Sosiaali- ja terveysalan VirtualLab-harjoitukset

Harjoituksista saadut kokemukset ja niistä nousseet kehitysehdotukset

XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
CyberCare Kymi

Sisällysluettelo

Tausta

Raportti on kirjoitettu Kaakkois-Suomen ammattikorkeakoulun toteuttamassa CyberCare Kymi -hankkeessa. Hankkeen rahoituksen myönsi Kymenlaakson liitto Euroopan Unionin osarahoittamana. Raportti perustuu hankkeessa kehitettyihin virtuaalisessa harjoitusympäristössä toteutettuihin kybertilanneharjoituksiin.

Harjoitusten tavoite

Hankkeen tavoitteena oli kehittää kaksi VirtualLab-ympäristössä toteutettavaa kybertilanneharjoitusta. Erikseen toteutettiin sosiaalihuollon ja terveydenhuollon toimijoille tarkoitetut harjoitukset.

Tavoitteena oli, että myös pienemmät sosiaali- ja terveysalan toimijat voisivat harjoitella kyberhäiriö- ja poikkeustilanteissa toimimista ja sen kautta parantaa varautumistaan ja aihepiireihin liittyviä suunnitelmia.

Harjoitusten suunnittelussa otettiin huomioon yrityksiltä nousseita tarpeita. Ideoita kerättiin muun muassa yritysten kanssa käydyistä keskusteluista ja hyödyntämällä keväällä 2025 järjestetyistä verkossa itsenäisesti toteutetuista työpöytäharjoituksista saatuja osallistujapalautteita.

Millaisia harjoituksia tehtiin?

Harjoitukset suunniteltiin niin, ettei niiden tekeminen vaatinut erityisiä tietoteknisiä taitoja. Harjoitusten kohderyhmää olivat erityisesti pienemmät yritykset, joista ei välttämättä löydy omia teknisessä roolissa olevia työntekijöitä vaan tilanteen teknisen selvittämisen ja korjaamisen hoitaisi tositilanteessa toinen palveluntarjoaja. Oleellisempaa oli varmistaa, että harjoitukseen osallistuvat toimijat tietävät, keneen tilanteessa oltaisi yhteydessä ja mistä yhteystiedot löytyvät.

Harjoitukset keskittyivät pääasiassa tilanteen johtamiseen, toiminnan jatkamiseen, lainsäädännöstä nouseviin ilmoitusvelvollisuuksiin sekä sisäiseen ja ulkoiseen viestintään. Ne pyrkivät erityisesti korostamaan tietoturvasuunnitelman merkitystä poikkeustilanteiden selvittämisessä ja toiminnan jatkuvuuden varmistamisessa. Kyberturvallisuuden lisäksi harjoituksiin liittyi oleellisesti tietosuoja sekä tietoturvaloukkausten asianmukainen käsitteleminen.

Harjoitusten tavoitteena oli myös se, että tositilanteessa tilanteen selvittämiseen osallistuvat henkilöt pääsevät miettimään toimintaa omien rooliensa kautta ja kokeilemaan tilanteen selvittämistä tiiminä. Harjoitustiimin kokoa tai kokoonpanoa ei ollut etukäteen määritelty tarkasti, sillä kohderyhmään kuului monentyyppisiä toimijoita. Harjoitukset suunniteltiin niin, että niiden tekeminen olisi ollut mahdollista myös yksinyrittäjille.

Molempiin harjoituksiin päätyi aiheeksi yrityksen potilas- tai asiakastietojärjestelmään kohdistuva kiristyshaittaohjelma. Osasyynä kiristyshaittaohjelman valikoitumiseen oli se, että kyseiset hyökkäykset nousevat selkeästi esiin yhtenä yleisimpänä sosiaali- ja terveysalan yrityksiä uhkaavista kyberhyökkäyksistä.

Harjoitukset keskittyvät asiakas- ja potilastietojärjestelmän ongelmatilanteisiin myös siksi, koska yrityksiltä tulisi lainsäädännön mukaan löytyä suunnitelma niiden tilanteiden varalle, joissa järjestelmä on poissa käytöstä. Järjestelmän ongelmatilanne mahdollisti monipuolisen ja laajan skenaarion, jossa korostui yrityksissä käytettävän tiedon kriittisyys.

Sosiaalihuollon harjoitus

Sosiaalihuollon harjoitus tehtiin kuvitteellisen hoivakodin näkökulmasta. Harjoitus pyrittiin pitämään mahdollisimman yleistasoisena, jotta se tuntuisi samaistuttavalta monelle toimijalle, joka tarjoaa erilaisia asumispalveluita.

Harjoitus käsitteli tilannetta, jossa yrityksen asiakastietojärjestelmään ilmestyy kiristyshaittaohjelma. Harjoituksen alussa tarkennettiin, että kyseistä järjestelmää käytetään myös yrityksen laskutuksen hoitamiseen. Harjoittelun aikana harjoitustiimin tuli miettiä, miten toimintaa jatketaan kyseisessä tilanteessa, keneen ollaan yhteydessä tilanteen selvittämiseksi ja kenelle tapahtuneesta tulee ilmoittaa.

Lisäksi tilanteessa reagoitiin yrityksestä verkossa liikkuviin negatiivisiin tietoihin. Tieto levisi yrityksen ulkopuolelle alun perin yrityksen työntekijöiden keskusteltua siitä sosiaalisessa mediassa. Sosiaalisen median keskustelun kautta aihe nousi esille myös paikallislehdessä, jossa tilanteesta levisi osittain väärää tietoa.

Lopulta harjoituksen tekijöille selvisi, että yrityksen työntekijä oli huijattu viemään haittaohjelma järjestelmään. Tämän tarkoituksena oli nostaa esiin sen merkitystä, että yrityksen työntekijöitä koulutetaan oikeisiin toimintatapoihin ja huijausten tunnistamiseen liittyen.

Terveydenhuollon harjoitus

Terveydenhuollon harjoitus tehtiin kuvitteellisen lääkäriaseman näkökulmasta. Harjoitus pyrittiin pitämään mahdollisimman yleistasoisena, jotta se tuntuisi samaistuttavalta monelle toimijalle, jotka tarjoavat ajanvarauksella toimivia palveluita.

Harjoituksen alussa potilastietojärjestelmässä huomattiin kiristyshaittaohjelma. Harjoituksen alussa tarkennettiin, että järjestelmän kautta hallitaan myös asiakkaiden ajanvarauksia. Kuten sosiaalihuollon harjoituksessa, myös tässä harjoituksessa tuli miettiä, miten toimintaa jatketaan, miten tilanne selvitetään teknisesti ja kenelle tilanteesta ilmoitetaan.

Harjoituksen viestintä keskittyi vahvasti asiakkaille viestimiseen. Harjoituksessa kiristyshaittaohjelman asentanut rikollinen kiristi

rahaa yrityksen lisäksi myös asiakkailta. Tämä selvisi, kun asiakas laittoi tuohtuneena viestiä ja kysyi tilanteesta. Harjoittelija pääsi harjoittelemaan tietoturvaloukkauksesta viestimistä. Lopulta tilanteesta levisi tieto myös paikallislehden toimittajalle, joka kysyi aiheeseen liittyen kommentteja.

Kokemukset ja palaute

Harjoituksista päästiin pilotoimaan yrityksen kanssa sosiaalihuollolle tarkoitettu harjoitus. Pilotointiin osallistunut yritys antoi harjoituksesta palautetta sekä suullisesti heti harjoituksen jälkeen että kirjallisesti myöhemmin harjoituksien pilotointia varten tehdyn palautelomakkeen kautta.

Tämän lisäksi harjoituksen järjestäjä kirjasi ylös pilotoinnista nousseita huomioita.

Harjoituksen järjestäjän huomiot

Harjoituksen järjestäjän näkökulmasta harjoitus eteni sujuvasti. Harjoitus oli rytmitetty niin, että seuraavaan vaiheeseen ehti valmistautua sillä aikaa, kun harjoitusta suorittava tiimi pohti reagointia tai suoritti harjoitukseen liittyviä tehtäviä.

Harjoituksen aikana ei ilmennyt teknisiä ongelmia. Hankkeen laitteiden käyttö harjoituksessa mahdollisti sen, että harjoituksen valmisteluun liittyviä toimia oli mahdollista tehdä ennen varsinaista

harjoituksen alkua, mikä tarkoitti sitä, että harjoitustilanteessa siihen ei tarvinnut käyttää aikaa. Harjoitukseen oli varattu kaksi tuntia, sisältäen harjoituksen alustamisen ja sen jälkeen käydyn purku- ja palautekeskustelun. Aika oli harjoituksen järjestämiseen sopiva. Harjoituksen tehtävät ja syötteet oli rytmitetty niin, että harjoituksen eteenpäin kuljettaminen onnistui luontevasti ilman kiirettä.

Haastavaksi osoittautui harjoituksen pilotoinnista kiinnostuneiden organisaatioiden löytäminen. Harjoituksista viestittiin laajasti mm. hankkeen uutiskirjeessä, laajemmassa Xamkin kyberturva-aiheisessa uutiskirjeessä, paikallisen yrittäjäjärjestön jäsenille lähtevässä suorasähköpostissa sekä kyberasema.fi-verkkosivuilla ja Kyberaseman LinkedIn-tilillä. Tietoa harjoitusmahdollisuudesta laitettiin myös kohdennetusti yrityksiin, jotka olivat olleet mukana hankkeen muissa toimissa, ja jotka olivat aiemmin osoittaneet kiinnostusta harjoittelua kohtaan.

Epäselväksi jäi, mikä oli syynä matalaan kiinnostukseen.

Sosiaali- ja terveydenhuollon toimijalta saatu palaute

Pilotointiin osallistuneelta yritykseltä saatu palaute oli erinomaista. Kouluarvosanalla arvioiden yrityksen edustaja antoi harjoitukselle arvosanan 10.

Harjoituksen jälkeisessä keskustelussa nousi esiin, että harjoituksen suorittajat kokivat hyödylliseksi sen, että hankkeen henkilökuntaa oli

paikalla osallistumassa keskusteluun ja antamassa vinkkejä asioista, jotka tilanteissa tulisi huomioida.

Myös he kokivat harjoitukselle olleen tarpeeksi aikaa ja sen edenneen sujuvasti. Harjoitus auttoi heitä kehittämään varautumista ja sen sisältö oli hyödyllinen. Harjoitus nosti esiin myös kehittämiskohtia. He suosittelisivat harjoitusta ja olisivat kiinnostuneet osallistumaan uudelleen, jos erilaisia harjoituksia olisi tarjolla. Aihe koettiin tärkeäksi ja säännöllinen harjoittelu hyödylliseksi.

Harjoitusten jatkokehittäminen

Hankkeessa tuotetut harjoitukset vaativat sen, että harjoituksen aikana joku kuljettaa niitä eteenpäin lähettämällä tarvittavia sähköposteja, käynnistämällä haittaohjelman ja liikuttamalla harjoituksen tarinaa eteenpäin. Tämä toimi hankkeen kannalta hyvin, sillä hankesuunnitelmassa on kuvattu, että harjoituksia järjestetään paikan päällä yrityksessä ja hankkeen työntekijä osallistuu harjoituksen eteenpäin kuljettamiseen, sekä harjoituksen aikana ja sen jälkeen tapahtuvaan keskusteluun.

Harjoituksia kannattaisi kuitenkin kehittää niin, että ne olisivat itsenäisesti suoritettavia. Näin kiinnostunut toimija voisi helpommin suorittaa harjoituksen haluamaansa aikaan ja ilman ulkopuolisten henkilöiden läsnäoloa. Tämä saattaisi madaltaa harjoitteluun osallistumisen kynnystä. Jotta tämä olisi mahdollista, tulisi harjoituksiin kuuluvat sähköpostit, haittaohjelma ja tarina ajastaa ja

automatisoida niin, etteivät ne vaadi manuaalista eteenpäin vientiä. Teknisesti tämä on VirtualLab-ympäristössä jo mahdollista.

Toisena kehittämisideana esiin nousi tekoälyn hyödyntäminen kyberharjoituksissa. Tekoälyn avulla harjoituksista olisi mahdollista tehdä yksilöllisempiä. Hankkeessa toteutetuissa harjoituksissa käytettiin etukäteen kirjoitettuja sähköposteja, uutisartikkeleja ja somekommentteja. Sisällyttämällä tekoälyelementtejä, harjoituksista olisi mahdollista tehdä immersiivisempiä, jos esimerkiksi sähköposteihin tulevat vastaukset eivät olisi geneerisiä vaan perustuisivat harjoituksen tekijän lähettämään viestiin.

Tekoälyä ei vielä hyödynnetä VirtualLab-ympäristössä, mutta sen mahdollisuuksia on kartoitettu ja asian selvittäminen jatkuu.

Myös pilotointiin osallistunut toimija nosti esiin kehittämisehdotuksen. Ehdotuksessa nousi esiin tarve laajemmalle harjoitustarjonnalle. Erilaiset harjoitukset mahdollistaisivat säännöllisen harjoittelun ja mahdollisesti eri rooleissa toimivien henkilöiden harjoittelun. Harjoituksia olisi siis hyödyllistä kehittää lisää eri aiheista, mahdollisesti niin, että ison ja laajan harjoituksen sijaan harjoitus olisi kohdennettu tarkemmin tietylle roolille tai valittavana olisi harjoituksia, joissa käsitellään erilaisia häiriö- ja poikkeustilanteita.

Tärkeintä kuitenkin olisi saada kohderyhmä tietoiseksi harjoittelun merkityksestä ja hyödyistä yritykselle. Harjoitusten kehittämisen konkreettiset hyödyt ovat pienet, jos niille ei löydy tekijöitä.

Selkeä ja kiinnostava viestintä, ymmärrys tarpeesta sekä osallistumiskynnyksen madaltaminen ovat tärkeitä elementtejä siinä, että kohderyhmä saadaan harjoitusten pariin. Mahdollisia syitä matalalle kiinnostukselle saattoi olla esimerkiksi se, että harjoittelu on vierasta, se koetaan haastavaksi tai sille ei löydetä aikaa. Viestinnässä pyrittiin korostamaan sitä, ettei harjoitukseen osallistuminen vaadi erityisiä tietoteknisiä taitoja. Viestinnässä pyrittiin myös käyttämään selkeää kieltä.

Osallistumiskynnystä on jo pyritty madaltamaan esimerkiksi Kyberkestävä-verkkoalustalta (https://treenit.kyberasema.fi/) löytyvien itsenäisesti suoritettavien työpöytäharjoitusten avulla. Myös VirtualLab-ympäristöön suunnitelluista harjoituksista on muokattu alustalle sopiva versio. Harjoittelun merkitystä on pyritty avaamaan mm. yrityskohtaisissa tietoturvaneuvonnoissa, laajemmin kaikille järjestetyssä webinaarissa, sekä harjoitteluun keskittyvässä artikkelissa.

Hankkeessa on laadittu konsepti sote-alan kyberharjoittelun simulaatioympäristölle. Konsepti yhdistää kyberpoikkeustilanteiden moniammatillisen harjoittelun fyysisessä ja virtuaalisessa ympäristössä. VirtualLab-ympäristöllä on merkittävä rooli kokonaisuudessa, ja konseptissa on avattu siihen liittyviä kehittämisideoita tarkemmin. Konseptissa kuvatut kehittämisideat keskittyvät mm. käyttäjätodennukseen, käyttöoikeuksien hallintaan, analytiikkaan, harjoitusten kehittämiseen ja käyttövarmuuteen.