DIGI- JA VÄESTÖTIETO-VIRASTO

Taisto-harjoitus 2022

Käsikirjoitus

9.12.2022

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Dokumentinhallinta

Omistaja	Hanna Heikkinen
Laatinut	Hanna Heikkinen, Laura Penttilä, Rosa Hyvärinen

Sisällys

Taisto-harjoitus 2022

Käsikirjoitus sisältää vuoden 2022 Taisto-harjoituksen harjoitusalustalle vietävät tiedot.

1 Ennakkomateriaali

Harjoitusalustalla julkaistaan ennakko-ohjeistus ennen harjoitusta. Sama ennakko-ohjeistus julkaistaan myös osoitteessa dvv.fi/taisto.

1.1 Ennakko-ohjeistus

Harjoitusinfo: Ohje Taisto-harjoituksen viranomaisilmoituksia tekevälle

Taisto-harjoituksessa olet organisaatiosi viranomaisilmoituksia tekevä henkilö, ja tehtävänäsi on laatia tarvittavat viranomaisilmoitukset Keskusrikospoliisille, tietosuojavaltuutetun toimistolle sekä Kybertuvallisuuskeskukselle.

Taisto-harjoituksessa viranomaisiin ei oteta yhteyttä samalla tavalla kuin todellisessa tilanteessa, vaan kaikki ilmoitukset tehdään harjoitusalustan webropol-lomakkeiden kautta. Nämä lomakkeet vastaavat Keskusrikospoliisin, tietosuojavaltuutetun toimiston ja Kyberturvallisuuskeskuksen aitoja viranomaisilmoituksia.

Keskusrikospoliisin ja tietosuojavaltuutetun toimiston viranomaisilmoitukset tehdään suoraan harjoitusalustalla. Sen sijaan Kyberturvallisuuskeskukselle ilmoitettavien tietoturvaloukkausten osalta harjoitusalustalla on linkki, joka ohjaa Kyberturvallisuuskeskuksen erilliselle webropol-lomakkeelle. Tämä menettely mallintaa heidän harjoituspäivystystään.

Viranomaisilmoituksen webropol-lomakkeen lähetettyäsi saat vahvistuksen ilmoituksen vastaanottamisesta. Tämä tarkoittaa, että viranomaisilmoitus on tehty onnistuneesti. Taisto-harjoituksen jälkeen toimitamme koontiraportit harjoituspäivänä tehdyistä viranomaisilmoituksista kullekin viranomaistaholle analysoitavaksi. Organisaatiosi ei kuitenkaan saa jättämistään viranomaisilmoituksista erillistä palautetta, vaan menettelyn tarkoituksena on viranomaistoiminnan kehittäminen.

Ohjeet ja linkit viranomaisilmoituksien tekemiseen löytyvät harjoitusalustalta.

HUOM. Käyttäjätunnuksesi on henkilökohtainen ja voit kirjautua harjoitusalustalle vain yhdeltä laitteelta kerrallaan. Muuten käyttäjätunnus lukittuu.

Harjoitusinfo: Ohje Taisto-harjoituksen viestintävastaavalle

Taisto-harjoituksessa olet organisaatiosi viestintävastaava, ja tehtävänäsi on laatia sisäisiä ja ulkoisia tiedotteita samalla tavalla kuin aidossa häiriö- tai poikkeamatilanteessa. Jos harjoitustiimiinne kuuluu tarkkailija ja/tai viestintätarkkailija, muista jakaa kaikki harjoituksessa laatimasi viestintäsisällöt myös heille.

Voit julkaista organisaatiosi ulkoisia tiedotteita ja sosiaalisen median julkaisuja vastaavia ”Quacker-päivityksiä” suoraan harjoitusalustalla. Noudatathan liitteenä olevaa julkaisuohjetta eli julkaiset kaikki ulkoiset sisällöt ”Taisto – Organisaation ulkoinen viestintä” -sivulla. Huomaathan, että harjoitusalustalle voi tehdä julkaisuja vain viestintävastaavan käyttäjätunnuksilla ja että harjoitusalustalle tehtävät julkaisut näkyvät kaikille harjoitukseen osallistuville organisaatioille.

Organisaatiosi sisäisiä tiedotteita ei julkaista harjoitusalustalla, vaan ne laaditaan organisaation omilla työvälineillä ja käsitellään sisäisesti.

Ethän tee julkaisuja ”Taisto-harjoitus”-sivulle!

Jos julkaiset virheellisesti organisaation sisäistä viestintää harjoitusalustalla, otathan välittömästi yhteyttä osoitteeseen taisto@dvv.fi ja otsikoit viestisi ”Taisto-harjoitus julkaisun poisto”.

HUOM. Käyttäjätunnuksesi on henkilökohtainen ja voit kirjautua harjoitusalustalle vain yhdeltä laitteelta kerrallaan. Muuten käyttäjätunnus lukittuu.

Harjoitusinfo: Ohje Taisto-harjoituksen näyttövastaaville

Taisto-harjoituksessa olet näyttövastaava, ja tehtävänäsi on jakaa harjoitusalustan näkymä muulle harjoitustiimille. Voit jakaa omalla näytölläsi olevan harjoitusalustanäkymän joko fyysisessä kokoustilassa tai virtuaalikokouksessa näytönjaon kautta.

Kun jaat harjoitusalustalla olevia videoita, huomioithan seuraavat seikat:

- Teamsin kautta videoiden äänet saa kuuluviin valitsemalla ”Jaa sisältö” ja ”Sisällytä tietokoneen ääni”.
- Skypessä videoiden ääntä ei saa jaettua, vaan videot kannattaa jakaa linkkeinä harjoitustiimille. ”Kopioi linkki” -valinnan löydät kunkin videon oikeasta yläkulmasta. Kaikki harjoitusalustan videot ovat YouTubessa, eli videot eivät vaadi harjoitusalustan käyttöoikeuksia toimiakseen.

Harjoitusalustan käyttöön liittyvissä ongelmatilanteissa otathan meihin välittömästi yhteyttä sähköpostilla taisto@dvv.fi ja otsikoit viestisi ”Taisto-harjoitus tekninen häiriö”.

HUOM. Käyttäjätunnuksesi on henkilökohtainen ja voit kirjautua harjoitusalustalle vain yhdeltä laitteelta kerrallaan. Muuten käyttäjätunnus lukittuu.

Tietoisku: Keskusrikospoliisi

Voit avata videon myös tämän linkin kautta: https://youtu.be/P0aqWAUhqp8
Voit myös jakaa linkkiä muille organisaatiosi osallistujille tarvittaessa.

Tietoisku: Liikenne- ja viestintävirasto Kyberturvallisuuskeskus

Voit avata videon myös tämän linkin kautta: https://youtu.be/QyAsC0fJCSk
Voit myös jakaa linkkiä muille organisaatiosi osallistujille tarvittaessa.

Taustamateriaalia harjoitukseen valmistautumista varten

Kaikki Taisto-harjoituksessa tarvittavat ohjeet ja materiaalit löytyvät osoitteesta dvv.fi/taisto.

Lisämateriaalit

Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla -koulutus
https://www.eoppiva.fi/koulutukset/digitaalinen-turvallisuus-jarjestykseen-arkkitehtuurin-avulla/

Turvaa digitaalinen toiminta häiriötilanteissa -koulutus
https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa/

Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta
https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisiasia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf

Kyberturvallisuuskeskuksen ohjeet ja oppaat organisaatioille ja yrityksille
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Taisto-somehaaste

Taisto-harjoituksessa on käynnissä vapaaehtoinen somehaaste, jossa kehitetään mielikuvaa digiturvasta. Toivomme, että koko harjoitustiiminne osallistuu haasteeseen.

Somehaasteessa haastamme teidät kuvaamaan fiiliksen ennen Taistoa. Valmistautuessanne haette kenties voimaa sotahuudosta ja -maalauksista, strategiapalaverista tai kunnollisesta eväiden tankkauksesta?

Julkaiskaa myös harjoituksen päätteeksi toinen kuva Taiston jälkeisistä tunnelmista, josta välittyy, miten Taistossa sujui. Kuvatkaa, millaista riemujuhlaa teillä vietetään tai kuinka harjoituksesta selviydyttiin vaikeuksista huolimatta maaliin asti.

Huomioittehan oman organisaationne some-ohjeistuksen esimerkiksi henkilöitä sisältävistä julkaisuista.

Jaattehan Ennen ja jälkeen -kuvat tai -tekstin harjoituspäivästänne Twitterissä ja/tai LinkedInissä tunnisteella **#Taisto**. Muistattehan tuoda julkaisuissanne esiin, että kyseessä on harjoitus.

1.2 Ennakkotehtävä

Ennakkotehtävä julkaistaan osoitteessa dvv.fi/taisto, ja lisäksi se toimitetaan harjoituksen yhteyshenkilöille sähköpostilla.

Ennakkotehtävä on vapaaehtoinen, mutta sen avulla harjoitustiiminne voi valmistautua harjoitukseen. Vastaukset jäävät omaan käyttöönne, eikä niitä tarvitse palauttaa.

Käykää läpi organisaationne varautumisen toimintamalleja ja ohjeita sähkönjakelun rajoituksista aiheutuvien sähkökatkojen varalta:

- Oletteko tunnistaneet ja dokumentoineet käytössänne olevat varavirtalaitteet sekä varmistaneet niiden toimivuuden?
- Mitä toimintoja niiden avulla on mahdollista ylläpitää vähintään kahden tunnin ajan?
- Miten toimitte, jos kahden tunnin kiertäviä katkoja osuu kohdallenne useamman kerran 12 tunnin sisällä?
- Kykenevätkö varavirtajärjestelmänne huolehtimaan niihin kytkettyjen laitteiden sammuttamisesta, jos varavirtalähteiden tuottama sähkö ei riitä koko sähkökatkon ajaksi? Jos näin ei ole, millaisia uhkia tästä voi syntyä?

Lisäksi pohtikaa asiaa myös seuraavista näkökulmista, jos sähkökatkot kohdistuvat:

a) organisaation toimitiloihin, esimerkiksi

   - miten sähkökatko vaikuttaa työskentelyyn ja liikkumiseen toimitiloissa?
   - onko toimitiloissa sellaisia operatiivisia järjestelmiä tai niiden osia, joiden toiminnan pysäyttäminen saattaa vaikuttaa muihin, toiminnassa oleviin, palveluihin tai prosesseihin?

b) henkilöstön koteihin, esimerkiksi

   - millaista ohjeistusta henkilöstölle annetaan, jos sähkökatko osuu työajalle?

c) kriittisiin palveluntarjoajiin, esimerkiksi

   - miten palveluntarjoaja pystyy huolehtimaan sen vastuulla olevien kriittisten palveluiden tuottamisesta sähkönjakelurajoitusten aikana?
   - onko kriittisten palveluiden sopimuksissa otettu sähkönjakelurajoitukset huomioon?

2 Harjoitusinfot

2.1 Aamupäivän harjoitus

Harjoitusinfo: Tervetuloa Taisto-harjoitukseen!

Taisto-harjoitus käynnistyy tällä sivulla harjoituspäivänä klo 09:00.

Harjoitukseen liittyvään ennakkomateriaaliin ja ohjeisiin voitte tutustua **Taisto-harjoituksen ennakkomateriaalit** -sivulla.

Lisätietoja Taisto-harjoituksesta saatte myös osoitteesta dvv.fi/taisto.

Harjoitusinfo: Taisto-harjoituksen viestintävastaava

Taisto-harjoituksen viestintävastaavan tehtävänä on laatia sisäisiä ja ulkoisia tiedotteita samalla tavalla kuin aidossa häiriö- tai poikkeamatilanteessa. Viestintävastaavan ohjeet ovat saatavilla ennakkomateriaalista ”Ohje Taisto-harjoituksen viestintävastaavalle” .

- Viestintävastaava voi julkaista organisaation ulkoisia tiedotteita ja sosiaalisen median julkaisuja vastaavia ”Quacker-päivityksiä” harjoitusalustan ”Taisto – Organisaation ulkoinen viestintä – Organisationens externa kommunikation 10.11.2022”-sivulla.
- Organisaation sisäisiä tiedotteita ei saa julkaista harjoitusalustalla, vaan ne laaditaan organisaation omilla työvälineillä ja käsitellään sisäisesti.

Harjoitusalustalle voi lisätä julkaisuja vain viestintävastaavan käyttäjätunnuksilla, ja nämä julkaisut näkyvät kaikille harjoitukseen osallistuville organisaatioille.

Julkaisuja ei tule tehdä ”Taisto-harjoitus”-sivulle!

Jos organisaation sisäistä viestintää julkaistaan virheellisesti harjoitusalustalla, otattehan välittömästi yhteyttä osoitteeseen taisto@dvv.fi ja otsikoitte viestin ”Taisto-harjoitus julkaisun poisto”.

Harjoitusinfo: Ohjeita harjoituspäivään

Taisto-harjoituksen kohderyhmä on laaja, joten harjoituksen tapahtumat ja syötteet kuvataan hyvin yleisellä tasolla. Suosittelemme miettimään jokaisen tapahtuman ja tehtävän osalta: ”Mitä jos tämä tapahtuisi meille?” ja ”Voisiko näin käydä myös meillä?”. Harjoituksessa kannattaa olla yhtä realistinen kuin tositilanteessa, jotta saatte harjoituksesta parhaan mahdollisen hyödyn. Toivomme, ettei harjoitustiiminne

pelaa harjoitusta vastaan eli etsi tapahtumista ja tehtävistä virheitä, joilla ne voidaan ohittaa tai kiertää.

Vinkit onnistuneeseen harjoitukseen

- tulkaa harjoitukseen positiivisella ja avoimella mielellä
- kirjautukaa harjoitusalustalle hyvissä ajoin ennen harjoituksen alkua
- katsokaa harjoituksen aloittava uutiskatsaus huolellisesti, sillä se pohjustaa harjoituksen maailmankuvaa
- toimikaa ja viestikää kuten todellisessa häiriötilanteessa
- peilatkaa harjoituksen tapahtumia ja tehtäviä omaan organisaatioonne
- tehkää tehtävät teille sopivassa tahdissa
- hyödyntäkää harjoituspäiväkirjaa (ladattavissa osiosta Liitteet)
- muistakaa, että yhteistyössä on voimaa!

Harjoitusinfo: Harjoituspäivän kulku

Taisto-harjoitus rakentuu Trasim-harjoitusalustalla julkaistavista tapahtumista, niihin liittyvistä syötteistä ja tehtävistä. Harjoituspäivänne pituus määräytyy ilmoittautumisen yhteydessä tekemänne valinnan perusteella: puolenpäivän harjoitus päättyy klo 12 ja kokopäivän harjoitus klo 15. Huomaattehan, että klo 11:30 alkaa tunnin tauko kokopäivän harjoitukseen osallistujille.

Aloittakaa harjoituspäivä kokoontumalla yhteen ja kirjautumalla harjoitusalustalle hyvissä ajoin ennen harjoituksen alkua. Tervehdys- ja harjoitusinfovideot ovat katsottavissa harjoitusalustalla harjoituspäivän aamuna klo 7 alkaen.

Liitteet

Taisto-harjoituspäiväkirja.xlsx

Tarkkailijan havaintolomake

Viestinnän tarkkailijan havaintolomake

08:00– **Harjoitustiimi kokoontuu**

09:00 **Harjoituspäivä alkaa harjoitusalustalla**
- Harjoituksen avaus
- Harjoituksen maailmankuvaa avaava uutislähetys

Tapahtuma 1 ja siihen liittyvät tehtävät
Tapahtuma 2 ja siihen liittyvät tehtävät
Tapahtuma 3 ja siihen liittyvät tehtävät
Tapahtuma 4 ja siihen liittyvät tehtävät
Tapahtuma 9 ja siihen liittyvät tehtävät **(VAIN puolenpäivän harjoittelijat)**

11:30–12:30 Kokopäivän harjoittelijoiden tauko

12:00 **Puolenpäivän harjoitus päättyy**
- Jälkitoimet puolenpäivän harjoituksen päättäneille

12:30 **Kokopäivän harjoitus jatkuu**
- Uutisextra

Tapahtuma 5 ja siihen liittyvät tehtävät
Tapahtuma 6 ja siihen liittyvät tehtävät
Tapahtuma 7 ja siihen liittyvät tehtävät
Tapahtuma 8 ja siihen liittyvät tehtävät
Tapahtuma 9 ja siihen liittyvät tehtävät

15:00 **Kokopäivän harjoitus päättyy**
- Jälkitoimet harjoituspäivän päättäneille

Harjoitusalustalla syötteiden otsikoissa näkyy numero, joka ryhmittelee tapahtumaan liittyvät syötteet. Tällä tavalla pystytte yhdistämään tilanne- ja mediasyötteet sekä niihin liittyvät tehtävät.

Harjoituksen kulkuun, tapahtumiin tai syötteisiin liittyvissä ongelmatilanteissa, otattehan meihin välittömästi yhteyttä sähköpostilla taisto@dvv.fi ja otsikoitte viestinne ”Taisto-harjoitus ongelmatilanne”.

Harjoitusinfo: Taisto-somehaaste

Taisto-harjoituksessa on käynnissä vapaaehtoinen somehaaste, jossa kehitetään mielikuvaa digiturvasta. Toivomme, että koko harjoitustiiminne osallistuu haasteeseen.

Somehaasteessa haastamme teidät kuvaamaan fiiliksen ennen Taistoa. Valmistautuessanne haette kenties voimaa sotahuudosta ja -maalauksista, strategiapalaverista tai kunnollisesta eväiden tankkauksesta?

Julkaiskaa myös harjoituksen päätteeksi toinen kuva Taiston jälkeisistä tunnelmista, josta välittyy, miten Taistossa sujui. Kuvatkaa, millaista riemujuhlaa teillä vietetään tai kuinka harjoituksesta selviydyttiin vaikeuksista huolimatta maaliin asti.

Huomioittehan oman organisaationne some-ohjeistuksen esimerkiksi henkilöitä sisältävistä julkaisuista.

Jaattehan Ennen ja jälkeen -kuvat tai -tekstin harjoituspäivästänne Twitterissä ja/tai LinkedInissä tunnisteella **#Taisto**. Muistattehan tuoda julkaisuissanne esiin, että kyseessä on harjoitus.

Harjoitusinfo: Harjoituksen medialähteet harjoitusalustalla

Taisto-harjoituksen tapahtumat ja mediatilannekuva välitetään harjoitusalustan kautta. Tilannesyötteet (tapahtumien tiedot ja tehtävät) julkaistaan harjoitusalustan vasemmalle puolelle eli tämän sivun vasempaan laitaan.

Harjoituksessa ”Organisaatiolla” tarkoitetaan omaa organisaatiotanne. Lisäksi harjoituksen tehtävissä teitä pyydetään valitsemaan organisaationne toiminnan kannalta kriittisiä tietojärjestelmiä/palveluja, joiden avulla tehtävät tehdään. Harjoituksen tapahtumissa, syötteissä ja tehtävissä ”kriittinen tietojärjestelmä/palvelu” viittaa itse valitsemaanne järjestelmään tai palveluun.

Harjoitusinfot ovat merkitty -symboleilla.

Tehtävät ovat merkitty -symboleilla.

Mediasyötteet (sosiaalinen media ja verkkomedia) näkyvät harjoitusalustanäkymän oikealla puolella. Kaikki syötteet ilmestyvät automaattisesti harjoitusalustalle, eikä sivua tarvitse erikseen päivittää. Harjoitusalustalla syötteiden otsikoissa näkyy numero, joka ryhmittelee jokaiseen tapahtumaan liittyvät syötteet. Tällä tavalla pystytte yhdistämään tilanne- ja mediasyötteet sekä niihin liittyvät tehtävät. Harjoituksen edetessä voitte selata aiempia syötteitä sivua vierittämällä.

Harjoituksessa on käytössä mediat:

Yleismedia: Valtakunnallinen, poliittisessa ohjauksessa toimiva, radio- ja TV-toimintaa harjoittava viestintäyhtiö.

Iltanen: Suomen suurin iltapäivälehti ja samalla Suomen suurin uutismedia.

Quacker: Suosittu sosiaalisen median yhteisöpalvelu, jossa lähetetään lyhyitä ajankohtaisviestejä #-tunnisteilla varustettuna.

Sanomat Uudeltamaalta: Alun perin Helsingissä ilmestynyt, valtakunnan tärkeimmäksi ja arvostetuimmaksi päivälehdeksi noussut media.

ViTi: Suomalainen tieto- ja viestintätekniikan uutislehti.

Lähteet kuvastavat tunnettuja medioita ja sosiaalisen median kanavia. Nämä syötteet sisältävät myös videoita, joita pääsette katsomaan painamalla videon play-painiketta.

Harjoitusinfo: Taisto-harjoituksen avaustervehdys

Käynnistä video play-painikkeesta. Videon saat koko ruudun näkymään, kun klikkaat oikeasta alareunasta. Videon kesto on 2:30 minuuttia.

Tarvittaessa voit jakaa videon linkkinä oman organisaatiosi osallistujille, tässä linkki: https://youtu.be/sxtnt7FJFo0

2.2 Iltapäivän harjoitus

Harjoitusinfo: Puolenpäivän harjoitus on päättynyt

Kokopäivän harjoitukseen osallistuvat organisaatiot

Seuraava syöte julkaistaan harjoitusalustalla klo 12:30, joten voitte pitää tauon tässä välissä.

Puolenpäivän harjoitukseen osallistuvat organisaatiot

Taisto-harjoitus on päättynyt!

Pyydämme jokaista harjoitustiiminne jäsentä vastaamaan lyhyeen Menti-kyselyyn osoitteessa www.menti.com. Kyselyn koodi on xxxx xxxx. Syötä tämä koodi Menti-järjestelmään.

Menti-kyselyyn vastattuanne käykää läpi kesken jääneet tehtävät ja täydentäkää vastauksianne tarvittaessa. Tämän jälkeen keskustelkaa lyhyesti harjoituspäivän tapahtumista: Miten harjoituspäivänne sujui? Missä onnistuitte? Missä voisitte jatkossa parantaa? Näin saatte koottua kaikkien harjoitustiimin jäsenten ensivaiheen huomiot harjoituspäivästä.

Harjoituksen jälkeen lähetämme yhteyshenkilöllenne myös erillisen palautekyselyn. Sen tarkoituksena on mitata Taisto-harjoituksen onnistumista ja vaikuttavuutta sekä kehittää tulevien vuosien Taisto-harjoituksia vastaamaan osallistujien tarpeisiin ja odotuksiin. Toivomme, että annatte palautetta aktiivisesti.

Lisäksi organisaationne kannalta on erittäin tärkeää, että käytte jälkikäteen läpi harjoituksen aikana tehdyt havainnot ja suunnittelette niiden pohjalta tarvittavat kehittämistoimenpiteet. Suosittelemme laatimaan havaituille kehittämiskohteille realistisen toteutusaikataulun, selvittämään niiden vaatimat resurssit ja nimeämään vastuuhenkilöt.

Kiitos osallistumisesta Taisto-harjoitukseen!

Harjoitusinfo: Tervetuloa harjoituksen iltapäiväosuuteen!

Taisto-harjoitus jatkuu

Harjoitusinfo: Taisto-somehaaste

Taisto-harjoituksessa on käynnissä vapaaehtoinen somehaaste, jossa kehitetään mielikuvaa digiturvasta. Toivomme, että koko harjoitustiiminne osallistuu haasteeseen.

Somehaasteessa haastamme teidät kuvaamaan fiiliksen ennen Taistoa. Valmistautuessanne haette kenties voimaa sotahuudosta ja -maalauksista, strategiapalaverista tai kunnollisesta eväiden tankkauksesta?

Julkaiskaa myös harjoituksen päätteeksi toinen kuva Taiston jälkeisistä tunnelmista, josta välittyy, miten Taistossa sujui. Kuvatkaa, millaista riemujuhlaa teillä vietetään tai kuinka harjoituksesta selviydyttiin vaikeuksista huolimatta maaliin asti.

Huomioittehan oman organisaationne some-ohjeistuksen esimerkiksi henkilöitä sisältävistä julkaisuista.

Jaattehan Ennen ja jälkeen -kuvat tai -tekstin harjoituspäivästänne Twitterissä ja/tai LinkedInissä tunnisteella #Taisto. Muistattehan tuoda julkaisuissanne esiin, että kyseessä on harjoitus.

Harjoitusinfo: Kokopäivän harjoitus on päättynyt

Taisto-harjoitus on päättynyt!

Harjoitusalustalle ei enää julkaista uutta sisältöä.

Pyydämme jokaista harjoitustiiminne jäsentä vastaamaan lyhyeen Menti-kyselyyn osoitteessa www.menti.com. Kyselyn koodi on xxxx xxxx. Syötä tämä koodi Menti-järjestelmään.

Menti-kyselyyn vastattuanne käykää läpi kesken jääneet tehtävät ja täydentäkää vastauksianne tarvittaessa. Tämän jälkeen keskustelkaa lyhyesti harjoituspäivän tapahtumista: Miten harjoituspäivänne sujui? Missä onnistuitte? Missä voisitte jatkossa parantaa? Näin saatte koottua kaikkien harjoitustiimin jäsenten ensivaiheen huomiot harjoituspäivästä.

Harjoituksen jälkeen lähetämme yhteyshenkilöllenne myös erillisen palautekyselyn. Sen tarkoituksena on mitata Taisto-harjoituksen onnistumista ja vaikuttavuutta sekä kehittää tulevien vuosien Taisto-harjoituksia vastaamaan osallistujien tarpeisiin ja odotuksiin. Toivomme, että annatte palautetta aktiivisesti.

Lisäksi organisaationne kannalta on erittäin tärkeää, että käytte jälkikäteen läpi harjoituksen aikana tehdyt havainnot ja suunnittelette niiden pohjalta tarvittavat kehittämis-

toimenpiteet. Suosittelemme laatimaan havaituille kehittämiskohteille realistisen toteutusaikataulun, selvittämään niiden vaatimat resurssit ja nimeämään vastuuhenkilöt.

Kiitos osallistumisesta Taisto-harjoitukseen!

3 Aamupäivän harjoitus (09:00–12:00)

Harjoituksen avausvideo, Hanna Heikkinen DVV

Mediasyöte: Yleismedian uutislähetys Suomeen kohdistuvasta valtiollisesta vaikuttamisesta

Aihe 1: Fingrid / TEM tiedottavat sähkönjakelun rajoittamisesta

Uutisankkuri: Kantaverkkoyhtiö Fingrid ja työ- ja elinkeinoministeriö ovat tiedottaneet sähkönjakelun rajoittamisesta. Sähkönjakelua voidaan tulevaisuudessa joutua rajoittamaan hyvinkin nopealla varoitusajalla, jos sähköpulatilanteeseen ajaudutaan. Sähköä on koko ajan tuotettava yhtä paljon kuin sitä kulutetaan. Sähköpula tarkoittaa tilannetta, jossa sähkön tuotanto ja tuonti eivät riitä kattamaan sähkön kulutusta. Tällöin kulutusta joudutaan rajoittamaan katkaisemalla sähkönjakelu hetkellisesti tietyltä alueelta.

Uutisankkuri: Fingridin toimitusjohtaja Pekka Kukkanen, hyvää päivää. Kansalaisilla on noussut suuri huoli tulevista sähkökatkoksista. Mitä vaikutuksia mahdollisilla tulevilla sähkökatkoilla on suomalaiseen yhteiskuntaan, ja voidaanko kaikista kriittisimpien toimintojen sähkönsaanti varmistaa?

Fingrid: Kun sähköjä joudutaan katkaisemaan, katkot eivät koske yhteiskunnan kaikkien kriittisimpiä toimintoja, kuten sairaaloita. Emme kuitenkaan voi taata, että kaikissa kriittiseksi nähdyissä kohteissa voidaan turvata häiriötön sähkönsaanti sähköpulatilanteessa. Siksi onkin tärkeää, että kyseisten toimintojen varajärjestelyitä mietitään etukäteen, aivan kuten normaalin – esimerkiksi myrskystä johtuvan – sähkökatkon varalta.

Uutisankkuri: Miten tavalliset ihmiset voivat toimia, jotta sähkönjakelun katkoksia voitaisiin välttää tai ainakin niiden määrää vähentää?

Fingrid: Jokainen voi vaikuttaa omalta osaltaan tarkkailemalla sähkön käyttöään ja ennen kaikkea käyttämällä sähköä säästeliäästi. Kulutusta kannattaa välttää etenkin silloin, kun sähkönkulutus on suurinta koko maassa eli arkiaamuisin ja -iltapäivisin.

Suomalaisissa kodeissa eniten sähköä kuluttavat kodinkoneet, saunominen ja valaistus. Sähkölämmitteisissä pientaloissa eniten sähköä kuluttaa kodin ja veden lämmitys. Säästöä saa säätämällä lämpötilaa hieman alaspäin ja käyttämällä sähköä vain kaikkein olennaisimpien laitteiden ohella. Nyt ei ole aika lämmittää saunoja tai ulkoporealtaita!

Uutisankkuri: Kiitos haastattelusta!

[**Grafiikka**: Voimalaitos]

Aihe 2: Maksukorteilla maksamisessa on laajoja ongelmia

Uutisankkuri: Maksukorteilla maksamisessa on ollut laajoja häiriöitä. Maksaminen korteilla on ollut hidasta tai epäonnistunut kokonaan. Tämä on saanut ihmiset sankoin joukoin pankkiautomaateille nostamaan käteistä rahaa. Pankkiautomaatit ovat olleet hyvin ruuhkautuneita ja pankkien konttoreihin on siirretty henkilökuntaa purkamaan kasvaneita jonoja. Toimittajamme on haastatellut muutamaa käteistä rahaa nostanutta henkilöä.

Toimittaja: Saitteko rahaa nostettua?

Kansalainen 1: No en ole saanut. Nyt on jo kolmas automaatti, mistä olen yrittänyt. Käsittämätön tilanne, kun neljä nälkäistä lasta kotona odottaa ja pitäisi ruokaa saada ostettua, mutta ei saa rahaa mistään. Korttimaksaminen ei toimi. Kyllä tässä tekisi mieli tili nostaa tyhjäksi, mutta ei sekään tunnu onnistuvan.

Toimittaja: Iltasen toimituksesta, terve. Saitte ilmeisesti rahaa nostettua?

Kansalainen 2: Kyllä, sain.

Toimittaja: Paljonko nostitte?

Kansalainen 2: Koko tilin tyhjäksi.

Toimittaja: Miksi näin?

Kansalainen 2: No lueskelin tuolta somesta, että käteinen raha saattaa loppua Suomesta kesken, ja korttimaksaminen ei kaikissa kaupoissa enää toimi.

Toimittaja: Jouduitteko käymään usealla automaatilla, että saitte rahaa nostettua?

Kansalainen 2: Kyllä, tämä taisi olla kuudes tai seitsemäs automaatti.

Aihe 3: Finanssisektoriin kohdistunut kyberhyökkäyksiä

[**Grafiikka**: Pörssikurssit]

Uutisankkuri: Usea suomalainen pankki ja finanssialan yritys on ilmoittanut joutuneensa kyberhyökkäyksen kohteeksi. Hyökkäykset ovat ilmeisesti alkaneet eilisillan aikana ja jatkuneet tänään. Tällä hetkellä ei ole tarkempaa tietoa aiheutuneista vahingoista, mutta useamman pankin verkkosivut ovat olleet alhaalla vielä tänään. Myöskään hyökkääjästä tai hyökkäyksen motiiveista ei ole tässä vaiheessa tietoa, mutta asiantuntijoiden mukaan taustalla on hyvin todennäköisesti valtiollinen taho, joka yrittää näillä toimilla vaikuttaa Euroopan maiden päättäjiin.

Uutisankkuri: Kyberturvallisuusasiantuntija Pekka Porkka, kuinka vakavasta hyökkäyksestä on kyse ja mikä taho voisi olla niiden taustalla?

Pekka Porkka: Kyseessä on hyvin vakava hyökkäys, koska se vaikuttaa koordinoidulta ja on kohdistettu yhteiskunnan kannalta kriittisiin toimijoihin.

Uutisankkuri: Onko vahinkojen laajuudesta tällä hetkellä tietoa?

Pekka Porkka: Tässä vaiheessa on liian aikaista arvioida vahinkojen laajuutta, koska hyökkäys on vielä käynnissä. Vaikuttaa siltä, että useampien finanssiyritysten sivut ovat alhaalla. Tämä viittaa palvelunestohyökkäyksiin. Myöhemmin selviää, kuinka nopeasti yritykset pystyvät palautumaan ja onko tietoihin tai järjestelmiin päästy käsiksi.

Uutisankkuri: Ovatko vain suomalaiset yritykset olleet hyökkäyksen kohteena, vai koskeeko hyökkäys esimerkiksi muita EU-maita?

Pekka Porkka: Oman analyysimme ja mediassa esiin tulleiden tapausten perusteella voimme olettaa, että tällä hetkellä hyökkäys kohdistuu vain suomalaisiin pankkeihin.

Uutisankkuri: Kiitos haastattelusta.

Aihe 4: Pääministeri kommentoi sähkönjakelun rajoittamista ja pankkien häiriöitä

[**Grafiikka**: Säätytalo]

Uutisankkuri: Fingrid on tiedottanut sähkönjakelun rajoittamisesta ja samaan aikaan useat suomalaiset pankit ovat kyberhyökkäyksen kohteena. Tämä on aiheuttanut vaikeuksia pankkiliikenteessä sekä herättänyt pelkoa suomalaisissa. Pääministeri Mikko Meikäläinen saapui juuri Säätytalolle vastaaman median kysymyksiin.

Uutisankkuri: Pääministeri Mikko Meikäläinen, kuinka kommentoitte tätä tilannetta?

Mikko Meikäläinen: Kansalaisten huoli on täysin ymmärrettävä ja tilanne on haastava, mutta olemme varautuneet sähkönjakelun rajoittamiseen sekä kyberhyökkäyksiin ennakoivasti. Kansalaiset voivat edelleen nukkua yönsä rauhassa.

Uutisankkuri: Kyberhyökkäyksen on julkisuudessa epäilty tulevan valtiolliselta taholta, kuinka kommentoitte tätä?

Mikko Meikäläinen: Tämänkaltaisiin kyberhyökkäyksiin on Suomessa varauduttu hyvin. Kyberhyökkäyksen alkuperämaata en lähde tässä vaiheessa spekuloimaan. Asia on selvityksessä ja tulemme uutisoimaan siitä myöhemmin.

Uutisankkuri: Vaikuttaa siltä, että suomalaista kriittistä infraa kohtaan on menossa sarja kyberhyökkäyksiä. Onko kyse laajemmasta valtiollisesta vaikuttamisesta?

Mikko Meikäläinen: Tällä hetkellä on vielä liian aikaista arvioida tilanteen laajuutta. Sähkönjakelun rajoittaminen on Fingridin ohjeistama toimenpide sähkön riittävyyden takaamiseksi, joten kyberhyökkäykset finanssialaa kohtaan ovat täysin erillinen tapahtuma.

Uutisankkuri: Voitteko kertoa, mitä Suomen valtio nyt konkreettisesti tekee tilanteen ratkaisemiseksi?

Mikko Meikäläinen: En valitettavasti voi lähteä julkisesti avaamaan varautumisen suunnitelmia ja toimenpiteitä, mutta poikkeustilanteisiin on varauduttu ennalta, meillä on erittäin hyvät resurssit ja paljon ammattilaisia tekemässä näitä toimia.

Uutisankkuri: Kiitos haastattelusta!

3.1 Tapahtuma 1: Palveluntoimittaja ilmoittaa epävarmuudesta tuottamansa palvelun osalta & KTK ilmoittaa nollapäivähaavoittuvuudesta

Tilannesyöte: Sähköposti Organisaation kriittisen IT-palveluntoimittajan yhteyshenkilöltä

Lähettäjä: yhteyshenkilo@it-yhtio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Sähkönjakelun ongelmien vaikutus tuotettavaan palveluun
---

Arvoisa asiakkaamme,

Mahdollisen sähkönjakelun rajoittamisen ja jatkuvien paikallisten sähkökatkojen takia pyydämme teitä varautumaan siihen, että Organisaation kriittisen tietojärjestelmän/palvelun käytössä voi esiintyä häiriöitä tai käyttökatkoja. Tällä hetkellä palvelu toimii normaalisti, mutta emme valitettavasti voi taata, että palvelu on luvatun palvelutasosopimuksen mukaisesti käytettävissä jatkossa.

Toivomme teidän ymmärtävän tämän poikkeuksellisen tilanteen mahdollisen vaikutuksen toimintaamme. Seuraamme tilannetta ja ilmoitamme teille, jos joudumme poikkeamaan palvelutasosopimuksesta.

Terveisin,

IT-yhtiön Asiakasyhteysjohtaja

Mediasyöte: Sanomat Uudeltamaalta: Sähkökatkot ovat haitanneet merkittävästi organisaatioiden toimintaa ympäri Suomea

Alueelliset sähkökatkokset haittaavat organisaatioiden toimintaa ympäri Suomen. Varavoimasta on suuri kysyntä, eikä sitä pystytä toimittamaan näin nopealla aikataululla kaikille. Toistaiseksi ei ole tietoa siitä, kuinka laajoiksi sähkökatkot voivat vielä yltyä.

Organisaatiot eivät ole lähteneet investoimaan varavoimaan yhtä innokkaasti kuin alkuvuodesta toivottiin. Syitä tähän on monia. Organisaatioiden varavoiman saantia on nyt yritetty parantaa, mutta työ on edennyt hitaasti. Lukuisille yrityksille varavoima on kallis investointi odotettuihin tuottoihin verrattuna.

Paikallisen IT-yhtiön toimitusjohtaja Jukka Isoselkä kertoo, että kiinteä varavoimakone on kallis investointi. Generaattorin hintalappu nousee helposti 150 000 euroon, mikä on merkittävä investointi pienille ja keskisuurille yrityksille.

IT-yhtiön näkemys on, että jos varavoimaa halutaan lisää, valtion on osallistuttava kustannuksiin.

– Kun investointeja tehdään yhteisen edun nimissä, oletus on, että rahoituksessa on mukana myös yhteistä rahaa, Isoselkä toteaa.

Kustannuksia suurempi syy on kuitenkin se, että aikaisemmin pitkät sähkökatkot ovat olleet harvinaisia.

Tilannesyöte: HAAVOITTUVUUS 47/2022: Microsoft Office nollapäivähaavoittuvuus

https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_47/2022

Microsoftin Office -tuoteperheestä on löytynyt haavoittuvuus, jonka avulla voidaan suorittaa mielivaltaista ohjelmistokoodia korotetuin valtuuksin. Haavoittuvuus on hyödynnettävissä paikallisesti. Haavoittuvuus koskee kaikkia Microsoft Office -versioita. Microsoft on julkaissut tiedotteen haavoittuvuudesta.

Haavoittuvuuteen ei tällä hetkellä ole korjaavaa päivitystä ja sen hyväksikäyttöä on jo havaittu erittäin paljon Euroopan maissa ja yksittäisiä tapauksia Suomessa. Haittaohjelma kryptaa tiedostoja ja hävittää avaimen. Salauksen purkaminen ei ole mahdollista.

Kohde

- Työasemat
- Palvelimet

Työasemat ja loppukäyttäjäsovellukset

Microsoftin virallisen tiedotteen lisäksi liikkeellä on myös huijausposti samasta haavoittuvuudesta. Tämä viesti on kopio Microsoftin tiedotteesta, ja se tulee microsoft.com-sähköpostiosoitteesta.

Haittaohjelma asentuu automaattisesti, kun käyttäjä avaa huijausviestin linkin valheelliseen haavoittuvuustiedotteeseen. Linkki tiedotteeseen tulee sähköpostiviestinä, joka kopioi Microsoftin aitoa tietoturvahaavoittuvuus – ilmoitusta. Linkistä avautuva sivu on kopio Microsoftin omasta tiedotteesta, mutta avautuva sivusto sisältää myös haittakoodia, joka suoritetaan käyttäjän huomaamatta käyttäjän työasemalla haavoittuvuutta hyödyntäen.

Saastutettuaan käyttäjän työaseman haittaohjelma yrittää tartuttaa itseään Windows-palvelimiin.

Palvelimet ja palvelinsovellukset

Onnistuttuaan saastuttamaan Windows-palvelimen, haittaohjelma käynnistää seuraavan alirutiinin, alkaa kryptata tiedostoja sekä hävittää avaimen. Salauksen purkaminen ei ole mahdollista.

Hyökkäystapa

- Roskapostin välityksellä, kiristyshaittaohjelma

Vaikutukset

- Suojauksen ohittaminen
- Käyttövaltuuksien laajentaminen
- Tietojen muokkaaminen

Suojauksen ohittaminen

Haittaohjelma ohittaa perinteisen suojauksen houkuttelemalla käyttäjän suorittamaan haittaohjelmakoodin käyttäjän valtuuksilla.

Käyttövaltuuksien laajentaminen

Haittaohjelma korottaa käyttövaltuuksiaan hyödyntämällä tuntematonta haavoittuvuutta.

Tietojen muokkaaminen

Haittaohjelma alkaa salata kohdejärjestelmän tiedostoja korotetuilla käyttövaltuuksilla ja tuhoaa salausavaimen.

Hyväksikäyttömenetelmä tiedossa

- Rikollisessa käytössä

Rikollisessa käytössä

Hyödynnettävän haavoittuvuuden tiedetään olevan rikollisessa käytössä ja siihen on luotu ainakin yksi tunnistettu haittaohjelma.

Ratkaisu

- Ei päivitystä

Ei päivitystä

Haavoittuvuuteen ei tällä hetkellä ole olemassa korjausta.

Haavoittuvat ohjelmistot

Kaikki Microsoft Office -versiot.

Tunnistettu haittaohjelma

- Tiedosto: Haittaohjelma
- MD5: 648effa354b3cbaad87b45f48d59c616

Tapahtuma 1: Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Peilatkaa harjoituksen tapahtumia ja niiden vaikutuksia oman organisaationne toimintaan.

Valitkaa myös organisaatiollenne kriittinen tietojärjestelmä/palvelu, jonka kautta käytte Tapahtuman 1 tehtävät läpi.

On mahdollista, että sähkönjakelua tullaan rajoittamaan tulevaisuudessa. Tällä hetkellä Suomessa on paikallisia sähkökatkoja, ja finanssialaan on kohdistunut kyberhyökkäyksiä.

Tapahtuma 1: Tehtävät

1.1 Miettikää, miten tapahtuma vaikuttaa organisaatiossanne.

1.2 Miten organisoidutte mahdollista häiriötilannetta varten?

1.3 Miten muodostatte ja jaatte tilannekuvaa mahdollisessa häiriötilanteessa?

1.4 Mitä vaikutuksia kriittisen tietojärjestelmän/palvelun mahdollisilla käyttökatkoilla on organisaationne toimintaan?

1.5 Miten kriittisen tietojärjestelmän/palvelun käyttökatkoihin voidaan varautua?

a. Onko palvelusopimuksissanne huomioitu kriittisen tietojärjestelmän/palvelun häiriöt ja häiriötilanteisiin varautuminen?

1.6 Mitä toimenpiteitä Kyberturvallisuuskeskuksen tiedote nollapäivähaavoittuvuudesta aiheuttaa?

Tapahtuma 1: Lisätehtävät

1.7 Miten finanssisektorin häiriöt vaikuttavat organisaationne toimintaan?

1.8 Miten finanssisektorin häiriöihin tulisi varautua?

Tapahtuma 1: Viestintätehtävät

1.9 Miten ja kenelle viestitte asiasta?

1.10 Tehkää tarvittavat viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 09.45

3.2 Tapahtuma 2: Epäily Organisaation käsittelemien henkilötietojen vuotamisesta, ja väärän tiedon leviäminen Organisaation nimissä verkossa ja sosiaalisessa mediassa

Mediasyöte: Quacker: @MikkoMeikäläinen (PM):

Käynnistä video play-painikkeesta. Videon saat koko ruudun näkymään, kun klikkaat oikeasta alareunasta. Videon kesto on noin 30 sekuntia.

Tarvittaessa voit jakaa videon linkkinä oman organisaatiosi osallistujille, tässä linkki: https://youtu.be/Ky5ZIeXRNkA

Mediasyöte: Quacker:

@pertti:

Nyt se alkoi, näyttäis siltä, että naapuri aloitti kostotoimet. Tää voi mennä vieläkin rummemmaksi…

Mediasyöte: Quacker:

@Pirjo:

Suomessa ei toimi yksikään maksupääte ja laajasti sähköt poikki. Miten hallitus voi antaa tämän tapahtua? Maksetaan hirveesti veroja ja palvelut ei toimi!

Mediasyöte: Quacker:

@Niko:

Herätkää! Kyseessä on NATO:n operaatio, jolla voidaan perustella entistä kovempia toimia ja Suomen alistamista Jenkkien tahtoon. Selkeästi näkyy näiden katkosten järjestelmällisyydessä!

Mediasyöte: Quacker:

@Daniela:

Mulla sulaa kaikki marjat ja lihat pakkaseen, satoja euroja menee hukkaan! Kuka korvaa? Miten meillä voi olla näin tunari hallitus, että antaa sähkön loppua?

Tilannesyöte: Sähköposti Organisaatiolle FBI:lta

Lähettäjä: FBI IC3 [do_not_reply@fbi.gov]
Vastaanottaja: tietoturva@organisaatio.fi
Aihe: Possible cyber breach and data leakage

Dear Organisaatio,

Our intelligence monitoring indicates possible breach in your corporate IT environment. Our monitoring on specific darkWeb trading forums has revealed content that has likely originated from your organization. This trading forum is known to be used by multiple threat actors to trade and sell stolen information to any interested parties.

Link to the trading forum with your organization's information is https://wesellthegood-stolenstuffcheapwithbitcoins.onion with sample images of the data content. Please see attached .jpg file of the sample data.

Take precaution when accessing the trading forum as the site is heavily infected with malware and may lead to compromise of your systems.

Best regards,

FBI | Cyber Threat Detection and Analysis | Network Analysis Group

Attachment file

Etunimi	Sukunumi	Henkilötunnus
Pekka	Pönttinen	110461-223H
Maija	Mallikas	211175-120J
Vuokko	Viitanen	300501A030S
Rikhard	Lindberg	070688-053R
Erkki	Saari	150390-123U
Esii	Karhu	120981-002L
Minja	Varvas	280660-600V
Vesa	Nieminen	241277-081K
Jarmo	Juutinen	050892-898N
Sini	Korpo	010769-100A
Auli	Lahti	030385-024B
Perttu	Virtanen	120189-807C
Anna	Erkkilä	091069-500Y
Ari	Aro	060682-441E
Unto	Kiuru	310107-302U
Kari	Mikkonen	090773-912D
Sami	Siukkonen	050595-654V
Sirpa	Salonen	071198-060M
Eija	Salmi	140286-042N
Vesa	Vuori	010889-987K
Timo	Timonen	210172-323J

Huom. sähköpostiosoite ja linkki ovat kuvitteellisia.

Tilannesyöte: Organisaation verkkosivuille on ilmestynyt väärää tietoa sisältävä tiedote

Organisaation uusi linjaus

Olemme johtoryhmän kanssa kokoontuneet tällä päivämäärällä ja päättäneet, että Organisaatiomme tukee jatkossa pakotteista luopumista. Olemme energiapoliittisesti tilanteessa, jossa toimintojemme jatkuminen ei ole mahdollista.

Tässä maailmantilanteessa emme voi käyttää Organisaatiomme resursseja vihreään siirtymään. Emme anna kylmyyden vallata kotejamme, vaan käymme aktiivisesti vastarintaan pakotteita vastaan.

Mediasyöte: Quacker:

@OrganisaationJohtaja

Pyydän kaikkia Organisaatiossa työskenteleviä ryhtymään yhteiseen vastarintaan pakotteiden poistamiseksi. Muista, että Organisaatio ei ole vain työpaikkasi, vaan olemme osa suurempaa tarkoitusta.

#Organisaatio #KylmäEiSaavu #Vastarinta

Tapahtuma 2: Tehtävät

Organisaationne on saanut FBI:lta tiedon, että verkossa kaupitellaan väitetysti teiltä varastettuja tietoja, ja verkkosivuillenne on ilmestynyt väärää tietoa sisältävä tiedote. Sosiaalisessa mediassa liikkuu paljon väärää tietoa. Lisäksi organisaationne johdon nimissä esiinnitytään sosiaalisessa mediassa ja kommentoidaan tapahtunutta asiattomasti.

Tapahtuma 2: Tehtävät

2.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

2.2 Olette saaneet ilmoituksen, jonka mukaan organisaationne käsittelemiä henkilötietoja on myynnissä Dark Webissä.

Valitkaa teille sopivin vaihtoehto epäillyn tietovuodon kohteesta:

a. organisaationne henkilöstön tiedot (HR-järjestelmästä)

b. erityisiä henkilötietoryhmiä sisältävät tiedot organisaationne ulkopuolelta (GDPR-määritelmä)

2.3 Miten toimitte tilanteessa, jossa organisaationne tietoja on mahdollisesti päätynyt vääriin käsiin.

2.4 Miten selvitätte, onko henkilötietoja vuotanut?

2.5 Oletteko FBI:lta saadun tiedon perusteella yhteydessä poliisiin?

a. Kuka organisaatiostanne tekee päätöksen yhteydenotosta?

b. Kuka organisaatiossanne vastaa yhteydenotosta?

2.6 Mitä toimia organisaationne verkkosivuille päätynyt, väärää tietoa sisäl- tävä tiedote aiheuttaa?

Tapahtuma 2: Viestintätehtävät

2.7 Miten ja missä viestitte

a. verkkosivuillenne päätyneestä väärää tietoa sisältävästä uutisesta?

b. organisaationne johtajan sosiaalisen median tilillä esitetystä väärästä tiedosta?

c. Tehkää tarvittavat viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 10.25

3.3 Tapahtuma 3: Organisaation kriittisessä palvelussa havaitaan haittaohjelma

Tilannesyöte: Sähköposti Organisaation omalta työntekijältä

Lähettäjä: maija.virtanen@organisaatio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi

Aihe: Mahdollinen henkilötietojen tietovuoto Organisaatiossa

Hei

Huomasin juuri, että **Organisaation kriittinen tietojärjestelmä/palvelu** ei toimi oikein / sen tietoja ei ole saatavilla. Onko teillä tiedossa häiriötä tähän liittyen ja osaatteko sanoa, milloin järjestelmä/palvelu olisi taas käytettävissä?

Terveisin

Maija Virtanen, Palvelun käyttäjä, Organisaatio

Tilannesyöte: Sähköposti Organisaation tietohallinnolta

Lähettäjä: tietohallinto@organisaatio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Haittaohjelma on kryptannut kriittisen tietojärjestelmän tietoja
---

Hei

Saimme **Organisaation kriittisen tietojärjestelmän/palvelun** ylläpidosta tiedon, että haittaohjelma on päässyt salaamaan järjestelmän/palvelun tietoja. Selvitämme parhaillaan tilanteen laajuutta ja vakavuutta.

Terveisin

Organisaation tietohallinto

Tapahtuma 3: Tehtävät

Valitkaa toinen kriittinen tietojärjestelmä/palvelu (HUOM. jokin muu kuin se järjestelmä/palvelu, minkä valitsitte Tapahtumassa 1) ja peilatkaa Tapahtuman 3 vaikutuksia organisaatioonne.

Tapahtuma 3: Tehtävät

3.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

3.2 Mitä vaikutuksia kriittisen tietojärjestelmän/palvelun salaamisella on organisaatioonne toimintaan?

3.3 Mitä toimenpiteitä kriittisen tietojärjestelmän/palvelun salaaminen aiheuttaa?

3.4 Mihin tahoihin olette yhteydessä?

Tapahtuma 3: Viestintätehtävät

3.5 Aiheuttaako tilanne sisäisen tai ulkoisen viestintätarpeen?

3.6 Millaisiin viestintätoimiin ryhdytte?

3.7 Tehkää tarvittavat viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 10.55

3.4 Tapahtuma 4: Organisaation kiristäminen vuodetulla tiedolla ja lisätietoa Organisaatioon kohdistuneesta haittaohjelmasta

Tilannesyöte: Sähköposti Organisaation johtoryhmälle

Lähettäjä: xyz1234@gmail.com
Vastaanottaja: johtoryhma@organisaatio.fi
Aihe: Hallussani on tietoja, jotka haluatte takaisin

Hei siellä!

Valitettavasti minulla on huonoja uutisia. Noin useita kuukausia sitten sain pääsyn Organisaatiosi laitteisiin, joita käytit Internetin selaamiseen. Tämän jälkeen olen jatkanut Internet-toimintojenne jäljittämistä.

Alla on menneiden tapahtumien järjestys: Aiemmin olen ostanut hakkereilta pääsyn useisiin sähköpostitileihin (tänään se on hyvin yksinkertainen tehtävä, joka voidaan tehdä verkossa).

On selvää, että olen vaivattomasti kirjautunut sisään organisaatiosähköpostitilille (etunimi.sukunimi@organisaatio.fi).

Viikko sen jälkeen olen onnistunut asentamaan troijalaisen viruksen kaikkien sähköpostien käyttöön käytettävien laitteidesi käyttöjärjestelmiin. Itse asiassa se oli melko yksinkertaista (koska napsautit postilaatikon sähköpostien linkkejä). Kaikki älykkäät asiat ovat melko yksinkertaisia. (>_<)

Ohjelmistoni avulla voin käyttää kaikkia laitteidesi ohjaimia, kuten videokameraa, mikrofonia ja näppäimistöä.

Tässä todiste:

Etunimi	Sukunumi	Henkilötunnus
Pekka	Pönttinen	110461-223H
Maija	Mallikas	211175-120J
Vuokko	Viitanen	300501A030S
Rikhard	Lindberg	070688-053R
Erkki	Saari	150390-123U
Esii	Karhu	120981-002L
Minja	Varvas	280660-600V
Vesa	Nieminen	241277-081K
Jarmo	Juutinen	050892-898N
Sini	Korpo	010769-100A
Auli	Lahti	030385-024B
Perttu	Virtanen	120189-807C
Anna	Erkkilä	091069-500Y
Ari	Aro	060682-441E
Unto	Kiuru	310107-302U
Kari	Mikkonen	090773-912D
Sami	Siukkonen	050595-654V
Sirpa	Salonen	071198-060M
Eija	Salmi	140286-042N
Vesa	Vuori	010889-987K
Timo	Timonen	210172-323J

Joten tähän mennessä sinun pitäisi jo ymmärtää syy, miksi jäin huomaamatta tähän hetkeen asti…

Ratkaistaan se näin:

Tarvitset vain 13 500 USD:n USD-siirron tililleni (bitcoin-vastaava vaihtokurssin perusteella), ja kun tapahtuma on onnistunut, poistan kaikki ne ohjelmat koneeltasi viipymättä. ……..

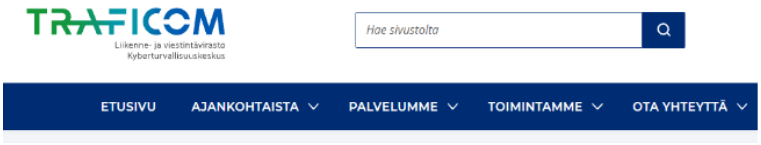
Alla on bitcoin-lompakkoni: 1B5ic9iQpyafTEfWxHM4Xq6PkzbickrL8g

Sinulle annetaan enintään 48 tuntia tämän sähköpostin avaamisen jälkeen (tarkemmin 2 päivää).

Parhaat terveiset

Hakkeri Vain

Tilannesyöte: https://www.kyberturvallisuuskeskus.fi



Antivirus-ohjelmien toimittajat ovat tunnistaneet wiper-ohjelman, ja siihen liittyvät tunnistetiedot.

Haittaohjelmaan ei tällä hetkellä ole korjaavaa päivitystä, ja sen hyväksikäyttöä on jo havaittu erittäin paljon Euroopan maissa ja yksittäisiä tapauksia Suomessa. Haittaohjelma kryptaa tiedostoja ja hävittää avaimen. Salauksen purkaminen ei ole tämänhetkisten tietojemme mukaan mahdollista.

Tunnistetietoja haittaohjelmaan liittyen

- Ennakkoon määriteltynä ajankohta haittaohjelman toinen vaihe käynnistyy ja haittaohjelma pyrkii leviämään verkon yli hyödyntäen Network Node Enumeration prosessia porttien 445 ja 139 kautta.
- Toisen vaiheen käynnistyessä haittaohjelma yrittää myös ottaa yhteyttä internetissä olevaan Command & Control (C2) -osoitteeseen uusia ohjeita varten.
- IOCs: (haittaohjelman tiedossa olevat tunnisteet)
    - Tiedosto: Haittaohjelma
    - Koko: 362360
    - MD5: 71B6A493388E7D0B40C83CE903BC6B04
    - SHA256: 027CC450EF5F8C5F653329641EC1FED91F694E0D229928963B30F6B0D7D3A745.
    - C2: 46.107.48.202

Tapahtuma 4: Tehtävät

Organisaatiotanne kiristetään henkilötietojen levittämisellä. Kiristysviesti on sisältänyt todisteen, jossa on organisaationne aitoja henkilötietoja. Kyberturvallisuuskeskus on tiedottanut laajasti levitetystä haittaohjelmasta.

Tapahtuma 4: Tehtävät

4.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

4.2 Mitä toimenpiteitä johdollenne lähetetty kiristysviesti aiheuttaa? Mihin tahoihin olette yhteydessä?

4.3 Mitä toimenpiteitä kriittisen tietojärjestelmän/palvelun salaaminen aiheuttaa?

a. Onko palautumiseen prosessi, ja onko sitä testattu?

b. Miten ja mistä palautuminen aloitetaan?

Tapahtuma 4: Lisätehtävät

4.4 Mitä toimenpiteitä Kyberturvallisuuskeskuksen tiedote aiheuttaa?

a. Mitä toimenpiteitä organisaationne pystyy suorittamaan Kyberturvallisuuskeskuksen tiedotteessa annettujen IOC:n (haittaohjelman tiedossa olevat tunnisteet) perusteella?

Tapahtuma 4: Viestintätehtävät

4.5 Onko organisaatiossanne prosessia, miten tällaisista tilanteista viestitään sisäisesti?

4.6 Pohtikaa, millaisiin viestintätoimiin ryhtyisitte, ja laatikaa tilanteen edellyttämät tiedotteet.

4.7 Tehkää tilanteen edellyttämät viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 11.30

Tapahtuma 5 (9): Totutut viestintäkanavat eivät käytössä

Puolenpäivän osallistujille aamupäivän viimeisenä tapahtumana, koko päivän osallistujille päivän päätteeksi, tapahtuman sisältö on sama kuin kohdasta 4.5 Tapahtuma 9.

4 Iltapäivän harjoitus (12:30–15:00)

Mediasyöte: Yleismedia: Ylimääräinen uutislähetys paikallisista sähkökatkoista

Uutisankkuri: Uutisista hyvää iltapäivää. Suomessa aloitetaan sähkönjakelun rajoitustoimet vallitsevan sähköpulatilanteen takia. Sähkönjakelun rajoitukset tulevat aiheuttamaan paikallisia sähkökatkoja, joiden kestot ovat noin kaksi tuntia. Fingridin toimitusjohtaja Pekka Kukkanen, miksi sähkönjakelua joudutaan nyt rajoittamaan?

Pekka Kukkanen: Ensinnäkin haluan todeta, että tilanne on täysin viranomaisten ja kantaverkkoyhtiön hallinnassa. Suomessa vallitsee tällä hetkellä sähköpulatilanne eli

sähkön tuotanto ja tuonti eivät riitä kattamaan sähkön kulutusta. Joudummekin rajoittamaan kulutusta, jotta sähköjärjestelmä ei kaadu. Vallitsevassa tilanteessa sähkönsiirtoa katkotaan alueellisesti, jotta saamme varmistettua sähköjärjestelmän toiminnan.

Uutisankkuri: Kuinka kauan arvioitte sähköpulatilanteen kestävän ja voiko sähköpulasta johtuvia sähkökatkoja tulla lähiaikoina lisää?

Pekka Kukkanen: Suomi kuuluu samaan sähköjärjestelmään Ruotsin, Norjan ja Itä-Tanskan kanssa. Tällä alueella on pidettävä sama tehotasapaino yllä. Kaikki riippuu nyt sähkön kulutuksen sekä tuotannon ja tuonnin suhteesta, jotta tasapaino saadaan säilytettyä. Sähköpulatilanne päättyy, kun sähkön tuotanto ja tuonti riittävät kattamaan sähkön kulutuksen. Me Fingridiltä ilmoitamme erikseen sähköpulan päättymisestä.

Sähköpulatilanne voi toki toistua myös tulevaisuudessa, ja siinä tapauksessa ryhdymme toteuttamaan uudelleen tilannetta varten laadittuja toimintamalleja ja suunnitelmia.

Uutisankkuri: Kiitos haastattelusta, toimitusjohtaja Pekka Kukkanen.

Uutisankkuri: Toimittajamme on parhaillaan Espoossa, jossa sähköt ovat nyt kytketty pois päältä.

Toimittaja: Kyllä, täällä Espoossa on tosiaan katkaistu sähköt. Kadulla näkyy jonkin verran ihmisiä ihmettelemässä liikkeiden ja asuntojen sammuneita valoja. Minulla on haastateltavana espoolainen perheenäiti Sara Suomalainen.

Sara, miten sähkökatko on vaikuttanut sinun arkeesi?

Sara Suomalainen: Vaikuttaa, ja paljon vaikuttaakin! Töissä alkoi sähkökatkosta täysi kaaos. Kun olin selvittämässä sitä, päiväkodista soitettiin, että pitää tulla hakemaan lapset sähkökatkon takia kesken päivän. Nyt ihmettelen, millä pääsen päiväkotiin, kun meidän Teslan akku on aivan tyhjä, eikä lataaminen tietenkään onnistu sähkökatkon aikana.

Toimittaja: Kiitos haastattelusta ja toivottavasti tilanne ratkeaa.

Uutisankkuri: Lisää aiheesta seuraavissa uutislähetyksissä ja verkkosivuillamme. Nyt näkemiin.

4.1 Tapahtuma 5: Organisaation kriittinen palvelu lakkaa toimimasta (case: sähkökatkot)

Sähköposti Organisaatiolle kriittisen IT-palveluntoimittajan yhteyshenkilöltä

Lähettäjä: yhteyshenkilo@it-yhtio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Sähkönjakelun ongelmien vaikutus tuotettavaan palveluun
---

Arvoisa asiakkaamme,

Ilmoitimme teille aiemmin mahdollisista käyttökatkoista Organisaation kriittisessä tietojärjestelmässä/palvelussa. Valitettavasti palveluympäristömme on jouduttu ajamaan hallitusti alas sähkönjakeluun liittyvien ongelmien vuoksi. Tämänhetkinen tilanne on hyvin vaikeasti ennakoitavissa sähkön saannin osalta, joten pyydämmekin teitä varautumaan jopa kolmen vuorokauden käyttökatkoon.

Vetoamme ylitsepääsemättömään esteeseen ja pahoittelemme teille mahdollisesti aiheutuvaa haittaa.

Terveisin, IT-yhtiön yhteyshenkilö

---------- edellinen viesti ----------

Lähettäjä: yhteyshenkilo@it-yhtio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Sähkönjakelun ongelmien vaikutus tuotettavaan palveluun
---

Arvoisa asiakkaamme,

Mahdollisen sähkönjakelun rajoittamisen ja jatkuvien paikallisten sähkökatkojen takia pyydämme teitä varautumaan siihen, että Organisaation kriittisen tietojärjestelmän/palvelun käytössä voi esiintyä häiriöitä tai käyttökatkoja. Tällä hetkellä palvelu toimii normaalisti, mutta emme valitettavasti voi taata, että palvelu on luvatun palvelutasosopimuksen mukaisesti käytettävissä jatkossa.

Toivomme teidän ymmärtävän tämän poikkeuksellisen tilanteen mahdollisen vaikutuksen toimintaamme. Seuraamme tilannetta ja ilmoitamme teille, jos joudumme poikkeamaan palvelutasosopimuksesta.

Terveisin, IT-yhtiön Asiakasyhteysjohtaja

Mediasyöte: Sanomat Uudeltamaalta: Energiapula iskee kovaa suomalaisten arkeen

Sähkökatkojen varalta joka kodissa tulisi olla riittävästi vettä ja ruokaa sekä paristokäyttöinen radio ajantasaisen tiedon vastaanottamiseksi.

Lämmitys on poikki, puhdasta vettä ei tule, kännykät ovat mykkinä, eikä vessakaan toimi. Yhden tai kaksi näistä vielä kestäisi, mutta pitkittynyt sähkökatko pysäyttää kerralla kaikki arjen perustoiminnot.

Kodin sähkölaitteiden lisäksi sähkönjakelun häiriö kaataa järjestäytyneen yhteiskunnan toiminnan. Maksuliikenne pysähtyy, pankkiautomaateista ei saa rahaa ja kaupatkin ovat kiinni, koska kassajärjestelmät eivät saa sähköä.

Miten itse kunkin tulisi varautua äkilliseen häiriötilanteeseen? Näin 72 tuntia -varautumisohjelma opastaa:

- Vesi on kaikkein tärkein asia, mutta se helposti unohtuu. Ihminen tarvitsee puhdasta juomavettä kaksi litraa päivässä. Sen lisäksi vettä tarvitaan ruoanlaittoon sekä hygieniaan.
- Kotivara on varautumisen kulmakivi. Kolmen päivän ruokavarasto on hyvä, mutta viikon varasto on vielä parempi.
- Häiriötilanteissa on saatava oikeaa ja reaaliaikaista tietoa. Paristokäyttöinen radio on oiva väline silloin, kun sähkönsaanti on häiriintynyt. Tällainen laite kuuluukin ko-tivarakalustoon, ja sen kautta tulisi seurata vakiintuneita valtakunnallisia medioita.

Mediasyöte: Quacker

@fingrid_oyj

FINGRID

Olemme ohjeistaneet paikallisia sähkönjakeluverkon haltijoita rajoittamaan kulutusta vallitsevan sähköpulatilanteen vuoksi. Sähköpulatilannetta varten on varauduttu ja harjoiteltu ennalta. Tilanne on viranomaisten ja kantaverkkoyhtiön hallinnassa.

#sähköpula

@PaikallinenSahkoverkkoyhtio

Paikalliset sähkönjakelun rajoitukset aloitetaan työ- ja elinkeinoministeriön päätöksen mukaisesti. Sähkönjakelun rajoitukset aiheuttavat paikallisia, ennalta suunniteltuja sähkökatkoja, joista ei ole syytä ilmoittaa sähköverkkoyhtiöille. Sähkökatkot ovat noin kahden tunnin mittaisia, minkä jälkeen sähköt palautuvat ilman erillistä ilmoitusta. Pahoittelemme asiakkaillemme aiheutuvaa haittaa.

#sähköpula

re-quack

@fingrid_oyj

FINGRID

Olemme ohjeistaneet paikallisia sähkönjakeluverkon haltijoita rajoittamaan kulutusta vallitsevan sähköpulatilanteen vuoksi. Sähköpulatilannetta varten on varauduttu ja harjoiteltu ennalta. Tilanne on viranomaisten ja kantaverkkoyhtiön hallinnassa.

#sähköpula

Mediasyöte: Iltanen: Sähkökatkoja luvassa koko Suomeen

Euroopan energiakriisi on kärjistynyt niin pahaksi, että Suomessa joudutaan turvautumaan kiertäviin sähkökatkoihin. Ennalta suunnitelluilla sähkökatkoilla pyritään turvaamaan sähkön riittävyys.

– Sähkön saatavuus on hyvin riippuvainen tulevista sääolosuhteista ja tuotantotilanteesta. Sitä on hyvin vaikea ennustaa pitkällä aikavälillä, kun emme esimerkiksi tiedä,

onko koittava talvi kylmä vai lauha, sanoo Korunan energiatehokkuuden asiantuntija Päivi Ohmi.

Ennalta suunnitellut sähkökatkot kestävät noin puolesta tunnista kahteen tuntiin, ja niistä tiedotetaan etukäteen. Ohmin mukaan sähkökatkoja suunnattaisiin vuorotellen eri alueille, jolloin vältettäisiin kulutuspiikki tarjonnan ollessa niukkaa. Esimerkiksi pääkaupunkiseudulla sähkökatko koskisi aina rajattua aluetta.

– Suomessa alueet ovat hyvin erilaisia asukasmäärien ja sähkönkulutuksen osalta. Todennäköisesti sähkökatkot koskisivat tiheästi asuttuja alueita, koska siten aikaansaadaan eniten vaikutusta.

Sähkön hinta lähti rajuun nousuun jo viime vuonna, ja Ukrainan sota on sekoittanut Euroopan energiamarkkinoita entisestään. Viranomaisten mukaan sähkön saannin rajoittaminen on viimesijainen keino sähköjärjestelmän toiminnan ylläpitämiseksi, ja alueelliset sähkökatkot ovatkin aina tilapäisiä.

Mediasyöte: Quacker

@Jugi

Jaahas, se olisi sitten mökille muutto takan ääreen, jos meinaavat sähköjä katkoa…

#Fingrid #paluumenneisyyteen #sähköpula

Mediasyöte: Quacker

@EconomyMan

Mitenköhän valtio meinasi selvitä tästä viennin vähentymisestä sähkönjakelun suunniteltujen katkojen takia?

#Lisäälainaa #Velkahallitus #Fingrid #sähköpula

Mediasyöte: Quacker

@Viherpeukalo

Kynttilän valossa illallista. Toisaalta romanttista, mutta vähän mietityttää pienhiukkaset, jos tämä jatkuu pitkään…

#Ilmansähköä #KuinkaKauan? #KeuhkoParat #sähköpula

Tapahtuma 5: Tehtävät

Käyttäkää alla olevissa tehtävissä samaa kriittistä tietojärjestelmää/palvelua, jonka valitsitte Tapahtuman 1 tehtäväosuudessa.

Tapahtuma 5: Tehtävät

5.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

5.2 Mitä vaikutuksia vähintään kolmen vuorokauden käyttökatkolla on kriittisen tietojärjestelmänne/palvelunne toimintaan?

5.3 Mitä toimenpiteitä toiminnan jatkaminen edellyttää?

5.4 Miten varaudutte tilanteen mahdolliseen pitkittymiseen, jos käyttökatko kestääkin useita vuorokausia?

Tapahtuma 5: Lisätehtävät

Jos teitte ennakkotehtävän, käykää nyt läpi vastauksenne ja peilatkaa niitä tähän tapahtumaan.

Jos ette ole tehneet ennakkotehtävää, käykää läpi organisaationne varautumisen toimintamallit ja -ohjeet sähkönjakelun rajoituksista aiheutuvien sähkökatkojen varalle.

Käykää läpi organisaationne varautumisen toimintamalleja ja ohjeita sähkönjakelun rajoituksista aiheutuvien sähkökatkojen varalta:

- Oletteko tunnistaneet ja dokumentoineet käytössänne olevat varavirtalaitteet sekä varmistaneet niiden toimivuuden?

- Mitä toimintoja niiden avulla on mahdollista ylläpitää vähintään kahden tunnin ajan?
- Miten toimitte, jos kahden tunnin kiertäviä katkoja osuu kohdallenne useamman kerran 12 tunnin sisällä?
- Kykenevätkö varavirtajärjestelmänne huolehtimaan niihin kytkettyjen laitteiden sammuttamisesta, jos varavirtalähteiden tuottama sähkö ei riitä koko sähkökatkon ajaksi? Jos näin ei ole, millaisia uhkia tästä voi syntyä?

Lisäksi pohtikaa asiaa myös seuraavista näkökulmista, jos sähkökatkot kohdistuvat:

5.5 organisaation toimitiloihin, esimerkiksi

a. miten sähkökatko vaikuttaa työskentelyyn ja liikkumiseen toimitiloissa?

b. onko toimitiloissa sellaisia operatiivisia järjestelmiä tai niiden osia, joiden toiminnan pysäyttäminen saattaa vaikuttaa muihin, toiminnassa oleviin, palveluihin tai prosesseihin?

5.6 henkilöstön koteihin, esimerkiksi

c. millaista ohjeistusta henkilöstölle annetaan, jos sähkökatko osuu työajalle?

5.7 kriittisiin palveluntarjoajiin, esimerkiksi

d. miten palveluntarjoaja pystyy huolehtimaan sen vastuulla olevien kriittisten palveluiden tuottamisesta sähkönjakelurajoitusten aikana?

Tapahtuma 5: Viestintätehtävät

5.8 Miten ja kenelle viestitte tilanteesta?

5.9 Tehkää tarvittavat viestintätoimenpiteet

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä **LINKKIÄ** kilkkaamalla.

Seuraava syöte julkaistaan klo 13.10.

4.2 Tapahtuma 6: Organisaation henkilötietoja julkaistaan sosiaalisessa mediassa

Mediasyöte: Quacker

@HakkeriVain

Pieni alkupala @Organisaatio tietoja hallussani. Ohitin heidän turvan vaivatta. Lisää luvassa, pysykää kanavalla! (>_<)

Etunimi	Sukunumi	Henkilötunnus
Pekka	Pönttinen	110461-223H
Maija	Mallikas	211175-120J
Vuokko	Viitanen	300501A030S
Rikhard	Lindberg	070688-053R
Erkki	Saari	150390-123U
Esii	Karhu	120981-002L
Minja	Varvas	280660-600V
Vesa	Nieminen	241277-081K
Jarmo	Juutinen	050892-898N
Sini	Korpo	010769-100A
Auli	Lahti	030385-024B
Perttu	Virtanen	120189-807C
Anna	Erkkilä	091069-500Y
Ari	Aro	060682-441E
Unto	Kiuru	310107-302U
Kari	Mikkonen	090773-912D
Sami	Siukkonen	050595-654V
Sirpa	Salonen	071198-060M
Eija	Salmi	140286-042N
Vesa	Vuori	010889-987K
Timo	Timonen	210172-323J

Mediasyöte: Quacker

@KalleKansalainen

Apua! Minun tietoni ovat vuotaneet! Mitä ihmettä **@Organisaatio**

Mediasyöte: Quacker

@SannaJarvinen

Ikävämpi juttu… Toivottavasti kyseessä ei ole laajempi tietovuototapaus.

Tapahtuma 6: Tehtävät

Verkossa jaetaan organisaatioltanne peräisin olevia henkilötietoja.

Tapahtuma 6: Tehtävät

6.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

6.2 Mitä toimenpiteitä tilanne edellyttää?

6.3 Mihin tahoihin olette yhteydessä?

Tapahtuma 6: Viestintätehtävät

6.4 Miten reagoitte somekeskusteluun vuodetuista henkilötietoaineistoista?

6.5 Miten viestitte eri kohderyhmille?

6.6 Mitä kanavia käytätte viestimiseen?

6.7 Tehkää tarvittavat viestintätoimenpiteet.

Tapahtuma 6: Haastattelutehtävä

Organisaationne on yhdistetty epäiltyyn tietovuotoon. Sosiaalisessa mediassa leviää kuva listasta, jossa näkyy organisaatioltanne peräisin olevia henkilötietoja.

Seuraavassa klo 13.15 julkaistavassa syötteessä YME-uutisten toimittaja soittaa organisaatioonne ja pyytää puhelinhaastattelua suoraan televisiolähetykseen. Käynnistäkää haastatteluvideo, kun olette valmiita antamaan haastattelun.

6.8 Valmistautukaa haastattelun antamiseen.

6.9 Kuka antaa haastattelun?

6.10 Mitä asioita kerrotte julkisuudessa? Mitä ette?

6.11 Voitte nauhoittaa haastattelun (esimerkiksi kännykällä) sisäistä läpi käyntiä varten, mikäli koette tämän hyödylliseksi.

Tallennus jää organisaationne omaan käyttöön, eikä sitä lähetetä edelleen, esim. harjoitusalustalle.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä **LINKKIÄ** kilkkaamalla.

Seuraava syöte haastatteluvideon jälkeen julkaistaan klo 13.50

Mediasyöte: Haastatteluvideo

Uutisankkuri: Suomessa epäillään laajaa henkilötietoihin kohdistunutta tietomurtoa. Toimituksemme saamien tietojen mukaan vuodetut tiedot ovat peräisin Organisaatiostanne.

Haastattelukysymykset:

- Miten näin on päässyt tapahtumaan?
- Kuinka laajasta vuodosta on kyse, ja millaisia tietoja on päässyt vuotamaan?
- Mitä toimenpiteitä olette käynnistäneet?
- Mitä toiminta ohjeistatte niitä henkilöitä, joiden tietoja on vuodettu?

Ohje haastattelun suorittamiseen:

Painakaa videon vasemmasta alakulmasta play-kuvaketta aloittaaksenne haastattelutehtävän. Toimittaja kysyy neljä kysymystä. Jokaiseen kysymykseen on aikaa vastata 30 sekuntia. Sekuntikello käynnistyy jokaisen kysymyksen jälkeen ja on näkyvillä ruudulla. Jos ette ehdi vastata kysymykseen annetussa ajassa, voitte painaa videon vasemmasta alakulmasta pause-kuvaketta ja jatkaa vastauksenne loppuun. Painakaa play-kuvaketta, kun haluatte siirtyä vastaamaan seuraavaan kysymykseen.

Tarvittaessa näyttövastaavanne voi jakaa videon linkkinä harjoitustiimin muille jäsenille: https://youtu.be/80WlCqX5-8s

4.3 Tapahtuma 7: Organisaation järjestelmään on päästy murtautumaan

Tilannesyöte: Turvasähköposti Organisaation tietohallinnolta

Lähettäjä: tietohallinto@organisaatio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Organisaation järjestelmään on päästy murtautumaan

Hei

Olemme perustaneet Cyber Incident Response -tiimin, ja Organisaatioon kohdistunutta kyberhyökkäystä ja mahdollista tietovuotoa selvitetään yhdessä luotetun palveluntoimittajan/viranomaisen kanssa.

Toistaiseksi olemme saaneet selville, että Organisaation järjestelmään on onnistuttu murtautumaan ja tietoja lataamaan. Hyökkäyksen tunnisteet ja tekotapa viittaavat siihen, että tekijätaho on hyvin suurella todennäköisyydellä APT1984 nimellä tunnettu, valtiollisen tahon tukema toimija.

Tästä eteenpäin tietojärjestelmään/palveluun ei saa tehdä muutoksia. Tämä tapaus sekä siihen liittyvä viestintä on erittäin luottamuksellista, joten kaikessa viestinnässä tulee käyttää ainoastaan Turvasähköpostia sekä puhelinta.

Jatkamme hyökkäyksen laajuuden selvittämistä.

Terveisin

Organisaation tietohallinto

Tapahtuma 7: Tehtävät

Organisaationne tietohallinto vahvistaa havainneensa tietomurron. Kyseessä on sama tietojärjestelmä/palvelu, jonka valitsitte Tapahtuman 3 tehtäväosuudessa. Valitkaa organisaatiollenne sopivin vaihtoehto alla olevista tehtävistä.

Tapahtuma 7: Tehtävät

VAIHTOEHTO 1

Cyber Incident Response -tiimi (tai vastaava) on perustettu selvittämään tilannetta.

7.1 Mikä on Cyber Incident Response -tiiminne rakenne eli keitä siihen kuuluu?

7.2 Onko Cyber Incident Response -prosessi dokumentoitu?

a. Onko tähän liittyvät roolit kuvattu?

b. Onko tähän sisältyvät tehtävät määritelty?

7.3 Miten tilannekuvan ylläpito sekä viestintä järjestetään, ja millaiseen tietoon eri tahot ovat oikeutettuja?

Huomioikaa erityisesti seuraavat:

c. Viestintä ydintiimin sisällä

d. Johdon viestintä

e. Viestintä teknisille tiimeille

7.4 Pohtikaa, onko tilanteesta syytä viestiä muille kuin edellä mainituille ta hoille. Jos näin on, miten ja kenelle viestitte?

7.5 Miten päätöksenteko ja valtuudet eri tason toimenpiteille on järjestetty?

Huomioikaa myös mahdolliset taloudelliset näkökulmat (esim. ylimääräiset kulut, kolmansien osapuolien käyttö ja teknologiainvestoinnit).

f. Kenellä on oikeus tehdä päätös organisaation irrottamisesta tietoverkosta?

7.6 Onko organisaatiollanne tekniset kyvykkyydet Incident Response- ja Forensics-toimenpiteiden suorittamiseen?

VAIHTOEHTO 2

7.7 Onko organisaatiossanne toimintamalli (ml. roolit ja vastuut) sekä ohjeet vakavan tietoturvauhkatilanteen varalle?

7.8 Jos tarvitaan ulkopuolista asiantuntija-apua (IT-palveluntarjoaja ja tietoturva-asiantuntija), onko organisaatiollanne hankintakanavat tai voimassa oleva sopimus tällaisia tilanteita varten?

Tapahtuma 7: Viestintätehtävät

7.9 Miten ja kenelle viestitte tilanteesta?

7.10 Toteuttakaa tilanteen edellyttämät viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 14.15

4.4 Tapahtuma 8: Kyberhyökkäyksen johdosta palvelu täytyy rakentaa täysin uudestaan

Tilannesyöte: Sähköposti Organisaation tietohallinnolta

Lähettäjä: tietohallinto@organisaatio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi

Aihe: Tietojärjestelmä voidaan palauttaa viikon takaiseen tietoon
---

Hei

Organisaation kriittinen tietojärjestelmä/palvelu on asennettava täysin uudelleen. Puhtaita asennusmedioita tulee käyttää. Käytännössä tämä tarkoittaa, että joudumme pystyttämään palvelun kokonaan uudelleen.

Olemassa olevia virtuaalisia koneita/kontteja ei voida käyttää, eikä myöskään varmuuskopioita. Tällä hetkellä ei ole tiedossa, että tietojen varmennuksiin olisi päästy käsiksi. Hyökkääjä APT1984 on ollut järjestelmissämme tiedettävästi ainakin kuusi kuukautta.

Terveisin

Organisaation tietohallinto

Tapahtuma 8: Tehtävät

Organisaationne tietohallinto on selvittänyt Tapahtumien 3 ja 7 tilannetta ja tullut siihen johtopäätökseen, että Organisaation kriittinen tietojärjestelmä/palvelu tulee rakentaa kokonaan uudestaan.

Tapahtuma 8: Tehtävät

8.1 Kuinka kauan arvioitte palautumisen kestävän?

8.2 Mitä vaikutuksia toimintaanne aiheutuu siitä, että palvelu on poissa käy tössä?

8.3 Mitä toimia menetetty työaika ja menetetyt tiedot aiheuttavat?

Tapahtuma 8: Viestintätehtävät

8.4 Miten ja kenelle viestitte tilanteesta?

8.5 Toteuttakaa tilanteen edellyttämät viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ kilkkaamalla.

Seuraava syöte julkaistaan klo 14.35

4.5 Tapahtuma 9: Totutut viestintäkanavat eivät ole käytössä

Mediasyöte: Quacker

@pilvipalvelu

Engineers are aware of an issue affecting resources in North Europe. For continued updates please visit status.pilvipalvelu.com

Tilannesyöte: status.pilvipalvelu.com www-sivuilla

News and press releases / Disturbance notice

CUSTOMER IMPACT: There are currently two identified impact workstreams. Starting 24.11.2022 14:30:

1. Customers with Active Directory may experience difficulties in SSO to resources hosted in this region.

2. Customers with hosted email and collaboration apps may experience failures in connecting to services

ENGINEERING STATUS: Investigation to cause and mitigation is ongoing.

NEXT UPDATE: 25.11.2022 12:00

Mediasyöte: Iltanen: Pilvi petti

Pilvipalveluntarjoaja Pilvipalvelu on ilmoittanut laajasta katkosta. Pilvipalvelua käyttävät useat suomalaiset yritykset ja julkishallinnon yhteisöt, ja katkolla on merkittäviä vaikutuksia näiden asiakkaiden toimintaan.

Pilvipalveluntarjoaja Pilvipalvelu on ilmoittanut laajasta katkosta. Pilvipalvelua käyttävät useat suomalaiset yritykset ja julkishallinnon yhteisöt, ja katkolla on merkittäviä vaikutuksia näiden asiakkaiden toimintaan.

Ongelmat alkoivat yhdestä palvelusta, mutta useat käyttäjät ovat raportoineet, etteivät sähköposti- ja pikaviestipalvelut toimi tällä hetkellä. Samoin kertakirjautuminen Active Directoryä käyttäviin palveluihin ei onnistu. Vikaraportteja on tullut myös muista Pohjoismaista.

Pilvipalvelu ei ole ilmoittanut katkon kestosta tai syystä, eikä Iltanen saanut kommenttia Pilvipalvelulta useista yrityksistä huolimatta. Uutinen päivittyy.

Tapahtuma 9: Tehtävät

Organisaationne pilvipalveluntoimittajan tarjoamat viestintävälineet, sähköposti ja pikaviestipalvelut (esim. Teams tai Skype) eivät toimi. Organisaation muissa viestintävälineissä, kuten intranet ja puhelimet, ei ole havaittu häiriöitä.

Tapahtuma 9: Tehtävät

9.1 Päivittäkää tilannekuva saamanne tiedon perusteella.

9.2 Mitä toimenpiteitä tilanne edellyttää?

9.3 Miten ohjeistatte henkilöstöä toimimaan?

9.4 Onko käyttäjien kriittiset puhelinnumerot talletettu suoraan puhelimen muistiin?

9.5 Onko organisaatiossanne määritelty viestivälineitä ja varajärjestelyjä? Mitä voidaan viestiä esim. pikaviestipalveluilla, jos ensisijaiset viestiyhteydet eivät toimi?

Tapahtuma 9: Viestintätehtävät

9.6 Miten viestitte tässä tilanteessa?

9.7 Miten ja kenelle viestitte tilanteesta?

9.8 Mitä viestintäkanavia käytätte?

9.9 Toteuttakaa tilanteen edellyttämät viestintätoimenpiteet.

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet Taisto-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä **LINKKIÄ** kilkkaamalla.

Seuraava syöte julkaistaan klo 15.00