huomioida tekninen kehitys, joka voi osaltaan vaikuttaa mahdollisuuksiin torjua uhka. [5] Teknologinen kehitys ja uudet kyberturvallisuutta uhkaavat tekijät edellyttävät riskienhallinnan jatkuvaa päivittämistä, jotta organisaation valmius torjua mahdollisia poikkeamia säilyy.

Direktiivin noudattamatta jättämiseen on määritetty hallinnollisesti seuraamukset, jotka ovat toimijalle merkittävät. Sanktiot voivat olla 10 miljoonaa tai 2 % organisaation vuotuisesta liikevaihdosta. [6] Merkittävät taloudelliset sanktiot toimivat osaltaan merkittävänä kannustimena organisaatioille panostaa systemaattisesti kyberturvallisuuteen ja noudattaa NIS2-direktiivin vaatimuksia. Ne voivat ohjata organisaatioita kehittämään riskienhallintaa, päivittämään toimintamalleja sekä lisäämään tilannetietoisuutta, jotta mahdolliset poikkeamat voidaan estää ennakoivasti ja siten välttyä mahdollisilta sanktioilta.

NIS2-direktiivi parantaa myös Euroopan unionissa toimivien organisaatioiden välistä luottamusta. Tietoturvaan liittyvien velvoitteiden selkeyttäminen mahdollistaa oikeudellisesti paremmin toimivamman kokonaisuuden valtioiden rajat ylittävissä toimissa sekä ulkoistamisiin liittyvissä järjestelyissä. [1] Luottamus organisaatioiden välillä voi tukea liiketoiminnan kehitystä, koska se mahdollistaa turvallisemman liiketoiminnan kansainvälisillä markkinoilla EU:n sisällä.

4 Kyberharjoittelu

Kyberturvallisuuden järjestelmät voivat olla hyvin suunniteltuja, mutta ne eivät siltikään kykene poistamaan kaikkia mahdollisia haavoittuvuuksia tai virheitä. Kyberturvallisuudessa ihmisen toiminta ja inhimilliset virheet ovat edelleen suurin kyberturvallisuutta uhkaava tekijä. Kyberturvallisuutta voidaan edistää kouluttamalla tietoturva-asiantuntijoita ajankohtaisista uhkista ja ratkaisuksista sekä lisäämällä lisäksi muun henkilöstön kyberturvallisuuteen liittyvää osaamista. [7] Kyberturvallisuus ei perustu pelkästään teknisiin ratkaisuihin, vaan sisältää myös henkilöstön osaamistason ylläpitämisen.

Organisaatioiden tulisi kehittää henkilöstön osaamista kyberturvallisuuteen liittyen säännöllisesti. Kyberhyökkäykset voivat vaikuttaa merkittävästi organisaation liiketoimintaan ja johtaa salassa pidettävän tiedon menettämiseen. Kyberturvallisuuteen liittyvät koulutukset ja kyberharjoitukset mahdollistavat osallistujien perehdyttämisen organisaation sääntöihin, ohjeisiin, politiikkoihin sekä toimintaan vaikuttaviin regulaatioihin. Kyberharjoittelulla on mahdollista kehittää henkilöstön kyberturvallisuustaitoja, joka osaltaan auttaa henkilöstöä tunnistamaan erilaisia kyberturvallisuutta vaarantavia tekijöitä ja uhkia. Kyberturvallisuuteen liittyvien koulutusten merkitys kasvaa, mutta toistaiseksi ei ole tehty systemaattista vertailua erilaisten kyberturvallisuuskoulutusten tai -harjoitusten välille oppimisen näkökulmasta. [7] NIS2-direktiivin näkökulmasta henkilöstön osaamisen kehittäminen ei ole pelkästään suositeltavaa, vaan osa direktiivin velvoitteiden täyttämistä. Koulutukset ja harjoitukset tukevat direktiivin edellyttämää riskienhallintaa.

Useat organisaatiot ovat panostaneet merkittävästi koulutuksiin, joiden tarkoituksena on kehittää henkilöstön kyberturvallisuuteen liittyvää tietoisuutta sekä parantaa heidän kykyään suojata organisaatioitaan. Harjoituksissa hyödynnetään enenevästi simuloituja tilanteita, joissa koulutettavat pääsevät harjoittelemaan kyberturvallisuuteen liittyviä taitoja käytännössä. Simuloidut harjoitukset sekä koulutukset vaativat kuitenkin räätälöintiä kohderyhmänsä tarpeiden mukaisesti ollakseen tehokkaita. Räätälöidyt harjoitukset ja koulutukset vaativat kohderyhmän tuntemista sekä koulutustarpeiden tunnistamista. [8] Räätälöidyt harjoitukset tukevat myös organisaation riskienhallintaa, sillä ne voivat auttaa tunnistamaan puutteita toimintamalleissa sekä testaamaan päätöksentekoa poikkeustilanteissa. Huolellisesti rakennetut koulutukset integroituvat osaksi organisaation kyberturvallisuutta sen sijaan, että olisivat irrallisia oppimistilanteita.

Simuloiduista harjoituksista saatujen tulosten ja havaintojen jakaminen kriittisten toimialojen kesken mahdollistaa yhteisen kyberturvallisuuden kehittämisen. Kriittiset sektorit saattavat kohdata samankaltaisia uhkia, jolloin tiedonvaihto voi osaltaan auttaa tunnistamaan yhteisiä haavoittuvuuksia, uhkia sekä mahdollisia torjuntakeinoja. Tiedon jakaminen toimialojen välillä edistää myös regulaatioiden noudattamista ja vahvistaa kyberturvallisuutta, mikä hyödyttää kaikkia toimialoja. Esimerkkinä toimialarajat ylittävistä uhkasta on toimitusketjuun liittyvät mahdolliset ongelmat. Toimitusketjun häiriö voi aiheuttaa laajoja ongelmia useilla toimialoilla samanaikaisesti, kuten esimerkiksi logistiikkapalvelutarjoajaan kohdistunut kiristyshaittaohjelma, mikä voi estää esimerkiksi raaka-aineiden kuljetukset teollisuudelle ja aiheuttaa sitä kautta kerrannaisvaikutuksia. Kerrannaisvaikutukset voivat vaarantaa samanaikaisesti useiden toimialojen toimintojen jatkuvuutta. [8] Yhteisten havaintojen jakaminen voi edistää myös toimintamallien ja käytäntöjen yhtenäistämistä eri toimialoilla, mikä voi helpottaa toimintaa häiriötilanteissa ja parantaa reagointikykyä laajoissa kyberturvallisuuteen liittyvissä kriisitilanteissa.

4.1 Cyber Defence-harjoitus (CDX)

CDX (Cyber Defence Exercise) on kyberpuolustukseen liittyvä harjoitus, jonka tavoitteena on testata ja kehittää teknisiä valmiuksia, päätöksentekoa, toimintamalleja sekä yhteistyötä eri roolien ja tiimien välillä. Harjoituksen osallistujat organisoidaan kahteen vastakkaiseen joukkueeseen, joille määritellään selkeät vastuualueet todellista toimintaympäristöä simuloivassa tilanteessa. Joukkueet luokitellaan useimmiten hyökkääviin ja puolustaviin osapuoliin. Näitä joukkueita kutsutaan tyypillisesti punaiseksi ja siniseksi joukkueeksi, joissa punainen joukkue vastaa kyberhyökkäysten toteuttamisesta ja sininen joukkue järjestelmien ja kyberturvallisuuden puolustamisesta. CDX-harjoitukset ovat yleinen, mutta usein myös kallis tapa kouluttaa henkilöstöä ja ne vaativat usein paljon suunnittelua sekä valmisteluita, jotka voivat kestää kuukausia. [9] CDX voidaan luokitella tekniseksi harjoitukseksi. [2] Korkeiden kustannusten sekä vaatimusten vuoksi CDX-harjoitukset eivät sovellu kaikille organisaatioille, mikä korostaa organisaation tarvetta arvioida kustannuksia suhteessa saavutettavaan hyötyyn.

CDX-harjoituksessa haasteena on yksittäisten osallistujien ja tiimien arviointi, sillä objektiivisia arviointimenetelmiä ei välttämättä ole riittävästi saatavilla. CDX on lähtökohdaisesti määritelty organisaatioissa toimiville kyberturvallisuudesta vastaaville henkilöille

tai muuten rajatulle kohderyhmälle. Kyberturvallisuuteen vaikuttavat kuitenkin kaikki organisaation työntekijät. Sotilaskoulutuksessa on huomattu CDX-harjoitusten olevan motivaatiota lisäävä harjoitustyyppi sekä tehokas keino osaamisen arviointiin. [9] CDX-harjoitukset voivat kehittää tehokkaasti rajatun kohderyhmän kyberturvallisuuteen liittyvää osaamista sekä vahvistaa teknisiä ja toiminnallisia valmiuksia poikkeustilanteissa. Organisaatioiden tulee huomioida, että CDX-harjoitusten vaikutus koko organisaation kyberturvallisuuteen on kuitenkin rajallinen.

4.2 Tabletop-harjoitus (TTX/TTE)

Tabletop-harjoitus (Tabletop Exercise, TTX/TTE) on harjoitusmenetelmä, joka perustuu kriisitilanteen simulaatioon tarkoituksenaan testata osallistujaryhmän osaamista sekä reagointia erilaisiin häiriöihin sekä kriisitilanteisiin. Simuloitu kriisitilanne sijoittuu usein organisaation liiketoimintaympäristöön ja sen skenaariona voi olla esimerkiksi organisaation tietojärjestelmiin levinnyt haittaohjelma. Tabletop-harjoitukset ovat toteutukseltaan usein huomattavasti kevyempiä verrattuna teknisiin harjoituksiin, sillä ne perustuvat useimmiten lomakkeiden ja muiden yksinkertaisten menetelmien käyttöön osallistujien vastausten keräämisessä. Samalla ne ovat usein kustannustehokkaita ja matalan kynnyksen harjoitusmuotoja. [10] Tabletop-harjoitukset ovat keskustelupohjaisia harjoituksia. [2]. Tabletop-harjoituksista voidaan käyttää lyhennettä TTX tai TTE.

Harjoituksen aikana osallistujat keskustelevat toimenpiteistä, jotka tulisi toteuttaa organisaation toimintamalleja sekä ohjeistuksia noudattaen. Osallistujat voidaan jakaa kahden eri ryhmään, joista toisen tehtävänä on laatia harjoitukseen sopiva skenario hyökkäjän näkökulmasta ja toisen ryhmän tehtävänä on puolustautua hyökkäyksiltä. Harjoituksen aikana tapahtuvaa keskustelua ohjaavat kouluttajat. Kouluttajien tehtävänä on järjestää harjoituksen lisäksi harjoituksen jälkeinen yhteenveto- ja purkutilaisuus. Tabletop-harjoituksia pidetään tehokkaana koulutuksellisenä välineenä, mikä kehittää osallistujien yhteistyötä, koordinointia sekä viestintää. Tabletop-harjoituksia hyödynnetään etenkin kyberturvallisuuden liittyvillä aloilla. [10]

Tabletop-harjoituksia on analysoitu varsin vähän oppimisen näkökulmasta. Kerätty palaute käsittää pääosin osallistujien kokemuksia harjoituksen kulusta, mikä voi olla harjoituksen järjestäjille tärkeää tietoa, mutta ei anna tutkittua tietoa harjoituksen oppimiseen

liittyvästä vasteesta. Harjoituksen ohjaajat saattavat puuttua harjoituksen kulkuun antamalla esimerkiksi vihjeitä tai vaikuttaa muulla tavoin harjoituksen aikana. [10] Tabletop-harjoituksella tarkoitetaan tässä yhteydessä keskustelupohjaista harjoitusta, jossa osallistujat käyvät yhdessä läpi ennalta määritellyn skenaarion ja harjoittelevat toimintaa poikkeama- tai kriisitilanteessa. Tabletop-harjoituksen kulkuun ja lopputulokseen voivat vaikuttaa eri asiat, kuten osallistujien määrä, osaamistaso, ohjaajien toimintatavat sekä toimintaympäristö. Nämä muuttujat voivat osaltaan vaikuttaa harjoituksen dokumentoinnin sekä analysoinnin haasteisiin sekä harjoitusten keskinäisten tulosten vertailemiseen.

4.3 Kyberstressitestausta

ENISA (European Union Agency for Cybersecurity) on virasto, joka pyrkii varmistamaan korkean yhteisen kyberturvallisuustason Euroopassa. ENISA on laatinut käsikirjan kyberstressitestejä (Cyber Stress Test) varten, jonka tavoitteena on ohjata kriittisillä toimialoilla toimivien organisaatioiden kyberturvallisuuden ja sietokyvyn stressitestaamisessa. ENISA:n käsikirja on suunnattu erityisesti NIS2-direktiivin mukaisille kyberturvallisuusviranomaisille. [11]

Kyberstressitestaamisen määrittelemisen riippuu asiayhteydestä. ENISA:n käsikirjassa se kuvataan kohdennetuksi arvioinniksi, joka mittaa organisaation resilienssiä ja sen kykyä selviytyä merkittävistä kyberturvallisuuspoikkeamista siten, että kriittiset palvelut voidaan varmistaa eri riskiskenaarioissa. Kyberstressitestit ovat pääosin niin sanottuja desktop-harjoituksia, jotka perustuvat tekniseen kyselylomakkeeseen keskittyen yhteen tai useampaan riskiskenaarioon. [11] Kyberstressitesti voidaan nähdä pääosin keskustelupohjaisena harjoituksena, mutta siihen sisältyy myös mahdollisuus ottaa mukaan teknisiä osa-alueita, jolloin se on mahdollista luokitella yhdistelmäharjoitukseksi, jossa yhdistyvät keskustelupohjaisen ja teknisen harjoituksen piirteitä.

Kyberstressitestin keskeisiä ominaisuuksia ovat painotus organisaation resilienssiin eli valmiuteen reagoida erilaisten kyberuhkien tilanteissa. Kyberstressitestit ovat apuvälineitä organisaatioille erilaisten haavoittuvuuksien mahdollisten kriittisten virheiden tunnistamiseen sekä erilaisten syy- ja seuraussuhteiden hahmottamiseen. Kyberstressitestit painottavat kysymystä ”mitä jos...” tavoitellen mahdollisimman todellisia riskiskenaarioita. Kyberstressitesteissä on mahdollista hyödyntää erilaisia mittareita, kuten esimerkiksi häiriön havaitsemisaikaa tai toipumisaikaa ja ne toteutetaan pääosin organisaation

toimintaan mukautettuna. Kyberstressitestille määritetään stressitasoja, joiden avulla arvioidaan organisaation valmiutta. Korkeimmalla tasolla tarkastellaan harvinaisia, mutta erittäin vakavia ”Black Swan” -tapahtumia. [11] Mustalla joutsenella (black swan) tarkoitetaan tässä laajasti vaikuttavaa ja vaikeasti ennustettavaa tapahtumaa. Esimerkkinä tällaisesta tapahtumasta on COVID-19-pandemia, jonka sosiaalisia ja taloudellisia seurauksia on ollut pandemian aikana haasteellista arvioida. [12] ”Black Swan” -tapahtumia kyberturvallisuuteen liittyen voivat olla esimerkiksi laajat palvelukatkokset, tietomurrot tai odottamattomat ohjelmistovirheet. Tämän kaltaiset tapahtumat ovat harvinaisia ja vaikeasti ennustettavia, mutta niillä voi olla organisaatiolle suuret taloudelliset vaikutukset. Varautuminen erittäin harvinaisiin ja epätodennäköisiin tapahtumiin voi olla haastavaa, mikä osaltaan lisää kyberharjoittelun merkitystä organisaation turvallisuuden ja jatkuvuuden varmistamiseksi.

5 Harjoitusten mahdollisuudet organisaatiolle

Tietoturvallisuuteen liittyvien turvallisuuspoikkeamien määrä kasvaa jatkuvasti. Tämä osaltaan lisää organisaatioiden kustannuksia tietoturvaan liittyen. Useat organisaatiot ovat lisänneet turvallisuuskoulutuksia, joilla lisätään työntekijöiden tietoisuutta liittyen kyberturvallisuuteen. Koulutusten tavoitteena on vaikuttaa työntekijöiden asenteisiin ja käyttäytymiseen turvallisuuden lisäämiseksi. Yleisimmät inhimilliset virheet ovat esimerkiksi oletuskäyttäjätunnusten ja -salasanojen käyttö tai helposti arvattavat salasanat, järjestelmien virheelliset konfiguroinnit, päivitysten puutteellinen hallinta sekä kannettavien tietokoneiden tai mobiililaitteiden kadottaminen. [13] Koulutusten avulla on mahdollista lisätä työntekijöiden tietoa liittyen kyberturvallisuuteen, mutta samalla se mahdollistaa myös käyttäytymiseen liittyvät muutokset, sillä monet tietoturvapoikkeamat syntyvät arkisista toimintatavoista ja rutiineista.

Organisaatioissa työntekijät saattavat kokea, että kyberturvallisuuteen liittyvät koulutukset eivät ole mielenkiintoisia. Kyberturvallisuuteen liittyvissä koulutuksissa mielenkiintoa vähentää etenkin erilaiset pitkät työntekijöille pakolliset videot, jotka sisältävät videon jälkeen monivalintakysymyksiä. Työntekijät saattavat kokea myös, että kyberturvallisuuden koulutukset eivät ole riittävän kohdennettuja tai relevantteja heidän työtehtäviensä kannalta. [13] Kyberturvallisuuteen liittyvät harjoitukset voivat lisätä työntekijöiden motivaatiota ja innostusta kyberturvallisuuteen liittyen, sillä niiden luonne kannustaa osallistujaa aktiivisesti olemaan osa harjoitusta. Lisäksi kyberturvallisuusharjoituksissa on tärkeää, että ne ovat kohdennettu oikein organisaation sisällä ja räätälöity vastaamaan organisaation tarpeita.

Kyberturvallisuuden koulutusten parhaiksi käytännöiksi korostetaan muun muassa personointia, vastuullisuutta, vuorovaikutteisuutta, hauskuutta, käytännönläheisyyttä, relevanssia, käytännönläheisyyttä, ajankohtaisuutta ja palkitsemista. [13] Organisaatiolla on mahdollisuus räätälöidä kyberturvallisuuden harjoituksia näiden viitekehysten avulla, mikä voi sitouttaa työntekijää itsensä kehittämiseen kyberturvallisuuden näkökulmasta.

Personoinnissa koulutuksen sisältö räätälöidään osallistujien tarpeiden mukaan, ja siihen voidaan sisällyttää ajankohtaista materiaalia, mikä tukee oppimista sekä osallistujien tietojen ja taitojen jatkuvaa päivittämistä. Relevanttius korostaa räätälöintiä osallistujien

roolien sekä vastuiden mukaan. [13] Nämä näkökulmat ovat tärkeitä kyberturvallisuuden harjoituksissa etenkin niiden rakennusvaiheessa.

Vastuullisuudessa korostetaan huolimattomuuden vaikutuksia kyberturvallisuuteen. Lisäksi koulutusten tulisi olla relevantteja työntekijän näkökulmasta ja tuoda konkreettisesti esille turvallisuusohjeiden tärkeys työntekijän arjessa. [13] Kyberturvallisuuden harjoituksessa osallistuja pystyy tunnistamaan erilaisia syy- ja seuraussuhteita, mikä osaltaan mahdollistaa kyberturvallisuuden merkityksen hahmottamisen työntekijän sekä organisaation näkökulmasta.

Vuorovaikutteisuus ja hauskuus ovat tärkeitä elementtejä kyberturvallisuuteen liittyvissä koulutuksissa. Vuorovaikutteisuus tarkoittaa tässä yhteydessä osallistujien kokemusten ja osaamisen jakamisen. Hauskuutta puolestaan on mahdollista tuoda osaksi harjoitusta tarinoiden, huumorin ja pelillistämisen avulla. [13] Etenkin Tabletop-harjoituksissa suositellaan osallistujien keskinäisen tiedon jakamista. Harjoitus voi osaltaan tukea kysymysten esittämisen, mikä voi tuoda esille mahdollisia puutteita tiedossa ja parhaimmillaan tarjota myös vastauksia harjoitusten aikana. Harjoitusten räätälöinti sekä ohjaajien osaminen voivat lisätä vuorovaikutteisuutta sekä hauskuutta.

Käytännönläheisyydessä tuodaan esille häiriön tai tapahtuman simulointia, joissa työntekijät pääsevät konkreettisesti toimimaan häiriön tai tapahtuman selvittämiseksi. [13] Erietyisesti CDX-tyylisissä harjoituksissa voidaan osallistua erilaisten simuloitujen uhkien ja hyökkäysten käsittelyyn, mikä lisää oppimisen realistisuutta ja vaikuttavuutta.

Koulutusten tulisi tukea myös vahvistamista eli kyberturvallisuustietoa ja -koulutusta tulisi tarjota työntekijöille säännöllisesti. [13] Tabletop-harjoitusten rakentaminen on lähtökohtaisesti nopeampaa ja vähemmän resursseja vaativaa verrattuna CDX-tyyppisiin harjoituksiin. Organisaation näkökulmasta koulutusten kustannukset voivat vaikuttaa siihen, miten harjoitukset suunnitellaan ja toteutetaan. Harjoitusmuotojen suora vertailu on kuitenkin haastavaa, sillä ne eroavat rakenteeltaan, sisällöltään ja kohderyhmiltään. Tämän vuoksi organisaation tulee arvioida, millainen harjoitusmuoto tukee parhaiten sen määrittelemiä tavoitteita ja tarpeita.

Palkitseminen voi motivoida työntekijöitä noudattamaan turvallisuuskäytäntöjä. [13] Harjoitusten näkökulmasta asiaan saattaa vaikuttaa organisaation kulttuuri ja ratkaisut

palkitsemiseen liittyen. Harjoitusten suunnittelussa ei selkeästi ole tuotu esille ratkaisuja työntekijän palkitsemisiin.

Työntekijät saattavat kokea väsymystä jatkuvien turvallisuushälytysten sekä mahdollisen pitkittyneen valppauden vuoksi. Kun organisaatio panostaa kyberturvallisuuskoulutukseen, voidaan samalla opettaa keinoja väsymyksen ja stressin hallintaan. [13] Organisaation näkökulmasta työntekijöiden väsymyksen ja stressin vähentäminen voivat tukea työntekijän jaksamista, mikä tukee organisaation toimintaa ja kehittymistä.

Organisaatio voi saavuttaa merkittäviä etuja, kuten parempaa suorituskykyä erilaisilla työntekijöille kohdistetuilla koulutus- ja kehitysohjelmilla. Hyvin rakennetut ja toteutetut koulutusohjelmat voivat lisätä työntekijöiden tuottavuuden lisäksi motivaatiota, työtyytyväisyyttä ja asiantuntemusta. Nämä voivat johtaa taloudellisesti parempiin tuloksiin organisaatiossa. Koulutus- ja kehitysohjelmien hyödyt ulottuvat yksilöiden lisäksi myös ryhmien ja osastojen tehokkuuteen ja sitä kautta koko organisaation menestykseen. [14]

6 Yhteenveto

Kyberturvallisuuteen liittyvä osaamisvajeen korjaaminen vaatii organisaatiolta aktiivista osallistamista, säännöllistä kohdennettua koulutusta sekä dokumentointia, jotta kaikki työntekijät ymmärtävät vastuunsa ja voivat tehokkaasti tukea organisaation kyberturvallisuutta. Osaamisvajeen korjaaminen edellyttää organisaatioilta jatkuvaa kouluttamista sekä tehokasta viestintää osana kyberturvallisuuden hallintaa. Jokaisen työntekijän tulisi tuntea organisaationsa käytännöt, politiikat ja toimintatavat sekä ymmärtää oma roolinsa osana kyberuhkien torjuntaa. [8]

Ensimmäinen tutkimuskysymys käsittelee, miksi kyberharjoittelu tukee organisaation riskienhallintaa. Koulutukset ja harjoitukset eivät ainoastaan lisää osaamista, vaan ne myös sitouttavat henkilöstöä turvallisuuskäytäntöihin ja vähentävät inhimillisiä virheitä. Simuloidut tilanteet ja käytännön harjoitukset auttavat hahmottamaan syy- ja seuraussuhteita sekä ymmärtämään turvallisuusohjeiden merkityksen. Lisäksi harjoitukset voidaan räätälöidä osallistujien roolin ja organisaation tarpeiden mukaan. Tämä vahvistaa oppimista sekä sitoutumista.

Vaikka harjoituksista kerättävä palaute antaa tietoa osallistujien kokemuksista ja harjoituksen kulusta, se ei välttämättä tarjoa luotettavaa tietoa harjoitusten oppimisvaikutuksesta tai niiden vaikutuksesta organisaation kyberturvallisuuteen. Lisäksi olisi tärkeää löytää harjoitustavat, joiden vaste osallistujien oppimiselle olisi mahdollisimman suurta.

Tietoa ja havaintoja tietoturvaan liittyvistä haavoittuvuuksista tulisi jakaa eri toimialojen välillä. Tiedonvaihto mahdollistaa yhteisten riskien tunnistamisen ja parhaiden käytäntöjen levittämisen, mikä edistää organisaatioiden ja toimialojen kokonaisvaltaista turvallisuutta. Samalla se vahvistaa valmiutta ennakoida uhkia ja reagoida poikkeamiin, mikä parantaa koko sektorin resilienssiä ja toimintavarmuutta.

Toinen tutkimuskysymys tarkastelee, miten kyberharjoittelu tukee NIS2-direktiivien vaatimusten täyttämistä. NIS2-direktiivi asettaa organisaatioille velvoitteita kyberturvallisuuden riskienhallintaan, jatkuvuuden suunnitteluun ja henkilöstön koulutukseen. Direktiivin velvoitteiden täyttämistä voidaan tehokkaasti tukea harjoitusten, kuten Tabletop-, CDX-harjoitusten sekä kyberturvallisuuteen liittyvien stressitestien avulla. Näin organisaatiot voivat kehittää teknisiä ja henkilöstön valmiuksia sekä parantaa kyberturvallisuuden tasoa keskeisissä ja tärkeissä organisaatioissa. NIS2-direktiivin asettamat velvoitteet,

kyberturvallisuusharjoitukset ja kohdennettu henkilöstökoulutus muodostavat yhdessä kokonaisuuden, jonka avulla organisaatiot voivat vahvistaa kyberturvallisuuttaan ja parantaa toimintavarmuuttaan.

Tutkielmassa on hyödynnetty vuosina 2019-2025 julkaistuja vertaisarvioituja artikkeleita sekä tutkimuksia. Kirjallisuudessa NIS2-direktiiviä käsitellään pääosin organisaatioille suunnattuina ohjeistuksina, vaatimuksina, velvoitteina ja sanktioina, kun taas organisaatioiden konkreettisia toteutuksia direktiivin vaatimusten täyttämiseksi on vähemmän tutkittu. Tarjolla oleva kirjallisuus ei aina huomioi riittävästi eri sektoreiden ja organisaatioiden välisiä toimialakohtaisia eroja. Tutkielman sisältöön vaikuttaa lisäksi se, että kyberturvallisuuteen liittyvät harjoitukset, kuten stressitestit, kyberharjoitukset ja koulutukset eivät ole täysin erillisiä, vaan ne limittyvät ja tukevat toisiaan osana organisaation kyberturvallisuuden kehittämistä. Tämä limittyneisyys voi johtaa siihen, että kirjallisuudessa käsitteitä määritellään epäyhtenäisesti, eikä eri harjoitusmuotojen välisiä eroja tai rajoja kuvata yksiselitteisesti.

Tutkielmaan on valittu maltillinen määrä lähteitä, mikä rajaa sen sisältöä ja laajuutta. Valitut lähteet tarjoavat pääosin teoreettisen viitekehyksen, mutta ne eivät sisällä organisaatioiden empiirisiä havaintoja tai käytännön kokemuksia, mikä kaventaa osaltaan tutkielman sisältöä. Toisaalta tässä tutkielmassa hyödynnetyt lähteet ovat ajankohtaisia, mikä lisää tämän tutkielman arvoa. Vaikka lähteet ovat pääosin ajankohtaisia, niin kyberturvallisuuden luonne sekä harjoitusten muodot kehittyvät, mikä voi vaikuttaa tämän tutkielman ajantasaisuuteen ja sovellettavuuteen tulevaisuudessa. On myös huomioitava, että tutkielmassa viitatus verkkosivustot saattavat muuttua viittauksen jälkeen.

Lähteet

- [1] Kun E. Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age. *Digital Decade*. 2025;:479–512 Saatavissa: <http://dx.doi.org/10.5771/9783748943990-479>
- [2] Pfaller T, Skopik F, Smith P, Leitner M. Exploring a comprehensive approach to customize cyber exercises utilizing a process-based lifecycle model. *International journal of information security*. 2025;24(2). Saatavissa: <https://doi.org/10.1007/s10207-025-00993-6>.
- [3] El Amin H, Samhat AE, Chamoun M, Oueidat L, Feghali A. An integrated approach to cyber risk management with cyber threat intelligence framework to secure critical infrastructure. *J Cybersecurity Privacy*. 2024;4(2):357–81. Saatavissa: <https://doi.org/10.3390/jcp4020018>
- [4] Traficom [Internet]. 2025 [viitattu 1. helmikuuta 2026]. Kyberturvallisuuslaki on hyväksytty eduskunnassa - NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025. Saatavissa: <https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet>
- [5] Kyberturvallisuuskeskus [Internet]. 2026 [viitattu 1. helmikuuta 2026]. Tärkeää tietoa Euroopan unionin kyberturvallisuusedirektiivistä (NIS2). Saatavissa: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusedirektiivi/tarkeaa-tietoa>
- [6] 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) [Internet]. OJ L jouluku 14, 2022. Saatavissa: <http://data.europa.eu/eli/dir/2022/2555/oj>
- [7] Taherdoost H. A Critical Review on Cybersecurity Awareness Frameworks and Training Models. *Procedia computer science*. 2024;235:1649–1663. Saatavissa: <https://doi.org/10.1016/j.procs.2024.04.156>
- [8] Floros E, Stavrou E, Smyrlis M, Nikoloudakis N, Potamos G, Apostolidis A, ym. Towards the Design of Cyber Range Training Programs for Enhanced Preparedness: Investigating the Training Needs in Critical Infrastructures. Teoksessa: 2025 IEEE Global Engineering Education Conference (EDUCON) [Internet]. 2025 [viitattu 26. tammikuuta 2026]. s. 1–10. Saatavissa: <https://ieeexplore.ieee.org/document/11016646/>
- [9] Brilingaitė A, et al. A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*. 2020;88. Saatavissa: <https://doi-org.libproxy.tuni.fi/10.1016/j.cose.2019.101607>
- [10] Švábenský V, Vykopal J, Horák M, Hofbauer M, Čeleda P. From Paper to Platform: Evolution of a Novel Learning Environment for Tabletop Exercises. Teo-

- ksessa: Proceedings of the 2024 on Innovation and Technology in Computer Science Education V 1 [Internet]. New York, NY, USA: Association for Computing Machinery; 2024 [viitattu 22. tammikuuta 2026]. s. 213–9. (ITiCSE 2024). Saatavissa: <https://dl.acm.org/doi/10.1145/3649217.3653639>
- [11] European Union Agency for Cybersecurity. *Handbook for cyber stress tests*. Luxembourg: Publications Office of the European Union; 2025. Saatavissa: <https://data.europa.eu/doi/10.2824/8248517>
- [12] Yarovaya L, Matkovskyy R, Jalan A, et al. The effects of a “black swan” event (COVID-19) on herding behavior in cryptocurrency markets. *Journal of international financial markets, institutions & money*. 2021;75. Saatavissa: <https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S1042443121000408>
- [13] He W, Zhang Z (Justin). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*. 2. lokakuuta 2019;29(4):249–57. Saatavissa: <https://doi.org/10.1080/10919392.2019.1611528>
- [14] Vanitha P, Sankar Ganesh R. Impact of Employee Training and Development on Organizational Performance. *Shanlax International Journal of Management*. 2024;11(4):51–4. Saatavissa: <https://doi.org/10.34293/management.v11i4.7470>