jamk

Kyberharjoitus osana organisaation jatkuvasti kehittyvää kyberturvahallintaa

Markus Uusikartano

Opinnäytetyö, AMK
Toukokuu 2023
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Uusikartano, Markus

Kyberharjoitus osana organisaation jatkuvasti kehittyvää kyberturvahallintaa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2023, 41 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: Suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Kyberturvallisuudesta voi kuulla puhuttavan jatkuvasti kaikkialla, kuten mediassa. Kyberympäristöön liittyvät häiriöt ja uhat yleistyvät nopeaa vauhtia ja maailmalla pyritään pysyä muutosten tahdissa mukana. Kyberympäristössä tapahtuvia kyberhäiriötä vastaan voi kuitenkin harjoitella kyberharjoituksen voimin. Kyberharjoittelu tuo monia etuja niin teknisen osaamisen kuin yhteistyön ja kehityksessä.

Opinnäytetyössä suunniteltiin ja toteutettiin kyberharjoitus Suomessa toimivalle ohjelmistoyritykselle Wapice Oy:lle. Kyberharjoituksessa tavoitteena oli luoda harjoituksen tapahtumista kokonaistilannekuva, jonka avulla pystyttäisiin luomaan näkemys organisaation kyvystä vastata kyberympäristön häiriötilanteisiin. Opinnäytetyön tavoitteena oli selvittää, voiko kyberharjoituksia käyttää organisaation kyberturvahallinnan kehittämiseen.

Kyberharjoitus todettiin onnistuneeksi ja sen tuloksista luotiin loppuraportti, jossa käytiin läpi yksityiskohtaisesti sen osa-alueet suunnittelusta jälkianalysointiin. Kyberharjoituksen jälkeisten palautetilaisuuksien, kerätyn palautteen ja kyberharjoituksen tulosten avulla pystyttiin analysoimaan parannuskohteita kyberhäiriötilanteissa toimimiseen sekä kyberharjoituksen toteutukseen.

Tutkimustyön tavoite saavutettiin saamalla mahdollinen vastaus tutkimuskysymykseen. Koska kyberharjoituksen analysointi tuotti tuloksia ja kehityskohteita, voitiin todeta sen tuovan hyötyä organisaatiolle kyberturvahallinnan kehittämisessä. Kyberharjoituksen oltua kuitenkin ensimmäinen harjoitus organisaatiossa, ei tutkimuskysymykseen voitu vastata täydellä varmuudella. Jotta varmuus tähän voitaisiin saada, tulisi organisaation toteuttaa useampi kyberharjoittelu ja analysoida niiden tulokset vastaavalla tavalla. Kyberharjoittelun kuitenkin voitiin todeta antaneen toimeksiantajan organisaatiolle etuja.

Avainsanat (asiasanat)

Kyberturvallisuus, kyberharjoitus, kyberhäiriö, kyberturvallisuuden tilannekuva, kybertoimintaympäristö

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Uusikartano, Markus

Cyber exercise as part of an organization's ever-evolving cyber security management

Jyväskylä: JAMK University of Applied Sciences, May 2023, 41 pages.

Information and Communications. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Cyber security is constantly being discussed everywhere, including in the media. Disruptions and threats related to the cyber environment are rapidly becoming more common, and efforts are being made worldwide to keep up with the changes. It is possible however to practice against cyber incidents occurring in the cyber environment through cyber exercises. Cyber exercises offer many advantages in terms of technical expertise and the development of collaboration and communication.

In the thesis, a cyber exercise was designed and executed for Wapice Oy, a software company operating in Finland. The goal of the cyber exercise was to create a comprehensive situational picture of the events in the exercise, which would enable an assessment of the organization's ability to respond to cyber incidents. The objective of the thesis was to determine whether cyber exercises can be used to develop an organization's cyber security management.

The cyber exercise was stated successful, and an after-action report was created to provide detailed analysis of the components of the exercise, from planning to post-analysis. Through feedback sessions, gathered feedback, and the results of the cyber exercise, the areas for improvement in responding to cyber incidents and the execution of the cyber exercise were possible to be analyzed.

The objective of the research in the thesis was achieved by gaining a possible answer to the research question. Since the analysis of the cyber exercise yielded results as well as areas for development, it could be concluded that it brought benefits to the organization in terms of cyber security management. The cyber exercise being the first exercise of its kind in the organization, the research question could not be answered with complete certainty. To obtain this certainty, the organization would have to execute multiple cyber exercises and analyze their results in a similar manner. The cyber exercise was determined to have provided advantages to the client's organization nevertheless.

Keywords/tags (subjects)

Cyber security, cyber exercise, cyber incident, cyber security situational picture, cyber environment

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

Kyberhyökkäykset ja kyberrikollisuus on jatkuvasti kasvava ja yhä enemmän esiintyvä ilmiö niin ympäri maailmaa kuin Suomessakin. Kyberrikollisuus on kasvanut jo niin paljon, että Euroopan komission mukaan se aiheuttaa nykyään jo yli viiden (5) biljoonan euron vuotuiset kustannukset maailmassa, mikä on jopa kaksinkertainen luku kuin vuoteen 2015 verrattuna (A cybersecure digital transformation in a complex threat environment — Brochure 2021). Kriittiset alat, kuten terveydenhuolto ja energia-ala, ovat jatkuvasti riippuvaisempia digiteknologiasta, joka tuo myös paljon kybermaailman haasteita ja uhkia yhteiskunnalle. Myös kotona olevia laitteita yhdistetään yhä useammin internetiin, eli niin sanottuun esineiden internetiin (eng. Internet of Things, IoT), joka vaatii entistä enemmän varovaisuutta tavalliselta kansalaiseltakin tuoden riskejä niin henkilön yksityisyydelle kuin kyberturvallisuudelle. (Kyberturvallisuus: miten EU torjuu kyberuhkia? 2023.)

Ihminen on inhimillinen tekijä, joka voidaan luokitella kyberturvallisuuden heikoksi lenkiksi. Ihmistä on helppo vedättää ja saada avaamaan esimerkiksi huijauslinkin, jonka on vastaanottanut sähköpostiin. Joskus kuitenkin näin pienellä virheellä voi olla valtavat, jopa lähes korjaamattomat seuraukset, esimerkiksi yritykselle. Jotta voitaisiin varmistaa, että löytyy oikeita asiantuntijoita, joilta löytyy tarvittava tietotaito, jopa Euroopan komissio tekee erinäisiä toimia, kuten kyberturvallisuuskuukausia yhdessä Euroopan kyberturvallisuusviraston ENISA:n (eng. The European Union Agency for Cybersecurity) kanssa. Näillä toimilla halutaan parantaa tietoisuutta kyberturvallisuudesta suurelle yleisölle, maailmalle. (A cybersecure digital transformation in a complex threat environment — Brochure 2021.)

Suomessakin on otettu kyberturvallisuuteen liittyvät uhat tosissaan. Vuoden 2021 julkaistussa valtioneuvoston kyberturvallisuuden kehittämisohjelmassa nykyinen valtion kyberturvallisuusjohtaja Paananen (2021, 14–15) toteaa, että ”Aktiivisella harjoitustoiminnalla on keskeinen merkitys kyberhyökkäyksien torjunnan, hallinnan ja niiden ratkaisemisen kehittämisessä”, sekä tuoden esiin tarpeen kyberturvallisuuden harjoitustoiminnan edistämiselle ja ylläpidolle. Kehittämisohjelmassa kehotetaan strategisten kumppanuuksien kehittämiselle yritysten ja korkeakoulujen kesken, mutta lisäksi yhteistyö viranomaisten, elinkeinoelämän ja järjestöjen välillä on erittäin kriittistä yhteiskunnan turvaamisen ja toiminnan vuoksi. (Mts. 14–15.)

Kyberharjoituksia järjestetään kansainvälisellä tasolla, muun muassa Euroopassa, mutta myös meillä Suomessa. Ne eivät kuitenkaan ole niin yleisiä, että kovin moni kybertoimintaympäristössä toimivista henkilöistä pääsisi sellaiseen osallistumaan. Harjoitusten on todettu kuitenkin olevan merkittäviä kyberuhkien hallinnan kannalta ja ihmisen olevan kyberturvallisuuden heikko lenkki (A cybersecure digital transformation in a complex threat environment — Brochure 2021), joten miksei niitä hyödyntäisi myös niin pienet kuin suuretkin yritykset ja organisaatiot kehittäessään kyberturvahallintaansa.

Opinnäytetyön tarkoituksena oli suunnitella ja toteuttaa kyberturvallisuuteen liittyvä toimintaharjoitus, eli kyberharjoitus. Harjoituksen tarkoituksena oli luoda kokonaistilannekuva, jonka avulla voitiin tarkastella organisaation sen hetkistä kykyä vastata kyberympäristössä tapahtuviin häiriötilanteisiin. Harjoitus toteutettiin Wapice Oy:lle, joka on teollisuuden johtava teknologiapartneri, ja jolta löytyy kokonaisvaltaista asiantuntijuutta niin ohjelmistokehityksen kuin elektroniikkasuunnittelun saralta (Yritys 2023).

Työn laajuuteen kuului itse kyberharjoitus ja siihen liittyvä viestintä, havainnointi ja avustaminen harjoituksen aikana sekä tulosten ja havaintojen dokumentointi. Tilannekuvaharjoituksessa käsiteltiin häiriötilanteita, joissa viestintä kaatuu, sekä tietomurtoa ja mahdollista haittaohjelman havainnoimista. Harjoituksen tuloksista luotiin loppuraportti, jossa käytiin läpi syntyneet aktiviteetit ja mahdolliset muutokset, sekä kyberympäristössä tapahtunut toiminta. Loppuraportissa käytiin myös läpi harjoituksen tulokset ja palautteet, sekä niiden analysointi. Loppuraportin tavoitteena oli tukea toimeksiantajaa ja seuraavan suunnittelijaa kyberharjoituksen luomisessa, sekä antaa toimeksiantajalle kuva häiriötilanteiden ratkaisemiskyvykkyydestä organisaation sisällä.

2 Tutkimusasetelma

Toimeksiantajan organisaatiossa kaivattiin yleiskuvan muodostamista, jotta voitaisiin määritellä ja selvittää organisaation sen hetkistä kykyä hallita kyberympäristössä tapahtuvia häiriöitä. Koska organisaatiossa ei ollut aikaisemmin järjestetty kyberharjoituksia, tutkimusongelmaksi muodostui kokonaistilannekuvan muodostaminen kyberharjoituksen avuin.

Tutkimusongelmaa lähdettiin tarkastelemaan useammasta näkökulmasta ja pyrittiin keskittymään tutkimuksen tarkoitukseen. Tutkimusongelman tarkastelu johti tutkimukseen liittyvään kysymykseen, johon työssä haetaan vastausta:

1. Voiko kyberharjoituksesta olla hyötyä organisaation kyberturvan kehittämiselle tulevaisuudessa?

Tutkimusongelman ja siihen liittyvän kysymyksen ratkaisemiseen parhaimmaksi menetelmäksi muodostui konstruktiivinen tutkimusmenetelmä. Konstruktiivisessa tutkimusmenetelmässä pyritään ratkaisemaan reaalimaailman ongelmia ja tuottamaan innovatiivisia konstruktioita. Konstruktiot itsessään ovat abstrakteja käsitteitä, joilla on loputtomasti mahdollisia toteutumia. Konstruktioiksi voidaan luokitella kaikki ihmisen luomat artefaktit, kuten tuotteet ja mallit, sillä niitä keksitään sekä kehitetään. (Lukka 2001.)

Konstruktiivinen tutkimusmenetelmä eroaa perinteisestä tutkimustavasta, jossa yleensä pyritään minimoimaan empiirinen häirintä. Koska tutkimusmenetelmä perustuu pragmatistiseen filosofiaan, se pyrkii tuottamaan merkittäviä teoreettisia kontribuutioita suoraan käytännön analyysin avulla. Ideaalitilanteessa konstruktiivinen tutkimus tuottaa uuden konstruktion, jonka avulla ratkaistaan reaalimaailman ongelma, tarjoamalla myös niin käytännön kuin teorian näkökulmaa. Jos tutkimus ei onnistu käytännön tasolla, voi se tuottaa silti huomattavaa teoreettista merkitystä. (Lukka 2001.)

Konstruktiivisella tutkimusmenetelmällä saadaan useita todennäköisiä etuja. Se tarjoaa tutkijoille mahdollisuutta tutkia mielenkiintoista kohdetta ja tuottaa selkeitä käytännön hyötyjä. Yhteistyössä toimiva organisaatio saa konstruktiivisesta tutkimuksesta hyötyä saadessaan ongelmiaan kriittisen analyysin kohteeksi ja ratkaisut niihin. Ongelmanratkaisuprosessissa myös tutkija pääsee tuomaan aikaisempaa tietotaitoa ja teoriaan perustuvaa tietämystä. Konstruktiivisessa tutkimusmenetelmässä voidaan pienentää käytännön ja tutkimuksen välillä olevaa tilaa, sekä edistää tietotaidon kehittymistä ja vuorovaikutusta toimijoiden ja tutkijoiden välillä. (Lukka 2001.)

Konstruktiivinen tutkimusmenetelmä toimi opinnäytetyön toteutukseen tuoden sille selkeän prosessin, jolla saatiin luotua konstruktiot: kyberharjoitus ja loppuraportti. Toimeksiantajan organisaatio toimi yhteistyössä tutkimuksessa ja toi siihen mukaan tietotaitoa, näkemystä ja ideoita.

Näin saatiin luotua yhteistyössä organisaation kanssa niin toimeksiantajan kuin tutkijan mielestä arvokas tutkimus.

3 Kyberturvallisuus

3.1 Mitä on kyberturvallisuus

Kyberturvallisuudeksi määritellään tavoitetila, jossa voidaan luottaa kybertoimintaympäristöön, joka on toiminnaltaan turvattu toimenpiteiden avulla, joilla pystytään hallita ennakoivasti kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristö yleensä määritellään koostuvan yhdestä tai useammasta digitaalisesta tietojärjestelmästä, jotka muodostavat toimintaympäristön. (Sanastokeskus TSK 2018)

Kybertoimintaympäristöön paljon riskejä, kuten ihmisen tekemät virheet, mutta sen lisäksi kehittyviä ja muuntautuvia uhkia, jotka voivat vaarantaa elintärkeitä toimintoja niin kybertoimintaympäristössä kuin yhteiskunnassa (Turvallisuuskomitea 2019).

3.2 Suomen kyberturvallisuus

Kyberturvallisuus Suomessa voidaan luokitella kansalliseksi turvallisuudeksi. Siinä on kyse koko suomalaisen yhteiskunnan kollektiivisesta turvallisuudesta ja Suomen suvereniteetista. Niin kyberturvallisuus että kansallinen turvallisuus voidaan määritellä dynaamiseksi, sillä se määrittyy Suomen uhka- ja toimintaympäristön mukaan muuttuen jatkuvasti. Tämän dynaamisuuden vuoksi muutokset vaikuttavat myös eri politiikkalohkoille, minkä vuoksi kansallista turvallisuutta ei suojella vain yhden viraston tai ministeriön toimin, joka niin ollen parantaa eri uhkiin vastaamista. (Kotipelto n.da)

Dynaamisuutta vaaditaan, sillä Suomen on pystyttävä muuttamaan ajankohtaisten tilanteiden mukaan nopeasti. Tästä hyvä esimerkki on Venäjän hyökkäys Ukrainaan vuoden 2022 helmikuussa. Tämä muutti Suomen mm. sisäministeriön toimintaympäristöä perusteellisesti ja pitkäaikaisesti. Suomeen kohdistuvan hybridivaikuttamisen riski on hyökkäyksen myötä kasvanut, vaikkei sotilaallista uhkaa varsinaisesti Suomeen kohdistukaan. Hybridivaikuttamisella tarkoitetaan poliittisesti motivoitunutta suunnitelmallista toimintaa, kuten kyberoperaatio, jossa hyödynnetään kohteen

heikkouksia, jotta saavutettaisiin omat tavoitteet. Venäjä on pyrkinyt käyttämään kyseistä vaikuttamisen keinoa Ukrainassa ja täten aiheuttanut laajamittaisia kyberhyökkäyksiä muun sotatoimen tukena. (Kotipelto n.da; Sanastokeskus TSK 2018)

Muuttuvan toimintaympäristön ja uhkien vuoksi tietoa ja osaamispääomaa Suomessa on tarpeen suojata paremmin kuin ennen, sillä Suomen tulee pystyä sopeutumaan ja menestymään nykymaailmassa, jossa öljyn ja mineraalien lisäksi data voidaan rinnastaa strategiseksi resurssiksi. Globaalit turvallisuusuhat vaikuttavat myös Suomeen, joka vaatii kansallisen turvallisuuden puolesta vahvaa yhteyttä myös ulko- ja turvallisuuspoliittiseen päätöksentekoon. (Kotipelto n.da)

Strategisena resurssina datan merkitys lisääntyy, koska yhteiskunta on globaalien tietoverkkojen ja datavirtojen puolesta sidoksissa, johon vaikuttaa jatkuvasti muuttuva digitalisaatio sekä teknologinen murros. Tämä muuttaa kansallisen turvallisuuden strategisia riippuvuuksia luoden uusia mahdollisuuksia, mutta rinnalle myös haavoittuvuuksia. (Kotipelto n.da)

Kyberturvallisuus on varsinkin nykyään yksi kansallisen turvallisuuden merkittävistä tavoitetiloista, jotta yhteiskuntaa voitaisiin suojata vihamieliseltä kybervaikuttamiselta. Kyberuhat, jotka määritellään kansallisen turvallisuuden uhiksi, ovat valtiollisia kyberuhkia. Kyberuhkaksi määritellään haitallinen mahdollisesti toteutuva tapahtuma tai kehityskulku, joka on kohdistettu kybertoimintaympäristöön ja täten vaarantaa siitä riippuvaisen toiminnon, kuten ydinvoimalan ohjauksen. Kyberuhat voivat kohdistua esimerkiksi terveydenhuollon toimijoihin ja voivat tapahtua alihankintana kyberrikollisryhmien puolesta, vaikka taustalla olisikin valtiollinen toimija. Valtiollisten kyberuhkien pyrkimyksenä yleensä on hankkia tietoa valtionhallinnon päätöksenteosta tai toimintakyvyn kannalta kriittisistä haavoittuvuuksista laittomasti. Kyberuhat ovat yksi hybridivaikuttamisen keinoista, jossa pyritään vaikeuttamaan valtionjohdon päätöksentekoa sekä horjuttaa yhteiskunnallista vakautta. (Kotipelto n.db; Sanastokeskus TSK 2018)

Kyberuhat, kuten tietoverkkovakoilu ei kohdistu pelkästään valtion kybertoimintaympäristöihin, vaan vaihtoehtoisesti myös niin pienten kuin suurten yritysten ja tutkimuslaitosten tietopääomaan. Tälle syy voi olla esimerkiksi hyökkääjän teollisuuden kilpailukyvyn vahvistaminen tai teknologioiden hankkiminen sotilaallisiin tarkoituksiin. Hyökkäyksellä voi olla siis poliittinen motiivi, tai täysin rahallinen hyöty (Mikä on kyber-hyökkäys? n.d). Kybervaikuttaminen on varsinkin näin

Venäjän hyökkäyksen luoman poikkeusolon vuoksi keskiössä, mutta myös rauhan aikana se on yhtä todellista. (Kotipelto n.db)

Kyberuhan taustalla oleva tekijä voi olla vaikea tunnistaa, sillä tekijä yleensä peittää jälkensä hyvin. Peitekeinona monesti käytetään harhauttamista tai monen kaupallisen palvelimen kautta reitittämistä. Joskus kuitenkin nämä toimintatavat myös auttavat tunnistamaan tekijän aikaisempien toimintatapojen, haittaohjelmien tai hyökkäyskohteiden perusteella. Näihin hyökkäyksiin vastaaminen edellyttää pääasiassa tunnistettujen haavoittuvuuksien korjaamista, mutta myös tekijän julkistaminen ja pakotteiden luominen toimivat kasvavassa määrin vastakeinona. (Kotipelto n.db)

3.3 Kyberturvallisuusstrategia ja kehittämisohjelma

Suomessa julkaistiin vuonna 2013 ensimmäistä kertaa kansallinen kyberturvallisuusstrategia. Strategiassa pyrittiin käsittelemään tavoitteita, jotka auttavat vastaamaan kybertoimintaympäristöön liittyviin haasteisiin (Turvallisuuskomitea 2017). Strategian avulla luotiin kyberturvallisuuden visio, jonka mukaan vuoteen 2016 mennessä Suomi olisi maailmanlaajuisesti edelläkävijä kyberuhkiin varautumisessa ja niiden hallinnassa (Takala 2013). Kyberturvallisuuden vision voidaan visualisoida kokonaisuudessaan kuvana (ks. Kuvio 1).

Kuvio 1. Kyberturvallisuuden visio (Takala 2013, 3)

Jotta visiossa mainitut tavoitteet voitaisiin saavuttaa, tarvittiin kyberturvallisuuden toimeenpano-ohjelmaa täydentämään strategiaa. Tässä ohjelmassa käsiteltiin yhteensä 74 toimenpidettä, joista keskeisimmät kehittämiskohteet todettiin olevan (Turvallisuuskomitea 2014):

1. *Kyberturvallisuuskeskus,*
2. *Valtion ympärivuorokautinen tietoturvatoiminta,*
3. *Salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (SATU),*
4. *Poliisin toimintakyky kyberrikollisuuden torjunnassa,*
5. *Kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen sekä*
6. *Tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen.*

Vuoden 2013 kyberturvallisuusstrategia oli määritelty vuosille 2014–2017, mutta sitä pidennettiin vuodella. Pidennyksen syynä oli valtioneuvoston raportin ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” mukaan se, ettei kaikkia asetet-

tuja tavoitteita ole vaaditulla tasolla saavutettu. Tämä vaikutti myös siihen, että seuraava kyberturvallisuusstrategia julkaistiin vasta vuonna 2019. Raportti osoittaa lisäksi sen, että ensimmäisen kyberturvallisuusstrategian visiota, että Suomi olisi kyberturvallisuuden edelläkävijä, ei ole suoranaisesti saavutettu. Raportissa todetaan, ettei vakavia puutteita kuitenkaan ollut, mutta silti ei voida todeta Suomen olevan kyberturvallisuuden huippumaa, verrattuna esimerkiksi Israeliin tai Yhdysvaltoihin. (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen 2017, 25 & 61.)

Suomen kyberturvallisuusstrategiassa vuonna 2019 annetussa valtioneuvoston periaatepäätöksessä, joka on osa yhteiskunnan turvallisuusstrategian ja EU:n kyberturvallisuusstrategian toimelle panoa, tunnistettiin tarve kansallisen kyberturvallisuuden kokonaistilan parantamiseksi. Suomen kyberturvallisuusstrategiassa haluttiin löytää keskeisimmät kansalliset tavoitteet, joiden avulla voitaisiin kehittää kybertoimintaympäristöä ja turvata sen tärkeitä toimintoja. Strategia on edellytys sille, että kansallisen kyberturvallisuuden kehittämisohjelman valmistelu voidaan aloittaa. Tavoitteiksi muodostuivat tilannekuvan parantaminen, kansallisen yhteistyön tiivistäminen ja kansallisen koordinaation tehostaminen. (Paananen 2021; Turvallisuuskomitea 2019)

Tässä nykyisessä Suomen kyberturvallisuusstrategiassa käydään Suomen kyberturvallisuutta strategisten linjausten kautta, jotka koskevat kansainvälisen yhteistyön kehittämistä, kyberturvallisuuden johtamista, suunnittelua ja varautumista, sekä kyberturvallisuuden osaamisen kehittämistä (Turvallisuuskomitea 2019). Nämä strategiat toivat myös kyberturvallisuuden kehittämisohjelman neljä pääteemaa: huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus sekä tehokkaat kansalliset kyberturvakyvykkyydet (Paananen 2021).

Kansallinen yhteistyö kyberympäristössä kyberturvallisuusstrategian mukaan luottaa varsinkin voimassa olevaan kansainväliseen oikeuteen, ihmisoikeuksien kunnioittamiseen ja kansainvälisiin sopimuksiin. Strategiassa todetaan, ettei Suomi halua rajata internetin vapautta eikä sen kautta yksilöiden perusoikeuksia tai perusvapauksia, vaan haluaa mahdollistaa vapaan ja vakaan internetin turvallisen käytön. Jotta se onnistuu, tarvitaan yhteistyötä kansainvälisten toimijoiden kanssa monin tavoin, ja Suomi vaikuttaakin aktiivisesti kyberturvallisuuteen liittyvään politiikkaan Euroopan unionissa ja kansainvälisissä järjestöissä, kuten YK:ssa. Yhteistyö varsinkin EU:ssa muodostaa myös

Suomen kansallisen kyberturvallisuuspolitiikan selkärangan. Tämän kansainvälisen yhteistyön kehittämisen avulla pyritään tuomaan suojaa kyberhyökkäyksiä vastaan kybertoimintaympäristössä, mm. parantamalla hyökkäysten havainnointi- ja vastatoimikykyä. (Turvallisuuskomitea 2019, 5.)

Vuoden 2021 heinäkuussa luotiin Suomelle kyberturvallisuuden kehittämisohjelma, jossa määritellään keskeiset toiminnot kyberturvallisuuden parantamiseksi, ja joka tarkastelee kansallista kyberturvallisuutta eri mahdollisuuksien näkökulmasta. Kehittämisohjelmassa todetaan, että toimintojen toteutuessa kansallinen kyberturvallisuus vahvistuu. Ensisijainen tavoite kehittämisohjelmalla on luoda Suomeen kyberturvallisuuden ekosysteemi, joka lisäisi elinvoimaa ja kasvua luoden uusia alan työpaikko ja parantaa tarvittavaa osaamista sekä parantaa yhteiskunnan kestävyyttä ja sietokykyä kybertoimintaympäristöön liittyviä ilmiöitä vastaan. (Paananen 2021)

Kehittämisohjelmassa ehdotetaan monenlaisia kehittämistoimenpiteitä kyberturvallisuuden ekosysteemin parantamiseksi. Jotta Suomessa olisi tehokasta kyberturvakyvykkyyttä, ehdotetaan muun muassa seuraavaa: kehitetään viranomaisten varautumista kyberhäiriötilanteisiin ja parannetaan niiden havainnointikykyä. Paananen (2021, 18) toteaa, että kybertoimintaympäristössä ehdotonta on, että kaiken salassa pidettävän ja arkaluontoisen tiedon, kuten henkilötiedot, eheys ja luottamuksellisuus on säilytettävä. Tämän vuosi on tunnistettava yhteiskunnan rajojen yli menevät huoltovarmuuskriittiset arvoketjut, joiden tilannekuvaa on kehitettävä kyberturvallisuuden näkökulmasta. Sen lisäksi kehittämistoimenpiteenä on käynnistettävä selvitystyö, jotta voidaan arvioida kansallisen kyberturvallisuuden varmistamisen edellytykset niin yleisesti kyberturvallisuuden varmistamisessa, kuten myös kyberrikollisuuden torjumisessa. (Paananen 2021, 18–19.)

Kehittämistoimenpiteet liittyvät myös vahvasti kyberharjoitteluun. Kuten Paananen (2021, 14) kirjoittaa, kyberharjoitustoiminnalla on huomattava merkitys niin kyberhyökkäysten hallinnan kuin myös torjunnan kehittämisessä. Siksi kehittämisohjelmassa ehdotetaan kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistamista, jotta yhteiskunnan toimivuuden vuoksi tärkeiden arvoketjujen toiminta voitaisiin turvata. Näissä harjoituksissa hyödynnettäisiin yhteisiä kybertoimintaympäristöjä, jotka ovat nimenomaan harjoitustarkoitukseen soveltuvia. (Paananen 2021, 14–15.)

Kehitysohjelmassa väitetään, että nykypäivän koulutusohjelmat itsessään eivät ole riittäviä tuottamaan tarpeeksi kattavaa osaamista niin kyberturvateollisuudelle kuin elinkeinoelämällekään. Jotta

ammatillista osaamista voitaisiin edistää, tarvittaisiin parempaa panostusta muun muassa tutkintoon johtavan koulukseen niin julkisella sektorilla, kuten korkeakouluissa, kuin yksityisellä sektorillakin. Koulutusta on siis kehitettävä, joten kehitysohjelmassa ehdotetaankin huomioimaan paremmin kyberturvallisuuden osaamistarpeita koulutuksia suunniteltaessa. Sen lisäksi ehdotetaan sisältämään myös yleissivistävään perusopetukseen koulutusta, joka antaisi tarvittavat taidot kybertoimintaympäristössä toimimiseen ja antaisi tietotaitoa kyberuhkilta suojautumista vastaan. Myös korkea-asteen koulutuksissa, kuten lukiossa, mentäisiin astetta syvemmälle kehittämään edellä mainittuja taitoja, joissa voitaisiin hyödyntää uusia sekä vanhoja osaamispolkuja, riippumatta siitä mihin ammattiin opiskellaan, kuitenkin alaan soveltuvin keinoin. (Paananen 2021, 11–13.)

4 Kyberharjoittelu

4.1 Mikä on kyberharjoitus

Kyberharjoituksella tarkoitetaan tapahtumaa, jossa harjoituksen kohdeyleisö, kuten organisaatio, testaa kyvykkyyttään selviytyä kyberhäiriöistä. Harjoitus on kuvitteellinen, mutta sillä simuloidaan häiriötilannetta, joka parhaiten sopii kohdeyleisön harjoittelun tarkoitukseen. Näin saadaan luotua olosuhteet, joissa voidaan kehittää kohdeyleisön toimintaa, valmiutta ja reagointikykyä häiriötilanteissa. (Kyberturvallisuuskeskus 2019; Harjoitustoiminta 2023.)

Kyberharjoitukseen kuuluu yleensä tarina tai kertomus, eli skenaario, joka johtaa harjoituksen tapahtumien kulkua. Skenaario voidaan keksiä tyhjästä tai peilata vaikka organisaation tunnistettuihin riskeihin ja käyttää niitä rakennuspalikoina skenaariota suunnitellessa. Ajankohtaiset tapahtumat voivat myös auttaa skenaarion ideoinnissa. Skenaarion keskipisteessä on yleensä jokin kuvattu ongelma, jota harjoittelijat selvittävät harjoituksen aikana. Ongelman ympärille voidaan alkaa miettimään aiheuttajia ja häiriöitä, joista yhdessä muodostuu harjoitukselle tarina. (Kyberturvallisuuskeskus 2019, 20.)

Harjoituksessa, varsinkin toiminnallisessa harjoituksessa, peli etenee skenaariota varten luotujen syötteiden mukaan. Syötteet sisältävät tietoa, jonka avulla kerrotaan harjoittelijoille harjoituksen aikana tapahtumista. Syötteitä voi olla monenlaisia, kuten tiketti, sähköpostiviesti tai puhelu. Syötteet voidaan viestiä harjoittelijoille teknisesti tai vaikka paperilla. Syötteet voivat olla ajastettuja,

joka tuo harjoittelijoille tietoa skenaariosta vähän kerrallaan. Kannattaa kuitenkin ottaa huomioon, että jotkin syötteet voivat olla tavallista haastavampia, jolloin harjoittelijoilla saattaa kulua enemmän aikaa syötteeseen vastaamiseen, kuin mitä alun perin on suunniteltu. Syötteiden määrä kannattaa siis olla kohtuullinen. Syötteitä voi käyttää myös tehostamaan harjoittelijoiden yhteistyötä antamalla syötteitä samanaikaisesti. (Kyberturvallisuuskeskus 2019, 20–22.)

4.2 Kyberharjoittelun edut

Kyberharjoitusten voidaan sanoa olevan korvaamaton teknisten taitojen kehittämisen ja kokemuksien lähde. Harjoitusten avulla voidaan saavuttaa tuloksia, joita on mahdollista käyttää edelleen uusien harjoitusten, koulutuksien ja taitoja kehittävien toimien valmisteluissa. Sen lisäksi, että kyberharjoitukset auttavat tunnistamaan ja kartoittamaan kyberturvallisuuden tilaa, esimerkiksi organisaatiossa, ne auttavat myös parantamaan sitä saavutusten ja tulosten avulla. Harjoituksista saatu kokemus on arvokasta, joten saatu tietotaito on hyvä jakaa muiden merkityksellisten osapuolten kanssa. Tietotaidon jakaminen auttaa vahvistamaan luottamusta ja yhteistyötä eri osapuolten kanssa. (Benefits of Exercise n.d.)

Kyberharjoitukset auttavat tunnistamaan heikkouksia ja puutteita kybertoimintaympäristössä. Tämän ansiosta harjoitukset auttavat suunnittelemaan ja toteuttamaan erinäisiä ratkaisuja ja toimenpiteitä esim. organisaation sisällä. Harjoitukset ovatkin suotuisa väline toimintaperiaatteiden ja prosessien, kuten viestinnän tai kriisinhallinnan, tarkastamiseen ja päivittämiseen. Kyberharjoitukset nostavat esiin myös vahvuuksia toimia kyberympäristössä. Poikkeamien- ja kriisinhallinnan toimiminen harjoituksessa kielii sen toimimisesta myös tositilanteessa. (Benefits of Exercise n.d; Kyberturvallisuuskeskus 2019, 5.)

Kyberharjoituksen järjestämiseen voi organisaatiolla olla kynnystä, koska se vaatii aikaa ja resursseja. Harjoittelu voidaan kuitenkin aloittaa kevyesti, ja toimivan harjoituksen voi toteuttaa hyvinkin yksinkertaisesti, esimerkiksi työpöytäharjoituksen voimin. Yksinkertaisellakin harjoituksella voi olla monia hyötyjä organisaatiolle. (Kyberturvallisuuskeskus 2019, 5.)

Kyberharjoitusoppaassa (2019, 5) on listattu todettuja yleisiä hyötyjä ja etuja organisaatiolle, joita kyberharjoituksesta voi saada:

- Kriisinhallinnan vahvistuminen organisaatiossa
- Tietojärjestelmäriippuvuuden merkityksen ymmärryksen syventyminen
- Lisääntynyt ymmärrys häiriötilanteiden vaikutuksista
- Lisääntynyt luottamus epävarmuuden hallintaan
- Parantunut kyky poikkeustilanteissa johtamiseen
- Sisäisen ja ulkoisen viestinnän vahvistuminen
- Yhteistyön edistäminen asiakkaiden ja palveluntarjoajien kanssa
- Vastuiden ja vastuualueiden selventyminen
- Organisaation prosessien kehittyminen tulosten avulla

4.3 Harjoitusmenetelmät ja -tyypit

Kyberharjoitusmenetelmiä on loputtomasti. Harjoituksen suunnittelussa kannattaa siis pitää mielessä, että myös toteutustapoja on monenlaisia. Harjoituksen suunnitteluvaiheessa tuleekin miettiä harjoitukselle paras menetelmä, kuten myös harjoituksen tyyppi. Niiden valitsemiseen kuitenkin vaikuttaa moni asia, kuten harjoitusympäristö, resurssit, tavoitteet ja kohdeyleisö. (Kyberturvallisuuskeskus 2019, 6.)

Kuten harjoituksen toteutustapoja, myös harjoitustyyppejä on useita. Harjoitus voidaan toteuttaa käyttäen yhtä harjoitustyyppiä, tai valita rakenneosia useasta erilaisesta harjoitustyypistä ja rakentaa niistä yhtenäinen toimiva kokonaisuus. Yhdistämällä harjoitustyyppejä voi kuitenkin tavoitteiden yhdistäminen olla haastavaa suunniteltaessa mutkikkaampaa harjoitusta. Esimerkiksi johtoryhmän ja teknisen ryhmän kriisihallintakykyä voi olla vaikea harjoittaa yhdellä samalla harjoituksella, mutta tuomalla niihin sopivista harjoitustyypeistä rakenneosia ja miettimällä, mitä harjoituksella halutaan kehittää, voidaan saada rakennettua toimiva harjoitus. (Kyberturvallisuuskeskus 2019, 6.)

Jotta organisaatio saisi kyberharjoituksesta paremman kokonaisuuden, selkeämmät tulokset ja paremman oppikokemuksen, tulisi kyberharjoitustyyppien teemat ja soveltuvuus ymmärtää. Tavoitteellisessa tapauksessa organisaatio pystyisi mukautumaan kevyistä työpöytäharjoituksista suurempiin ja monimutkaisempiin teknisiin harjoituksiin (Kick 2014, 9). Kyberharjoitustyypit, joita yleisesti esiintyy, voidaan esittää taulukkomuodossa (ks. Taulukko 1). Taulukossa kerrotaan millaisia eri harjoitustyypit ovat sisällöltään ja millaisia keskeisiä teemoja niihin liittyy.

Taulukko 1. Kyberharjoitustyypit (Kick 2014; Kyberturvallisuuskeskus 2019; Live exercise n.d.)

Harjoitustyyppi	Kuvaus	Teemat
Työpöytäharjoitus (eng. Tabletop exercise)	Kevyt kirjalliseen materiaaliin perustuva harjoitus. Yleensä keskustelupohjainen ja syötteet toimitetaan paperisena, eli ei vaadi teknistä ympäristöä. Sopii harjoittelijoille, joilla ei ole aikaisempaa kokemusta kyberharjoituksista.	Prosessien läpikäynti, johtaminen, kyberhäiriöiden hallinta, kouluttaminen.
Juurisyyharjoitus (eng. Pre-mortem)	Työpöytäharjoituksen kaltainen kevyt harjoitus. Tavoitteena häiriön keskeltä aloittaen selvittää alkuperäinen kyberhäiriön aiheuttaja.	Ongelmien ennakointi, riskienhallinta sekä häiriöiden aiheuttajat.
Toiminnallinen harjoitus (eng. Functional exercise)	Realistisempi ajastettuja syötteitä hyväksikäyttävä harjoitus. Harjoituksen tarina selviää harjoittelijoille pelin aikana vähän kerrallaan. Monipuoliset tapahtumat ja haasteet, kuten median kanssa kommunikointi, tekevät harjoituksesta haastavamman.	Yhteistyö, viestintä ja johtaminen kriisitilanteessa.

(jatkuu)

Taulukko 1. Kyberharjoitustyypit (Kick 2014; Kyberturvallisuuskeskus 2019; Live exercise n.d.)(jatkuu)

Lipunryöstö (eng. Capture the Flag)	Lipunryöstö, eli CTF, on tekninen harjoitus, jossa etsitään kybertoimintaympäristöstä sinne piilotettuja lippuja. Jotta harjoittelija voi saada lippuja haltuunsa, tulee hänen yleensä murtaa kohteen suojaus ja päästä järjestelmään sisään. Liput voivat olla esimerkiksi sanoja, lauseita tai satunnaisia kirjainjonoja. CTF-harjoitukset ovat monesti kilpailumuotoisia, joissa kilpailee useampi joukkue keskenään.	Järjestelmien tutkiminen ja niihin tutustuminen, teknisen- ja ongelmanratkaisukyvyn kehittäminen.
Yhteisharjoitus (eng. Live exercice)	Yhteisharjoitus on suurempi harjoitus, johon yleensä osallistuu monia organisaatioita, jossa mallinnetaan todellisia tapahtumia luoden realistisen tarinan. Harjoituksessa voi olla teknisen, toiminnallisen ja työpöytäharjoituksen piirteitä. Yhteisharjoituksen tavoitteena yleensä on luoda yhteinen tilannekuva ja saada yhteistyö eri yhteistyökumppaneiden kanssa toiminaan. Harjoitus koostuu yleensä useammasta tiimistä, esim. valkoisesta-, sinisestä- ja punaisesta tiimistä. Keskeistä harjoituksen toiminnassa on harjoittelijoiden tarkat roolit ja vastuut kybertoimintaympäristössä.	Tilannekuvien muodostaminen, yhteistyötoiminnan kehittäminen, arvoketjujen tarkasteleminen ja verkostojen luonti.

4.4 Tiimit harjoituksessa

Kyberharjoituksissa, varsinkin teknisessä harjoituksissa, osallistujat jaetaan värikoodattuihin tiimeihin. Yleensä tiimien värikoodit ovat sininen, punainen, valkoinen sekä vihreä. Muita värikoodeja voi myös esiintyä, jos harjoituksessa sille koetaan tarve. Kaikilla tiimeillä on oma päätehtävänsä, josta myös värikoodi kielii. (Kyberturvallisuuskeskus 2019, 24.)

Sininen tiimi (eng. Blue Team, BT) harjoituksessa koostuu yleensä kohdeyleisön osallistujista, eli koulutettavista henkilöistä. Tiimin tarkoituksena on vastata harjoituksessa tietojärjestelmien puolustamisesta ja turvallisuuden ylläpidosta, joten tiimin sisäiset roolit ovat yleensä myös sen mukaiset. Harjoituksessa voi olla mukana useita sinisiä tiimejä, jotka voivat joko toimia yhteistyössä keskenään, tai jopa kilpailla toisiaan vastaan. (Kick 2014, 2; Kyberturvallisuuskeskus 2019, 25.)

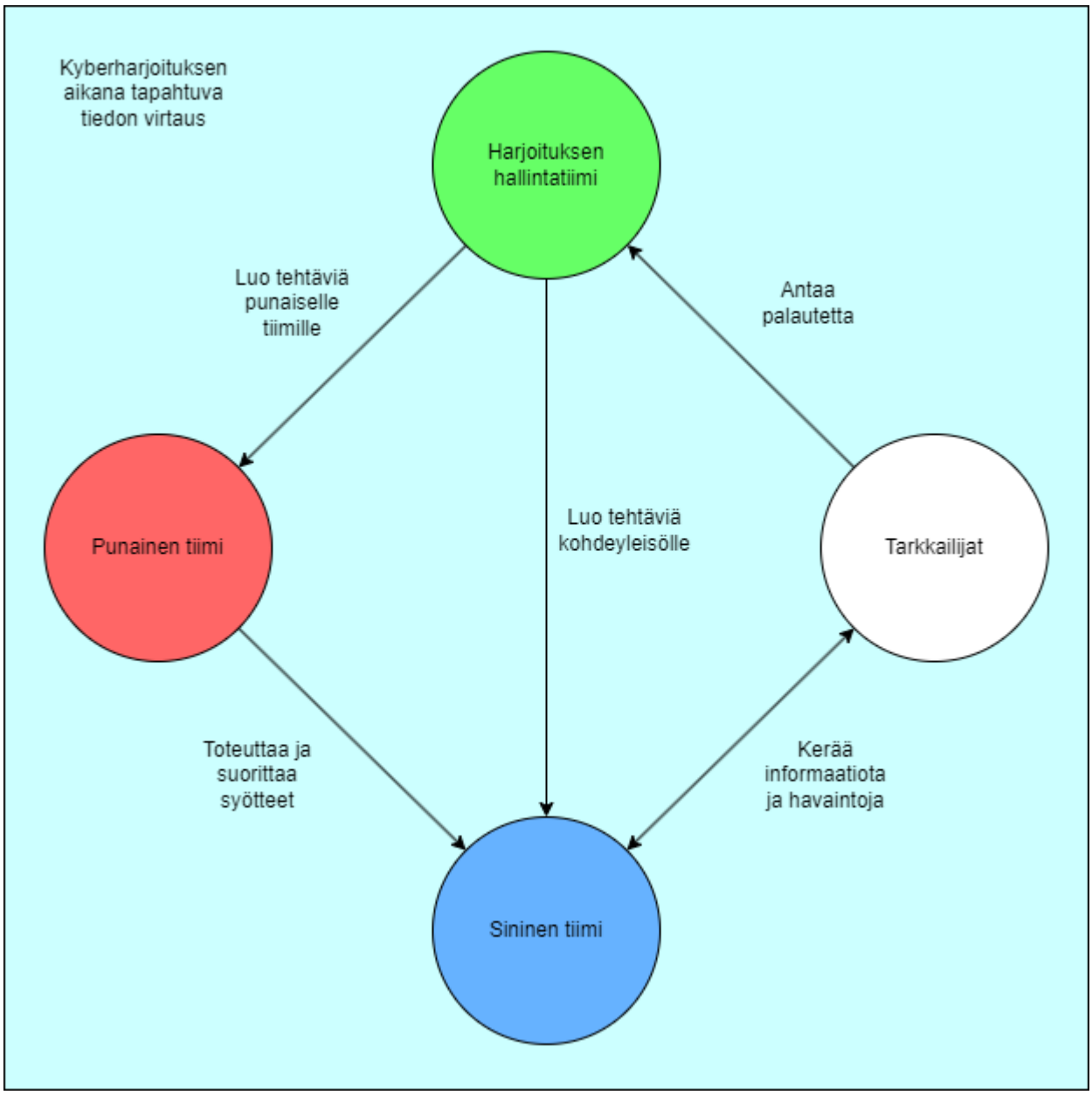
Punainen tiimi (eng. Red Team, RT) koostuu yleensä henkilöistä, jotka ovat valtuutettuja ja määrätty mallintamaan hyökkäyksiä sekä luomaan häiriöitä harjoituksen kybertoimintaympäristössä sen turvallisuutta vastaan. Punainen tiimi toimii siis käytännössä sinisen tiimin vastustajana ja syötteiden toteuttajana. Punainen tiimi luo haasteita siniselle tiimille, joka joutuu selvittämään häiriöt ja mukautumaan puolustukseen tapahtumien edetessä. Punaisen tiimin tavoitteena voidaan pitää tietoturvan parantamista, sillä tiimin toiminta voi osoittaa niin epäonnistuneiden kuin onnistuneiden hyökkäysten vaikutuksia. Kyseisen tiimin yleensä muodostaa harjoituksen järjestäjät ja muut asiantuntijat. (Kick 2014, 3; Kyberturvallisuuskeskus 2019, 25.)

Valkoisen tiimin (eng. White Team, WT) tehtävänä on vastata kyberharjoituksen valvonnasta ja havainnoimisesta. Tiimi tarkastelee sinisen ja punaisen tiimin toimintaa ja tuomaroi. Valkoinen tiimi myös varmistaa, että harjoitus on oikeudenmukainen ja ratkoo ongelmat, joita harjoituksen aikana saattaa ilmetä. Valkoinen tiimi voi toimia myös pisteyttäjänä, jos harjoituksessa kilpaillaan. Kyseisen tiimin yleensä muodostavat harjoituksen järjestäjät ja muut yhteistyössä toimivat henkilöt. Valkoinen tiimi tarkkailee siis niin kohdeyleisöä kuin harjoituksen kulkua ja antaa palautetta tiimeille. (Kick 2014, 3; Kyberturvallisuuskeskus 2019, 25.)

Vihreän tiimin (eng. Green Team tai Exercise Control Group, ECG) tarkoituksena on vastata harjoituksen toteutusvaiheen hallinnasta. Tiimi ohjaa ja avustaa harjoituksen kulussa ja skenaariossa.

Vihreän tiimin tavoitteena on antaa harjoituksen aikaista teknistä tukea ja vastata syötteistä. (Kick 2014, 2; Kyberturvallisuuskeskus 2019, 25.)

Tiimien välillä tapahtuu paljon informaation vaihdosta. Tiimien keskeinen informaation kulku harjoituksen aikana voidaan havainnollistaa kuviona (ks. Kuvio 2). Nykypäivän terminologia on kääntynyt kuitenkin enemmän siihen, että vihreä tiimi toimii vain teknisenä ylläpitona ja valkoinen tiimi tarkkailijoina.



Kuvio 2. Informaation virtaus harjoituksen aikana (Kick 2014, 18, muokattu)

4.5 Locked shields -kyberharjoitus

Maailmalla tunnetuksi tullut Locked Shields kyberpuolustusharjoitus on hyvä esimerkki kyberharjoittelusta kansainvälisellä tasolla. Sen järjestää joka vuosi Naton kyberpuolustuksen osaamiskeskus CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence). CCDCOE on perustettu yhdessä Viron, Saksan, Italian, Latvian, Liettuan, Slovakian sekä Espanjan toimesta vuonna 2008, ja myöhemmin samana vuonna sai myös Pohjois-Atlantin neuvoston puolesta täyden akkreditoinnin, mutta myös kansainvälisen sotilasorganisaation aseman. Keskuksen tarve oli saanut keskustelua aikaiseksi jo aikaisemminkin, mutta vasta, kun Viroon kohdistui poliittisia kyberhyökkäyksiä, heräsi muutkin sen aikaiset Nato-maat tukemaan keskuksen perustamista. (History n.d.)

Kyberkonfliktit olivat yksi tutkimuskohteista heti ensimmäisessä kyberturvallisuuskonferenssissa vuonna 2009, jonka CCDCOE järjesti (History n.d). Konferenssissa esiteltiin jopa 29 esitystä kyberturvallisuudesta, ja mukana puheissa oli myös F-Securen asiantuntija Mikko Hyppönen (Czosseck & Geers 2010). Tämän jälkeen kyberkonferenssia CyCon on järjestetty vuosittain ja sen tarkoituksena on ollut muun muassa yhteisöllisyyden rakentaminen kyberturvallisuuden ammattilaisille, ja se noudattaa korkeimpia akateemisia tutkimusstandardeja (History n.d).

Jotta kyberhyökkäyksiä ja konflikteja vastaan osattaisiin taistella tehokkaasti, alettiin vuodesta 2010 eteenpäin järjestämään Locked Shields kyberharjoituksia. Locked Shields keskittyy realistisiin skenaarioihin huipputeknologian parissa tuottaen suuria kyberhyökkäyksiä simuloiden sen kaikkia osa-alueita, jotka sisältävät strategista päätöksentekoa, viestintää ja lakituntemusta. Locked Shields on perinteinen punainen joukkue vastaan sininen joukkue tyylinen harjoitus. Tiimeihin kuuluu useampi henkilö, esimerkiksi vuonna 2021 sinisiä tiimejä oli 22 kappaletta, joihin jokaiseen kuului jopa keskimäärin 40 asiantuntijaa. Jokainen tiimi toimii fiktiivisen maan avustajina, kun vastassa on massiivinen kyberhyökkäys ja tehtävänä käsitellä se seurausten sanelemana. Harjoituksessa voi olla mukana tuhansia virtualisoituja järjestelmiä, tuhansia hyökkäyksiä ja vielä tuhansia asiantuntijoita, joten tiimien on oltava aktiivisia ja tehdä oikeanlaisia päätöksiä. Tiimit joutuvat digitaalisen rikostutkimuksen eteen ilmoittaessaan harjoituksen aikana tapahtuvista tapauksista sekä ratkaisemaan median ja oikeuden tuomien haasteita. Harjoituksessa tiimit pääsevät todella taistelemaan ja suojaamaan kriittistä infrastruktuuria kyberhyökkäysten ja häiriöiden aiheuttaman paineen alla, joka vaatii paljon yhteistyötä ja toimivaa viestintää. (Locked Shields n.d.)

Kyseinen tekninen Locked Shields harjoitus on levinnyt ja kehittynyt massiivisesti siitä, mitä se ensimmäisen kerran järjestettäessä oli, ja nykyään harjoituksen avulla voidaan simuloida nykypäivän kyberhyökkäyksen monimutkaisuutta perinpohjaisesti, keskittyen mahdollisimman realistisiin skenaarioihin ja hyökkäysmenetelmiin. Vuoden 2022 Locked Shields harjoituksen voittajaksi kruunattiin Suomi. (History n.d; Locked Shields n.d). Kaiken tämän vuoksi Locked Shields on mahdollisesti maailmanlaajuisesti mielenkiintoisin ja kehittynein kyberharjoitus.

5 Kyberharjoitus Wapice Oy:lle

5.1 Harjoituksen tarve

Toimeksiantajan organisaatiolla Wapice Oy:llä ei aikaisemmin ollut järjestetty kyberharjoituksia. Organisaatiossa haluttiin hyödyntää tilaisuutta käyttää kyberharjoitusta tilannekuvaharjoituksen keinoin, jolla voitaisiin muodostaa näkemys organisaation kyvystä hallita häiriötilanteita kybertoimintaympäristössä. Toimeksiantajan organisaatiossa kyberturvallisuus on läsnä kaikessa ja sitä kehitetään jatkuvasti, muun muassa hankkimalla tietoturvasertifiointeja. Kyberturvallisuuteen liittyvää koulutusta on myös tarjolla, mutta varsinaisiin häiriötilanteisiin on harjoiteltu ainoastaan niiden sattuessa todellisuudessa. Tämän vuoksi kyberharjoitus nähtiin sopivana uutena keinona kouluttaa työntekijöitä sekä olla apuna kyberturvallisuuden kehityksessä. Harjoituksen nimeksi valikoitui sattumanvaraisesti Hugo. Nimen tarkoitus oli ainoastaan toimia tunnisteena harjoitukselle.

5.2 Harjoituksen suunnittelu ja sisältö

5.2.1 Osallistujat ja tavoitteet

Kyberharjoituksen kohdeyleisöksi valittiin organisaation IT-osaston työntekijöitä. Kohdeyleisöstä osallistujia harjoituksessa oli kolme (3). Osallistujat valittiin sillä perusteella, että häiriötilanteissa ensivaste ja ongelmien ratkaiseminen tapahtuu ensisijaisesti heidän puolestaan. Osallistujilla on myös pääsy organisaation järjestelmiin, joista harjoitukseen liittyviä tapahtumia pystyy seuraamaan ja havainnoimaan. Kohdeyleisön osallistujat muodostivat sinisen tiimin (BT). Tiimin oli tarkoitus toimia harjoituksessa tietoturvaloukkausten vastausryhmänä CSIRT (eng. Computer Security Incident Response Team). Harjoituksen järjestäjiä oli kaksi, tutkija ja organisaation työntekijä, jotka toimivat yhdessä harjoituksen läpiviejinä sekä havainnoijina. Järjestäjät käytännössä muodostivat yhdessä punaisen tiimin (RT) ja valkoisen tiimin (WT).

Kyberharjoituksen tavoitteiksi muodostui seuraavat asiat:

1. Tilannekommunikaation toimiminen ja tilannekuvan muodostaminen erityisesti etätyöskentelytilanteessa.
2. Totuttautuminen kirjaamaan helposti ymmärrettävää tilannepäiväkirjaa häiriötilanteiden jälkianalyysia ja aikajanan muodostamista varten.
3. Toimiva ongelmanratkaisuun liittyvä viestintä (pois lukien asiakasviestintä).

Tilannekommunikaatio todettiin olevan tärkeässä roolissa tilannekuvan muodostamisen yhteydessä. Nykypäivän etätyöskentelyn todettiin mahdollisesti myös tuottavan edellä mainittuihin tavoitteisiin hankaluuksia, joten tavoitteessa keskityttiin nimenomaan etätyöskentelytilanteeseen. Todettiin, jos tilannekommunikaatio ei toimi, eikä havaintoja häiriötilanteen ilmennettyä saada kommunikoitua, voi muun muassa ensivasteen tuottaminen olla hankalaa. Tavoitetta mitattiin havainnoimalla osallistujien tehokkuutta kommunikoinnissa syötteiden, eli häiriötilanteiden ilmetessä ja sitä myötä kokonaistilannekuvan muodostamisessa.

Häiriötilanteista halutaan saada selkeä kuva myös jälkikäteen, joten täytyy ne saada kirjattua ylös. Tähän ongelmaan sopi tilannepäiväkirjan kirjoittaminen (ks. Liite 1). Tilannepäiväkirjaa tuli kirjata harjoituksen aikana sitä mukaa, kun vastasi syötteisiin. Jokaisesta syötteestä haluttiin saada erillinen tilannepäiväkirja jokaiselta osallistujalta. Tilannepäiväkirjan avulla haluttiin saada selkeämpi kuva tapahtumista, niihin tehdyistä vasteista ja aikajanasta. Tavoitetta mitattiin sillä, saiko tilannepäiväkirjoista selväksi syötteen, johon vastattiin, vasteen ja yhteisen aikajanan.

Lopuksi haluttiin tarkastella ongelmanratkaisuun liittyvää viestintää. Tavoitteena oli, että osallistujat viestisivät toisilleen selvittäen ratkaisua ongelmiin. Samalla haluttiin nähdä, miten työnjako hoituu, kun ongelmat alkavat kasaantumaan niiden lisääntyessä. Ongelmien sattuessa helposti voidaan alkaa ratkomaan samaa ongelmaa, jos viestintä ei toimi. Tavoitteessa mitattiin kykyä viestiä toisilleen ongelmista ja siitä, miten he aikovat ongelmaa ratkaista. Mitattiin myös sitä, kuinka hyvin työtä jaetaan, jolloin johtajaroolin merkitys korostuu. Ongelmanratkaisutapoja eikä asiakasviestintää arvioitu eikä mitattu, vaan tavoite keskittyi pääsääntöisesti viestintään sisäisesti.

5.2.2 Viestintä- ja materiaalikanavat

Harjoituksessa käytettiin useampaa kanavaa niin tiimien väliseen, kuin tiimien sisäiseen viestintään. Viestintäkanavina toimi Mattermost ja Microsoft Teams, sekä tarvittaessa tikettijärjestelmä. Mattermost on avoimen lähdekoodin alusta, joka keskittyy tarjoamaan turvallisempaa ja luotettavampaa yhteistyötä niin teknisille kuin operatiivisille tekijöille (Mattermost overview n.d). Microsoft Teams on viestintäsovellus organisaation käyttöön, joka mahdollistaa reaaliaikaisen kommunikoinnin, kokoukset ja tiedostojen jakamisen (What is Microsoft Teams n.d). WT jäsenillä oli pääsy kaikille kanaville, jotta pystyttiin havainnoimaan harjoituksen kulkua.

Mattermost kanavat harjoituksessa olivat seuraavat:

1. Proj: HUGO: Syötteet
2. Proj: HUGO: Kysymykset
3. Proj: HUGO: Viranomaiset/Muut
4. Proj: HUGO: BT keskustelu

Kanava Proj: HUGO: Syötteet oli ainoastaan syötteitä varten. Kaikki harjoituksen syötteet annettiin kanavan kautta. Kanava Proj: HUGO: Kysymykset oli ainoastaan WT ja BT välistä keskustelua varten, jossa BT pystyi kysymään tarvittaessa mitä tahansa, esimerkiksi harjoituksen kulusta. Kanava Proj: HUGO: Viranomaiset/Muut toimi kanavana, jossa tarkoitus oli mallintaa keskustelua viranomaisten tai muiden tahojen kanssa, jos häiriötilanne sitä vaati. Mallintajina toimi WT:n jäsenet. Kanavan Proj: HUGO: BT keskustelu tarkoituksena oli toimia kohdeyleisön tiimin, eli BT:n sisäisenä keskustelukanavana.

Teams kanavien kautta jaettiin pääasiassa osallistujille tarvittava materiaali harjoitusta varten. Jaettuihin materiaaleihin kuului perehdytysesitys, tilannepäiväkirjapohja ja palautekysely. Tarkoituksena oli, että harjoituksen aikana ja sen jälkeen osallistujat pääsisivät tarvittaessa tarkastelemaan perehdytysmateriaalia. Osallistujat myös pääsivät tallentamaan tilannepäiväkirjapohjat valmiiksi itselleen, ja täytettyään lataisivat täytetyt tilannepäiväkirjat niille varattuun kansioon Teams:iin. Myös palautekysely jaettiin tätä kautta ja täytetyt palautekyselyt palautettiin niille varattuun kansioon.

Todettiin, että tarpeen vaatiessa voidaan myös luoda tikettejä järjestelmään. Ensisijaisesti kuitenkin kaikki kommunikaatio hoituisi edellä mainittuja kanavia pitkin. Jos kuitenkin tikettejä haluttiin luoda, ne tuli merkata selkeästi tunnisteella ”HUGO HARJOITUS”, jotta ne voidaan erotella oikeista, harjoituksen ulkopuolelta tulevista tiketeistä.

5.2.3 Harjoitusskenaario

Kyberharjoitusta varten luotiin skenaario, joka mallinsi ja vastasi mahdollista tosielämän tilannetta. Skenaariosta ja sen syötteistä luotiin sellainen, että siitä pystyttäisiin luomaan tilannekuvaa pala kerrallaan ja lopuksi kokonaistilannekuva. Skenaarioon pyrittiin sisällyttämään useampi syöte ja syöttää ne tietyin aikavälein, jotta harjoittelijat ehtisivät vastaamaan syötteisiin.

Skenaario alkoi prosessihäiriösyötteellä, jonka tarkoituksena oli luoda häiriötilanne, jossa organisaation viestintäpalveluissa sekä muissa yleisesti käytettävissä palveluissa on katkoksia. Syötteen ideana oli tuoda lisähaastetta ja toimia tietynlaisena mittarina harjoituksen tavoitteiden arvioinnissa. Melko nopeasti prosessihäiriön ilmetessä skenaarioon tuli mukaan porttiskannauksia. Porttiskannausten tieto mallinnettiin ja toimitettiin, kuten automatiikka sen tuottaisi, ensin sähköpostina ja sen jälkeen tikettinä. Porttiskannausten oli tarkoitus toimia mahdollisen vakavamman häiriön alkutapahtumana.

Harjoittelijoiden selvittäessä porttiskannauksia, skenaarioon tuli mukaan käyttäjätiketti, jonka tarkoituksena on hämätä harjoittelijoita, sillä tiketin tapahtumat eivät liittyneet ilmentyneisiin häiriöihin. Hämäystiketin avulla voitiin siis havainnoida sitä, että yhdistävätkö harjoittelijat tapahtuman heti olemassa olevaan tilannekuvaan vai ymmärtävätkö selvittää asiaa ensin. Jonkin ajan kuluttua skenaariossa tuli esiin tietomurtoepäily. Palvelinylläpito ilmoitti epäilystä harjoittelijoille ja syötteessä mainitaan porttiskannaukset. Syöte ei kuitenkaan paljastanut kuka ja mistä skannauksia on tehty.

Skenaarion loppuvaiheessa palvelinylläpito informoi harjoittelijoiden CSIRT tiimiä uudelleen, että tietomurtotutkintaa on tehty ja on selvinnyt, että tietynlaista kiristyshaittaohjelmaa on levitetty organisaation verkossa. Informaatio sisälsi myös tunnisteita, kuten verkkolevyn ja tiedoston nimen, jotta harjoittelijoiden oli helpompi toteuttaa vaste syötteelle. Syötteen yhteydessä ei heti tuotu esiin, onko haittaohjelma aktiivinen. Lopulta kuitenkin saapui käyttäjätiketti, jossa käyttäjä

kertoo tietokoneensa käyttäytyvän oudosti, kun jotkut tiedostot ovat lukittuina. Syötteen tarkoitus oli luoda tapahtuma, jossa harjoittelijoiden tuli ymmärtää, että haittaohjelma on aktivoitunut ainakin yhdessä tietokoneessa. Kun harjoittelijat olivat saaneet aikaa kokonaistilannekuvan muodostamiseen, viimeinen syöte palveluiden palautumisesta lopetti varsinaisen skenaarion, jolloin harjoittelijat pystyivät viimeistelemään kesken olevia tehtäviä.

5.3 Harjoituksen toteutus

Harjoitus aloitettiin lyhyellä perehdytyksellä. Perehdytyksessä käytiin läpi viestintäkanavat ja varmistettiin, että osallistujilla oli pääsy kanaville. Käytiin läpi myös materiaali, ja korostettiin tilannepäiväkirjan ja palautekyselyn tärkeyttä ja sitä, että jos jonkun syötteen selvittämiseen ei riitä aika, se tulisi kirjata tilannepäiväkirjaan. Harjoitukselle asetettiin kesto: 9:45-12:00, mutta todettiin, että harjoituksen todellinen kesto voi muuttua.

Perehdytyksessä korostettiin lopuksi sitä, ettei harjoituksen aikana hoidettaisi normaaleja työtehtäviä, vaan keskitytään ainoastaan harjoituksen suorittamiseen. Osallistujia kehotettiin olemaan taistelematta skenaariota vastaan tai kyseenalaistamaan syötteiden oikeellisuutta, vaan kohtaamaan syötteet olettaen, että syöte olisi tosi.

5.3.1 Harjoituksen kulku ja toiminta

Kappaleessa käydään yksinkertaistettuna harjoituksen aikana tapahtuneet syötteet ja toiminta. Syötteet ovat aikajärjestyksessä sisältäen aikaleiman, kun ne on viestintäkanavalle osallistujien nähtäväksi syötetty. Syötteiden yhteydessä käydään läpi järjestäjien oletukset siitä, miten syötteisiin reagoitaisiin. Samassa yhteydessä käydään läpi myös huomiot, joita osallistujatiimin BT keskuudessa tuli, kuten myös huomiot järjestäjien tiimin WT keskuudessa BT:n toiminnasta. Syötteiden yhteydessä lopuksi käydään läpi lyhyesti myös BT toiminta, eli vaste kyseiseen syötteeseen. Harjoitukseen sisältyvien IP-osoitteiden (eng. Internet Protocol Address) ja tiettyjen palvelinten nimet on poistettu ja korvattu täytetekstillä ”xxx”.

Syöte 1: Aloitus.
Syöte: [10:00]: Harjoitus alkaa.

Syöte 2: Prosessihäiriö Microsoft 365 palveluissa.

Syöte: [10:01]: Wapicen SharePoint, Teams, AzureMFA ja Exchange palveluissa on käyttökatko maailmanlaajuisen häiriön seurauksena. Kyseiset palvelut eivät ole EU-alueella käytettävissä 9–16 UTC välisenä aikana, kun korjauksia ajetaan EMEA-alueella toimiviin konesaleihin. Azure AD toimii, mutta siinäkin saattaa olla hidastumisia ja hetkittäisiä katkoksia.

Oletus: Tiedote saapuu, että Wapicen palveluita on alhaalla, joten joudutaan käyttämään vaihtoehtoisia tapoja häiriön selvittämiseen ja viestittämiseen organisaation sisällä.

Huomiot: Asiaa tulisi tutkia tarkemmin. Mahdollisista ilmenevistä ongelmista tulisi tiedottaa käyttäjille. Ilmoitettu katko on poikkeuksellisen pitkä. Sähköpostipalvelussa on häiriötä, eikä sen avulla tavoita välttämättä kaikkia. Tiedotustapaa pitää siis vaihtaa, ja perinteinen tekstiviesti (SMS) on mahdollinen tapa viestiä asiasta.

Toiminta: Käyttäjien puhelinnumerot haetaan AD:sta, siirretään tiedostoon ja lähetetään skriptin avulla kaikkiin puhelinnumeroihin tiedote häiriöstä xxx-palvelimelta.

Syöte 3: Porttiskannaus tuntemattomasta osoitteesta.

Syöte: [10:04]: ABUSE-sähköpostiviesti: xxx.xxx.xxx.xxx osoitteesta porttiskannaukselle ominaista liikennettä. Liikenne tunnusomaista netcat-ohjelmistolle. ABUSE-sähköpostiviesti: xxx.xxx.xxx.xxx osoitteesta porttiskannauksen omaista liikennettä. Liikenne tunnusomaista Windows Powershell scriptille IPV4PortScan.ps1.

Oletus: Harjoittelijat löytävät eri tapoja selvittää sähköpostissa mainitun häiriön, esim. logitiedostoista.

Huomiot: Sähköpostit ja niissä mainitut skannaukset analysoitiin. Edellisen syötteen työ vielä kesken, joten tarkempaa tutkimusta ei voitu vielä tehdä ja aiheutti sen, ettei pystytty ajattelemaan montaa asiaa samaan aikaan. Ei nähty kuka oli tehnyt skannaukset, koska vain ulostuleva IP-osoite oli näkyvissä. Palvelimelta xxx oli ”huudeltu” uwasa-osoitteeseen klo 9.32 ja AD oli aiheuttanut toisen abuse-sähköpostiviestin klo 9.31 alkaen.

Toiminta: Palomuurilogien tarkastus.

Syöte 4: Porttiskannausta Wapice:n sisäverkosta.

Syöte: [10:10]: Seuraavat tiketit IoT-xxx segmentistä. Tiketti: Kohteeseen sataa porttiskannauksia. Ping skannauksia tulee Wapicen sisäverkosta segmenttiin xxx.xxx.xxx.xxx. Tiketti: Porttiskannauksia Wapicen sisäverkosta osoitteeseen xxx.xxx.xxx.xxx.

Oletus: Kaapattu Rojala-käyttäjätunnus löytyy. Palvelinlogien ja tunnuksen historiatietojen kautta syötteen selvittäminen.
Huomiot: Palvelimella xxx on havaittu ongelma, koska sisäverkon osoite on lähtöosoitteena. Vastaava ongelma havaittu palvelimesta xxx. Yhteenvetona porttiskannauksia palvelimista xxx ja xxx. Vastaavia skannauksia ei pitäisi normaalisti olla. Logeista havaittu myös tuntematon Rojala-käyttäjätunnus. Palvelimelta xxx on tullut skannausta ja se on kohdistunut verkkoon xxx.
Toiminta: Palvelinten xxx ja xxx logien tarkastelu, joista havaittiin tuntematon Rojala-käyttäjätunnus.

Syöte 5: Käyttäjätiketti 1 – Hämäystiketti.
Syöte: [10:15]: Tiketti. Käyttäjä ilmoittaa, että työasema käynnistelee uudelleen jatkuvasti itsekseen. Käyttäjä on ollut viikon lomalla, eikä koneen käynnistettyä tietokoneen pääse hän edes kirjautumisnäkymään.
Oletus: Hämäystiketti. Huomataan, että kyseessä on satunnainen laitevika eikä liity aikaisempiin skannauksiin. Siirretään sivuun odottamaan tai ratkaistaan nopeasti, jos tilanteessa mahdollista.
Huomiot: Todettiin, ettei tiketin lähettäjän ongelma ole tässä tilanteessa kriittisin asia. Huomattiin samalla, ettei asia mahdollisesti liity edellisiin tapahtumiin. Tästä ei voitu kuitenkaan sulkea mahdollisuutta pois. Havaittiin, että jos työaseman käyttäjä on toimistolla, voi liittyä tapaukseen, mutta jos käyttäjä on etänä, voi asian jättää toistaiseksi ratkaisemattomaksi. Päätettiin kuitenkin ratkaista asia tai ainakin ohjeistaa käyttäjää.
Toiminta: Tiketin luoneelle käyttäjälle soittaminen ja tarkempi selvitys siitä, miten ongelma ilmenee ja onko käyttäjä toimistolla vai etätöissä. Ohjeistettiin ottamaan kone pois virrasta ja viemään se IT:lle mahdollisimman pian toistaiseksi karanteeniin.

Syöte 6: Tietomurtoepäily.
Syöte: [10:26]: Palvelinylläpito raportoi CSIRT:ille. Palvelimelta xxx herännyt epäily tietomurrosta tai tunnuksen oikeudettomasta käytöstä. Tarkempia tietoja ei käyttäjätunnuksesta ole, mutta tietojen mukaan koneelta on skannattu verkkoa.
Oletus: Ilmoitus on edellisten tapahtumien jatkoa. Osataan yhdistää tapahtumiin ja havaittuun Rojala-käyttäjään. Logien ja tunnuksen historiatietojen kautta asian selvittäminen jatkuu.
Huomiot: Havaittu Rojala-tunnus voitaisiin väliaikaisesti sulkea. Tarkkaa tietoa tai viitettä ei vielä

ole havaittu, onko kyseinen skannaus aiheutettu tällä tunnuksella.

Toiminta: Havaitun, mahdollisen murretun, tunnuksen väliaikainen sulkeminen.

Syöte 7: Kryptolocker-tiedosto (EICAR).

Syöte: [10:39]: Palvelinylläpito raportoi CSIRT:ille. Tietomurtotutkinnan seurauksena selvinnyt, että AD-palvelimen kautta on levitetty kryptolocker-ohjelmistoa Windows-verkkolevylle \\ad\xxx\HUGO-HARJOITUS. Epäilyttävän tiedoston tunnisteet: sha-1: xxx ja nimi: HUGO-HARJOITUSTIEDOSTO-CSIRT.txt.

Oletus: Jos tiedostot löytyvät, on olemassa historiatietoja palvelimilla, joilla voidaan saada kiinni tieto, että on ollut kiinnitettynä AD-palvelimelle.

Huomiot: AD:lla havaittiin haittaohjelma. Tiedostojen alkuperä on saman Rojala-tunnuksen tiedostoissa. Virustorjunnan logeista voidaan nähdä, että se on asettanut tiedostot karanteeniin eli ensivaste on hoitunut automaattisesti. Todettiin, että tiedostopolku (\\ad\xxx\HUGO-HARJOITUS) tulisi eristää, etteivät muut käyttäjät pääse haitalliseen tiedostoon käsiksi. Havaittiin, että pitäisi tutkia onko tiedostoa jo ladattu tai avattu. Todettiin kuitenkin, ettei tiedostoa ole avattu polusta. Tiedoston tarkisteen (hash) voisi lisätä virustorjuntaan ja skannata työasemat. Ei kuitenkaan ole varmaa tietoa, voiko skannausta pakottaa etänä työasemille.

Toiminta: Tiedoston tunnetun tarkisteen lisääminen virustorjunnan tarkistemalleihin, jotta virustorjunta havaitsee tiedoston työasemilta. Työasemille tullaan tekemään täysi skannaus, jos se on mahdollista toteuttaa etänä.

Syöte 8: Käyttäjätiketti 2 – Kryptolocker on aktiivinen.

Syöte: [10:45]: Tiketti. Käyttäjän tietokone käyttäytyy oudosti. Jotkut tiedostot aukeavat, mutta toiset ei, eikä koneen uudelleenkäynnistys auta ongelmaan. Sähköpostin lukeminen ja internetin selailu toimii kuitenkin normaalisti.

Oletus: Saadaan ymmärrys, että kryptolocker-tiedosto on kuitenkin avattu ja aktivoitunut ja tiedostoa on käsitelty tiketin lähettäneen käyttäjän koneelta. Ongelmasta on mahdollista löytää historiajälkiä.

Huomiot: Pitäisi laittaa kaikille käyttäjille viestiä, ettei kytke työasemia Wapicen verkkoon. Tämä on jo toinen tapaus oudosti käyttäytyvästä työasemasta, joten selvästi on ongelmia järjestelmässä. Todettiin, että olisi pitänyt tiedottaa jo aikaisemmin asiasta. Tiedotteessa tulisi mainita, että Wapice:lla on epäilty kyberhyökkäys ja työasemat pitää ottaa pois Wapice:n verkosta. Myöskään VPN

ei saa käyttää. Työnjakoa pitää alkaa tekemään enemmän. Huomattiin, että tiedotteessa pitäisi lisäksi mainita, että ilmoitetaan erikseen, kun työaseman voi kytkeä takaisin verkkoon. Ennen ilmoitusta sitä ei kuitenkaan saa tehdä. Todettiin, että olisi myös hyvä mainita, jos työasema käyttäytyy oudosti, tulee se sammuttaa, eikä sitä saa käyttää. Tärkeänä huomiona tuli esiin, että tietosuojavastaavalta pitää varmistaa, mitä viranomaisvelvotteita on vastaavassa tilanteessa. Saatiin selvyys, että 72:den tunnin kuluessa tulee tehdä ilmoitus valvontaviranomaiselle, joten sen suhteen ei tarvitse pitää vielä kiirettä.

Toiminta: Tietosuojavastaavalta velvoitteiden varmistaminen. Tiketin lähettäneelle käyttäjälle soittaminen ja tarkempi selvitys siitä, miten ongelma ilmenee. Pyydetään sen jälkeen ottamaan työasema pois virrasta ja viemään se IT:lle toistaiseksi karanteeniin. Lähetetään tiedote kaikille työntekijöille, että Wapicella on epäilty kyberhyökkäys, eivätkä työntekijät saa yhdistää VPN-palvelimiin.

Syöte 9: Microsoft 365 palveluiden palautuminen.

Syöte: [10:51]: Wapicen Microsoft 365 palvelut ovat palautuneet.

Oletus: Palveluita voidaan taas käyttää häiriötilanteiden selvittämiseen ja viestimiseen.

Huomiot: Palveluiden palautumisesta tulisi tiedottaa työntekijöille viestillä ja korostaa vielä sitä, ettei kuitenkaan verkkoon ole vieläkään turvallista kytkeä työasemia.

Toiminta: Käyttäjien tiedotus viestillä, että Microsoft palvelut ovat palautuneet ja niiden käyttö vaatii työaseman uudelleenkäynnistyksen. Korostetaan kuitenkin, ettei työasemaa saa vielä kytkeä Wapice:n verkkoon, ennen kuin IT antaa siihen luvan.

Syöte 10: Lopetus

Syöte: [10:55]: Harjoituksen lopetus.

5.3.2 Kysymykset harjoituksen aikana

Kyberharjoituksen aktiivisen osan aikana Proj: HUGO: Kysymykset -kanavalla esitettiin harjoitukseen liittyviä kysymyksiä niin BT:n kuin WT:n puolesta. Kysymykset on esitetty alla siinä muodossa, kun ne ovat viestintäkanavalla esiintyneet.

- Kysymys (BT): Mikä on IoC?
    - Vastaus (WT): Indicator of compromise.
- Kysymys (BT): Voiko kanavan kautta tikettiin liittyen "soittaa" vai soitetaanko oikeasti?

    - Vastaus (WT): Kirjataan toimenpiteisiin, jos oikeasti olisi soitettu.
- Kysymys (BT): Onko tiketin lähettäjä toimistolla vai etänä?
    - Vastaus (WT): Käyttäjä on etänä.
- Kysymys (BT): Pidetäänkö lounastauko ja pidennetään sotaa loppupäästä?
    - Vastaus (WT): Syödään harjoituksen jälkeen, jos pystyy venymään.
- Kysymys (BT): Millasia velvotteita on viranomaisten suuntaan, kun selvästi epäillään, että Wapicelle on murtauduttu ja tilannekuva on vielä epäselvä?
    - Vastakysymys (WT): Onko epäilys, että henkilötietoja on vuotanut?
    - Vastaus (BT): Vähintäänkin nimiä, puhelinnumeroita ym.
        - Vastaus (WT): Tietosuojaviranomaiselle ilmoitus 72h kuluessa. Lisäksi täytyy arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu kohteelle, esim. ei aiheudu riskiä, aiheutuu riski, aiheutuu korkea riski.

5.4 Harjoituksen jälkeen

5.4.1 Palautetilaisuus

Heti harjoituksen päätyttyä käytiin läpi osallistujien kesken harjoituksen palautetilaisuus (eng. Hot Wash). Välittömän palautetilaisuuden tarkoitus on purkaa harjoituksen kulku, jossa katsotaan takaisinpäin tapahtumiin harjoituksen aikana, sekä heijastaa tapahtumia toimintaan ja oppia, miten suoritusta voidaan parantaa. Sen tarkoituksena ei ole kritisoida harjoituksen onnistumista, vaan esittää havainnot ja tunnistaa heikkoudet, parannusta vaativat asiat sekä vahvuudet. (Metz n.d.)

Palautetilaisuudessa käytiin ensimmäisenä läpi havaintoja. WT:n puolesta oli havaittu, ettei mahdollisesti skenaarion murretun käyttäjätunnuksen historiatietoja oltu katsottu tarkkaan palvelimilta. BT kuitenkin totesi huomanneensa, ettei käyttäjätunnuksella ollut liikaa oikeuksia, eikä se kuulunut ryhmiin, joilla olisi korkeampia oikeuksia. BT havaitsi siis, ettei murretun käyttäjätunnuksen avulla pystytty tekemään suoraan laajempaa haittaa verkossa.

Tilannepäiväkirja oli aiheuttanut haasteita harjoituksen aikana. BT totesi, ettei tilannepäiväkirjaa ehtinyt kunnolla kirjoittaa, koska syötteisiin vastaaminen ja tilanteen hahmottaminen vei aikaa. Huomio kuitenkin keskittyi siihen, että kyse oli ennemmin osallistujan omasta toimintatavasta ja -mallista kuin siitä, että aikataulu syötteiden välissä olisi ollut liian tiukka. Keskustelussa kuitenkin todettiin yhteisesti, että aikataulu oli melko tiukka. Pidempi vasteaika syötteiden välissä olisi ollut tarpeen, jotta tilannepäiväkirjoja olisi ehtinyt tarkemmin täyttämään. Oikean tilanteen sattuessa vastaavaa tilannepäiväkirjaa pitäisi pystyä täyttämään nopeasti ja kirjata toimet tarkasti, jotta

myöhemminkin voitaisiin helposti rakentaa tarkka tilannekuva. Tilannepäiväkirjojen sisältö todettiin myös melko vähäiseksi ja monesta jäi puuttumaan selkeä viite löydettyihin asioihin, jotta ne voitaisiin löytää jälkikäteen uudestaan.

Palautetilaisuudessa oltiin yhtä mieltä siitä, että työnjako ja viestintä oli vajavaista. Työnjakoa olisi pitänyt tehdä jo alusta lähtien ja jakaa keskenään selkeät roolit. Työnjako kuitenkin parani loppua kohden. Viestinnän todettiin olleen alussa tehokasta, mutta loppua kohden väheni. Harjoittelijoiden keskeinen viestintä olisi voinut olla selkeämpää ja tapahtumien kohdalla tiedotukseen olisi voinut reagoida nopeammin. Lopulta kuitenkin harjoittelun aikana muiden työntekijöiden tiedottaminen oli tehokasta.

Muutamia huomioita heräsi jälkeenpäin. Organisaation järjestelmistä pois kytketyt käyttäjätunnukset jäävät ns. kummittelemaan, eikä niitä yleensä poisteta heti. Pohdittiin, voisiko se olla tietoturvariski, mutta kunnon syytä ei siihen löytynyt. Harjoittelijat totesivat loppujen lopuksi kyberharjoituksen olleen heille ja heidän osastolleen hyvä harjoitus.

5.4.2 Palautekysely

Kyberharjoituksen osallistujilta kerättiin palaute palautekyselylomakkeen tavoin (ks. Liite 2). Palautekyselyyn vastasi jokainen harjoittelija, joita oli kolme. Palautekyselyn vastaustulokset ja jakauma voidaan esittää taulukkomuodossa (ks. Taulukko 2). Palautteesta tehtiin myöhemmin palauteanalyysi.

Taulukko 2. Palautekyselyn vastausjakauma

Kysymys	Vastaustulokset (kpl)				
	Täysin erimieltä	Osittain eri mieltä	En osaa sanoa	Osittain samaa mieltä	Täysin samaa mieltä
Harjoituksesta oli hyötyä minulle					3
Harjoituksesta oli hyötyä Wapicelle			1		2
Tehtäväni harjoituksen aikana olivat selkeät		1		2	
Harjoituksen syötteet olivat selkeät				2	1
Harjoituksen syötteet olivat riittävän haastavia			1	1	1
Harjoituksen syötteet vastasivat osaamistani		2		1	
Sain tarvittaessa apua ongelmatilanteissa					3
Osallistun mielelläni tuleviin harjoituksiin					3

Palautekysely mahdollisti myös vapaamuotoisen palautteen antamisen. Vapaamuotoiset palautteet sisälsivät ajatusta siitä, että harjoitus oli hyvä, mielenkiintoinen ja opettavainen. Harjoituksen todettiin olevan myös ajatuksia herättävä ja koettiin, että vastaavista harjoitteluista on todellista hyötyä, koska pystytään kehittämään toimintamalleja ja miettimään, miten todellisessa tilanteessa tulisi toimia. Käytännön harjoituksen koettiin olevan myös parempi tapa oppia, kuin sen, että asiat käytäisiin teoriassa läpi vain esimerkiksi palaverissa.

5.4.3 Palauteanalyysi

Palautteita analysoidessa todettiin, että kyberharjoitus koettiin erittäin hyödylliseksi harjoittelijoille itselleen. Harjoituksen koettiin todennäköisimmin olleen myös hyödyllinen organisaatiolle. Vastauksissa tähän kysymykseen oli jakaumaa, joka todettiin mahdollisesti johtumaan siitä, että

yksittäisen työntekijän voi olla vaikea arvioida kokonaiskuvaa harjoituksen hyödyllisyydestä muille, kuin itselleen.

Harjoittelijoiden tehtävät harjoituksen aikana koettiin jokseenkin epäselviksi. Tämä saattoi johtua siitä, ettei selkeää rooli- ja työnjakoa tehty harjoituksen aikana. Johtaja-roolin tärkeys korostui tässä tapauksessa. Koska harjoitus toteutettiin etätilanteessa, puhekanavan todettiin mahdollisesti voineen helpottaa työnjakoa. Vastuualueiden jako, esim. palomuuri, työnjaon yhteydessä olisi voinut myös selkeyttää omia tehtäviä.

Harjoituksen syötteet olivat jokseenkin selkeät harjoittelijoille. Todettiin kuitenkin, että syötteet olisivat voineet olla selkeämpiä varsinkin, koska harjoitus oli organisaation ensimmäinen. Syötteiden haastavuus oli suurimmalle osalle riittävää. Todettiin, että vastaavan harjoituksen suunnittelussa voisi ottaa paremmin huomioon osallistujien kyvyt, mutta kaikilla on kuitenkin oma osaamistaso, jota on vaikea arvioida ilman aikaisempaa tarkastelua. Tämän vuoksi todettiin, että syöteskaalaa olisi voinut laajentaa ja ottaa harjoitukseen mukaan niin hieman haastavampia kuin helpompia syötteitä. Tämän todettiin mahdollisesti auttavan myös työnjakoon, sillä toinen henkilö voi kokea syötteeseen vastaamisen helpommaksi kuin toinen. Syötteiden ei kuitenkaan koettu vastaavan harjoittelijan omaa osaamistasoaan. Kuten aikaisemmin todettiin, kaikilla on oma osaamistaso, mutta tähänkin syöteskaalan laajentaminen voisi auttaa. Myös tulevissa harjoituksissa, joissa kohdeyleisöön kuuluu sama osasto, voidaan kenties laatia paremmin heidän osaamistaan vastaavia syötteitä.

Ongelmatilanteissa harjoittelijat kokivat kaikki saaneen apua tarvittaessa. Kysymys- ja keskustelukanavien todettiin olleen harjoituksissa tärkeässä roolissa. Kanavia käytettiin ahkerasti ja vastausaika kysymyksiin oli lyhyt harjoituksen ollessa kevyt ja WT:n ollessa vapaampi havainnoimaan harjoituksen kulkua. Kaikki osallistujat kokivat myös mielenkiinnon osallistua tulevaisuudessa järjestettäviin harjoituksiin. Voitiin siis todeta, että harjoitus oli riittävän mielenkiintoinen kaikille. Vastaavien tapahtumien todettiin olevan harvassa, eikä moni välttämättä pääse harjoittelemaan. Tähän varmasti vaikutti lisäksi se, että kyberharjoitus oli ensimmäinen niin organisaatiolle, kuin kaikille harjoittelijoille itselleenkin.

5.5 Harjoituksen tavoitteiden saavuttaminen ja onnistuneisuus

Ensimmäinen kyberharjoituksen tavoitteista oli tilannekuvan muodostaminen ja tilanteisiin mukautuminen. Tavoitteessa haluttiin keskittyä nimenomaan tilannekommunikaation toimimiseen, kykyyn mukauttaa toimintamalli häiriötilanteiden mukaan, sekä kykyyn muodostaa kokonaistilannekuva etätyöskentelytilanteessa. Tavoite todettiin onnistuneeksi, sillä jokaisen syötteen kohdalla tilannekuvan muodostaminen oli nopeaa ja onnistunutta. Kokonaiskuva saatiin lopuksi selvitettyä ja se vastasi harjoituksen skenaariota. Tilannekuvan muodostamiseen liittyvä tilannekommunikaatio oli harjoittelijoiden kesken onnistunutta.

Toinen harjoituksen tavoitteista oli raportointi. Tavoitteen ideana oli totuttautua kirjaamaan helposti ymmärrettävää tilannepäiväkirjaa häiriötilanteiden jälkianalyysia ja aikajanan muodostamista varten. Kyseinen tavoite todettiin kuitenkin vain osittain onnistuneeksi. Tilannepäiväkirjoihin kirjaaminen oli vähäistä ja siihen kaivataan harjoittelua. Täytettyjen tilannepäiväkirjojen sisältö oli epäselkeää ja niiden avulla oli vaikeaa muodostaa lopullista tilannekuvaa jälkikäteen. Lisäksi tarkan aikajanan muodostaminen tilannepäiväkirjoja tarkastelemalla oli erittäin vaikeaa. Jokaisesta syötteestä kuitenkin raportoitiin, joten tavoitetta ei voitu todeta epäonnistuneeksi.

Kolmas kyberharjoituksen tavoitteista oli viestintä. Erityisesti ongelmanratkaisuun liittyvä viestintä etätyöskentelytilanteessa. Tavoite todettiin vain osittain saavutetuksi, sillä työnjakoon, vastuualueisiin ja rooleihin liittyvä kommunikaatio oli vajavaista, joka aiheutti työtehtävien epäselkeyttä. Vaikka lopuksi työnjakoa saatiin aikaiseksi, tapahtui se hieman liian myöhään ja hitaasti. Ongelmanratkaisu oli kuitenkin nopeaa ja häiriötilanteisiin löytyi aina ratkaisut.

Kokonaisuudessaan kyberharjoitus todettiin onnistuneeksi. Harjoituksesta löytyi puutteita ja epäkohtia, mutta harjoitus saatiin suoritettua toivotulla tavalla. Harjoituksen lopputulokseen päästiin ja parannettavia asioita saatiin selvitettyä. Koettiin, että harjoittelun suunnittelu vaatii parannusta, jotta kokonaisuudesta saadaan eheämpi.

Koulutusyleisö onnistui heidän eteensä asetetuissa tehtävissä ja keskeinen häiriöihin liittyvä viestintä oli sujuvaa. Tämän ansiosta myös ongelmanratkaisu oli hyvää ja häiriötilanteet saatiin selvitettyä. Koulutusyleisön keskeinen työnjako ja vastuualueiden määritys, sekä tilanteiden raportointi

vaatii silti parannusta. Yksikään harjoituksen tavoite ei jäänyt kokonaan saavuttamatta, mutta niiden täydelliseen saavuttamiseen tarvitaan muutos ainakin seuraavassa kappaleessa mainittuihin kohteisiin.

5.6 Parannuskohteet

Kyberharjoituksen yhteydessä havaittiin epäkohtia ja parannusta vaativia kohteita. Tässä kappaleessa mainitut parannuskohteet perustuvat niin harjoituksen aikana kuin palautetilaisuudessa ja palautekyselyssä tehtyihin havaintoihin harjoittelijoiden sekä järjestäjien puolesta. Parannuskohteet on jaettu kahteen osaan: harjoituksen suunnittelu ja toteutus, ja koulutusyleisö.

Harjoituksen suunnittelussa ja toteutuksessa tulisi ottaa useita asioita huomioon paremmin. Harjoitusaikataulu tulisi olla selkeämpi ja siihen tulisi sisällyttää paremmin perehdytys, harjoituksen kesto taukoineen sekä lopuksi järjestettävä palautetilaisuus. Harjoituksen keskustelukanavat olivat toimivia, mutta puhekanavan sisällyttäminen harjoitukseen toisi harjoittelijoille mahdollisuuden helpompaan kommunikaatioon. Syöteaikaväliä voisi pidentää, jotta harjoittelijoilla olisi paremmin aikaa syötteisiin reagointiin ja sen myötä tehokkaampaan raportointiin. Lyhyemmät syötevälit voitaisiin kuitenkin jättää tapahtumiin, jotka selkeästi vaativat harjoittelijoilta selkeää työnjakoa. Syötteiden haastavuus ja skaalautuvuus voisi olla parempaa, joten mukaan voisi ottaa niin helpompia kuin vaikeampiakin syötteitä, ja syötteitä siltä väliltä. Syötteiden sisältö voisi olla ymmärrettävämpää ja tulisi kirjoittaa siihen muotoon, että ne olisivat selkeämpiä. Syötteiden sisällä olevat mahdolliset lyhenteet olisi hyvä selittää etukäteen, jos mahdollista, mutta vähintään syötteen yhteydessä. Tämäkin parantaisi syötteiden ymmärrettävyyttä. Syötteille tulisi paremmin myös syötteiden luojan puolesta esittää toivottu vaste, koska se helpottaisi arvioimaan syötteiden ja niihin vastaamisen onnistuneisuutta.

Harjoituksen koulutusyleisön IT-osaston parannuskohteita havaittiin myös useampia. Roolien jakoon häiriötilanteissa tarvitaan tehokkuutta. Vastuualueiden määritys etukäteen ja häiriötilanteen aikana samalla, kun niihin mukaudutaan, on tärkeää, koska useamman häiriön sattuessa päällekkäin, on erityisen haastavaa keskittyä moneen asiaan yhtä aikaa. Häiriötilanteista tiedottaminen ja käyttäjien ohjeistus oli hyvää, mutta vakavamman häiriötilanteen sattuessa nopeampaa ja selkeämpää tiedottamista tarvitaan. Tämä voi vaikuttaa erityisesti uusien häiriöiden muodostumisen

ehkäisyyn, kuten esimerkiksi työntekijöiden apupyyntöjen aiheuttamaan tukokseen tikettijärjestelmissä. Viranomaisvelvoitteet tulisi myös olla esillä ja helposti löydettävissä, että häiriötilanteen sattuessa ja tarvittaessa tiedetään lailliset velvoitteet, esimerkiksi tietoturvaloukkauksen ilmoitus. Raportointi koettiin vajavaiseksi ja se vaatii parannusta. Tarvittaessa tulisi pystyä kirjaamaan tilannepäiväkirjaa tai vastaavaa, jotta lopullinen tilannekuva ja aikajana voitaisiin muodostaa myös myöhemmin. Raportointi helpottaa selvitykseen liittyvien askelten replikoimista, jos häiriötilanne vaatii jälkitarkastelua ja -selvittelyä.

6 Pohdinta

6.1 Tutkimuksen onnistuminen

Opinnäytetyössä suunniteltiin ja toteutettiin kyberharjoitus toimeksiantajan organisaatiolle, jonka avulla muodostettiin näkemys organisaation kyvystä vastata kyberympäristön häiriötilanteisiin sillä hetkellä. Työssä haluttiin vastata tutkimuksessa todettuun kysymykseen, johon voitiin vastata viimeistään harjoituksen jälkeen tulosten analysoinnissa loppuraportin avuin. Työssä saatujen tulosten ja palautteen perusteella voidaan todeta, että tutkimuskysymykseen saatiin vastaus, mikä on niin tutkimuksen kuin toimeksiantajan puolesta positiivinen asia. Tutkimuksessa syntyi haluttu kyberharjoitus ja harjoituksen loppuraportti, jotka molemmat olivat tutkimuksessa todettuja ja tavoiteltuja konstruktioita. Tutkimuksen tavoitteet koettiin siis saavutetuiksi.

Vaikka tutkimus olisi onnistunut, täytyy nostaa esiin erinäisiä huomioita. Kyberharjoitus oli kevyt ja lyhyt, joten siihen ei tietenkään pystytty sisältämään kaikkia, edes yleisimpiä häiriötilanteita. Ei yhden kyberharjoituksen perusteella voitu luoda johtopäätöstä, että organisaatiolla olisi täysi kyky selvitä kaikista häiriöistä, mutta sen sijaan antaa näkemystä asiasta ja auttaa kehittämään kyberhäiriöiden hallittavuutta. Harjoitukseen osallistui vain muutama henkilö organisaation useasta sadasta työntekijästä. Harjoittelijoilla oli kuitenkin organisaatiossa todella tärkeä rooli, varsinkin häiriötilanteiden selvittämisen ja ensivasteen tuottamisen suhteen. Todellisen häiriötilanteen sattuessa, voi toimintamalli poiketa harjoituksessa esiintyneestä, mutta organisaatiolla on hyviä ohjeita ja prosesseja tilanteiden selvittämistä varten. Lopuksi voidaan todeta, ettei vain yhden harjoituksen perusteella voida todeta täysin sitä, että tutkimuskysymykseen olisi varmasti vastattu. Harjoitus oli organisaation ensimmäinen laatuaan ja niitä tulisi toteuttaa useampi, jotta tarkempi vastaus tutkimuskysymykseen voitaisiin saada.

6.2 Kyberharjoituksen onnistuminen ja tulokset

Opinnäytetyössä toteutettu kyberharjoitus voidaan todeta onnistuneeksi. Harjoituksen aikana ei ilmennyt harjoitusta haittaavia ongelmia ja se eteni suunnitelman mukaisesti. Harjoituksen kohderyhmän osallistuneet jäsenet olivat toimeliaita ja täysillä mukana harjoituksessa, mikä teki harjoituksesta mielekkään niin osallistujille kuin järjestäjille. Kyberharjoituksen skenaariosta saatiin toteutettua realistinen, ajankohtainen ja osallistujien näkökulmasta ymmärrettävä.

Onnistuneen kyberharjoituksen analysoinnin perusteella pystyttiin muodostamaan näkemys siitä, että organisaatiolla on kykyä hallita kyberympäristön häiriötilanteita ja siitä, oliko itse harjoitukseen luodut tavoitteet saavutettu. Pystyttiin päättelemään, että jotkut tavoitteet jäivät saavuttamatta, vaikkakin eivät täysin. Tulokset toivat esiin myös parannuskohteita niin häiriötilanteissa toimimisen kuin kyberharjoituksen suunnittelun ja järjestämisen puolesta. Osallistujilta kerätyn palautteen avulla pystyttiin myös tuomaan parannuskohteisiin ajatusta ja sisältöä, joka teki palautteesta erityisen arvokasta.

6.3 Toimeksiantajan etu ja jatkokehitys

Kyberharjoituksen voidaan todeta antaneen toimeksiantajalle etuja. Koska opinnäytetyössä tehdyssä tutkimuksessa toimeksiantajan organisaatio toimi yhteistyössä tutkijan kanssa ja harjoitukseen osallistui organisaatiosta työntekijöitä, sai myös toimeksiantaja arvokasta koulutushyötyä, ja sanonta kuuluukin: Harjoitus tekee mestarin. Kyberympäristön häiriötilanteiden, varsinkin kyberhyökkäysten, hallitseminen ja niiden aiheuttamasta häiriöstä selviytyminen voi olla haastavaa, ellei sellaista ole aikaisemmin kohdattu. Kyberharjoituksen avulla toimeksiantajan työntekijät saivat tällaisiin tilanteisiin harjoitusta, mikäli tulevaisuudessa organisaatio sellaisten kohteeksi joutuu.

Kyberharjoituksessa saatiin luotua onnistuneesti kokonaistilannekuva, jonka avulla voitiin pohtia organisaation häiriönhallintakykyä, jota pystyttiin analysoimaan harjoituksen tulosten perusteella. Tuloksista pystyttiin luomaan raportti, jossa yksityiskohtaisesti käytiin harjoitus läpi. Toimeksiantaja pystyy hyödyntämään tätä tutkimusta ja raporttia jatkokehittäessään organisaation kyberturvallisuutta, sillä ne käsittelevät harjoituksen kaikki osa-alueet, mukaan lukien löydökset ja tärkeät parannuskohteet.

Kyberharjoituksen ollessa ensimmäinen laatuaan toimeksiantajan organisaatiossa, voidaan toteutettua harjoitusta hyödyntää tulevaisuudessa toteutettavien kyberharjoitusten suunnittelussa. Harjoituksen loppuraportin pohjalta pystytään muun muassa suunnittelemaan uusia tavoitteita. Mukaan pystytään ottamaan myös vanhoja tavoitteita, joihin ei ensimmäisessä harjoituksessa päästy. Myös harjoitukseen osallistuneet organisaation työntekijät ymmärtävät paremmin kyberharjoitusten tarkoituksen ja toimintatavan. Sen puolesta he ovat kykeneviä tuomaan seuraaviin kyberharjoituksiin jonkinlaista sisältöä, esimerkiksi ideoita tai perehdytystä harjoitustoimintaan. Kyberharjoitus toi siis näkemystä ja kokemusta jatkokehittää tulevia kyberharjoituksia organisaatiossa, tai jopa yhteistyössä muille organisaatioille. Kyberharjoituksia voidaan mahdollisesti käyttää myös referenssinä harjoitusten järjestämisestä palveluna organisaation asiakkaille.

Lähteet

A cybersecure digital transformation in a complex threat environment — Brochure. 2021. Esite Euroopan komission virallisilla verkkosivuilla. Viitattu 8.5.2023. https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure.

Benefits of Exercise. N.d. Artikkeli National Cyber and Information Security Agency:n verkkosivuilla. Viitattu 19.3.2023. https://nukib.cz/en/cyber-security/exercises/benefits-of-exercise/.

Czosseck C. & Geers K. 2010. The Virtual Battlefield: Perspectives on Cyber Warfare (Proceedings 2009). Viitattu 2.5.2023. https://ccdcoe.org/library/publications/the-virtual-battlefield-perspectives-on-cyber-warfare-proceedings-2009/.

Harjoitustoiminta. 2023. Artikkeli Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskuksen verkkosivuilla. Viitattu 19.3.2023. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta.

History. N.d. Artikkeli Naton kyberpuolustuksen osaamiskeskus CCDCOE:n verkkosivuilla. Viitattu 2.5.2023. https://ccdcoe.org/about-us/.

Kick, J. 2014. Cyber Exercise Playbook. Viitattu 19.5.2023. https://www.mitre.org/sites/default/files/2022-09/pr_14-3929-cyber-exercise-playbook%20.pdf.

Kotipelto, H. N.da. Mitä on kansallinen turvallisuus?. Artikkeli sisäministeriön verkkosivuilla. Viitattu 21.4.2023. https://intermin.fi/kansallinen-turvallisuus/mita-on-kansallinen-turvallisuus.

Kotipelto, H. N.db. Kyberturvallisuus osana kansallista turvallisuutta. Artikkeli sisäministeriön verkkosivuilla. Viitattu 21.4.2023. https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus.

Kyberturvallisuus: miten EU torjuu kyberuhkia?. 2023. Artikkeli Eurooppa-neuvoston virallisilla verkkosivuilla. Viitattu 8.5.2023. https://www.consilium.europa.eu/fi/policies/cybersecurity/.

Kyberturvallisuuskeskus. 2019. Kyberharjoitusohje. Viitattu 17.3.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf.

Lehto M., Limnéll J., Innola E., Pöyhönen J., Rusi T. & Salminen M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Helsinki: Valtioneuvoston kanslia. Viitattu 30.4.2023. https://tietokayttoon.fi/julkaisu?pubid=17805.

Live exercise. N.d. Artikkeli Jyvsectec:in virallisilla kotisivuilla. Viitattu 19.5.2023. https://jyvsectec.fi/services/exercises/live/.

Locked Shields. N.d. Artikkeli Naton kyberpuolustuksen osaamiskeskus CCDCOE:n verkkosivuilla. Viitattu 3.5.2023. https://ccdcoe.org/exercises/locked-shields/.

Lukka, K. 2001. Konstruktiivinen tutkimusote. Artikkeli Metodix:in verkkosivuilla. Viitattu 12.5.2023. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/.

Mattermost overview. N.d. Dokumentaatio Mattermost:in verkkosivuilla. Viitattu 13.5.2023. https://docs.mattermost.com/about/product.html.

Metz T. N.d. How to Facilitate an After-Action Review (AAR or Hot Wash): Agenda and Tips. Blogiteksti Mgrush:in verkkosivuilla. Viitattu 14.5.2023. https://mgrush.com/blog/after-action-review/.

https://www.f-secure.com/fi/articles/what-is-a-cyber-attack. Artikkeli F-Secure:n verkkosivuilla. Viitattu 21.4.2023. https://www.f-secure.com/fi/articles/what-is-a-cyber-attack.

Paananen, R. 2021. Kyberturvallisuuden kehittämisohjelma. Viitattu 23.4.2023. http://urn.fi/URN:ISBN:978-952-243-599-6.

Sanastokeskus TSK. 2018. Kyberturvallisuuden sanasto. Helsinki: Huoltovarmuuskeskus. Viitattu 21.4.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf.

Takala T. 2013. Suomen kyberturvallisuusstrategia. Helsinki: Forssa print. Viitattu 30.4.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf.

Turvallisuuskomitea. 2014. KANSALLISEN KYBERTURVALLISUUSSTRATEGIAN TOIMEENPANO-OHJELMA. Viitattu 30.4.2023. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf.

Turvallisuuskomitea. 2017. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020. Viitattu 30.4.2023. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020/.

Turvallisuuskomitea. 2019. Suomen kyberturvallisuusstrategia 2019. Viitattu 23.4.2023. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/.

What is Microsoft Teams. N.d. Esite Microsoftin kotisivuilla. Viitattu 13.5.2023. https://support.microsoft.com/en-us/topic/what-is-microsoft-teams-3de4d369-0167-8def-b93b-0eb5286d7a29.

Yritys. 2023. Esite Wapice Oy:n virallisilla verkkosivuilla. Viitattu 8.5.2023. https://www.wapice.com/fi/yhteystiedot/yritys.

Liitteet

Liite 1. Tilannepäiväkirja

Tilannepäiväkirja	
Nimi	
Kellonaika	
Reagoitu syöte	
Toimenpiteet	
Muita huomioita	

Liite 2. Palautekyselylomake

Wapice tilannekuvaharjoituksen palautekysely

Vastaa allaolevassa taulukossa olevaan kysymykseen valitsemalla se vastausvaihtoehto, joka parhaiten vastaa mielipidettäsi aiheesta.

Kysymys	Vastaus				
	Täysin erimieltä	Osittain eri mieltä	En osaa sanoa	Osittain samaa mieltä	Täysin samaa mieltä
Harjoituksesta oli hyötyä minulle					
Harjoituksesta oli hyötyä Wapicelle					
Tehtäväni harjoituksen aikana olivat selkeät					
Harjoituksen syötteet olivat selkeät					
Harjoituksen syötteet olivat riittävän haastavia					
Harjoituksen syötteet vastasivat osaamistani					
Sain tarvittaessa apua ongelmatilanteissa					
Osallistun mielelläni tuleviin harjoituksiin					

Vapaamuotoinen palaute harjoituksesta:

Click or tap here to enter text.