Digi- ja väestötietovirasto

8.10.2020

TAISTO20 -harjoituskäsikirja

Ohjeita TAISTO20-harjoitukseen valmistuville organisaatioille

8.10.2020

Sisällysluettelo

Digi- ja väestötietovirasto

8.10.2020

TAISTO20-harjoituskäsikirja

TAISTO-harjoitus on julkishallinnolle suunnattu tietosuoja- ja tietoturvaloukkauksien hallinnan harjoitus, jossa organisaatiot harjoittelevat toimintamalleja ja prosesseja erilaisten häiriötilanteiden varalle. Harjoituksen avulla reagointi tietoturva- tai tietosuojaloukkaukseen voidaan hoitaa tositilanteessa hallitummin, jolloin toipuminen on nopeampaa.

Digi- ja väestötietovirasto vastaa TAISTO-harjoituksen toteuttamisesta ja ohjaamisesta. Harjoituksen johtajana toimii Digi- ja väestötietoviraston tietoturva-asiantuntija Hanna Heikkinen. Lisäksi harjoituksen toteuttamisessa on mukana Digi- ja väestötietoviraston asiantuntija Laura Penttilä. Harjoituksen suunnittelu tehdään yhteistyössä Keskusrikospoliisin, Kyberturvallisuuskeskuksen, tietosuojavaltuutetun toimiston, Valtorin ja Turvallisuuskomitean kanssa.

Loka- ja marraskuussa pidettävien TAISTO20-harjoitusten jälkeen Digi- ja väestötietovirasto julkaisee harjoitusmateriaalin kaikkien saataville. Toivomme, että TAISTO20-harjoitukseen osallistujat eivät jaa harjoituksen sisältöön liittyvää materiaalia sitä ennen julkisesti.

TAISTO20-harjoituksen tavoitteet ovat

- Tunnistaa eri viranomaisten tehtävät erilaisissa tilanteissa.
- Kehittää tietoturvallisuuden hallintaa, johtamista ja viestintää häiriötilanteissa.
- Kehittää henkilötietojen tietoturvaloukkauksissa tarvittavia prosesseja, kuten kykyä arvioida syntynyttä riskiä, tehdä tarvittavat ilmoitukset viranomaisille, sidosryhmille ja rekisteröidyille.
- Kehittää toiminnan jatkuvuuteen, varautumiseen ja häiriötilanneviestintään liittyvää ohjeistusta ja toimintaprosesseja.

Organisaatioiden on hyvä käydä TAISTO20-harjoituksen tavoitteet läpi harjoittelijaryhmän kanssa ennen harjoitusta. Lisäksi organisaatio voi halutessaan lisätä omia tavoitteita TAISTO20 harjoitukselle yleisten tavoitteiden lisäksi.

1 Valmistautuminen harjoitukseen

Harjoituksessa pääpaino on organisaation omien prosessien, ohjeiden ja toimintamallien kehittäminen.

- Varmistathan, että organisaatiolla on käytössä ajan tasalla olevat henkilötietojen tietoturvaloukkauksiin liittyvät prosessit ja ohjeet. Lisäksi harjoitusta varten organisaatiolla on hyvä olla käytössä jatkuvuuden ja varautumisen suunnitelmat ja ohjeet, joiden mukaan toimitaan erilaisissa häiriö- ja poikkeustilanteissa.

Organisaation harjoituksen yhteyshenkilö vastaa siitä, että organisaatiolla on sopivat viestintävälineet ja tilat käytössä harjoitusta varten.

- Muistathan tehdä tarvittavat kalenterivaraukset myös organisaation harjoitusryhmälle.

Huomaathan, että harjoitukseen tulee osallistua henkilöitä eri rooleista, joilla on vastuita häiriö- ja poikkeamatilanteiden hallinnassa ja jatkuvuuden turvaamisessa. Näitä rooleja ovat mm. johdon edustaja, tietoturvallisuuden vastuuhenkilö, tietosuojavastaava, viestinnän asiantuntija sekä ICT-asiantuntija.

- Yhdellä henkilöllä kannattaa olla vain yksi rooli harjoituksessa, jotta harjoitus etenee sujuvasti. Roolit on hyvä käydä läpi harjoituspäivän aamuna, jotta jokainen ymmärtää roolinsa/tehtävänsä harjoituksessa.

Suosittelemme, että organisaatio ottaa harjoitukseen tarkkailijan, joka dokumentoi päivän tapahtumat ja havainnot.

- Harjoituspäivään kannattaa kytkeä ulkopuolinen tarkkailija, jotta organisaatio saa harjoituksesta mahdollisimman suuren hyödyn. Hän kirjaa objektiivisesti ylös tilanteeseen liittyneitä havaintoja organisaation toiminnasta.

- Tarkkailijan ohje ja havaintolomake julkaistaan viikolla 42 osoitteessa www.dvv.fi/taisto

Tänä vuonna harjoituksessa käytettään Trasim-harjoitusalustaa harjoituksen tapahtumien, syötteiden ja maailmankuvaa vastaavan mediatilannekuvan välittämiseksi. Harjoituspäivä rakentuu tapahtumista ja niihin liittyvistä syötteistä. Syötteet julkaistaan aikataulun mukaisesti harjoitusalustalla.

- Huomaathan, että syötteistä ei laiteta erillistä sähköpostiviestiä/herätettä.

- Jos sinulle tulee harjoitusalustaan liittyviä ongelmia harjoituspäivän aikana laita välittömästi sähköpostia osoitteeseen digiturva@dvv.fi otsikolla: TAISTO20-harjoitus: Tekninen häiriö harjoitusalustalla.

Harjoituksessa ei tutkita tarkemmin mahdollisen tietoturvapoikkeaman, hyökkäyksen tai henkilötietojen tietoturvaloukkauksen syitä, eikä tehdä tarkempaa tapahtuneeseen liittyvää tutkintaa (forensiikka). Organisaation tulee osana harjoituksen jatkotoimenpiteitä ja oman toiminnan kehittämistä selvittää ja arvioida, kuinka se harjoituksen kaltaisissa tilanteissa jatkaisi tarvittavaa tilanteen selvitystä.

Organisaatio voi halutessaan käyttää harjoituksessa mukana esimerkiksi palveluntuottajia. Organisaation tulee itse sopia näiden käytöstä. Digi- ja väestötietovirasto ei vastaa näiden osapuolien harjoituksessa mukana olosta, eikä niihin liittyvistä kustannuksista. Palveluntoimittajat laskuttavat tästä työstä teitä voimassa olevan sopimuksenne mukaisesti.

Harjoituspäivän aikana organisaation pitää toimia kuten oikeassa tilanteessa. Organisaation pitää toteuttaa sisäiset yhteydenotot, sähköpostiviestit, pikaviestikeskustelut, mahdolliset tiedotteet ja muut toimenpiteet, kuten se aidossa tilanteessa tekisi. Muistakaa käyttää kaikissa viesteissä tunnisteena TAISTO20-HARJOITUS, ettei kukaan erehdy luulemaan tilannetta oikeaksi.

2 Näyttövastaavat

Organisaatioilla on kaksi nimettyä näyttövastaavaa harjoituksessa. Näyttövastaavien tehtävänä harjoituksessa on jakaa harjoitusalustan seurantanäkymä ja siinä julkaistut syötteet organisaation harjoitusryhmälle. Näyttövastaavat jakavat oman näytön (harjoitusalustanäkymä) organisaation omassa itse järjestämässä virtuaalikokouksessa tai vastaavasti fyysisessä tilassa, kuten neuvotteluhuoneessa. Näyttövastaavien täytyy olla mukana harjoituksessa. Organisaation harjoituksen yhteyshenkilö vastaa siitä, että organisaatiolla on sopivat viestintävälineet ja tilat käytössä harjoitusta varten.

Näyttövastaaville toimitetaan ohjeet käyttäjätilin aktivointiin ja näyttövastaavana toimimiseen harjoituksessa. Ennakkotehtäväksi näyttövastaaville on annettu kirjautua harjoitusalustalle ja varmistaa, että tunnukset toimivat.

Ohjeet näyttövastaavana toimimiseen harjoituksessa ja harjoitusalustalle kirjautumiseen löytyvät www.dvv.fi/taisto.

3 Ennakkotehtävät

Kaikille harjoitteleville organisaatioille

- Varmistakaa, että organisaatiolla on tarvittavat henkilötietojen tietoturvaloukkauksiin liittyvät prosessit ja ohjeet.
- Varmistakaa, että organisaatiolla on jatkuvuuden ja varautumisen suunnitelmat ja ohjeet, joiden mukaan toimitaan siihen kohdistuvissa häiriöissä, poikkeamissa ja loukkaustilanteissa.
- Varmistakaa, että organisaatiolla on prosessi viranomaisilmoitusten (tietoturva- ja tietosuojaloukkaus) tekemiseen.
- Suosittelemme tutustumaan koulutukseen Turvaa digitaalinen toiminta häiriötilanteissa. Koulutus löytyy osoitteesta: https://www.eoppiva.fi/kurssit/turvaa-digitaalinen-toiminta-hairiotilanteissa/#/. Koulutus auttaa organisaatiota valmistautumaan harjoitukseen.

Suosittelemme varmistamaan, että organisaatiolla on kyky

- Toimia henkilötietojen tietoturvaloukkauksessa, kuten tehdä arviointi rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä.
- Toimia tilanteessa, jossa organisaation henkilötietoja on päätynyt ulkopuolisille tahoille.
- Todeta, että sen käyttämissä palveluissa on tapahtunut tietomurto ja/tai henkilötietojen tietoturvaloukkaus.
- Aloittaa tilanteen johtaminen.

- Arvioida toteutuneiden riskien suuruutta.
- Tehdä ilmoituksia viranomaisille ja rekisteröidyille.
  - tietoturvaloukkauksesta Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle.
  - rikosilmoituksesta Poliisille.
  - henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle.
  - ilmoitukset rekisteröidyille.

Kokopäivän harjoitukseen osallistuvat organisaatiot

Iltapäivän osuus alkaa sillä, että yksi organisaatiolle kriittinen henkilö siirtyy sivuun harjoituksesta. Iltapäivän harjoitusosuuden teemat keskittyvät haavoittuvuuksien ja maksuliikenteen hyväksikäyttämiseen. Suosittelemme valitsemaan henkilön näistä rooleista. Vaihtoehdot henkilön siirtymisestä ovat:

1. Henkilö siirtyy tarkkailemaan harjoitusryhmän toimintaa siitä näkökulmasta, miten toiminnot organisoidaan ja tehtävät saadaan suoritettua, kun kyseinen rooli on pois käytöstä tehtävien hoidosta. Kyseinen henkilö ei saa osallistua keskusteluun tai antaa neuvoja.
   - Onko roolin tehtävät ohjeistettu ja koulutettu riittävän hyvin, jotta tehtävät pystytään hoitamaan harjoituksessa?
   - Henkilö seuraa harjoitusryhmän toimintaa ja tekee havaintoja, jotka koskevat hänen vastuualueellaan olevia tehtäviä ja muodostaa niiden pohjalta kehittämistoimenpiteitä.
2. Henkilö vapautetaan kokonaan harjoituksesta.

Suosittelemme vaihtoehtoa yksi, jolloin organisaatio saa enemmän hyötyä harjoituksesta.

4 Harjoituspäivä

Varmistakaa hyvissä ajoin harjoituspäivän aamuna, että näyttövastaava pääsee kirjautumaan harjoitusalustalle ja pystyy jakamaan näytön organisaation harjoitusryhmälle. Tarkistakaa harjoituksen alkaessa, että harjoitusryhmään kutsutut henkilöt ovat paikalla joko organisaationne omassa virtuaalikokouksessa tai fyysisesti neuvotteluhuoneessa.

Harjoituspäivä alkaa harjoitusalustalla julkaistavalla tervehdyksillä. Lisäksi harjoitusalustalla julkaistaan Kyberturvallisuuskeskuksen, Keskusrikospoliisin ja tietosuojavaltuutetun toimiston lyhyet tietoiskut viranomaisilmoitusten tekemisestä. Harjoitusalustalla olevat uutiskatsaukset avaavat harjoituksen maailmankuvaa. Pyydämme, että organisaation harjoitusryhmä katsoo nämä huolellisesti läpi harjoituspäivän aluksi. Videoiden kokonaiskesto on noin 15 minuuttia.

Harjoituksessa mallinnetaan tilanteita, joissa on jo moni asia mennyt pieleen. Näin organisaatio voi samanaikaisesti harjoitella useampaa mahdollisesti vastaan tulevaa asiaa samanaikaisesti. Harjoituspäivä rakentuu erilaisista tapahtumista, niihin liittyvistä syötteistä ja tehtävistä. Syötteet julkaistaan aikataulun mukaisesti harjoitusalustalla. Huomaathan, että syötteistä ei laiteta erillistä sähköpostiviestiä/herätettä, vaan kaikki toiminta tapahtuu harjoitusalustalla.

Harjoituksessa käytetään ensimmäistä kertaa harjoitusalustaa harjoituksen maailmankuvaa vastaavan mediatilannekuvan välittämiseksi. Mediasyötteet näkyvät harjoitusalustanäkymän oikealla puolella, joiden alapuolella on näkyvissä kommentointilaatikko. Jos kommenttilaatikkoon lisää kommentin, se näkyy kaikille harjoitukseen osallistuville organisaatioille. Tästä syystä pyydämme, ettei kommentointilaatikkoon kirjata omia kommentteja harjoituksen aikana.

Harjoitukseen kannattaa tulla positiivisella ja avoimella mielellä. TAISTO-harjoituksen kohderyhmä on laaja, jonka takia tapahtumat ja syötteet on pyritty kuvaamaan mahdollisimman geneerisesti. Toivomme, että harjoittelijat eivät pelaa "peliä" vastaan eli etsi syötteistä virheitä, joilla tapahtumat ja syötteet voidaan ohittaa. Lisäksi harjoitustilanteessa kannattaa olla yhtä realistinen kuin tositilanteessakin, jotta organisaatio saa harjoituksesta mahdollisimman paljon irti.

Suosittelemme, että organisaatio pitää harjoituspäivänä harjoituspäiväkirjaa. Harjoituspäiväkirjaan kirjataan harjoituksessa tehdyt havainnot ja toimenpiteet. Kirjatkaa harjoituksen aikana saman tien ylös sellaisia havaintoja, jotka edellyttävät teiltä ohjeistuksen tai toimintaprosessien kehittämistä. Se auttaa organisaatiota harjoituksen jälkeen palaamaan harjoituspäivän tapahtumiin, analysoimaan omaa toimintaa harjoituksen aikana ja kokoamaan harjoituksessa esiinnousseita kehittämistoimenpiteitä. Organisaatio voi halutessaan käyttää harjoituspäivänä oman toiminnan seuraamiseen ja tehtyjen toimenpiteiden raportointiin TAISTO20-harjoituspäiväkirjaa, joka löytyy osoitteesta www.dvv.fi/taisto.

Organisaatio on tehnyt ilmoittautumisen yhteydessä valinnan harjoituspäivän pituudesta, puolipäivä tai kokopäivä, omien tarpeiden mukaisesti. Harjoituspäivän pituus määrittyy tehdyn valinnan mukaisesti, osalla harjoittelevista organisaatioista harjoitus päättyy kello 12, jonka jälkeen organisaatio suorittaa harjoituksen määritellyt jälkitoimet. Kokopäivän harjoitus jatkuu kello 12:30 ja päättyy kello 15:00, jonka jälkeen kokopäivälle osallistuvat organisaatiot suorittavat jälkitoimet. Huomatkaa, että kello 12:00 alkaa puolen tunnin tauko kokopäivän harjoitukseen osallistujille.

Harjoituspäivän kulku

9:00 Harjoituspäivä alkaa harjoitusalustalla
- Videotervehdykset ja tietoiskut
- Tapahtuma 1 ja siihen liittyvät syötteet
- Tapahtuma 2 ja siihen liittyvät syötteet
- Tapahtuma 3 ja siihen liittyvät syötteet
- Tapahtuma 4 ja siihen liittyvät syötteet

11:30 Puolenpäivän harjoitus päättyy

- Jälkitoimet puolenpäivän harjoituksen päättäneille

12:30 Kokopäivän harjoitus jatkuu
- Tapahtuma 5 ja siihen liittyvät syötteet
- Tapahtuma 6 ja siihen liittyvät syötteet
- Tapahtuma 7 ja siihen liittyvät syötteet
- Tapahtuma 8 ja siihen liittyvät syötteet

15:00 Kokopäivän harjoitus päättyy
- Jälkitoimet harjoituspäivän päättäneille

Viranomaisilmoitusten tekeminen harjoituksessa

Kaikki viranomaisilmoitukset TAISTO20-harjoituksessa tehdään harjoitusalustan kautta. Ohjeet ja linkit viranomaisilmoituksien tekemiseen löytyvät harjoitusalustalta. Toivomme organisaatioilta aktiivista otetta viranomaisilmoitusten tekemiseen TAISTO20-harjoituksessa. Huomioikaa, että viranomaisiin ei otetta yhteyttä, kuten todellisessa tilanteessa, vaan kaikki yhteydenpito harjoituksen aikana tapahtuu harjoitusalustan kautta.

Keskusrikospoliisin ja tietosuojavaltuutetun toimiston viranomaisilmoitukset tehdään TAISTO20-harjoituksessa harjoitusalustalla olevilla webropol-lomakkeilla. Lomakkeiden pohjat ovat mallinnettu oikeista viranomaisilmoituksista. Viranomaisilmoituslomakkeen täydentämisen jälkeen organisaatio saa webropol-lomakkeella tiedon kyseiseltä viranomaiselta ilmoituksen vastaanottamisesta. Siinä kerrotaan ensivaiheet siitä, miten prosessi käynnistyy kyseisellä viranomaisella. TAISTO20-harjoituksen jälkeen koontiraportit harjoituksen aikana tehdyistä viranomaisilmoituksista toimitetaan kyseiselle viranomaiselle analysoitavaksi.

Kyberturvallisuuskeskuksen osalta harjoitusalustalta löytyvä linkki ohjaa suoraan Kyberturvallisuuskeskuksen webropol-lomakkeelle, jonka kautta ilmoitukset tietoturvaloukkauksista tehdään heille. Tämä menettely mallintaa heidän harjoituspäivystystä.

5 Harjoituksen päätyttyä

Harjoituspäivän päätteeksi jokaiselta harjoittelijalta kysytään fiilis harjoituspäivästä Menti-kyselyllä. Menti-kysely löytyy osoitteesta www.menti.com. Mentissä käytettävä koodi julkaistaan harjoituspäivänä harjoitusalustalla.

Menti-kyselyn jälkeen käykää läpi päivän tapahtumat harjoitusryhmän kanssa, miten harjoitus onnistui, mikä meni hyvin ja missä on parannettavaa. Näin organisaatio saa ensivaiheen huomiot harjoituksen onnistumisesta sekä kaikkien äänet kuuluviin.

Harjoituksen jälkeen pyydetään organisaation yhteyshenkilöä, tai organisaation nimeämää henkilöä, vastaamaan Digi- ja väestötietoviraston lähettämään palaute- ja raportointikyselyyn. Palautteen ja raportoinnin tarkoitus on mitata harjoituksen onnistumista ja vaikuttavuutta sekä selkeyttää tulevien vuosien TAISTO-harjoitusten tavoitteita vastaamaan organisaatioiden tarpeisiin ja odotuksiin. Toivomme, että

organisaatiot antavat aktiivisesti palautetta harjoituksen toteutumisesta, tarvitsemme sekä positiivista että rakentavaa palautetta.

Tarkemmat ohjeet palautteen ja raportoinnin antamiseen julkaistaan ennen ensimmäistä harjoituspäivää www.dvv.fi/taisto.

Lisäksi on erityisen tärkeää, että organisaatio käy läpi harjoituksen jälkeen harjoituksen aikana tehdyt havainnot ja niiden pohjalta suunnittelee tarvittavat kehittämistoimenpiteet. Organisaatioiden tulee laatia toimenpide-ehdotuksille realistinen aikataulu, selvittää resurssitarpeet ja nimetä vastuuhenkilöt. Useimmissa organisaatioissa tämä edellyttää kehittämistoimenpiteiden hyväksymistä organisaation johtamisjärjestelmän mukaisesti.

6 Muut asiat

Tänä vuonna TAISTO20-harjoituksessa on käynnissä twiitti- ja kuvakisa. Kisa on vapaaehtoinen. Julkaiskaa twiittejä ja/tai kuvia liittyen TAISTO20-harjoitukseen sopivalla tervehdyksellä Twitterissä! Harjoituspäivän aikana julkaistujen twiittien kesken jaamme palkintoja. Muistakaa lisätä #TAISTO20 –tunniste, jotta olette kisassa mukana.

Muistattehan viestiä omassa organisaatiossanne ja esim. sosiaalisessa mediassa TAISTO20-harjoituspäivästä ja siihen osallistumisesta. Käytättehän julkaisuissa aihetunnisteena #TAISTO20 ja huomioikaa, että julkaisuista tulee käydä ilmi myös se, että kyseessä on harjoitus.

Digi- ja väestötietovirasto järjestää TAISTO20-palaute- ja harjoitustoiminnan seminaari 27.1.2021. Varaattehan päivän kalenterista. Toimitamme yhteyshenkilöille kutsun tilaisuuteen.

7 Yhteydenpito harjoituspäivänä

Harjoituspäivänä esiintyvissä harjoituksen kulkuun, tapahtumiin tai syötteisiin liittyvissä ongelmatilanteissa ota välittömästi yhteyttä sähköpostilla digiturva@dvv.fi , otsikolla **TAISTO20-harjoitus: 29.10. / 12.11. / 19.11. ongelmatilanne harjoituksessa.**

Jos kyseessä on harjoitusalustaan liittyvä tekninen ongelma harjoituspäivän aikana laita välittömästi sähköpostia osoitteeseen digiturva@dvv.fi otsikolla: **TAISTO20-harjoitus: Tekninen häiriö harjoitusalustalla.**

Lisätietoa TAISTO20-harjoituksesta löytyy osoitteesta https://dvv.fi/taisto tai voit kysyä sähköpostilla osoitteesta digiturva@dvv.fi.