TAISTO19-harjoitusraportti ja yhteenveto

Kimmo Rousku

DIGI- JA VÄESTÖTIETOVIRASTO

Yleistä

- Valtiovarainministeriön asettama julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) valmisteli ja valtiovarainministeriö julkaisi joulukuussa 2019 Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman: http://urn.fi/URN:ISBN:978-952-251-975-7.
- Väestörekisterikeskus käynnisti alkuvuodesta 2019 JUDO-hankkeen digitaalisen turvallisuuden kehittämiseksi julkisen hallinnon organisaatioissa. Digitaalinen turvallisuus käsittää viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan.
- JUDO-hanke hyödyntää erilaisia, osin uudenlaisia toteutustapoja sekä tietysti oppeja aiemmista hankkeista. Tavoitteena on varmistaa, että julkisen hallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Tätä tavoitetta edistetään kehittämällä digiturvan johtamista, henkilöstön digiturvaosaamista sekä tarjoamalla tukea turvallisempien palveluiden kehittämiseksi.

Yleistä

- JUDO-hanke hyödyntää erilaisia, osin uudenlaisia toteutustapoja sekä tietysti oppeja aiemmista hankkeista. Tavoitteena on varmistaa, että julkisen hallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Tätä tavoitetta edistetään kehittämällä digiturvan johtamista, henkilöstön digiturvaosaamista sekä tarjoamalla tukea turvallisempien palveluiden kehittämiseksi.
- Yksi JUDO-hankkeessa toteutettava kokonaisuus on JUDO-harjoitukset. Nyt toteutettujen vuosien 2018-2019 ohella tuotamme harjoitukset vuosina 2020 ja 2021 sekä luomme muita digiturvan harjoitustoimintaan liittyviä tukipalveluja, ohjeita ja materiaaleja.

TAISTO19-harjoituksen vastuutahot

- Harjoituksen operatiivisena toteuttajana toimi Väestörekisterikeskus. Harjoituksen suunnittelussa sekä harjoituspäivien toteuttamisessa olivat mukana myös Huoltovarmuuskeskus, Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, Poliisi, tietosuojavaltuutetun toimisto, Turvallisuuskomitea sekä Valtion tieto- ja viestintätekniikkakeskus (Valtori).
- Harjoituksessa mahdollistettiin viranomaisilmoitukset tietosuojavaltuutetun toimistoon, Poliisille sekä Kyberturvallisuuskeskukselle.
- Vuodesta 2020 alkaen Digi- ja väestötietovirasto vastaa JUDO-hankkeen ja sitä kautta TAISTO-harjoitusten tuottamisesta.

Budjetti

- Vuoden 2018 TAISTO-harjoituksen perusteella harjoituksen budjetiksi arviointiin noin 20 000 € poisluettuna VRK:n ja muiden harjoituksen toteuttajien sekä harjoitukseen osallistuneiden organisaatioiden henkilötyöpanokset.
- Vuoden 2019 TAISTO-harjoitus maksoi noin 15 000 €, joka jakaantui
  - Harjoitussyötteiden tuottamisessa käytettyjen videoiden tuottaminen
  - Kieliversioiden tuottaminen
  - Mediasoitto organisaatioiden antamille yhteyshenkilöille
  - 23.1.2020 TAISTO19- ja harjoitustoiminnan seminaari
  - Muun tukimateriaalin tuottaminen

Mitä harjoituksessa harjoiteltiin?

1) Kehittää organisaation tietoturvallisuuden hallintaa, johtamista ja viestintää tietoturvaloukkauksissa, erityisesti erilaisissa kyberhyökkäyksissä kuten palvelunestohyökkäys, lunnashaittaohjelmahyökkäys tai tietomurto.

2) Kehittää organisaation henkilötietojen tietoturvaloukkauksissa tarvittavia prosesseja, muun muassa kykyä arvioida syntynyttä riskiä ja tehdä sen perusteella tarvittavat viranomaisilmoitukset sekä viestiä tilanteesta.

3) Kehittää organisaation toiminnan jatkuvuuteen ja valmiuteen liittyvää ohjeistusta ja toimintaprosesseja jatkuvuus-, valmius- ja toipumissuunnittelun osalta. Varmistaa, että organisaatio osaa tunnistaa sen kriittiset palvelut ja prosessit sekä osaa priorisoida ne tärkeyden mukaan.

Kenen harjoitukseen olisi tullut osallistua organisaatiosta?

- **Johdon edustaja(t)**
  - 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
  - harjoituksessa harjoitellaan kriisiviestintää median suuntaan, median edustaja soittaa organisaation määrittämälle yhteyshenkilölle (johdon edustaja, asiantuntia) sekä esittää hänelle sellaisia kysymyksiä, joita tällaisessa tilanteessa voi kuvitella esitettävän

Kenen harjoitukseen olisi tullut osallistua organisaatiosta? 1/3

- **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

Kenen harjoitukseen olisi tullut osallistua organisaatiosta? 2/3

- **Viestintä-asiantuntija(t)**
- 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(t)**
- harjoitus liittyy 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

Kenen harjoitukseen olisi tullut osallistua organisaatiosta? 3/3

- **Tarkkailija**
  - jotta organisaatio saa mahdollisimman suuren hyödyn harjoituksesta, kannattaa kaikesta harjoituspäivään ja sitä edeltäneisiin tilanteisiin kytkeä ulkopuolinen tarkkailija, joka kirjaa objektiivisesti ylös tilanteeseen liittyneitä tapahtumia, eräänlaista lokia. Toimitamme ensimmäisen syötteen yhteydessä 10.10.2019 Excel-tiedoston, jota voi käyttää esimerkkinä tällaisesta raportoinnista. Tätä raportointia tarvitaan myös apuna, kun organisaatio arvioi ja raportoi omasta toiminnastaan VRK:lle osana harjoitukseen liittyvää raportointia.

Taustatietoja ja syötteet

MISTÄ TAISTOSSA OLIKAAN KYSYMYS JA MITEN HARJOITUS ETENI SYÖTTEIDEN OSALTA?

Varautuminen kyberhyökkäykseen

- Harjoituksen tarkoituksena oli muun muassa:
  - Varautuminen kyberturvallisuuteen liittyvään uhkaukseen
  - Viranomaisilmoitukset
  - Toiminnan jatkuvuuteen ja varautumiseen liittyvät ohjeet, suunnitelmat ja prosessit
  - Toiminta ICT-häiriöissä (palvelunestohyökkäys) sekä lunnashaittaohjelmauhka
  - Häiriö- ja kriisiviestintä
  - Edellisten perusteella kehittää organisaation omaa toimintaa sekä tunnistaa kehittämiskohteita lyhyellä- ja pitemmällä aikajänteellä

Osallistujamäärät

Osallistujat - organisaatiot	TAISTO19		TAISTO18	
Kunnat	134	57,0%	132	56,4%
Valtionhallinto	55	23,4%	74	31,6%
Yliopistot, oppilaitokset	19	8,1%	19	8,1%
Sairaanhoitopiirit	5	2,1%	9	3,8%
Yritykset	16	6,8%	-	
Muu	6	2,6%	-	
Yhteensä	**235**		**234**	

TAISTO19-ennakkosyötteet ja harjoituspäivä

Yleistä

- TAISTO19-harjoitus toteutettiin eri tavalla kuin edellisen vuoden, nyt harjoitus aloitettiin kahdella ennakkosyötteellä viikon välein lokakuun alussa. Tämän avulla harjoitusorganisaatioita ohjattiin valmistautumaan Tietovuoto321-aktivistiryhmän toteuttamaan uhkaukseen. Samoin tämä ohjasi organisaatioita tunnistamaan organisaation toiminnalle kriittiset palvelut ja tarkistamaan niiden toiminnan jatkuvuuteen ja valmiuteen liittyviä prosesseja.
- Itse harjoituspäivänä toteutettiin organisaation kriittistä palvelua vastaan palvelunestohyökkäys (DoS) sekä myös organisaation yhdestä johtoryhmän jäsenen työasemasta löydettiin lunnashaittaohjelma (ransomware). Organisaatioiden tuli kyetä samanaikaisesti huolehtimaan molempien häiriöiden hallinnasta ja tarvittavasta viestinnästä.

Yleistä

- TAISTO19-harjoituksessa toteutettiin myös ensimmäistä kertaa puhelimella median yhteydenotto organisaation antamalle median yhteyshenkilölle. Palaute sekä harjoitusorganisaatioilta että soitot toteuttaneilta henkilöiltä olivat myönteiset, pääosin vastaukset kysymyksiin sujuivat hyvin ja rutiinilla, mutta osalla toki kehitettävääkin löytyy. Tämän takia toivoimme, että organisaatiot nauhoittaisivat nämä haastattelut, jotta niistä jokainen voisi oppia. Puhelinsoiton ohella osa organisaatioista hyödynsi myös kuvitteellista median yhteydenotto-videota ja harjoitutti sen avulla laajemminkin myös asiantuntijoita.
- Seuraavilla sivuilla vielä kertauksen vuoksi, etenkin niille lukijoille, jotka eivät ole harjoitukseen osallistuneet, harjoituksen ennakkosyötteet sekä harjoituspäivän syötteet.

1. Syöte julkaistiin lokakuun alussa – Tietovuoto321 esitti uhkauksen

1. SYÖTE: TAISTO19 (Ennakkosyöte)

Tämä on harjoituksen ensimmäinen ennakkosyöte, jossa pohjustetaan TAISTO19-harjoitusta. Lukekaa tämä syöte huolella ja tehkää sen pohjalta syötteen lopussa olevat tehtävät. Tehtävien suorittaminen auttaa organisaatiotanne suoriutumaan varsinaisesta harjoituspäivästä.

Voitte kirjata ylös havaintonne ja tarvittavat kehittämistoimenpiteet päivitettyyn LOKIEXCEL-TIEDOSTOON.

TAISTO19 – harjoituksen johdanto

Harjoitus alkaa katsauksella jo aikaisemmin tapahtuneeseen:

Organisaationne on saanut seuraavan uhkausviestin sekä -videon #Tietovuoto321-ryhmältä:

Haluamme rahaa
Olemme #Tietovuoto321-ryhmä ja olemme palanneet takaisin.
Vaikka perustajamme istuukin häkissä, olemme entistä vahvempia.
Kostoksi perustajamme vangitsemisesta haluamme teidän maksavan 1 Bitcoinin (BTC) korvauksen tilillemme 132wrCKwcEMFnUuYKoEqzPseuEz7P9Un
Bitcoinin pitää näkyä tilillämme viiden vuorokauden kuluessa!!!!

Tämän lisäksi #Tietovuoto321-ryhmä on julkaissut sosiaalisessa mediassa alla olevan uhkausvideon:

Voit katsoa videon myös osoitteessa: HTTPS://DREAMBROKER.COM/CHANNEL/WSR9RGZS/Q0NT2RDQ

2. Syöte julkaistiin viikkoa myöhemmin– Tietovuoto321 esitti uhkauksen, että se hyökkää organisaatiota vastaan, koska ei ole saanut rahoja

Voit katsoa videon myös osoitteessa: HTTPS://DREAMBROKER.COM/CHANNEL/WSR9RGZS/4BNKMRWC

2. SYÖTE: TAISTO19 (Ennakkosyöte)

Tämä on harjoituksen toinen ennakkosyöte, jossa pohjustetaan TAISTO19-harjoituspäiväänne. Lukekaa tämä syöte huolella ja tehkää sen pohjalta syötteen lopussa olevat tehtävät. Tehtävien suorittaminen auttaa organisaatiotanne suoriutumaan varsinaisesta harjoituspäivästä.

Voitte kirjata ylös havaintonne ja tarvittavat kehittämistoimenpiteet päivitettyyn LOKIEXCEL-TIEDOSTOON. Kopioikaa välilehti 17.10 Syöte 2 nyt käytössänne olevan LokiExcel-tiedoston vastaavalle tyhjälle välilehdelle.

#Tietovuoto321-ryhmä on lähettänyt teille jälleen uuden uhkauksen:

Tämä on viimeinen varoitus
Emme ole vieläkään saaneet meille kuuluvia rahoja. Mikäli emme saa niitä 6.11. / 18.11. / 25.11. mennessä, hyökkäämme teidän kaikista tärkeintä tietojärjestelmää vastaan ja palaatte takaisin keskiajalle. Vaikka nyt tiedätte, milloin ja mihin hyökkäämme, ette siitä huolimatta kykene torjumaan hyökkäystämme. Jotkut teistä ovat rikkoneet meidän käskyä ja menneet lavertelemaan kytille – kostoksi tästä nostamme nyt lunnasvaatimuksemme 20 Bitcoiniin.
Tilimme on:132wrCKwcEMFnUuYKoEqzPseuEz7P9Un
Maksakaa tai itkekää ja maksakaa.

Samanaikaisesti #Tietovuoto321-ryhmä on julkaissut myös oheisen videon:

3. Syöte aloitti harjoituspäivän - #Tietovuoto321 ryhmä vähätteli harjoituksen merkitystä

Klo 8.45
3. SYÖTE: TAISTO19

Tervetuloa TAISTO19-harjoituspäivään!

#Tietovuoto321-ryhmä on julkaissut sosiaalisessa mediassa seuraavan viestin:

4. Syöte – organisaatio sai ilmoituksen toimimattomasta palvelusta

Klo 9.00
4. SYÖTE: TAISTO19

Palvelussanne on vakava häiriö!

Aina kun harjoituksessa mainitaan palvelu, sillä tarkoitetaan teidän ennalta valitsemaanne oman organisaatio toiminnalle kriittistä palvelua. Ohjeet palvelun valitsemiseen saitte SYÖTTEESSÄ 2.

Saatte seuraavan ilmoituksen palvelutuottajalta:

HÄIRIÖTIEDOTE:

ICT-palvelutuottajan ilmoitus – palvelutiketti #WTF07112019k€l€

Palvelussanne on havaittu ongelma, jonka johdosta palvelu ei vastaa enää asiakaspyyntöihin.

Olemme käynnistäneet häiriönselvitysprosessin häiriön paikallistamiseksi. Ilmoitamme häiriöselvityksen etenemisestä, kun olemme saaneet vian paikallistettua tai **viimeistään klo 10.15**.

Toivomme, että vastaatte tarvittavasta asiakastiedottamisesta sekä muista sopimistanne toimenpiteistä häiriötilanteen vaikutuksen rajoittamiseksi ja pienentämiseksi.

Oy ICT-palvelutuottaja ab

TAISTO 2019
TIETOTURVA- JA TIETOSUOJALOUKKAUSTEN HALLINNAN HARJOITUS

5. Syöte – TAISTOTV-julkaisi uutisen:

Voit katsoa videon osoitteessa: HTTPS://DREAMBROKER.COM/CHANNEL/WSR9RGZS/1Z7CW42E

Klo 9.30
5. SYÖTE: TAISTO19

TAISTO-TV-uutinen:

Mikäli upotus ei näy, voit katsoa videon myös osoitteessa: HTTPS://DREAMBROKER.COM/CHANNEL/WSR9RGZS

6. Syöte – organisaation tulisi selvittää, voiko sen ulkomaan liikennettä suodattaa, jotta palvelunestohyökkäystä olisi mahdollista rajoittaa

Klo 10.15
6. SYÖTE: TAISTO19

Häiriötilanne jatkuu. Palveluntoimittaja ilmoittaa häiriötilanteen selvittämisen jatkumisesta sovitun mukaisesti.

HÄIRIÖTIEDOTE:

ICT-palvelutuottajan ilmoitus – palvelutiketti #WTF07112019k€l€

Palvelussanne havaittu ongelma jatkuu, jonka johdosta palvelu ei edelleenkään vastaa asiakaspyyntöihin. Osana häiriönselvitysprosessia olemme havainneet palveluun kohdistuvan poikkeuksellisen paljon verkkoliikennettä, minkä johdosta palvelu ei pysty suoriutumaan sille annetuista tehtävistä. Kyseessä on **palvelunestohyökkäys**, joka pysäyttää palvelun toiminnan, kunnes verkkokuormitusta saadaan pienennettyä.

Toivomme teidän selvittävän ja päättävän, voimmeko suodattaa palveluun tulevaa liikennettä siten, että **kaikki ulkomailta tuleva liikenne suodatetaan / tiputetaan pois**, koska osa verkkohyökkäysliikenteestä tulee ulkomailta. Tulemme kysymään tätä suodatusmahdollisuutta seuraavassa yhteydenotossa klo 11.45, mikäli emme ole ennen sitä saaneet ongelmaa ratkaistua.

Ilmoitamme häiriöselvityksen etenemisestä, kun olemme saaneet häiriön korjattua tai **viimeistään klo 11.45.**

Toivomme, että vastaatte edelleen tarvittavasta asiakastiedottamisesta sekä muista sopimistanne keinoista häiriötilanteen vaikutuksen rajoittamiseksi ja pienentämiseksi.

Oy ICT-palvelutuottaja ab

TAISTO 2019
TIETOTURVA- JA TIETOSUOJALOUKKAUSTEN HALLINNAN HARJOITUS

Saatte myös asiakkailta huolestuneita yhteydenottoja koskien palvelunne toimivuutta.

7. Syöte – havaitaan uusi häiriö!

Klo 10.30
7. SYÖTE: TAISTO19

Havaitaan uusi häiriö. Palveluntoimittaja ilmoittaa johdon työasemasta löytyneestä lunnashaittaohjelmasta. Samanaikaisesti tämän uuden häiriön kanssa on käynnissä palvelunestohyökkäykseen liittyvä häiriötilanteen selvitys- ja hallintaprosessi.

HÄIRIÖTIEDOTE:

ICT-palvelutuottajan ilmoitus –palvelutiketti #TAIo7112019Ransu

Olemme saaneet tietoomme, että johtoryhmänne jäsenen kannettavaan tietokoneeseen on iskenyt uusi **#Ransu321-niminen lunnashaittaohjelma**, joka on lukinnut kaikki tietokoneen tiedostot.

On mahdollista, että pystymme palauttamaan tietokoneen tiedostot varmuuskopioista, mutta haluamme ensin varmistaa, että tämä lunnashaittaohjelma ei ole levinnyt tai leviämässä organisaationne verkossa muihin laitteisiin.

Oy ICT-palvelutuottaja ab

TAISTO 2019
TIETOTURVA- JA TIETOSUOJALOUKKAUSTEN HALLINNAN HARJOITUS

7. Syöte – lunnashaittaohjelma kaappaa johdon työaseman

Tehtävät 4:

- Miten reagoitte uuteen häiriöön?
- Miten priorisoitte resursseja kahden häiriötilanteen osalta?
- Tehkää riskiarvio, minkälainen uhka tästä yhden tietokoneen lunnashaittaohjelmakaappauksesta syntyy?
- Selvittäkää, onko nyt lukittuna olevalla tietokoneella henkilötietoja. Miten pitäisi toimia?
- Kannattaako lunnaat maksaa, jotta työasema saadaan nopeasti takaisin käyttöön?

8. Syöte – median yhteydenotto

Klo 11.00
8. SYÖTE: TAISTO19

Median yhteydenotto

Organisaation ilmoittamalle yhteyshenkilölle tulee puhelinsoitto annettuun matkapuhelinnumeroon klo 11-12 välillä. Taisto-TV:n toimittaja haluaa saada tarkempia tietoja organisaation palveluiden toimimattomuudesta ja häiriötilanteesta. Voitte videoida haastattelun, jos haluatte arvioida, miten haastattelutilannetta voisi kehittää.

Tehtävät 5:

- Miten median yhteydenotto sujui?
- Mikä meni haastattelussa hyvin?
- Miten haastattelu olisi voinut sujua paremmin?
- Mitä muuta kehitettävää tällainen yhteydenotto antoi?

Haastattelun jälkeen, voitte julkaista valokuvan Twitterissä haastattelusta, jossa kerrotte mitä valokuvassa tapahtuu sekä ketä kuvassa haastatellaan. Muistakaa käyttää #TAISTO19 -tunnistetta.

8.1 Syöte – median yhteydenotto - videoharjoitus

- Voit katsoa videon myös osoitteessa: HTTPS://DREAMBROKER.COM/CHANNEL/WSR9RGZS/MF40AEU5

KLO 11:40
SYÖTE 8.1: TAISTO19

Mikäli emme ole jostain syystä saaneet organisaationne yhteyshenkilön numeroa, voitte harjoitella median yhteydenottoon vastaamista Taisto-TV:n toimittajan videohaastattelussa esittämiin kysymyksiin.

Voitte itse nauhoittaa yhteyshenkilön vastaukset älypuhelimella videotiedostoksi, jos haluatte arvioida, miten tällaista haastattelua tulisi kehittää. Lisäksi tätä videohaastattelua voidaan käyttää myös muiden TAISTO19-harjoitukseen osallistuvien asiantuntijoiden mediavalmennus-koulutuksena.

Kysymysten välillä on 60 sekuntia aikaa vastata niihin.

9. Syöte – KRP tiedottaa tilanteesta

Klo 11.50
9. SYÖTE: TAISTO19

Keskusrikospoliisi tiedottaa, että kiitos laaja-alaisen viranomaisyhteistyön, se on pysäyttänyt #Tietovuoto321-ryhmän toiminnan.

10. Syöte – Sisäinen läpikäynti ja raportointi

Klo 13.30
10. SYÖTE: TAISTO19

Vuorossa on harjoituksen sisäinen läpikäynti sekä raportointi harjoituksesta.

Tehtävät 8:

- Oheisesta linkistä löytyy UUSI TAISTO19-RAPORTOINTI-EXCEL. Tiedosto kattaa harjoituspäivää edeltäneet viikot ja tilanteet sekä tämän harjoituspäivän. Se toimii nyt keskeisenä raportointityökaluna sekä oman toimintanne kehittämisen työkaluna.
- Käynnistäkää taulukon täyttäminen hyödyntäen harjoituksessa käyttämäänne RapoExcel-tiedostoa tai muita organisaationne käyttämiä työkaluja harjoituksen toimenpiteiden kirjaamiseen.
- Lähettäkää tämä Excel viikon kuluessa turvapostilla osoitteeseen DIGITURVA@VRK.FI – laittakaa viestin otsikoksi ”TAISTO19-raportti”.
- Jos käytössänne ei ole turvapostia, voitte lähettää tiedoston VRK:n turvapostilla, jonka saatte käyttöönne: HTTPS://SECUREMAIL.VRK.FI/

Uusi twiitti sosiaalisessa mediassa – Tietovuoto321 1/2

TAISTO BREAKING-NEWS 13:30

Aikaisemmin uutisoitiin #Tietovuoto321-ryhmän toiminnan pysäyttämisestä. Ryhmä on ilmeisesti kuitenkin tehnyt ajastetun hyökkäyksen. Ryhmittymä on julkaissut myös sosiaalisessa mediassa uuden viestin:

Tietovuoto321
@Tietovuoto321

Following

Luulitteko, että meidän toiminta lakkaisi, vaikka kytät raidasi meidän CyberHQ? No way - Yllätys - miksi? #koska_me_voimme #nähdään

Uusi twiitti sosiaalisessa mediassa – Tietovuoto321 2/2

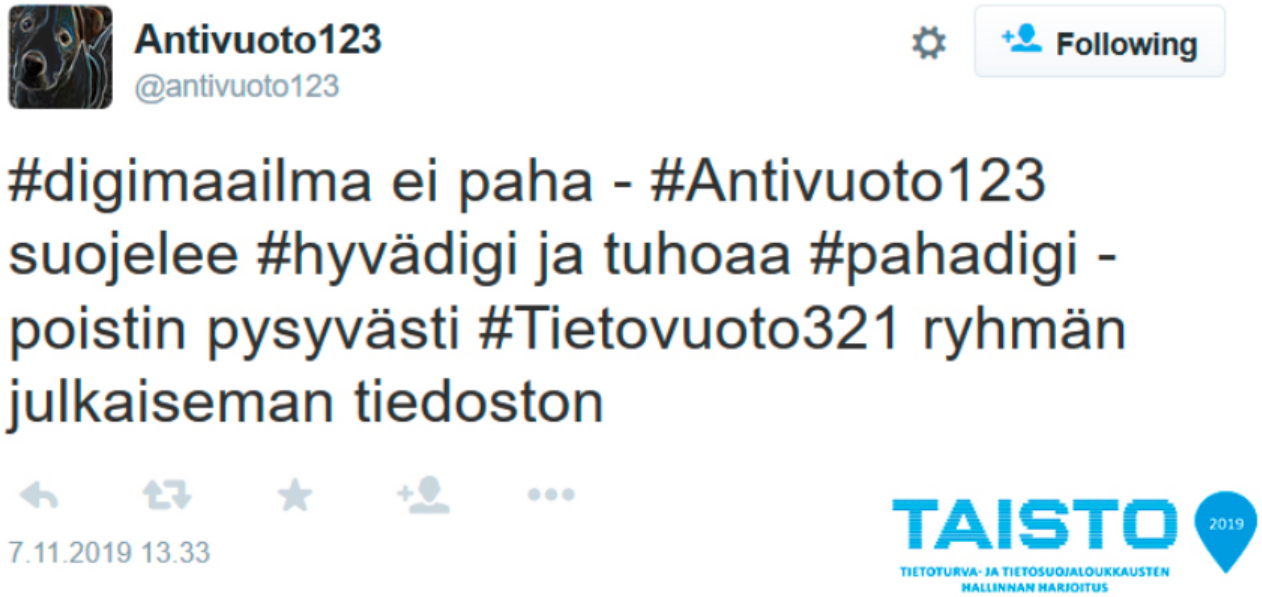
- Hyökkäyksen johdosta verkkoon on vuotanut merkittävä määrä suomalaisten yritysten ja julkishallinnon johtajien tiedostoja. Tiedostot sisältävät organisaatioiden taloudelliseen toimintaan liittyviä salaiseksi määriteltyjä asiakirjoja sekä esimerkiksi luottamuksellisia alaisten kanssa käytyjä keskusteluja. Lisäksi kokonaisuudesta on löytynyt listauksia niistä www-sivuista, joilla kyseiset henkilöt ovat vierailleet viimeisen vuoden aikana. Tietojemme mukaan joukossa on lisäksi valtavasti kyseisten henkilöiden tietokoneilta löytyneitä valokuvia, joista osa on selvästi otettu vapaa-ajalla. Ilmeisesti tämä tietovuoto on seurausta aktivistiryhmän kaappaamista johdon työasemista

10.1. Syöte – Antivuoto123 uusi syöte sosiaalisesssa mediassa

Klo 13.55
10.1 SYÖTE: TAISTO19

TAISTO BREAKING-NEWS 13:55

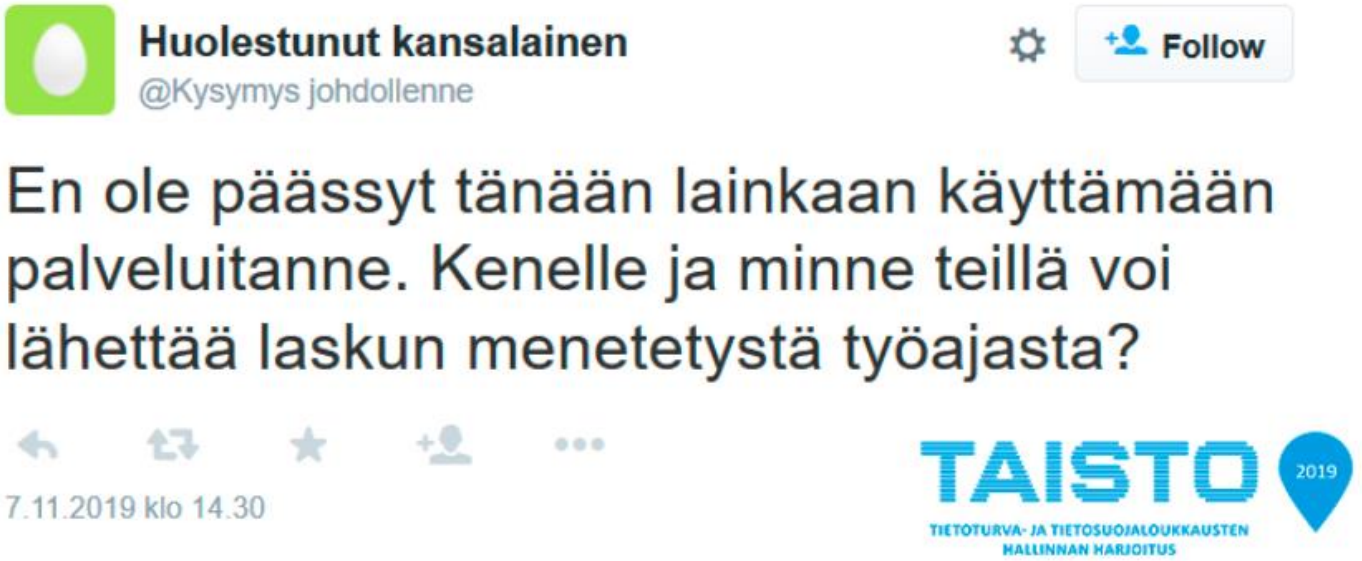
Juuri saamamme tiedon mukaan tämä valtava tiedostokokonaisuus on poistunut verkosta! Käsittääksemme tiedostot on poistanut yksittäinen ns. valkohattukrakkeri (@Antivuoto123), joka toteaa viestissään haluavansa osoittaa, että #digipahisten sijaan maailmasta löytyy myös #digihyviksiä.



11. Syöte – huolestunut kansalainen kysyy sosiaalisessa mediassa

Klo 14.30
11. SYÖTE: TAISTO19

Viestintänne löytää Twitteristä oheisen johdollenne esitetyn kysymyksen.



11.1 Syöte – sosiaalisen median kautta kerrottu netissä löydetystä salatusta tiedostosta

Klo 15.00
11.1 SYÖTE: TAISTO19

TAISTO BREAKING-NEWS 15:00

LIVE #DARKNET

TAISTO 2019
TIETOTURVA- JA TIETOSUOJALOUKKAUSTEN HALLINNAN HARJOITUS

TAISTO-TV

HUHU - VOIKO OLLA TOTTA?

2019-11-19 NETIN SYÖVEREISTÄ LÖYTYNYT ISO SALATTU TIEDOSTO

12. Syöte – harjoituksen operatiivinen osuus on päättynyt

Klo 15.30
12. SYÖTE: TAISTO19

Tehtävät 11:

- Sopikaa, kuinka jatkatte harjoituspäivän jälkeen oppien keräämistä sekä TAISTO19-harjoituksen raportointi-Excelin täyttämistä. Osana tätä raporttia joudutte keräämään ja priorisoimaan tärkeimmät kehittämiskohteet toteutettavaksi mahdollisimman nopeasti.
- Varatkaa kalentereista 23.1.2020 TAISTO19-palauteseminaaria varten. Toimitamme yhteyshenkilöille kutsun tilaisuuteen osana harjoituksen palautekyselyä koskevaa sähköpostiviestiä ensi viikolla.
- Viestikää omassa organisaatiossanne ja esim. sosiaalisessa mediassa TAISTO19-harjoituksenne päättymisestä – muistakaa kuvakisamme! Käytättehän aihetunnistetta #TAISTO19.

Onneksi olkoon – harjoituksen varsinainen operatiivinen osio on nyt päättynyt!

Harjoituksen yhteenveto

Palautekyselyn tulokset

- Olemme koonneet ja verranneet seuraaville sivuille saamamme palautekyselyn tulokset sekä verranneet niitä TAISTO18-harjoituksen palautekyselyyn.
- Palautteen perusteella harjoitusta voidaan pitää erittäin hyvänä, vaikka pääosin useimmat keskeiset mittarit laskivat jonkin verran laskivat. Todennäköisesti suurin syy tässä on sillä, että valtaosa organisaatioista (noin 200) osallistui harjoitukseen jo toista kertaa, joten harjoitus ei tarjonnut samanlaista uutuudenviehätystä mitä edellinen harjoitus.

4. Palautekyselyyn vastanneet - toimialamme on:

Nimi	Prosentti
Valtionhallinto	26,2%
Kunta tai muu kunnallinen toimija	51,5%
Yliopisto, oppilaitos tai muu opetustoimen toimija	6,9%
Sairaanhoitopiiri tai muu sote-toimija	5,4%
Yritys	1,5%
Jonkin edellisen omistama tai hallinnoima yritys	4,6%
Muu, mikä?	3,8%

- N130
  - Erityisesti kuntatoimijat vastasivat palautekyselyyn aktiivisesti, erityiskiitos heille siitä!

5. Osallistuimme harjoitukseen:

Harjoituspäivä	Prosentti
7.11.	21,7%
19.11.	40,3%
26.11.	38,0%

- Palautekyselyyn vastanneiden organisaatioiden jakauma noudattelee myös harjoituspäivään osallistuneiden organisaatioiden jakaumaa.

6. Miten saitte tiedon TAISTO19-harjoituksesta:

Nimi	TAISTO19	TAISTO2018
JUDO-hankkeen uutiskirjeen kautta	51,5%	52,3% (JUHTA-hanke)
JUDO-hankkeen työpajoista	56,9%	
Valtiovarainministeriön lähettämä kirje	40,0%	34,4%
Sosiaalisen median kautta	3,8%	1,3%
Muuta kautta, miten?	13,1%	11,9%

- Tieto harjoituksesta levisi usean eri kanavan kautta.

7.2 Kuinka moni organisaationne jäsen osallistui TAISTO-harjoituspäivään, harjoituksen valmisteluihin tai harjoituksen jälkeisiin toimenpiteisiin? Voitte arvioida vuoden 2019 aika työhön osallistuneiden määrän.
Arvioikaa, kuinka monta henkilötyöpäivää organisaationne työpanos koko harjoitukseen on vuoden 2019 aikana (htp)?
Jos käytitte ulkopuolisia asiantuntijoita, arvioikaa heidän työpanoksensa määrä (htp)

	TAISTO19	TAISTO18
• Harjoitusorganisaatioita	235	234 organisaatiota
• Henkilöiden määrä	2412 henkilöä	2215 henkilöä
• Henkilötyömäärä	3990 htp	4318 htp
• Ulkopuolisia	142 henkilöä	127 henkilöä

- Harjoitukseen osallistuneiden määrä sekä henkilötyömäärä ovat hyvin samalla tasolla mitä vuoden 2018 harjoituksessa, henkilöiden määrä on kasvanut noin 10% ja henkilötyömäärä saman verran. Ulkopuolisia asiantuntijoita on käytetty suhteellisen vähän, esimerkiksi tarkkailijoina ja konsultoimassa ennen harjoituspäivää.

10.3. Tiedottaminen, ohjeistus ja yhteydenpito TAISTO19-harjoitukseen – ennen harjoitusta

	TAISTO19	18
Saimme riittävästi tietoa harjoitukseen liittyen ennen kuin päätimme osallistua harjoitukseen	4,42	4,36
Harjoitukseen Ilmoittautuminen oli helppoa	4,83	4,63
Ilmoittautumiseen liittyvät muutokset onnistuivat hyvin (jos teitte muutoksia)	4,53	4,45
Saamamme ohjeistus ja muu materiaali palvelivat hyvin harjoitusta	4,17	4,36
Harjoituksen viestintä onnistui hyvin	4,15	4,36
Harjoituksen ennakkosyötteet ohjasivat valmistautumista oikeaan suuntaan	4,27	-
Keskiarvo	**4,39**	**4,43**

- **Vuosien 2018-2019 välillä ei merkittävää eroa. Harjoitukseen valmistautumisen osalta VRK suoriutui vähintäänkin hyvin, mutta kaikki kehittämisideat otetaan huomioon vuoden 2020-harjoitusta suunniteltaessa.**

16. Millaisen arvosanan antaisitte Väestörekisterikeskukselle harjoitusta edeltävistä toimenpiteistä ennen harjoituspäivää 7.11. | 19.11. | 26.11.?

	TAISTO19	TAISTO18
1 erittäin huono	0,0%	
2	0,0%	
3	6,9%	
4	59,2%	
5 erittäin hyvä	33,8%	
Keskiarvo	**4,27**	**4,38**

Edeltävien toimenpiteiden osalta keskiarvo vastaa edellä nostettujen yksittäisten kysymysten tulosta. Keskiarvo laski 0,09 yksikköä, joka osin johtuu uutuudenviehätyksen vähentymisestä.

Avoin palaute - poimintoja

Ennakkosyötteet olivat hyödyllisiä ja antoi hieman ennakkotietoja tulevasta harjoituspäivästä.

Ennakkoon olisi voinut maanitella meitä harjoittelijoita suurempaan ”leikkimielisyyteen” eli heittäytymiseen. Mikään ei estänyt meitä, mutta ei vaan tullut pelattua täysin eläytyneenä. Varsinkaan viimeisinä käytetyt asiantuntijat

Yhteiset Skype palaverit eivät täysin toimineet teknisten ongelmien vuoksi.

Materiaalia ja viestintää paljon, osin sopivasti, jossakin jopa kenties liikaa?

Aivan riittävän hienosti kaikki sujui.

Kaikki palautteet läpikäydään vuoden 2020 harjoituksen suunnittelussa.

18.4. Organisaationne valmistautuminen harjoitukseen:

	TAISTO19	18
Organisaatiomme johto sitoutui harjoitukseen ennakolta hyvin	3,99	4,11
Asiantuntijamme sitoutuivat harjoitukseen ennakolta hyvin	4,28	4,36
Meillä oli tarvittavat ohjeet ja prosessit valmiina ennen harjoitusta	3,61	3,99
Pystyimme valmistautumaan harjoituspäivään kokonaisuutena ennakolta hyvin	3,92	4,09
Meillä oli riittävästi aikaa valmistautua harjoitukseen	4,10	-
Pystyimme jo ennen harjoituspäivää kehittämään toimintaamme	3,70	-
Keskiarvo	**3,94**	**4,09**

Organisaation valmistautumisessa matalin pistemäärä liittyi tarvittaviin ohjeisiin ja prosesseihin ennen harjoitusta (3,60). Yllättävän hyvä on sen sijaan tieto, että useat pystyivät kehittämään toimintaa jo ennen varsinaista harjoituspäivää. Keskiarvo laski 0,45 yksikköä, eniten laski ohjeistukset ja prosessit, joka osin saattoi johtua siitä, että harjoituksessa keskityttiin vuotta 2018 enemmän toiminnan jatkuvuuteen.

Avoin palaute 1/2

- Harjoituksen viitekehys oli rakennettu hyvin, koska se otti kantaa palvelujen jatkuvuuteen ict-varautumisen lisäksi. Henkilöstöä on vaikea sitouttaa ennen varsinaista harjoituspäivää.
- Alussa oli hiukan epätietoisuutta, kuinka harjoitus etenee. Positiivinen asia oli se, että jokainen henkilö tiesi nopeasti oman roolinsa ja olivat sitoutuneita harjoitukseen.
- Oli jo viime vuonna harjoiteltu lähes vastaavaa, nyt helpompi tehdä kun osa tuntui tutulta.
- Johto oli nyt edustettuna paikalla koko päivän, mikä oli hyvä asia. Ulkopuolinen järjestelmäntoimittaja olisi ollut hyvä saada paikalle, mutta se ei valitettavasti onnistunut.
- Osa avainhenkilöstä oli poissa ja tavoittamattomissa.
- Organisaation sisällä kommunikointi toimii kohtuullisella tasolla. Organisaation sisällä parannettavaa vastuiden määrittelyssä.
- Ajan ja resurssien löytäminen digitaalisen turvallisuuden jatkuvaan kehittämiseen on haaste.

Avoin palaute 2/2

- Juuri ennakkotehtävät ja niiden kysymysten miettiminen sujuvoitti harjoituspäivää. Harjoituspäivänä eteen tuli asioita, jotka piti olla tiedossa. Organisaatiomme suoriutui TAISTO19-päivästä mielestäni loistavasti. Toimimme keskustelevana tiiminä, ratkaisuja haettiin yhteisesti. Yhteinen tila ja aika mahdollisti osaltaan harjoituspäivän onnistumisen. Pientä turnausväsymystä oli ennen lounasta ja päivän loppupäässä havaittavissa.
- Edellisen vuoden tapaan johtaminen muodostui ongelmaksi. Emme ehkä osanneet hyödyntää tarpeeksi viime vuotisia kokemuksia. Tilannekuva oli välillä vähän epäselvä, ehkä osittain juuri johtamiseen liityvien ongelmien vuoksi. Meillä oli kolme eri ala organisaatiota harjoituksessa ja se myös vähän sekoitti pakkaa.
- Päivä eteni hyvin ja saimme toteutettua asioita konkreettisemmin, kuin vuonna 2018. Esim viestintä oli konkreettisempaa kuin aikaisemmin.

25.5. Harjoituspäivä oman organisaationne toiminnan osalta 1/2

	TAISTO19	18
Organisaatiomme johto osallistui harjoituspäivään sovitusti	4,37	4,34
Asiantuntijamme osallistuivat harjoituspäivään sovitusti	4,71	4,67
Harjoituspäivän tapahtumat kehittivät omaa toimintaamme tietoturva- ja tietosuojaloukkaustilanteiden sekä kyberhyökkäysten hallinnan osalta oleellisesti	4,07	4,02
Tunnistimme useita kehittämistä vaativia osa-alueita tai muita toimenpiteitä	4,02	3,87
Saimme odotetulla tavalla harjoiteltua tarvittavia viranomaisilmoituksia koskien häiriöitä, kyberhyökkäyksiä ja henkilötietojen tietoturvaloukkaustilanteita	4,02	4,31
Organisaatiomme pystyy jatkossa suoriutumaan vastaavanlaisessa tilanteessa selvästi paremmin kuin ennen harjoitusta	3,93	4,06
Pystyimme sovittamaan harjoituspäivän skenaarion ja tapahtumat hyvin omaan toimintaympäristöömme	3,85	4,09
Omat harjoituksessa käyttämämme ICT-palvelut toimivat harjoituspäivän osalta hyvin	4,38	4,43
Käytössämme olivat tarkoituksenmukaiset ICT-palvelut harjoituspäivän aikaiseen toimintaan, esimerkiksi viestinnän ja muun yhteydenpidon osalta	4,34	4,46
Keskiarvo	**4,19**	**4,25**

25.5. Harjoituspäivä oman organisaationne toiminnan osalta 2/2

- Organisaatioiden oman arvioinnin perusteella keskiarvo laski 0,06 eli laskua on hyvin vähän. Matalimman pistemäärän sai kohta “Pystyimme sovittamaan harjoituspäivän skenaarion ja tapahtumat hyvin omaan toimintaympäristöömme” (3,85)
- Lisäksi “Organisaatiomme pystyy jatkossa suoriutumaan vastaavanlaisessa tilanteessa selvästi paremmin kuin ennen harjoitusta” (3,93)
  - Osoittaa sen, että harjoitus on edesauttanut organisaation kyvykkyyttä, mutta toisaalta uusille harjoituksille on edelleen tarvetta
- Parhaimpia pistemääriä saivat kohdat “Organisaatiomme johto osallistui harjoituspäivään sovitusti” (4,37), ja ”Asiantuntijamme osallistuivat harjoituspäivään sovitusti” (4,71) – mitkä osoittavat harjoituksen yhden tavoitteen saavuttamisen, jossa niin asiantuntijat kuin johto yhdessä kehittävät organisaation toimintaa – lisäksi molemmat nousivat aavistuksen edellisen vuoden tulokseen verrattuna.

35. Millaisen arvosanan antaisitte harjoituspäivästä?

	TAISTO19	TAISTO18
1 erittäin huono	0,0%	
2	0,0%	
3	10,2%	
4	63,8%	
5 erittäin hyvä	26,0%	
Keskiarvo	**4,16**	**4,32**

Harjoituspäivän keskiarvo on jonkin verran parempi (4,16) kuin valmistautuminen harjoituspäivään (3,94), keskiarvo putosi 0,16 yksikköä verrattuna vuoteen 2018.

Avoin palaute 1/3

- Harjoittelu oli hyvää ennakointia ja avasi toivottavasti toimialueille konkreettisemmin mahdollista kyberhyökkäystilannetta. Hieman oli nähtävissä sitoutumisen puutetta joillakin toimialoilla. Johto oli tällä kertaa paremmin edustettuna kuin edellisellä kerralla.
- Valittu sisäinen järjestelmä ei täysin soveltunut harjoituksen teemaan, mutta pystyimme soveltamaan.
- Harjoitus kohdistui ulkopuolisen palveluntarjoajan toimittamaan järjestelmään. Osa syötteistä oli sellaisia, että emme voineet oikein todeta muuta kuin, että olemme yhteydessä palveluntarjoajaan ja varmistamme, että he selvittävät tilannetta. Oman organisaation sisällä jäi pääosin tehtäväksi tiedottamisen harjoittelu sekä ilmoituslomakkeiden täyttäminen ja tilanteen seuraaminen.
- Harjoitus oli hyödyllinen, mutta koska olimme harjoitelleet aikaisemminkin ja perusprosessit olivat kunnossa, mitään merkittävää edistysloikkaa harjoitus ei tuonut.

Avoin palaute 2/3

- Harjoitteet ja aikataulutus hyvin sekä toimivasti mietitty, harjoitus oli huomattavasti jäsentyneempi kuin 2018.
- Harjoituksen toteutus olisi voinut olla toiminnallisempi kuin nyt toteutui.
- Päivä sujui pääosin hyvin, joissain kohdissa olisi voinut leikata keskustelua ja ohjata toimintaa enemmän.
- Haasta kokonaisuus ja kriisi läpi ns. pikakelauksella.. Uskottava skenario ja kova, herättelevä koulu kaikille osallistujille.
- Hyvin organisoitu ja tarpeellinen harjoitus. Koetaan, että tällaiseen halutaan jatkossakin lähteä mukaan.
- Pyrimme tarkoituksella keskittymään tällä kertaa vähemmän henkilötietoihin ja enemmän muuhun toimintaamme, mikä hieman heikensi harjoituksen osuvuutta.

Avoin palaute 3/3

- Kokonaisuudessaan harjoitus antoi tukea mahdolliseen loukkaustilanteeseen ja omien ohjeiden läpikäyntiin. Harjoituspäivän iltapäivällä intensiteetti laski ja oli tyhjäkäyntiä. Syötteiden implementointi valittuun järjestelmäämme oli osittain epäselvää ja jouduimme jälkikäteen tekemään joitain muutoksia.
- Ilmoituksia emme oikeasti lähettäneet, mutta olimme dokumentoineet ne kuitenkin lähetetyiksi.
- Harjoituspäivä on antoisa vaikka yllättävä poissaolokin ilmeni. Kokoontuminen onnistui kuitenkin sovitulla tavalla ja roolit istuivat henkilöille tehtävineen hyvin. Pieni sähellys loi realismia peliin.

37.6. Väestörekisterikeskuksen toiminta harjoituspäivänä

	TAISTO19	18
Harjoituspäivän tapahtumat olivat realistiset ja voisimme kuvitella tällaista tapahtuvan myös oikeasti	4,08	4,17
Harjoituspäivän vauhti oli meille sopiva	3,69	-
Päivän aikana tulleet syötteet olivat harjoitukseen sopivia	3,98	4,18
Harjoituspäivän aikana oli riittävästi aikaa keskittyä syötteissä kuvattujen tapahtumien arviointiin ja sen perusteella oman organisaation toiminnan kehittämiseen	4,27	4,31
Syötteet, tukivideot ja muu materiaali tukivat hyvin harjoituspäivää	4,23	4,39
Syötteet, tukivideot ja muu materiaali olivat laadultaan korkeatasoisia	4,11	4,38
Raportointi-Excelissä kysyttiin oikeita asioita	3,81	4,21
Saimme tarvittaessa nopeasti apua harjoituspäivän aikana	4,21	4,27
Harjoitus toteutui teknisesti korkeatasoisesti	4,13	4,45
Keskiarvo	**4,16**	**4,30**

37.6. Väestörekisterikeskuksen toiminta harjoituspäivänä 1/2

- Kohdan keskiarvo laski 4,30 -> 4,16 ei 0,14 yksikköä.
- Eniten kehitettävää harjoituspäivän osalta liittyy “Harjoituspäivän vauhti oli meille sopiva” (3,69) ja ”Raportointi-Excelissä kysyttiin oikeita asioita” (3,81)
- Osa organisaatioista totesi, että etenkin iltapäivän osalta olisi ollut mahdollista tehdä enemmä asioita, vastaavasti osa organisaatioista totesi päivän toteutusvauhdin olleen heille sopivan. Eräs yllättävä seikka oli se, että kahdessa vuodessa on harjoitellut 234 + 235 organisaatiota, joista kuitenkin uusia on ollut vain reilut 30 organisaatiota eli kaikkiaan eri organisaatioita on ollut reilut 260. Seuraavissa harjoituksissa näille organisaatioille tulee kyetä tarjoamaan uudenlaisia harjoitusmalleja, mutta samalla varmistaa ensimmäistä kertaa harjoitteleville korkeatasoinen harjoitus.
- Vastaavastai harjoituksen raportointiin tulee luoda paremmin toimiva malli ja työkalu, jolla se voidaan toteuttaa.

37.6. Väestörekisterikeskuksen toiminta harjoituspäivänä 2/2

- Kaksi korkeimman keskiarvon saanutta kohtaa ovat “Harjoituspäivän aikana oli riittävästi aikaa keskittyä syötteissä kuvattujen tapahtumien arviointiin ja sen perusteella oman organisaation toiminnan kehittämiseen” (4,27) sekä ”Syötteet, tukivideot ja muu materiaali tukivat hyvin harjoituspäivää” (4,23).
- Edellinen kohta tarkoittaa sitä, että organisaatioilla on olut riittävästi aikaa käsitellä harjoituspäivän syötteitä ja omaa toimintaa, joka yhdistettynä edellisen sivun kehittämiskohteeseen mahdollistaa tiiviimmän harjoituspäivän.
- Olemme ensimmäisestä harjoituksesta alkaen panostaneet harjoituksen sisällön ja tukimateriaalien laadukkuuteen ja se näyttää toimivan.

46. Minkä arvosanan antaisitte VRK:lle harjoituspäivän toteutumisesta?

	TAISTO19	TAISTO18
1 erittäin huono	0,0%	
2	0,0%	
3	10,7%	
4	60,7%	
5 erittäin hyvä	28,7%	
Keskiarvo	**4,18**	**4,40**

VRK:n toimintaan liittyvien yksittäisten kysymysten keskiarvo (4,16) vastaa hyvin tätä yleisarvosanaa (4,18). Erittäin positiivista havaita, että yli neljäsosa on pitänyt harjoitusta eritäin hyvänä (28,7%). Keskiarvo on laskenut 0,22 yksikköä verrattuna vuoteen 2018 – tätä selittää osin se, että valtaosa organsaatioista harjoitteli toistamiseen.

Avoin palaute 1/2

- Alkupään syötteiden välissä olisi pitänyt olla enemmän aikaa (ilmoitusten tekemisen vuoksi). Meni vähän hosumiseksi. Loppupäivästä aikaa jäi vähän liikaakin.
- Aina on varaa parantaa, nyt ehkä aihe oli vähän kaukaa haettu.
- Oli odotettavissa viime vuodesta, että harjoituspäivän syötteiden tahti hiipuisi iltapäivään mentäessä, joten kehittelimme omia lisäsyötteitä, pitääksemme pelaajien mielenkiintoa yllä. Pääosa videoista oli hyviä.
- Skype-keskustelu oli ajoittain vähän häiritsevää. Sen voisi estää tulevaisuudessa.
- Raportointi Excel ei jotenkin ollut meille sopiva. Kysymykset jotenkin tuntuivat oudoilta. Välineenä Excel kätevä.
- Harjoituksen sisältö saisi olla realistisempi, toki tuokin on mutta jokin mittava realistinen uhka. Johtokeskukselle ei olut riittävästi tekemistä eli harjoitukseen pitäisi sisällyttää skenaarioita joihin asiantuntijat esittävät kenties ratkaisuvaihtoehtoja mutta johtokeskus linjaa.

Avoin palaute 2/2

- Harjoituspäivänä emme saaneet kaikkea tarvitsemaamme tietoa palveluntoimittajilta.
- Välillä, varsinkin johtoryhmä jäsenet, jotka tulivat paikalle vasta kriisin eskaloiduttua rupesivat ”ylianalysoimaan” ja ”etsimään kompaa” syötteitä. Eivät osanneet eläytyä yhtälailla, kuin alusta/alummasta mukana olleet. Joidenkin asioiden kanssa olisimme voineet jumpata hieman pidempään. Kun kirjoitimme oikeita ”harjoitusviestejä” ja tiedotteita, osa syötteistä tuli vähän syliin. Piti viivästää niiden käsittelyä. Yllättävät käänteet ja uutiset olivat kivoja. Hyvä, ettei ollut täysin ennalta arvattavaa.
- Tämän vuoden harjoitus oli paremmin kohdennettu kuin viime vuonna. Harjoituksesta saa paremmin hyötyä pienemmällä kokoonpanolla, joka harjoittelee omaa toimintaansa ottaen huomioon toimintaympäristön kokonaisuutena. Kaupungin ylin johto oli tietoinen ja osallistettiin harjoitukseen.
- Aivan sopiva kiireen tuntu, mutta ei liian kiire. Valmistelupäivät antoivat hyvän rytmin koko harjoituskokonaisuudelle.
- Harjoitus oli laadukkaasti, nuorekkaasti ja virkeästi toteutettu.

48. Viranomaisilmoitukset - jos teitte, miten arvioisitte niitä?

	TAISTO19	TAISTO18
• Ilmoitusten tekeminen tai lomakkeiden täyttäminen tietosuojavaltuutetun toimistolle oli sujuvaa n=86	3,63	3,64
• Ilmoitusten tekeminen tai lomakkeiden täyttäminen keskusrikospoliisille tapahtui oli sujuvaa n=89	4,13	3,49
• Ilmoitusten tekeminen tai lomakkeiden täyttäminen Viestintäviraston Kyberturvallisuuskeskukselle oli sujuvaa n=91	4,19	4,16

- Verrattuna edelliseen vuoteen, viranomaisilmoitukset ovat saaneet keskiarvoltaan paremman palautteen, etenkin KRP:n osalta on tapahtunut merkittävä parannus.

53.8. Tulevaisuuden harjoitustoiminta – osallistuminen TAISTO20?

	TAISTO19	TAISTO18
Kyllä	54,6%	64,1%
Todennäköisesti	36,2%	30,1%
Todennäköisesti emme	9,2%	5,9%
Emme	0,0%	0,0%

- Ilahduttavaa on havaita, että edelleen yli puolet on valmis osallistumaan vuonna 2020 ja yli 90% vähintään todennäköisesti. Käytännössä harjoitusten uudistaminen on tässä merkittävässä roolissa, jotta jo useimmat kahteen kertaan harjoitukseen osallistuneet näkevät harjoituksen itselleen riittävän hyödylliseksi osallistuakseen.

54. Millaisia harjoituksia toivoisitte tulevaisuudessa toteutettavan ja mitä niissä pitäisi harjoitella? 1/2

- Koska organisaatiot ovat hyvin eri tasoisia, toivoisin tiettyä väljyyttä kehykseen
- Kyllä tämän kertainen harjoitus lienee tätä päivää ja tulee valitettavasti lisääntymään, joten mielestäni vastaavanlainen harjoitus voisi olla paikallaan myös ensi vuonna.
- Todentuntuista täytyy olla ja muiden kriisivalmiusharjoitusten kaltaisia. Enemmän kuntien välistä yhteistä harjoittelua.
- Haittaohjelmien torjunta, sähköverkon ongelmat, tietoliikenteen katkot. Entä voisiko sosiaalisesta hakkeroinnista toteuttaa harjoituksen?
- Nyt kaksi Taistoa taistelleena harjoitukset tällaisenaan eivät enää meidän osaamista kehitä. Jatkossa Taistoon pitäisi saada jotain uutta, monimuotoisempaa, haastavampaa ym.
- Jatkossa voisi harjoitukseen ottaa mukaan organisaation toiminnan kannalta krittisen materiaalin tilaus/toimitusketjun häiriöt.

54. Millaisia harjoituksia toivoisitte tulevaisuudessa toteutettavan ja mitä niissä pitäisi harjoitella? 2/2

- Toimialakohtaisesti suunnattuja harjoituksia. Simulaattorissa toteutettavia pienempiä (ja suurempia) harjoituksia.
- Organisaation henkilöstön liittyviä harjoituksia.
- Tulevaisuuden harjoituksissa voisi käsitellä toimitiloihin liittyviä asioita, jotka ovat jääneet vähemmälle vuonna 2018 ja 2019.
- Onko mahdollista jakaa harjoituksia eri kohderyhmiin ja syventää kohdentamista?
- Taisto-formaatti on hyvä; vuosittainen osallistuminen ei kuitenkaan ole organisaatiollemme todennäköistä. Kevyempiin, järjestelmä/prosessikohtaisiin harjoituksiin malleja, joiden avulla esim. työpöytäharjoitus olisi helposti toteutettavissa.

55. Muuta palautetta TAISTO19-harjoituksesta?

- Kaiken kaikkiaan positiivinen harjoitus. Toivotaan ehdottomasti jatkoa uudella twistillä.
- Mukava humoristinen ote helpottaa sinänsä varsin teoreettisen aiheen käsittelyä ja harjoittelua. Sellaiset organisaatiot selviävät, joilla on osoittaa henkilövuoden tasolla tietoturvaan resurssia mutta pienempien kuntien onnistuminen riippuu yhteisresurssien käytön onnistumisesta.
- Taisto19 oli liiaksi toistoa v. 2018 harjoituksesta.
- TAISTO-harjoituksen konsepti on toimiva ja tarpeellinen. Kokonaisuutena harjoitus ansaitsee hyvän arvosanan ja toivon että TAISTOa kehitetään edelleen!
- Kiitos, että järjestätte TAISTO-harjoituksia. Näen, että tämä on hyvä kanava sitouttaa johtoa tietosuojaan ja tietoturvaan.

Yhteenveto - TAISTO18 vs TAISTO19

	v. 2018	v. 2019
• Osallistuneita henkilöitä	2215	2412 henkilöä
• Henkilötyöpäiviä	4318	3990 henkilötyöpäivää
• Ulkopuolisia	127	142 henkilötyöpäivää
• Tiedottaminen, ohjeistus ja yhteydenpito TAISTO19-harjoitukseen – ennen harjoitusta	4,43	4,39
• Millaisen arvosanan antaisitte Väestörekisterikeskukselle harjoitusta edeltävistä toimenpiteistä ennen harjoituspäivää	4,38	4,27

Organisaatioiden raportointi ja toiminta harjoituksessa

YHTEENVETOA

Raportointi

- Osana TAISTO19-harjoitusta pyysimme osallistuvia organisaatioita täyttämään RaportointiExcelin, jonka avulla halusimme selvittää,
  - miten organisaation tietoturvallisuuden hallintaa toteutetaan esimerkiksi tietoturvapäivitysten hallinnan osalta sekä muita tietoturvallisuuteen liittyviä keskeisiä kysymyksiä (koulutus, toimitilaturvallisuus)
  - kuinka organisaatio arvioi itse onnistuneensa syötteissä ja niissä annetuissa tehtävissä sekä
  - mitä asioita organisaatiot ovat itse tunnistaneet kehittämiskohteiksi.
- Olemme pisteyttäneet organisaation vastaukset ja tuottaneet niistä keski, minimi- ja maksiarvot, joihin raportointiin osallistuneet organisaatiot voivat omia tietojaan verrata.

Raportointi - yleistä

- Kysymykset liittyivät:

1. **Tietoturvapäivitysten hallinta**
   - Olemme tunnistaneet, että lukuisat eri organisaatioihin kohdistuneet onnistuneet hyökkäykset ovat onnistuneet johtuen palveluihin, järjestelmiin sekä palvelimiin ja päätelaitteisiin jääneistä tietoturvahaavoittuvuuksista

2. **Tietovuoto321-ryhmän uhkausten käsittely sekä viranomaisilmoitusten tekeminen sekä yleisiä kysymyksiä koskien tietoturvallisuutta**
   - kuinka organisaatio on toiminut ennen harjoituspäivää ennakkosyötteissä sekä tehnyt viranomaisilmoituksia

3. **Organisaationne toiminta harjoituksessa**
   - organisaationne toiminta harjoituspäivän ja ennakkosyötteiden osalta arviointinne mukaan

4. **Kehittämiskohteiden tunnistaminen**
   - Kuinka organisaatiot ovat tunnistaneet harjoituksessa olleita tehtäviä ja ilmiöitä erilaisiksi kehittämiskohteiksi – erityisen tärkeää on huolehtia nyt harjoituksen jälkeen sovittujen toimenpiteiden toteuttamisen seurannasta

Esimerkki arvioinnista:

Edellä esimerkki syötteisiin liittyvistä tehtävistä.

1) Kuinka arvioitte, että tämä osaltanne toimi?	5 Erittäin hyvin 4 Hyvin 3 Tyydyttävästi 2 Huonosti 1 Erittäin huonosti	2) Oletteko tunnistaneet tämän kehitys-kohteeksi?	5 Ei tarvitse kehittämistä 4 Ei tarvitse akuuttia kehittämistä , seurattava 3 Kehityskohde - korjattava 12 kk sisällä 2 Kehityskohde - korjattava 6 kk sisällä 1 Akuutti kehityskohde - korjattava ASAP

Organisaation tuli vastata, kuinka hyvin se selviytyi tästä tehtävästä asteikolla 1-5 sekä onko kyseinen tehtävä nostettu organisaatiossa kehityskohteeksi (1-5).

Raportointi – tulokset 1/3

	Keskiarvo	Minimi	Maksimi
1. Tietoturvapäivitysten hallinta (-4 - +12)	6,34	-1,75	12,00

- RaportointiExcelin kysymykset 1.1 – 1.6.

Yleisenä havaintona voisi todeta, että osalla organisaatiosta tilanne on varsin hyvin hallinnassa (jopa maksimipisteet), mutta osalla organisaatioista on enemmänkin kehitettävää. Mitä enemmän organisaation tulos on alle keskiarvon, sitä enemmän suosittelemme heitä tutkimaan tietoturvapäivitysten hallintaan liittyviä prosesseja. Usein näissä vastuussa on ulkoinen palveluntarjoaja, joka päivityksistä vastaa. Tällöin kannattaa tarkistaa, mitä esimerkiksi sopimuksissa niistä velvoitetaan ja tuottaako palveluntarjoaja sopimusten mukaista palvelua, esimerkiksi päivitysten toteuttamisen raportoinnin osalta.

Raportointi – tulokset 2/3

2. Tietovuoto321-ryhmän uhkausten käsittely sekä viranomaisilmoitusten tekeminen, yleiset tietoturvallisuuteen liittyvät kysymykset (-9 - + 19 pistettä)

- RaportointiExcelin kysymykset 2.1 – 3.6.

Keskiarvo	Minimi	Maksimi
12,21	4,25	19,00

Kyseinen kohta on saanut varsin hyvän keskiarvon. Organisaatiot arvioivat, että ne ovat pystyneet aika hyvin toteuttamaan syötteiden harjoitustehtävissä olleet asiat liittyen uhkausten hallintaan sekä tekemään viranomaisilmoitukset. Erityisesti ne tietoturvaan liittyvät kohdat, joissa organisaatio on vastannut eli kohtiin 3.1 – 3.6 tulee käydä läpi. Myös jokaisen selkeästi alle keskiarvon olevan organisaation kannattaa katsoa, mitkä kohdat he ovat arvioineet **huonoksi** tai **erittäin huonoksi ja kiinnittää niiden kehittämiseen erityistä huomiota.**

Raportointi – tulokset 3/3

3. Organisaationne toiminta harjoituksessa

Keskiarvo	Minimi	Maksimi
4,01	2,93	4,93

- RaportointiExcelin välilehti **Syötteet ja toiminta niissä**

Tässä kohdassa on arvioitu sitä, miten organisaation on onnistunut toiminnassaan itse harjoituspäivänä. Keskiarvo 4,01 tarkoittaa sitä, että keskimäärin organisaatiot ovat onnistuneet tehtävissä hyvin. Mitä kauempana oman organisaationne pistemäärä on keskiarvosta, sitä tarkemmin kannattaa katsoa kohdat, jossa olette **arvioineet oman toimintanne 2 Huono tai 1 Erittäin huono.**

Raportointi – tulokset

Oletteko tunnistaneet tämän kehityskohteeksi?
5 Ei tarvitse kehittämistä
4 Ei tarvitse akuuttia kehittämistä, seurattava
3 Kehityskohde – korjattava 12 kk sisällä
2 Kehityskohde – korjattava 6 kk sisällä
1 Akuutti kehityskohde – korjattava ASAP

4. Kehittämiskohteiden tunnistaminen

Keskiarvo	Minimi	Maksimi
3,74	2,25	4,82

- RaportointiExcelin välilehti **Syötteet ja toiminta niissä**

Keskiarvo 3,74 tarkoittaa sitä, että organisaatioiden näkökulmasta tilanne on varsin hyvin hallinnassa. Organisaation tulisi varmistaa, että kaikki ne kohdat jotka ovat 3) kehityskohde – korjattava 12 kk, 2) kehityskohde – korjattava 6 kk sekä ennen kaikkea **1) Akuutti – kohdattava ASAP ovat seurannassa ja huolehditaan sovittujen korjaustoimenpiteiden toteuttamisesta.**

Yhteenveto - raportointi

- TAISTO19-harjoitukseen liittyy kolme vaihetta:
  - Ennen harjoitusta tehty valmistelutyö
  - Harjoitusta edeltäneiden ennakkosyötteiden ja harjoituspäivän mukainen toiminta
  - Toimenpiteet harjoituksen jälkeen
- Toivomme, että jokainen harjoitusorganisaatio nyt noin 4 kk harjoituksen jälkeen käy huolella läpi ja arvioi sekä katselmoi vielä omia vastauksiaan ja varmistaa, miten harjoituksen perusteella tehtyjen, sovittujen kehittämistoimepiteiden osalta tilanne on edennyt.

Sosiaalinen media ja TAISTO19

Sosiaalisen median rooli TAISTO19

- Vuoden 2019 harjoituksessa aktivoitiin harjoitusorganisaatioita käyttämään sosiaalista mediaa, erityisesti Twitteriä osana harjoitusta. Tämä kutsu otettiin innolla vastaan. Samoin osa harjoituspäivän syötteistä liittyivät sosiaalisen median hyödyntämiseen.
- TAISTO19-tunniste nousikin harjoituspäivinä yhdeksi päivän suosituimmista tunnisteista.

TAISTO-harjoituksen uutisointi maailmalla

Fínsko chce posilniť odolnosť verejnej správy simulovanými kyberútokmi

Redakcia CyberSec / 25.11.2019 / Zo sveta

Doposiaľ sa uskutočnili dve cvičenia.

10. októbra obdržalo 235 obcí a verejných inštitúcií vo Fínsku výhražnú správu od aktivistickej skupiny nazývanej #Tietovuoto321 (únik dát 321). Správa obsahovala ultimátum, v ktorom hekeri požadovali zaplatiť výkupné v bitcoinoch do určitého dátumu pod hrozbou uskutočnenia kybernetických útokov.

NAJNOVŠIE ČLÁNKY

17.1.2020
Česko zorganizovalo celorepublikový workshop k ochrane nemocníc pred kyberútokmi

16.1.2020
Čína verbuje hekerov pomocou nastražených technologických firiem

15.1.2020
Ruskí hekeri údajne útočili na Ukrajine, hľadali špinu na Trumpovho súpera vo voľbách

13.1.2020
Americká vláda financuje predaj čínskych telefónov s predinštalovaným malvérom

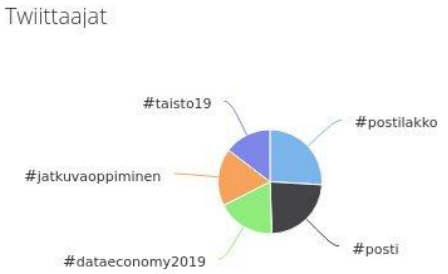
12.1.2020
Skupina Lazarus pokračuje v kradnutí kryptomien s novými nástrojmi

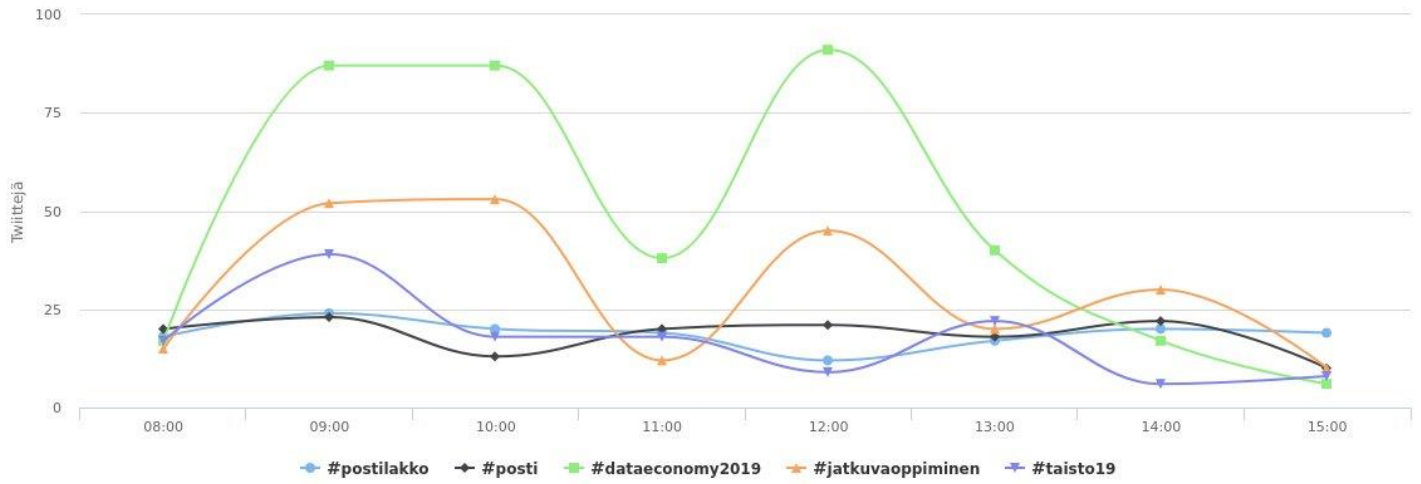
- Harjoitus huomattiin myös ulkomaalaisissa medioissa, YLEn englanninkieliseen uutiseen ja siihen liittyvään twiittiin viitattiin muutamassa uutisessa.

#TAISTO19 tiiviste nousi hyvin esille Twitterissä

ti 26.11.2019 klo 08:00 – ti 26.11.2019 klo 16:00

	Twiitit	Twiittaajat	Tavoittavuus
# postilakko	149 (n. 1 / hlö)	135	545 133
# posti	147 (n. 1 / hlö)	122	451 082
# dataeconomy2019	383 (n. 4 / hlö)	94	316 797
# jatkuvaoppiminen	237 (n. 3 / hlö)	93	299 334
# taisto19	137 (n. 2 / hlö)	76	191 518

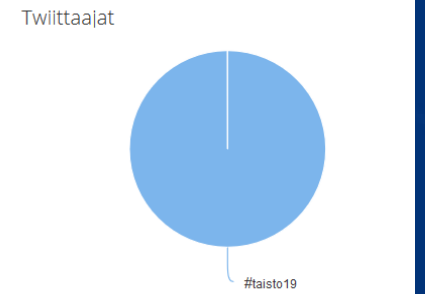


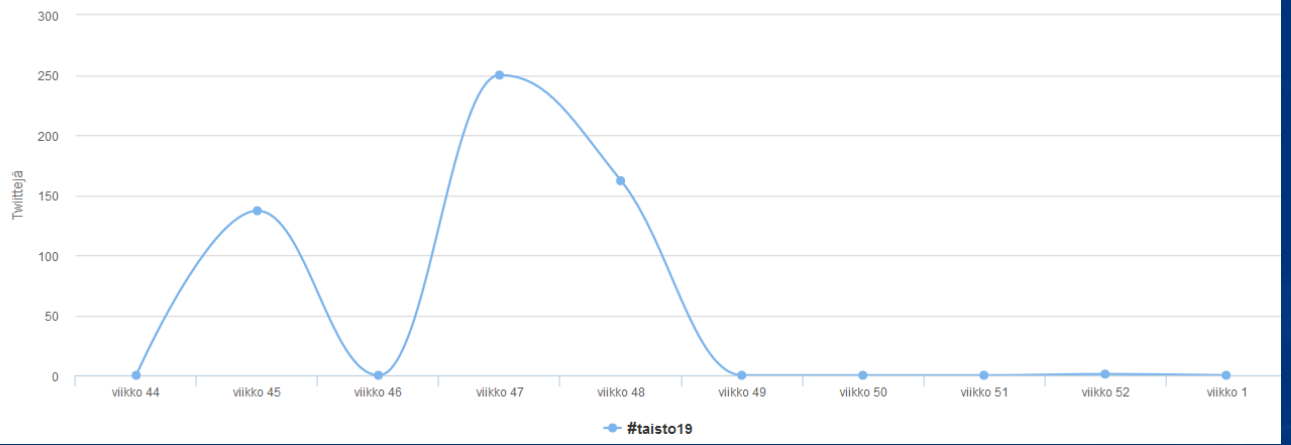


Kolmesta harjoituspäivästä 19.11 saavutti eniten huomiota somessa, Twitterissä tavoitettavuus yli puoli miljoonaa

pe 1.11.2019 klo 05:28 – ti 31.12.2019 klo 08:28

	Twiitit	Twittaajat	Tavoittavuus
# taisto19	550 (n. 2 / hlö)	240	557 565





Yhteenveto - tiivistys

- Kuten TAISTO18-harjoitusta, TAISTO19-harjoitusta voidaan pitää menestyksenä. Kaikista yllättävin havainto on ollut se, että uusien harjoitukseen osallistuneiden organisaatioiden määrä harjoituksessa on ollut varsin pieni (noin 30 organisaatiota) eli valtaosa osallistuneista organisaatioista on osallistunut harjoitukseen kahteen kertaan. Tämä asettaa erityisesti tarvetta tarjota näille TAISTO-veteraaneille vuonna 2020 merkittävästi uudistunut harjoitus.
- Vastaavasti, jotta saamme vielä yli puolet niistä organisaatioista mukaan, jotka eivät ole vielä osallistuneet tuleviin harjoituksiin, tulemme erityisesti kiinnittämään huomiota viestintään, jotta saamme mukaan uusia osallistujia.
- Ilahduttavaa oli havaita, että harjoitus kiinnosti muutamia huoltovarmuuskriittisiä yrityksiä, joilla on kriittinen rooli myös koko yhteiskunnan toiminnan kannalta. Toivomme saavamme myös näitä organisaatioita jatkossa enemmän mukaan.

Lisätietoa:

- TAISTO18 ja TAISTO19-harjoitukset
  - Kimmo.Rousku@dvv.fi, puh. 0295 535 120

- TAISTO20-harjoitus
  - Hanna.Heikkinen@dvv.fi, puh. 0295 535 121
  - Laura.Penttila@dvv.fi, puh 0295 535 290