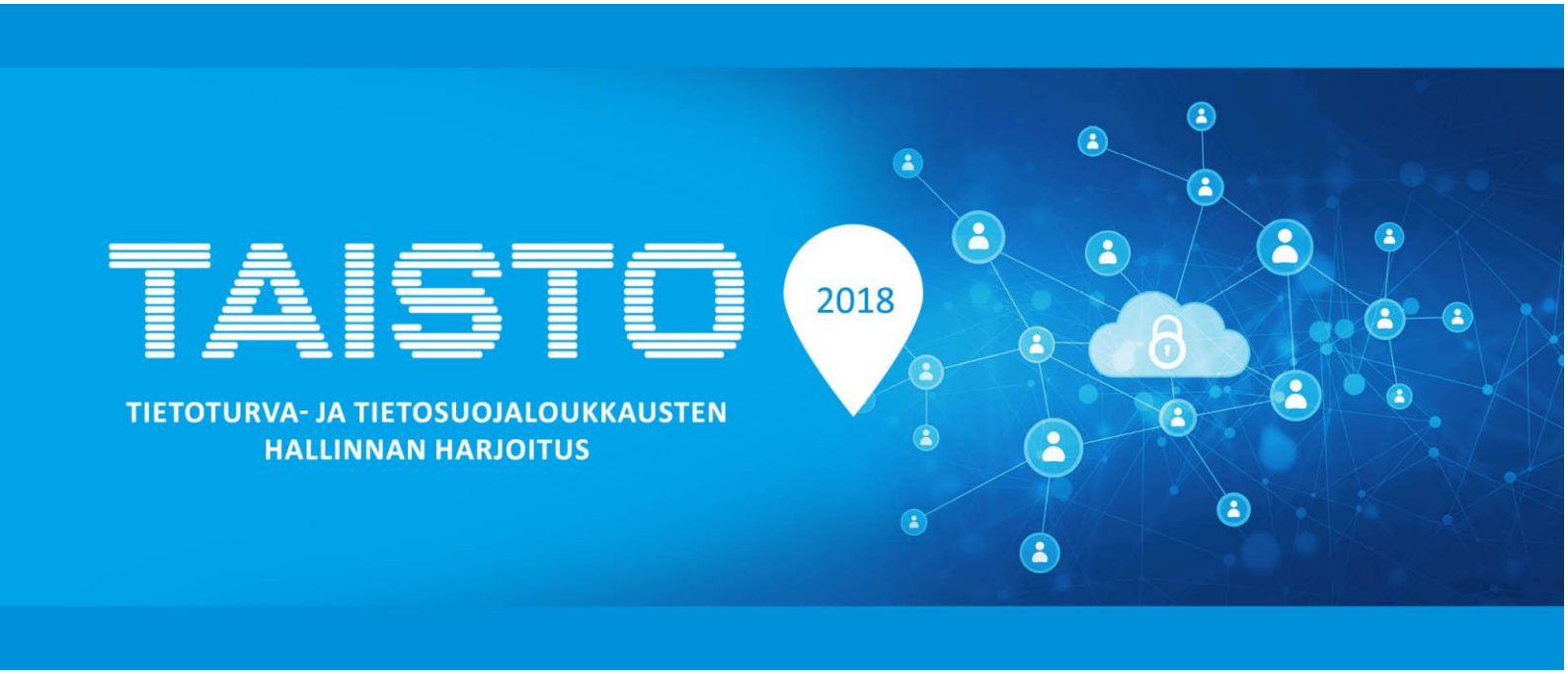

TAISTO18-HARJOITUSKÄSIKIRJA - PÄIVITETTY VERSIO 1.02

Ohjeita TAISTO18 -harjoitukseen valmistautuville organisaatioille

Väestörekisterikeskus

Väestörekisterikeskus

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

DOKUMENTINHALLINTA

Omistaja	Kimmo Rousku
Laatinut	Kimmo Rousku
Tarkastanut	Juhta- ja VAHTI-asiantuntijaryhmät
Hyväksynyt	21.8.2018 Kirsi Janhunen, Juha Kirves, Hanna Heikkinen

VERSION HALLINTA

versionro	mitä tehty	pvm/henkilö
0.72	Luonnosversio	2.8.2018 KR
0.75	Ensimmäisen kommentointikierroksen perusteella päivitetty versio laajemmalle kommentointikierrokselle	9.8.2018 KR
1.00	TAISTO18-harjoitukseen osallistuville organisaatioille tarkoitettu harjoituskäsikirja	21.8.2018 KR
1.02	Lisätty Liite 2 – päivitettyjä ohjeita harjoitukseen liittyen	18.10.2018 KR

Palvelut | Digitalisaatio ja digitaalinen turvallisuus 16.10.2018
Rousku Kimmo

Sisällysluettelo

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

TAISTO 2018
TIETOTURVA- JA TIETOSUOJALOUKKAUSTEN HALLINNAN HARJOITUS

TAISTO18-HARJOITUSKÄSIKIRJA - PÄIVITETTY VERSIO 1.02

Tämän käsikirjan tarkoituksena on valmentaa julkishallinnonorganisaatioita valmistautumaan TAISTO18-harjoitukseen. Käsikirjassa kerrotaan harjoituksesta yleisesti sekä opastetaan, miten keskeiset prosessit täyttävät niin tietoturvallisuudelta kuin tietosuojalta edellytettävät vaatimukset. Käsikirjassa kerrotaan myös, miten organisaation tulisi hyödyntää harjoituksen oppeja sekä kuinka jokainen organisaatio voi antaa palautetta harjoituksesta, sekä kuinka se tulee itse saamaan palautetta harjoituksen aikaisesta toiminnasta.

Toivomme, että tätä asiakirjaa ei julkaista avoimesti netissä ennen marraskuun harjoituskuukauden päättymistä, jonka jälkeen julkaisemme kaiken harjoitusmateriaalin yleisesti kaikkien saataville.

1 Taustalla valtiovarainministeriön yhteishankkeet tietosuojan- ja tietoturvallisuuden kehittämiseksi

Valtiovarainministeriön asettamat julkisen hallinnon tietohallinnon neuvottelukunta (Juhta) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) järjestävät 2017 – 2018 kaksi yhteishanketta, joiden tarkoitus on kehittää julkisen hallinnon organisaatioiden tietosuojaa sekä tietoturvallisuutta.

Yhteishankkeeseen osallistumalla organisaatio saa hyvät valmiudet muuttuvan tietosuojalainsäädännön edellyttämiin muutoksiin. Yhteishankkeissa on tuotettu tietosuojakoulutusvideoita, nettitestejä ja järjestetty työpajatilaisuuksia. Työpajoissa on käsitelty tietosuoja-asetuksen eri osa-alueita, riskienhallintaa ja tietoturvallisuutta julkishallinnon näkökulmasta. Tarkempaa tietoa pidetyistä ja tulevista työpajoista sekä niiden materiaalit ovat tietosuojanyhteishankkeiden verkkosivulla vm.fi:ssä (http://vm.fi/tietosuojan-yhteishankkeet). Tietosuojaan liittyvät koulutusvideot löytyvät osoitteesta http://www.arjentietosuoja.fi. Materiaalit ja tilaisuudet ovat maksuttomia.

1.1 Loppuvuoden työpajat

Loppuvuoden 2018 aikana toteutetaan vielä kaksi työpajaa, jotka järjestetään:

20.11.2018 VM Nh Paja tai verkkolähetys
4.12.2018 Yhteishankkeen päätöstilaisuus pidetään Säätytalolla

Jokaisessa näistä tilaisuuksista kerrotaan TAISTO18-harjoituksen valmistelun etenemisestä sekä annetaan vinkkejä harjoitukseen valmistautumiseen.

Tämän lisäksi kerromme yleisesti harjoittelun tärkeydestä osana tietoturvallisuuden ja tietosuojan kehittämistä VAHTI-kesäseminaarissa 31.8. Seminaariin voi osallistua paikan päälle tai sitä voi seurata netistä ilmoittautumalla osoitteessa:

https://www.webropolsurveys.com/S/D78A6C995180738 1.par
- voit myös katsoa tilaisuuden verkkotallenteen jälkikäteen

Mikäli julkisen hallinnon organisaatiosi ei ole ilmoittautunut osallistuvansa työpajoihin, se on edelleen mahdollista osoitteessa:
https://www.lyyti.fi/questions/46d441ee05

Mikäli yksittäinen asiantuntija haluaa saada lisätietoa tulevista työpajoista ja osallistua niiden seuraamiseen nettilähetyksen avulla, toivomme myös tästä ilmoittautumista:
https://www.lyyti.fi/questions/f243109a0d

Kaikki yhteishankkeissa tuotettu materiaali löytyy osoitteesta:
https://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

- jokaisesta työpajatilaisuudesta löytyy videotallenne sekä tilaisuudessa läpikäydyt esitysmateriaalit ja mahdolliset harjoitustehtävät

- lisäksi sivustolla on paljon muita hyödyllisiä työkaluja, joita suosittelemme jokaista TAISTO18-harjoitukseen osallistuvaa organisaatiota soveltamaan omassa toiminnassaan.

1.2 Ajankohtaiskatsaukset

Näiden lisäksi Valtiovarainministeriö toteuttaa vuonna 2018 kolme ajankohtaiskatsausta digitaalisen turvallisuuden eri osa-alueista yhteistyössä Turvallisuuskomitean, Viestintäviraston Kyberturvallisuuskeskuksen, tietosuojavaltuutetun toimiston sekä Väestörekisterikeskuksen kanssa.

Ajankohtaiskatsausten ideana on koota ajankohtaista tietoa digiturvallisuuden eri osa-alueista niin, että hallinnon henkilöstö voi hyödyntää sitä työssään. Jokainen katsaus sisältää useita videoita eri kohderyhmille, esimerkiksi henkilöstölle, ICT- ja tietoturva- sekä tietosuojahenkilöille sekä organisaation johdolle. Organisaatio voi itse päättää miten se jakelee ja hyödyntää julkaistavia videoita.

Nämä videoblogit ovat vapaasti kaikkien katseltavissa:
https://vm.fi/digiturva

Toukokuussa julkaistussa katsauksessa on kaksi videota liittyen TAISTO18-harjoitukseen:

Miksi ja miten organisaatio voi osallistua henkilötietojen tietoturvaloukkausten hallintaa edistävään TAISTO18-harjoitukseen?

Miksi organisaatiollesi on tärkeää osallistua TAISTO18-harjoitukseen?

1.3 Ketkä vastaavat harjoituksen toteuttamisesta

Harjoituksen operatiivisena toteuttajana toimii Väestörekisterikeskus. Harjoituksen suunnittelussa sekä harjoituspäivien toteuttamisessa ovat mukana myös Poliisi, tietosuojavaltuutetun toimisto, Valtion tieto- ja viestintätekniikkakeskus (Valtori) sekä Viestintäviraston Kyberturvallisuuskeskus ja Kuntaliitto.

Lisätietoa harjoituksesta antaa:

VAHTI-pääsihteeri Kimmo Rousku, puh. 029553 5120, kimmo.rousku@vrk.fi

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

2 Kenelle harjoitus on tarkoitettu?

Harjoitus on tarkoitettu kaikille julkishallinnon organisaatioille. Harjoitukseen voi osallistua myös sellaiset toimijat, jotka valtionhallinnon tai muu julkisen hallinnon organisaatio omistaa 100-prosenttisesti. Tällainen voi olla esimerkiksi kunnan omistama yritys, joka toimii organisaation sellaisena palvelutuottajana, jonka tulee tällaiseen harjoitukseen osallistua.

Harjoitus ei ole tarkoitettu tässä vaiheessa yrityksille. Sen sijaan kaikki keskeiset harjoitukseen liittyvät materiaalit tullaan jakamaan avoimesti joulukuussa 2018 siten, että jokainen organisaatio voi halutessaan toteuttaa itsenäisesti vastaavanlaisen harjoituksen julkaistun materiaalin perusteella. Materiaali julkaistaan TAISTO18-harjoituksen nettisivustolla ja siitä tiedotetaan erikseen.

3 Mitä harjoituksessa harjoitellaan?

Tässä harjoituksessa emme anna suoraan vinkkejä tai tulkintaohjeita siitä, tapahtuuko harjoituksessa tietoturva- tai henkilötietojen tietoturvaloukkaus vaan se on harjoitukseen osallistuvien organisaatioiden arvioitava.

Harjoituksessa harjoitellaan kahta keskeistä, jokaisen organisaation toimintaan liittyvää kokonaisuutta:

1) tietoturvallisuuden hallinta
    - miten organisaation on toteuttanut kulunvalvonnan sen toimitiloihin, jotta sellaisiin tiloihin, joissa käsitellään salassa pidettäviä tietoja, ei ulkopuolisilla ole pääsyä
    - miten varmistetaan, että esimerkiksi ICT-palveluissa ja käytettävissä päätelaitteissa (esimerkiksi tietokoneet, tabletit, älypuhelimet) on huolehdittu tarvittavista tietoturvapäivityksistä, jotta tietoturvahaavoittuvuuksien hyödyntäminen ei ole helppoa
    - miten toimitaan, jos nousee epäilys siitä, että organisaation (salassa pidettäviä) tietoja on päätynyt ulkopuolisille tahoille, esimerkiksi tietomurron johdosta
        - mahdollisesti tarvittava yhteydenpito organisaation ICT-palveluita tuottavaan toimittajaan
        - ICT-palvelutoimittajan tällöin suorittamat toimenpiteet
        - muu tällaisessa tilanteessa edellytettävä johtaminen
2) tietosuoja-asetuksen mukainen toiminta henkilötietojen tietoturvaloukkauksessa
    - onko tehty arviointia rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä?

- miten organisaatiossa toimitaan, jos käy ilmi, että organisaation henkilötietoja on päätynyt ulkopuolisille taholle
- mikäli organisaatio toteaa, että sen käyttämissä palveluissa on tapahtunut tietomurto ja/tai henkilötietojen tietoturvaloukkaus, miten tällöin toimitaan?
    - miten tilannetta johdetaan?
    - miten organisaatio arvioi, onko henkilötietojen tietoturvaloukkauksesta muodostunut riskiä rekisteröityjen oikeuksiin ja vapauksiin?
    - miten organisaatio arvioi edellä mainitun riskin suuruuden?
    - kuinka tämän mahdolliset ilmoitukset viranomaisille ja rekisteröidyille toteutetaan, esimerkiksi
        - tietoturvaloukkausten osalta Viestintäviraston Kyberturvallisuuskeskukselle
        - rikosilmoituksen osalta Poliisille
        - henkilötietojen tietoturvaloukkausten osalta tietosuojavaltuutetun toimistolle
        - sekä mahdollisesti rekisteröidyille tehtävät ilmoitukset
    - miten organisaatio viestii mahdollisesti tapahtuneesta tietoturva- tai henkilötietojen tietoturvaloukkauksesta organisaation sisällä, asiakkaille, muille sidosryhmille ja mediaan?

Harjoituksessa on pääpaino henkilötietojen tietoturvaloukkauksiin liittyvissä prosesseissa ja toiminnassa, mutta tätä edeltää tilanteeseen johtava tietoturvaloukkaus.

Edellä on kuvattu keskeisimmät harjoituspäivän aikana nousevat asiat, joihin organisaation tulee valmistautua. Organisaatio voi myös laajentaa tai muuten lisätä harjoituspäivään muita sellaisia asioita, joiden toteutumista se haluaa harjoituksessa arvioida.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

4 Miten harjoitukseen tulee valmistautua?

Edellisessä luvussa on kuvattu niitä asioita, joihin harjoituspäivän aikana tulee varautua. Käytännössä tämä tarkoittaa sitä, että organisaatiolla tulisi olla ohjeistus / sopimus / prosessi esimerkiksi seuraavista asioita:

1) Miten toimitaan, jos organisaatiossa havaitaan tai sille ilmoitetaan tietoturvaloukkauksesta, esimerkiksi tietomurrosta sen järjestelmään?
    - Miten organisaatio on sopinut ja miten voidaan valvoa, että sille ICT-palveluita tuottavat toimittajat huolehtivat tietoturvapäivitysten jakelusta organisaation käytössä oleviin tai sen omistamiin palveluihin ja sen henkilöstön käytössä oleviin päätelaitteisiin?
    - onko organisaation nettisivuilla ja intranetissä ohjeet siitä, miten sille voidaan ilmoittaa mahdollisista tietoturvapoikkeama-epäilyistä? Miten näiden ilmoitusten käsittely on vastuutettu, myös loma-aikoina?
2) Miten tulee toimia, jos organisaatiossa havaitaan tai sille ilmoitetaan henkilötietojen tietoturvaloukkauksesta?
    - Miten selvitetään ja voidaan varmistua tiedon laadusta ja alkuperästä?
    - Mikäli voidaan varmista, että on tapahtunut henkilötietojen tietoturvaloukkaus, millainen ohjeistus ja prosessi sillä on tällaisessa tilanteessa toimimiseen?
    - Miten organisaatio arvioi rekisteröityyn tällaisessa tilanteessa kohdistuvat uhat?
    - Onko organisaatiossa valmiina ohjeet mahdollisten viranomaisille tehtävien ilmoitusten sekä niiden rekisteröityjen tavoittamiseksi, joita on tarpeen informoida?
    - Millaisia, turvallisia välineitä käytetään esimerkiksi rekisteröidyille suunnatussa viestinnässä?
    - Miten tapahtuman aiheuttanut poikkeama, esimerkiksi tietoturvaloukkaus saadaan korjattua ja estettyä sen toistumasta?
3) Yleistä tietoturvallisuuden ja tietosuojan kehittämisessä ja ylläpitämisessä huomioitavaa
    - Onko organisaatiolla voimassa oleva, ajan tasalla oleva ohjeistus toimitilaturvallisuuden osalta esimerkiksi vieraiden vastaanottamisesta ja pääsystä sen toimitiloihin? Milloin ohjeistus ja toimintamalli on läpikäyty tätä palvelua tuottavan alihankkijan tai/ja organisaation oman henkilöstön kanssa
    - Onko organisaatiolla voimassa olevat sopimukset sisältäen sovitut toimenpiteet henkilötietojen ja salassa pidettävien tietojen käsittelyn osalta niiden alihankkijoiden tai henkilötietojen käsittelijöiden kanssa, jotka näitä käsittelevät?

- Miten organisaatio on velvoittanut sille palveluita tuottavat alihankkijat ilmoittamaan mahdollisista tietoturvapoikkeamista tai henkilötietojen tietoturvaloukkauksista?
- Onko organisaatio ohjeistanut, missä tilanteissa ja keneltä edellytetään minkä tasoista henkilöturvallisuusselvitystä?

4.1 Mistä edellisiin löytyy lisätietoa?

Edellä kuvattuja asioita on läpikäyty useammassa Juhta/VAHTI-hankkeiden työpajoissa, joista keskeisimpiä ovat:

Riskienhallinta	– työpajat #2 #3 #4 sekä
Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta	- työpajat #6 #7
Viestintä häiriö- ja kriisitilanteissa	- työpaja #12

Lisäksi:

Tietosuoja-asetus, artiklat 32–34 sekä lisäksi johdanto-osan kohdat 83, 85–88

https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Näiden ohella tietosuojavaltuutetun toimiston sivustolla on hyödyllisiä ohjeita:

https://tietosuoja.fi/etusivu

Riskien arviointi osana henkilötietojen käsittelyä
https://tietosuoja.fi/arvioi-riskit

- sivun alaisuudesta löytyy kohta Vaikutustenarviointi, jossa on mm. kriteerit korkean riskin arvioimiseksi

https://tietosuoja.fi/vaikutustenarviointi

Ohjeita koskien tietoturvaloukkausta
https://tietosuoja.fi/tietoturvaloukkaukset

Muita materiaaleja:

- VM –julkaisu 22/2017 Ohje riskienhallintaan
  Riskienhallintatyökalu - Excel - perusversio
  Riskienhallintatyökalu - Excel - laajempi versio
  Ohje riskienhallintatyökaluun

8/2017 Tietoturvapoikkeamatilanteiden hallinta

Palvelut | Digitalisaatio ja digitaalinen turvallisuus 16.10.2018
Rousku Kimmo

Ohjeita koskien henkilöturvallisuusselvitysten tekemiseen

http://www.supo.fi/turvallisuusselvitykset/henkiloturvallisuusselvitys

4.2 Kenen tulisi osallistua harjoitukseen organisaatiosta?

Koska kyseessä on tietoturva- ja henkilötietojen tietoturvaloukkaustilanteiden hallinnan harjoitus, edellyttää tämä seuraavien roolien mukaisten henkilöiden osallistumista harjoituspäivään ja myös ennakolta siihen valmistautumiseen

Johdon edustaja

- koska on mahdollista, että harjoituspäivän aikana tilanne eskaloituu sellaiseksi, että se vaatii johdon edustajalta päätöksiä ja/tai asian viemistä myös organisaation ylimmän johdon tietoon, johdon edustaja tulee olla tavoitettavissa harjoituspäivän aikana ainakin sähköisesti
    - tulemme tarjoamaan mahdollisuuden harjoituksessa harjoitella kriisiviestintää median suuntaan, julkaisemme videon, jossa median edustaja esittää organisaation (johdon tai muun sovitun tahon) edustajalle sellaisia kiperiä kysymyksiä, joita tällaisessa tilanteessa voi kuvitella esitettävän

Tietoturvallisuuden vastuuhenkilö(t)

- vastuuhenkilöä tarvitaan niissä tilanteissa, joissa organisaatio toteaa, että kyseessä on tietoturvaloukkaus tai tietoturvapoikkeama. Vastuuhenkilön tehtävänä on tällöin huolehtia tämän tilanteen hoitamisesta olemassa olevien ohjeiden ja prosessien mukaisesti

Tietosuojavastaava(t)

- vastuuhenkilöä tarvitaan niissä tilanteissa, joissa organisaatio toteaa, että kyseessä on henkilötietojen tietoturvaloukkaus. Vastuuhenkilön tehtävänä on tällöin huolehtia tämän tilanteen hoitamisesta olemassa olevien ohjeiden ja prosessien mukaisesti

Viestintä-asiantuntija

- viestintä-asiantuntijaa tarvitaan siinä vaiheessa, kun organisaatio toteaa, että joko/tai on tapahtunut sellainen tietoturvapoikkeama | henkilötietojen tietoturvaloukkaus, jossa organisaation tulee viestiä eri ryhmille

ICT-asiantuntija

- harjoitus liittyy vahvasti organisaation käytössä oleviin tai myös sen tuottamiin ICT-palveluihin ja sen henkilöstön käytössä oleviin päätelaitteisiin, joten harjoituksessa tarvitaan henkilöä, jolla on tieto siitä, miten näitä palveluita organisaatiolle tuotetaan tai hän tietää ne henkilöt, jotka näistä asioista vastaavat

Edellisen lisäksi harjoitukseen on mahdollista ottaa mukaan myös muita henkilöitä / rooleja. Eräs suositeltava rooli on harjoituksen ulkopuolinen tarkkailija, joka voisi kirjata ylös havaintoja harjoituspäivän aikana. Tällöin niiden kirjaaminen ei olisi varsinaisten harjoitukseen osallistuvien

henkilöiden tehtävä. Harjoituksen jälkeen organisaation olisi mahdollista tehokkaasti tunnistaa ja kehittää omaa toimintaa näiden havaintojen perusteella.

4.3 Käytännön vinkkejä onnistuneen harjoituspäivän ja harjoituksen toteuttamiseksi

Varaa harjoituspäivää varten sellainen tila, jossa siihen osallistuvat henkilöt voivat rauhassa kokoontua. Varmista, että ne henkilöt jotka eivät osallistu harjoitukseen paikan päälle fyysisesti, ovat yhteydessä ryhmään tarvittavia viestintävälineitä käyttäen. Varaa myös harjoituspäivään osallistuvien henkilöiden kalentereista kyseinen ajankohta.

Kokoontukaa mielellään vähintään kaksi kertaa ennen harjoitusta, käykää läpi tämä harjoituskäsikirja, varmistakaa että olette lukeneet ja ymmärtäneet tässä käsikirjassa käsitellyt asiat.

Tarkistakaa, että teillä on olemassa toimintaohjeet (prosessit) aikaisemmin tässä luvussa kuvattuja tilanteita varten.

Tarkistakaa, että teillä on tarvittavat yhteystiedot esimerkiksi kriittisten ICT-palvelutuottajien tukipalveluihin sekä kirjattuna ja ohjeistettuna muun muassa seuraavat linkit ja ilmoituskanavat:

- Viestintäviraston Kyberturvallisuuskeskus – ilmoitus tietoturvapoikkeamasta

  https://www.viestintavirasto.fi/asioikanssamme/ilmoituksetjamuutlomakkeet/tietoturvailmoituksetja-hakemukset/ilmoitustietoturvaloukkauksesta.html

- Tietosuojavaltuutetun toimisto – ilmoitus henkilötietojen tietoturvaloukkauksesta

  https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

- Poliisi – rikosilmoitus

  https://www.poliisi.fi/rikokset/sahkoinen_rikosilmoitus

Suosittelemme tutustumaan näihin ilmoitussivustoihin ennakolta ja etenkin varmistamaan, että organisaatio on käynyt läpi niissä olevat tarvittavat tiedot.

Vastatkaa huolella harjoitukseen liittyviin raportointipisteisiin, joissa organisaatio vastaa, kuinka se on toiminut harjoituksessa esille nousseisiin tilanteisiin.

Kirjatkaa päivän aikana ylös saman tien sellaisia havaintoja, jotka edellyttävät teiltä ohjeistuksen tai toimintaprosessin kehittämistä.

Sopikaa mielellään muutaman päivän sisälle harjoitukseen osallistuneen ryhmän kokous, jossa tarkastelette harjoituspäivää ja käytte läpi keskeiset havainnot harjoitukseen liittyen sekä sovitte, miten harjoituspäivän aikana tehtyjä havaintoja johdetaan toiminnan kehittämiseksi.

Kirjatkaa keskeiset tapahtumat ja toimenpiteet erilliseen harjoituslokiin. Lokista on malli liitteessä 1.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus 16.10.2018
Rousku Kimmo

5 Miten harjoitus tulee käytännössä etenemään?

Organisaatio osallistuu harjoitukseen sinä päivänä, jonka se on ilmoittautuessaan valinnut eli joko 7.11. | 15.11. | 22.11. tai 27.11. Päivämäärää on mahdollista muuttaa vielä lokakuun loppuun saakka. Toimitamme jokaiselle kyseiseen päivään osallistuneelle organisaatiolle muistutusviestin viikkoa ja vielä päivää ennen harjoitusta.

5.1 Harjoituspäivän aikataulu sekä käytettävät palvelut

Alustava aikataulu harjoituspäivän osalta on seuraava:

9.00 Harjoitus käynnistyy

Ensimmäinen, mahdollisesti toimenpiteitä edellyttävä tapahtuma - organisaatio saa ensimmäisen harjoitukseen liittyvän sähköpostiviestin

9.30 Toinen, mahdollisesti toimenpiteitä edellyttävä tapahtuma

9.45 Kolmas, mahdollisesti toimenpiteitä edellyttävä tapahtuma

11.00 – 12.00 Raportointipiste 1 – organisaatio täyttää sähköisen kyselyn, jossa kysytään aamupäivän tapahtumiin liittyviä kysymyksiä siltä osin, miten organisaatio on niissä toiminut

12.30 Neljäs, mahdollisesti toimenpiteitä edellyttävä tapahtuma

13.45 Viides, mahdollisesti toimenpiteitä edellyttävä tapahtuma

14.00 Kuudes, mahdollisesti toimenpiteitä edellyttävä tapahtuma

15.00 – 16.00 Raportointipiste 2 – organisaatio täyttää sähköisen kyselyn, jossa kysytään iltapäivän tapahtumiin liittyviä kysymyksiä siltä osin, miten organisaatio on niissä toiminut

15.45 Harjoituksen organisaation oma debriefing-tilaisuus, sen jälkeen, kun raportointipisteen vastaukset on lähetetty. Tässä kokouksessa on tarkoitus läpikäydä päivän aikana kerätyt havainnot niiden ollessa tuoreessa muistissa.

16.30 Harjoitus päättyy

Harjoituksessa käytetään neljää erilaista palvelua, joiden avulla harjoituspäivä toteutetaan. Yksittäinen harjoituspäivä on pyritty toteuttamaan siten, että se voidaan toteuttaa vaikka yksittäisessä palvelussa esiintyisi satunnainen tekninen häiriö.

5.2 Sähköposti

Sähköpostia käytetään ennen harjoitusta yleisesti TAISTO18-harjoitukseen liittyvään viestintään. Lähetämme viestejä joko kaikille osallistujaorganisaatioiden edustajille tai kohdistetummin yksittäiseen harjoituspäivään osallistuville.

Harjoituspäivä lähtee liikkeelle siitä, että osallistujaorganisaation yhteyshenkilö ja mahdollisesti muuhun määritettyyn osoitteeseen (esimerkiksi tarkoitusta varten perustettu jakelulista) tulee ensimmäinen sähköpostiviesti, joka käynnistää harjoituksen.

5.3 Taisto-harjoituksen www-palvelu

Harjoitusta varten on perustettu oma www-sivusto Väestörekisterikeskuksen www-palvelun alaisuuteen. Sivuston tarkoitus on

- toimia yleisenä harjoitukseen liittyvänä tiedotus- ja viestintäkanavana, myös muille kuin harjoitukseen osallistuville organisaatioille
- harjoituspäivän aikana sivustolla julkaistaan vastaavat harjoitukseen liittyvät syötteet, jotka organisaatio saa sähköpostitse. Lisäksi sivustolla toimii erillinen TAISTO-TV, joka tulee lähettämään harjoituspäivän aikana ajankohtaishaastatteluita sekä muita videoita harjoituspäivään liittyen
- marraskuun harjoituskuukauden jälkeen sivustolla julkaistaan harjoituksissa käytetty materiaali avoimesti siten, että jos joku julkishallinnon organisaatio, tai yritys tai muu yhteisö joka ei ole voinut harjoitukseen osallistua, pystyy sen toteuttamaan itsenäisesti harjoituksen jälkeen.

Toimitamme sivuston osoitteen kaikille organisaatioille lokakuun aikana, jotta organisaatiot voivat tutustua sivustolla olevaan materiaaliin. Sivustolla ei julkaista mitään sellaista tietoa tai materiaalia, jota organisaatio ei tule saamaan muuten ennen harjoitusta, sivusto toimii enemmän yleisenä tiedottamiskanavana ja aktivoituu varsinaisesti vasta harjoituspäivänä.

5.4 Skype-kokous

Harjoituspäivän ajaksi Väestörekisterikeskus perustaa Skype-kokouksen, johon kutsutaan organisaation harjoituksen yhteyshenkilö. Skype-kanava toimii harjoituksen teknisenä yhteydenpitokanavana. Skype-kokouksessa voi kysyä esimerkiksi syötteisiin, organisaatiolta edellytettävään raportointiin tai muihin harjoituksen hallinnollisiin ja teknisiin asioihin liittyviä kysymyksiä. Skype-kanavalla päivystää Väestörekisterikeskuksen harjoitukseen osallistuva valmisteluryhmän jäsen, joka voi tarvittaessa kysyä lisätietoja vastaukseen muulta valmisteluryhmältä.

Toivomme, että kanavaa ei käytetä kysymyksiin liittyen siihen, miten organisaation tulisi toimia tai miten heidän tulisi tulkita esimerkiksi syötteissä olevia tietoja – tämä on juuri harjoituksen yksi keskeinen tarkoitus; organisaatio arvioi ja tulkitsee sekä toimii itsenäisesti harjoituksessa käyttäen sen omia asiantuntijoita hyödyntäen laadittuja ohjeita sekä toimintaprosesseja.

5.5 Deltagon D-forms-lomakealusta

Tulemme keräämään harjoituspäivänä ja viikon päästä sen jälkeen organisaatiolta tietoa harjoituksen etenemisestä. Käytämme tässä Valtion tieto- ja viestintätekniikkakeskuksen (Valtori) tuottamaa Deltagon D-forms lomakealustaa, joka toimii osana valtionhallinnon yhteistä sähköposti/viestintäratkaisua. Palvelu mahdollistaa salassa pidettävän tiedon käsittelyn turvallisesti

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

Harjoituspäivän aikana organisaatio saa kaksi kyselyä (linkkiä lomakkeisiin) liittyen harjoituspäivän aikana organisaatiolle lähetettyihin syötteisiin (harjoitustapahtumiin). Organisaatio vastaa lomakkeella oleviin kysymyksiin sen mukaisesti, miten se on toiminut harjoitustehtävään liittyvissä asioissa. Kysymykset ovat pääosin erilaisia valmiita valintakysymyksiä, mutta näiden lisäksi on mahdollista antaa myös avovastauksia.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

6 Mitä organisaation kannattaa tehdä harjoituksen jälkeen

Jokaisessa harjoituksessa tulee olla selkeä päämäärä ja tavoite. TAISTO18-harjoituksessa se on ollut tietoturvan ja tietosuojan osalta harjoitella ja arvioida organisaation tietoturva- ja henkilötietojen tietoturvaloukkaustilanteissa tarvittavia prosesseja sekä tämän perusteella tehdä tarvittavia kehittämistoimenpiteitä prosessien osalta.

Mikäli organisaatio on tämän käsikirjan mukaisesti kerännyt harjoituksen aikana a) nopeasti ja helposti parannettavia asioita ja b) pitemmän ajan vaativia kehittämiskohteita, nämä tulisi käydä läpi ja kuvata tarkemmin. Samassa yhteydessä niille tulisi laatia realistinen aikataulu, selvittää kehittämisen edellyttämät resurssitarpeet ja vastuuttaa nämä. Tämä edellyttää useissa organisaatioissa kehittämistoimenpiteiden hyväksymistä organisaation johtamisjärjestelmän mukaisesti.

Organisaatio tulee saamaan vuoden 2018 loppuun mennessä kirjallisen palautteen liittyen sen antamiin vastauksiin harjoituspäivän aikana ja myöhemmin palautekyselyssä sen antamien vastausten pohjalta. Tämä raportti toimii myös yhtenä työkaluna, jonka avulla organisaation tulisi kehittää sen toimintaa tietoturva- ja henkilötietojen tietoturvaloukkausten osalta.

Valtiovarainministeriö tekee myöhemmin vuoden 2019 aikana uuden kyselyn, jonka avulla halutaan selvittää harjoituksen vaikuttavuutta sekä organisaation tunnistamien kehittämiskohteiden kehittämisen etenemistä.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

7 Palautteen antaminen sekä palauteseminaari 23.1.2019

TAISTO18 on ensimmäinen näin laajasti koko julkiseen hallintoon suunnattu harjoitus. Toivomme, että organisaatio osallistuu aktiivisesti palautteen antamiseen harjoituksen toteutumisesta, sekä positiivista että rakentavaa palautetta. Valtiovarainministeriö kerää harjoituksesta palautetta harjoituksen jälkeen palautekyselyllä, muun muassa näiden kyselyiden perusteella saadun palautteen perusteella tehdään päätös, miten jatkossa tällaisia harjoituksia on tarkoitus toteuttaa.

Harjoituksen palauteseminaari järjestetään 23.1.2019 valtiovarainministeriön auditoriossa (Nh Paja). Organisaatioiden yhteyshenkilöt saavat kutsun tähän tilaisuuteen erikseen loppuvuoden aikana. Seminaarissa käydään läpi sekä harjoituksen yleinen eteneminen, mutta samalla nostetaan esille niitä kehittämiskohteita, joita organisaatiokohtaisen raportoinnin perusteella on pystytty tunnistamaan. Näihin kehittämiskohteisiin liittyen pyrimme tarjoamaan ratkaisuja, joiden avulla organisaatiot pystyivät niiden osalta kehittämään toimintaa. Lisäksi tilaisuudessa annetaan tunnustuspalkintoja eri kategorioissa harjoitukseen osallistuneille organisaatioille. Tilaisuuteen voi osallistua paikan päällä tai sitä on mahdollista seurata myös verkon välityksellä.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

8 Liitteet

8.1 Liite 1. Harjoitusloki

Kirjatkaa harjoituslokiin päivän aikana tehdyt kaikki sellaiset keskeiset tapahtumat ja havainnot, jotka edellyttävät toimenpiteitä tai päätöksiä. Sopikaa ennen harjoittelun alkua, kuka vastaa harjoituslokiin vietävien asioiden kirjaamisesta.

Organisaatio		
Tapahtuma/havainto	Aika (pvä, klo) sekä kirjaaja (esimerkiksi nimikirjaimet)	Toimenpiteet/päätökset

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

8.2 Liite 2. Päivitetty ohjeistus koskien harjoitukseen valmistautumiseen ja itse harjoituspäivään liittyen

Yleistä

Pääpaino harjoituksessa on organisaation omien prosessien, ohjeiden ja toimintamallien kehittäminen. Harjoituspäivänä mallinnetaan tilanne, jossa on jo monta asiaa mennyt pieleen. Näin mahdollistetaan se, että organisaatio voi harjoitella useampaa oikeissa tilanteissa mahdollisesti vastaan tulevaa asiaa.

Ennen harjoitusta

- Varmistakaa, että käytössänne on harjoitusta varten sopiva kokoustila tai muu tilanteen johtamisen, toteuttamisen ja seurannan mahdollistava tila (ns. tilannehuone).
- Varatkaa tilaan harjoitusta varten yksi esitystietokone, joka pelkästään näyttää harjoituksessa julkaistavaa www-sivustoa videoprojektorilla tai riittävän isolle monitorille. Sivustolle tulee päivän aikana harjoituspäivään liittyvää tukimateriaalia ja videoita.
- Varatkaa organisaatiostanne harjoituspäivään yksi varsinaisen harjoituksen ulkopuolella toimiva henkilö, jonka tehtävä on kirjata ylös harjoituspäivän tapahtumia. Tällöin harjoitukseen osallistuvat asiantuntijat voivat keskittyä itse harjoitukseen eikä heidän tarvitse samalla kirjata ylös havaintoja. Tarkkailijan ei tarvitse olla tämän osa-alueen asiantuntija. Harjoitukseen osallistuvat asiantuntijat voivat tarkkailijalle ilmoittaa, mitä asioita missäkin vaiheessa tulee kirjata ylös. Mikäli tarkkailijalla on aiheen asiantuntemusta, voi hän lisäksi kirjata ylös omia havaintojaan ja kehittämisideoita.

Harjoituspäivänä

- Organisaatio saa syötteet jakelulistalle tai yhteispostilaatikkoon, jossa on useampia vastaanottajia. Tällä tavalla organisaation harjoitus ei esty edes mahdollisten vikatilanteiden ja akuuttien poissaolojen vuoksi.
- Jokaisen organisaation tulee ennakolta sopia, ja varmistaa harjoituspäivän aamulla, kuka organisaatiossa vastaa syötteiden lukemisesta ja sen perusteella niiden jakelusta organisaation harjoitusryhmälle. Tämän henkilön pitää olla mukana harjoituksessa.
- Varmistakaa, että yhdellä henkilöllä on vain yksi rooli. Jos henkilö(t) joutuvat sijaistamaan toisiaan, saattaa se sotkea harjoitustilannetta.

Palvelut | Digitalisaatio ja digitaalinen turvallisuus
Rousku Kimmo

16.10.2018

Tärkeää - syöte numero 3 – harjoituspäivänä klo 9.45

Jotta harjoitus toteutuu kaikilla samankaltaisesti ja saatte harjoituksesta mahdollisimman suuren hyödyn, valitkaa tämän syötteen yhteydessä yksi tietojärjestelmä, jonka kuvittelette olevan syötteessä olevan tapahtuman kohteena. Käyttäkää tätä tietojärjestelmäänne esimerkkinä koko muun harjoituspäivän ajan. Emme tässä yhteydessä paljasta syötteestä sen enempää, mutta ohjeistamme tästä tarkemmin myös kyseissä syötteessä.

Harjoituspäivän aikana voitte ottaa yhteyttä seuraaviin viranomaisiin **harjoituksessa kuvaillulla tavalla**, mikäli päädytte päivän tapahtumien yhteydessä siihen, että yhteydenotto on tarpeellinen:

- Poliisi
- tietosuojavaltuutetun toimisto
- Viestintävirasto | Kyberturvallisuuskeskus
- Valtori (vain valtionhallinnon VALTTI-työasemapalvelun käyttäjät)
    - Valtoriin voitte välittää kysymykset, jotka koskevat aamupäivän syötteiden mukaista tilannetta ja sen perusteella esittäisitte oikeassakin tilanteessa
    - huomatkaa, että koska kyseessä on harjoitus, organisaatioiden antamat viestit on sovitettu harjoitukseen liittyen
    - tarkoitus ei ole käydä sen laajempaa viestintää ulkopuolisten toimijoiden kanssa vaan keskittyä organisaation sisäisen, oman toiminnan kehittämiseen

Huomioikaa, että näihin tahoihin ei tule ottaa yhteyttä, kuten todellisessa tilanteessa tehtäisiin, vaan nimenomaan harjoituksen ohjeistuksen mukaan.

Mikäli organisaationne haluaa käyttää harjoituksessa muita osapuolia, organisaation tulee sopia siitä erikseen ja tämä ei liity tällöin Väestörekisterikeskuksen toteuttamaan TAISTO18-harjoitukseen.

Harjoituspäivän aikana tulee toimia, kuten oikeassa tilanteessa. Organisaation tulee toteuttaa ne sisäiset yhteydenotot, sähköpostiviestit, pikaviestikeskustelut, mahdolliset tiedotteet ja muut toimenpiteet, jotka se aidossa tilanteessa toteuttaisi. Muistakaa kuitenkin käyttää kaikissa viesteissä TAISTO18-HARJOITUS-aloitusta, jotta kukaan ei erehdy luulemaan tilannetta oikeaksi.

Tässä yhteydessä tulee huomata, että harjoituksessa ei käytännössä päästä eikä ole tarkoitus tutkia tarkemmin mahdollisen tietoturvapoikkeaman tai henkilötietojen tietoturvaloukkauksen syitä tai päästä tekemään tarkempaa tapahtuneeseen liittyvää tutkintaa (forensiikka). Organisaation tulee osana harjoituksen jatkotoimenpiteitä ja oman toiminnan kehittämistä arvioida ja selvittää, kuinka harjoituksen kaltaisissa tilanteissa se jatkaisi tarvittavaa tilanteen selvitystä.