Tietoturvasuunnitelman rooli tietoturvaharjoittelussa

Tietoturvasuunnitelman tarkoitus on toimia organisaation tietoturvaan ja toki myös tietosuojaan liittyvänä omavalvonnan välineenä. Suunnitelmaa on tarkoitus päivittää vähintään vuosittain, sekä aina silloin, kun toimintaympäristössä, riskeissä, lainsäädännössä, omavalvonnassa tai tietoturvaan liittyvissä harjoituksissa on havaittu kehitettävää tai tarvetta muutoksille. Tietoturvan omavalvonnan tarkoituksena on varmistaa ensinnäkin se, että organisaatio toimii vaatimuksien, lainsäädännön ja ohjeistuksien mukaisesti. Omavalvonnan kautta halutaan varmistaa myös toiminnan säännöllinen seuranta, ettei toimintaan ole päässyt syntymään turvattomia toimintatapoja esimerkiksi osaamispuutteiden tai viestintäkatkoksien vuoksi. Tietoturvaharjoitukset toimivatkin omavalvonnassa tärkeänä tukena, sillä niiden avulla voidaan käytännössä testata suunniteltujen tietoturvakäytäntöjen toimivuutta.

Tietoturvaharjoittelun tarkoituksena on mallintaa ja testata oman varautumisen tasoa erilaisten tietoturvaan liittyvien häiriötapahtumien osalta. Näin ollen onkin perusteltua, että sote-alan tietoturvaharjoituksissa testataan aina myös tietoturvasuunnitelmaan kuvattujen asioiden toimivuutta arjessa. Tämä on tärkeää siitä syystä, että varmistetaan, että tietoturvasuunnitelmasta on tosiasiallista apua mahdollisten häiriö- ja poikkeamatilanteiden yhteydessä. Harjoituksissa päästään lähimmäksi varsinaista kriisitilannetta, ilman kriisin aiheuttamia seurauksia.

Euroopan unionin osarahoittama
KYMEN LAAKSON LIITTO
XAMK Kaakkois-Suomen ammattikorkeakoulu

Kappale 3. Yleiset tietoturvakäytännöt

Tässä kappaleessa ajatuksena on kuvata organisaation keskeisiä tietoturvakäytäntöjä, tietoturvaperiaatteita, asiakirjoja ja vastuita. Tästä kappaleesta tulisi käydä ilmi se, millaisia erilaisia vastuita tietoturvaan liittyen on määritelty ja keneen ollaan konkreettisesti yhteydessä, mikäli vaikkapa työskennellessä havaitaan jotakin poikkeavaa. Tietojärjestelmään liittyvien häiriöiden osalta ollaan todennäköisesti yhteydessä organisaation koon mukaan, joko suoraan järjestelmätoimittajaan, järjestelmän pääkäyttäjään tai esihenkilöön. Tietosuojahuolien osalta taasen ollaan yhteydessä organisaation tietosuojavastaavaan. Erilaiset häiriötilanteet ja niihin liittyvät vastuut ja vastuuhenkilöt kannattaakin tuoda esille tässä kappaleessa. Samoin kappaleessa on ajatuksena niputtaa yhteen kaikki organisaatiosta löytyvät tietoturvaan ja tietosuojaan liittyvät ohjeet, joita voimme tarvita myös harjoituksessa. Harjoituksessa on hyvä arvioida muiden asiakirjojen osalta myös näiden ajantasaisuutta, helppokäyttöisyyttä ja saavutettavuutta.

Kappale 4. Menettelyt virhe- ja ongelmatilanteissa

Riippumatta harjoituksen varsinaisesta skenaariosta tietoturvasuunnitelman kappale 4 Menettelyt virhe- ja ongelmatilanteissa, on yksi keskeisimmistä kappaleista, jonka sisältöä tulisi arvioida harjoituksen aikana. Harjoituksessa tulisi kriittisesti arvioida, antaako nykyinen tietoturvasuunnitelma riittävästi tukea häiriötilanteessa toimimiseksi ja toiminnan jatkuvuuden varmistamiseksi. Ovatko virhe ja poikkeamatilanteissa noudatettavat toimintatavat kirjattu selkeästi ja onko niitä helppo noudattaa? Onko organisaatiolla olemassa jo tietoturvasuunnitelmasta kuvattu selkeä toimintatapa, miten virhe ja

ongelmatilanteita lähdetään selvittämään ja miten niistä myös toivutaan? Onko vaihtoehtoiset työskentelytavat kuvattu erilaisten häiriötilanteiden osalta, jotta työntekijöiden on helppo lähteä niitä noudattamaan? Löytyykö kappaleesta myös ajantasaiset yhteystiedot operaattorille, tietojärjestelmätoimittajille ja muille keskeisille toimijoille, joiden apua saatetaan häiriö- ja poikkeamatilanteessa tarvita, tai joille häiriötilanteesta tulisi informoida? Informointikäytäntöjä kannattaa harjoitella aina informaation laatimiseen ja omien viestintäohjeiden testaamiseen saakka.

Kappale 5. Henkilöstön koulutus ja osaamisen sekä tietojärjestelmien käyttöohjeet ja tietoturvallinen käyttäminen

Tietojärjestelmien ja henkilöstön toimintaan kytkeytyvässä harjoituksessa on hyvä tarkastella myös kappaleen 5 sisällön avulla. Harjoituksen aikana on hyvä pohtia, onko henkilöstöllä riittävät valmiudet tietojärjestelmien käyttäjinä, myös häiriötilanteissa. Löytävätkö he helposti tietojärjestelmien käyttöohjeet ja entäpä jos käyttöohjeisiin ei olekaan pääsyä? Onko tähän mietitty vaihtoehtoista toimintatapaa? Koska kappale keskittyy myös harjoitusta edeltäneisiin koulutuksiin, on hyvä arvioida mahdollisimman realistisesti ovatko käydyt koulutukset antaneet organisaatiolle riittäviä valmiuksia toimia myös häiriö- ja poikkeamatilanteissa, ja nouseeko harjoittelun aikana siten myös osaamisenvarmistamiseen liittyviä tarpeita. Tämän kappaleen tulisi antaa ohjeita ja neuvoja myös siihen, miten asiakas- ja potilastietojen käsittely normaalisti toteutetaan organisaatiossa ja miten tämä taasen toteutetaan mahdollisen häiriö ja poikkeamatilanteen aikana.

Kappale 6. Tietojärjestelmien tietoturvakäytännöt

Kappale 6 on keskeisessä roolissa silloin, jos harjoitus tai sen osa linkittyy organisaation käytössä oleviin tietojärjestelmiin. Yleisesti kappale keskittyy erityisesti siihen, että organisaation käytössä oleva (olevat) tietojärjestelmät soveltuvat käyttötarkoitukseensa ja täyttävät niille asetetut vaatimukset. Harjoituksen aikana kannattaa tarkistaa järjestelmää koskeva tuorein status Valviran Astori- tietojärjestelmärekisteristä: https://astori.cloud.valvira.fi/. Harjoituksen aikana kannattaa myös tarkastella ja keskustella siitä ketkä voivat organisaation laitteille tehdä asennuksia, päivityksiä ja ylläpitotoimia. Onko tämä ohjeistettu ja kuvattu selkeästi, onko tämä mahdollisesti ulkoistettu ja millaisia vastuita ulkoistamisen osalta on sovittu ja millaisia vastuita tietojärjestelmiin sisältyy muutoin, mitä on sovittu esimerkiksi sopimuksissa? Päivittyvien tietojärjestelmien osalta on tärkeää huolehtia henkilöstön osaamisen varmistaminen päivittyneen tietojärjestelmän käytön osalta. Niinpä harjoituksen aikana on hyvä tarkistaa, onko muutoksiin, kuten päivityksiin liittyvät toimintamallit kuvattu ja onko tässä huomioitu myös järjestelmää käyttävien osaamisen varmistaminen.

Kappale 6 keskittyy myös järjestelmiä käyttävien käyttöoikeuksiin ja käyttöoikeuksienhallintaan. Käyttäjien käyttöoikeuksien osalta tulee varmistaa, että organisaatiolta löytyy ajantasainen listaus, joka sisältää kaikki organisaation käytössä olevat tietojärjestelmät ja niitä käyttävät henkilöt ja heidän käyttöoikeuksiensa tason. Harjoituksen aikana on suositeltava tarkastaa myös organisaation käyttöoikeushallintaan liittyvät käytännöt, kuka voi myöntää käyttöoikeuksia, onko käyttöoikeuksien muuttaminen ja poistaminen hallittua? Entä millainen on organisaation realistinen reagointinopeus, mikäli käyttöoikeus pitääkin poistaa kiireellisesti mahdollisen väärinkäyttöepäilyn vuoksi? Samoin

käyttöoikeuksiin kytkeytyy oleellisesti myös vahvaan tunnistautumiseen ja salasanojen hallintaan liittyvät organisaatiokohtaiset käytännöt. Tunnistautumisten ja kirjautumisten osalta on hyvä huomioida myös mobiililaitteisiin liittyvät käytännöt.

Viimeinen mutta ei vähäisin harjoituksessa huomioitava näkökulma kappaleen 6 osalta on järjestelmien pääsynhallintaan ja käytön seurantaan liittyvien käytäntöjen tarkastelu. Vähintään suunnitelmassa tulisi tämän osalta olla kuvattuna lokienhallinnan ja käytön seurannan toimintamalli. Tarkastelkaa millä tasolla tietoturvasuunnitelmassa on kuvattu myös tietopyyntöihin liittyviä käytäntöjä, kuten tietopyyntöihin vastaamiseen liittyviä keskeisiä rooleja. Tämän osalta tulisi olla kuvattuna ainakin tietosuojavastaavan, mahdollisen tietohallinnon ja rekisterinpidosta vastaavien tehtävät. Lokitietojen seuranta on myös tärkeässä roolissa harjoituksia, kun selvitetään mahdollisia häiriötilanteita. Tämän osalta tulisi olla kuvattuna kuka tai ketkä seuraavat lokiraportteja ja kuinka usein tätä tehdään ja miten seuranta dokumentoidaan.

On tärkeää kuvata myös pääsynhallinnan tekniset käytännöt ei-sallitun käytön estämiseksi sosiaalihuollon asiakastietoja tai potilastietoja käsittelevissä tietojärjestelmissä sekä organisaation omat ohjeet ja toimintatavat asiakas- ja potilastietojen käsittelyn osalta. Organisaatiolla tulee olla myös toimintamalli, mikäli havaitaan lainsäädännön vastaista asiakas- tai potilastietojen käsittelyä. Kirjallinen toimintamalli tulisi olla ainakin sen osalta, kuinka toimitaan, jos lokitiedoista paljastuu virhetilanteita tai epäilyjä rikkomuksia tai epäasianmukaista käytöstä ja kuvaus sisäisen valvonnan toimintatavoista.

Kappale 7. Tietojärjestelmien käyttöympäristön tietoturvakäytännöt

Viimeinen tietoturvaharjoituksissa huomioitava kappale keskittyy organisaation fyysiseen turvallisuuteen liittyviin näkökulmiin, eli tarkemmin toimitilojen ja etätyöskentelyn turvallisuuteen. Tämän osalta kappaleen tulisi antaa tietoa, miten esimerkiksi toimitilojen lukitseminen ja mahdollinen kulunvalvonta on järjestetty. Samoin toimitilojen kalustaminen ja esimerkiksi näyttöpäätteiden sijoittuminen ja suojauskäytännöt ovat keskeisiä näkökulmia, jottei sivullisilla ole näköyhteyttä ruuduille. Tämän osalta organisaation on hyvä kuvata päätteiden ja tulostimien sijoittelua ja muita käyttöönotettuja suojauskäytäntöjä kuten näytönsuojakalvoja, käyttämättömän päätteen automaattista lukittumista, lukittumisaikaa ja päätteen salasanakäytäntöä. Kappaleessa on hyvä kuvata myös mikä on organisaation suhtautuminen ulkoisten kovalevyjen ja muistitikkujen käyttöön ja mikäli näitä käytetään, millaiset ovat näiden suojauskäytännöt. Samoin organisaation on hyvä kuvata myös sitä, miten on estetty se, etteivät ulkopuoliset toimijat pysty tuomaan muisti- tai seurantavälineitä työasemiin, työpöydille tai reitittimiin.

Tässä kappaleessa keskitytään myös manuaalisten arkistojen suojaamiseen ja turvaamiseen. Varmista harjoituksen aikana, että manuaalisten arkistojen suojauskäytännöt on kuvattu ja ne ovat asianmukaiset. Suositeltavaa on, että manuaaliset arkistot suojataan hyvin ja säilytetään paloturvallisesti lukittuna ja suojassa sivullisilta. Arkistojen hallinnan osalta on kuvattava ja huolehdittava myös niiden hävittäminen siten, etteivät sivulliset pääse tietoihin myöskään elinkaaren loppuvaiheessa.

Turvallisuuden varmistamisen osalta kappaleessa kuvataan myös tukipalveluiden hallintaa työasemien, mobiililaitteiden ja käyttöympäristön

osalta. Tässä näkökulmassa tärkeässä roolissa ovat mm. virusturvan toimivuuden ja päivityksien varmistaminen työasemilla ja käytössä olevissa mobiililaitteissa. Samoin laitteiden hallintaan ja mahdolliseen laiterekisteriin liittyvien toimintatapojen arviointi on hyvä tehdä harjoituksen aikana. Onko tämä kuvattu millä tasolla tietoturvasuunnitelmassa ja ovatko toimintamallit selvät kaikille. Työsuhteen päättyessä tulee varmistaa, ettei työntekijän käyttöön jää käyttöoikeuksia tai organisaation laitteita.

Harjoituksessa on hyvä huomioida myös tietoverkkoon liittyviä turvallisuusnäkökulmia, jotka myös tässä kappaleessa kuvataan. Miten on sovittu esimerkiksi tietoliikenteen tietoturvaan liittyvistä vastuista, onko sopimuksissa mukana tietoturvallisuus- ja palvelun saatavuusasioita, mukaan lukien yhteydenotot ja menettelyt häiriötilanteissa? Entä miten käytössä olevien verkkojen tietoturvallisuuskäytänteet on järjestetty (esimerkiksi verkon segmentoinnit, palomuurit, reititykset). Jos käytössä on puolestaan langaton verkko, vaaditaanko verkkoon salasana, mitkä ovat verkon salasanojen vaihtamiskäytännöt ja miten verkko on suojattu muutoin organisaation ulkopuolisilta? Tietoturvasuunnitelman tulisi antaa vastaus myös siihen kenen vastuulla on reitittimien ja muiden verkkolaitteiden päivitysten ja suojausten huolehtiminen ja näihin mahdollisesti liittyvät sopimukset?

Tietoturvasuunnitelma kattaa siis paljon näkökulmia, jotka perinteisesti ovat tavalla tai toisella mukana erilaisissa harjoitusskenaarioissa. Aina harjoituksissa ei välttämättä huomioida jokaista edellä kuvattua kappaletta, mutta tyypillisesti harjoituksiin on sisällytetty useimpia edellä kuvatuista elementeistä. Näin ollen tietoturvasuunnitelma on tärkeä apuväline harjoituksessa, ja toisaalta harjoitukset voivat avata uusia näkökulmia ja huomioita, jotka tulisi omaan suunnitelmaan päivittää.

Koska harjoituksissa saatetaan kattaa kohtalaisen laajastikin organisaation tietoturvaan ja tietoturvasuunnitelmaan liittyviä näkökulmia on harjoituksen aikana hyvä kirjata muistiin kaikki esille tulleet huomiot, riippumatta havainnon laajuudesta. Tällä tavoin päästään kehittämään sekä tietoturvasuunnitelmaa, että organisaation ennakointikykyä häiriö- ja poikkeamatilanteiden osalta. Harjoituksissa voi olla haastavaa muodostaa tilannekuvaa omasta toiminnasta, mutta viestintätapoja, vastuita ja toimintamalleja testaamalla tilannekuvakin selkiytyy. Harjoituksiin ja myös omiin asiakirjoihin kannattaa suhtautua ajatuksella ”loistavaa jos löytyy jotain kehitettävää” tällä tavoin annamme itsellemme luvan hyväksyä mahdolliset harjoituksessa eteen tulevat virheet tai puutteet. Näin pääsemme myös kehittämään sekä ohjeistustamme, että käytäntöjämme niiden asioiden osalta, jotka kehittämistä tosiasiassa kaipaavat. Harjoituksen jälkipuinnissa onkin hyvä käydä läpi kaikki tunteet ja kokemukset mahdollisimman avoimesti ja ratkaisukeskeisesti.

Euroopan unionin osarahoittama
KYMEN LAAKSON LIITTO
XAMK Kaakkois-Suomen ammattikorkeakoulu