DIGI- JA VÄESTÖTIETO-VIRASTO

Taisto-harjoitus 2024

Käsikirjoitus

20.12.2024

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

Sisällysluettelo

Taisto-harjoitus 2024

Käsikirjoitus sisältää vuoden 2024 Taisto-harjoituksen harjoitusalustalle vietävät tiedot.

1 Ennakkomateriaalit

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

1.1 Ennakko-ohjeistus

Harjoitusinfo: Taisto-harjoituksen viestintävastaava

Viestintävastaava voi julkaista organisaation ulkoisia tiedotteita ja sosiaalisen median julkaisuja vastaavia ”Quacker-päivityksiä” harjoitusalustan ”Taisto – Organisaation ulkoinen viestintä – Organisationens externa kommunikation”-sivulla. Julkaisuja ei tehdä ”Taisto-harjoitus”-sivulle.

Organisaation sisäisiä tiedotteita ei saa julkaista harjoitusalustalla, vaan ne laaditaan organisaation omilla työvälineillä ja käsitellään sisäisesti. Jos organisaation sisäistä viestintää julkaistaan virheellisesti harjoitusalustalla, otattehan välittömästi yhteyttä osoitteeseen taisto@dvv.fi ja otsikoitte viestin ”Taisto-harjoitus julkaisun poisto”.

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

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

Liitteet
Taisto-harjoitus: viestintävastaavan julkaisuohje
Taisto-harjoitus: viestintävastaavan ohje

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.

Liitteet
Taisto-harjoitus: näyttövastaavan ohje

Harjoitusinfo: Ohje Taisto-harjoituksen viranomaisilmoituksia tekevälle

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

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

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.

Liitteet
Taisto-harjoitus: viranomaisilmoituksia tekevän ohje

Harjoitusinfo: Harjoitukseen valmistautuminen

Harjoituksessa tullaan käsittelemään organisaation tai sen palveluntuottajien kriittisiin järjestelmiin kohdistuvia häiriötilanteita. Harjoitustilanteessa osallistujia pyydetään valitsemaan omalle toiminnalle kriittinen järjestelmä tai palvelu. Pohtikaa jo ennen harjoitusta käytössänne olevia kriittisiä järjestelmiä ja/tai palveluita, jotta valinta harjoitustilanteessa käy nopeasti. Suosittelemme valitsemaan järjestelmän, joka sisältää henkilötietoja tai organisaation toiminnan kannalta kriittistä tietoa.

Esimerkki: Omalle toiminnallenne kriittinen palveluntuottajan toimittama palvelu tai järjestelmä, johon kohdistuva häiriö vaikuttaisi laajasti toimintaanne. Suosittelemme pohtimaan kertaluonteisen häiriön lisäksi myös pitkäaikaista palveluun kohdistuvaa häiriötä.

Osallistuminen ei vaadi syvällistä teknistä tietämystä järjestelmistä, sillä harjoituksessa keskitytään häiriötilanteiden johtamiseen, tilannekuvan muodostamiseen, päätöksentekoon ja viestintään.

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

Lisämateriaalit

- Tekoäly tulee muuttamaan myös kyberhyökkäyksiä
- Turvaa digitaalinen toiminta häiriötilanteissa -koulutus
- Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta
- Poliisin alkutoimintaohjeet organisaatiolle tietoverkkorikosasiassa

VAHTI hyvät käytännöt -tukimateriaalit tekoälyn hyödyntämiseen

- Tekoälyn hyödyntämisen huoneentaulut ja tarkistuslistat – VAHTI hyvät käytännöt-tukimateriaali, versio 1.0 (pdf, 9/2023)

- Vinkkejä tekoälypalveluiden hyödyntämiseen – VAHTI hyvät käytännöt -tukimateriaali,versio 1.0. (pdf 9/2023)

1.2 Tietoiskut

Voit avata videot alla olevien linkkien kautta.

- Kyberturvallisuuskeskus: https://youtu.be/-1qzY-sCYL4
- OP Ryhmä: https://youtu.be/zzSK2dbjYnY
- Digi- ja väestötietovirasto - Tervetuloa Taisto-harjoitukseen: https://youtu.be/qvHPd3Rwd5c

1.3 Taisto-somehaaste: jakakaa harjoituspäivän huippuhetkenne!

Taisto-harjoituspäivään sisältyy vapaaehtoinen somehaaste, jonka tarkoituksena on tuulettaa mielikuvaa digiturvasta ja sen harjoittelusta. Toivomme, että harjoitustiiminne laittaa itsensä likoon ja osallistuu perinteiseen mutta leikkimieliseen haasteeseen harjoituspäivän aikana.

Tällä kertaa haastamme teidät jakamaan oman huippuhetkenne Taisto-harjoituksesta. Mikä oli sellainen hetki, kun oivalsitte jotain uutta, koitte onnistumisen tai ratkaisitte kimurantin haasteen yhdessä? Kuvatkaa tilanne sellaisena kuin se on, olettepa sitten toimistolla tiimin kanssa tai etänä kotona ruokapöydän ääressä tai sohvan nurkassa yöpaita päällä.

Laittakaa kuvat ja tekstit jakoon valitsemassanne sosiaalisen median palvelussa – tai vaikka useammassakin – aihetunnisteella **#Taisto**. Tägätkää mukaan Digi- ja väestötietovirasto (@DVVfi), niin voimme nostaa julkaisuja myös meidän kanaviimme. Muistakaa tuoda julkaisuissa esiin, että kyseessä on harjoitus.

Huomioittehan myös oman organisaationne ohjeet somejulkaisujen tekemisestä. Voitte tutustua somessa myös muiden tiimien harjoitusfiiliksiin!

1.4 Ennakkotehtävä

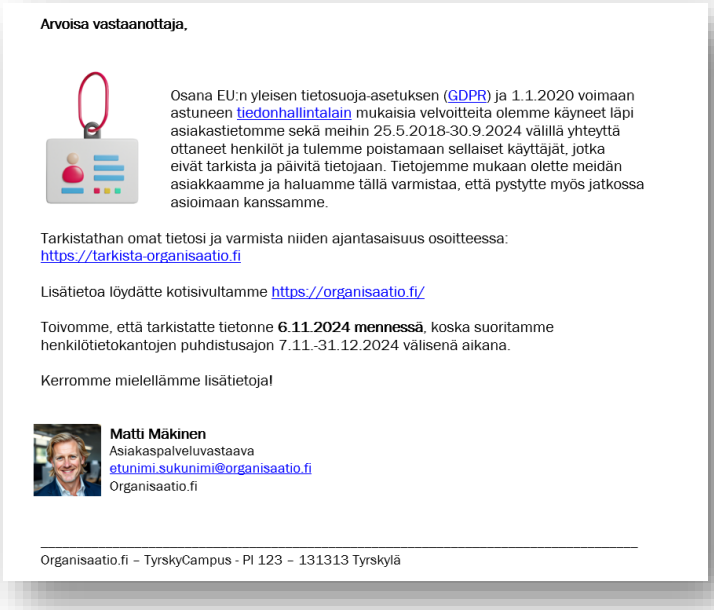
Verkkorikollisuus on yleistynyt kuluvan vuoden aikana. Kansalaisia huolestuttaa verkkorikollisuuden kasvu ja sen vaikutus digitaalisiin palveluihin. Kuitenkin Digi- ja väestötietoviraston Digiturvabarometri osoittaa kansalaisten luottamuksen digitaalisiin palveluihin säilyneen erittäin hyvällä tasolla. Verkkorikolliset pyrkivät käyttämään mahdollisimman luottavalta vaikuttavia url-osoitteita, jotta mahdollisimman moni päätyisi klikkaamaan kyseistä osoitetta.

Huijaussivuston osoite yleensä muistuttaa läheisesti organisaation virallista osoitetta. Osoitteissa voidaan käyttää esimerkiksi ulkomaalaisia erikoismerkkejä, jotka muistuttavat meidän kirjaimiamme. Viimeisen vuoden aikana verkkorikolliset ovat myös hyödyntäneet .fi-domain osoitteita. Verkkorikolliset voivat rekisteröidä minkä tahansa ”hyvän tavan mukaisen” nettiosoitteen. Myös sellaisen, joka läheisesti muistuttaa jonkin yrityksen tai viranomaisen osoitetta. Kun kyseistä osoitetta käytetään laittomasti, voi Liikenne- ja viestintävirasto Traficom puuttua osoitteen käyttöön ohjeistamalla palveluntarjoajaa pysäyttämään osoitteen käytön. Virheellisten osoitteiden ilmaantuessa verkkoon on tärkeää toimia mahdollisimman nopeasti.

Ennakkotapahtuma

Taisto-harjoituksen ennakkotehtävässä ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Peilatkaa ennakkotehtävän tapahtumaa ja sen vaikutusta oman organisaationne toimintaan. Tämä tehtävä kohdistuu organisaationne käyttämään viralliseen url-osoitteeseen. Tehtävän esimerkissä käytetään organisaatio.fi osoitetta ja sen pohjalta rikollisten luomaa tarkista-organisaatio.fi -osoitetta.

Organisaationne viestintä- ja tietoturvaryhmät saavat useamman ilmoituksen huolestuneilta työntekijöiltä, asiakkailta ja sidosryhmiltä alla olevasta viestistä, jonka he ovat vastaanottaneet:



Arvoisa vastaanottaja,

Osana EU:n yleisen tietosuoja-asetuksen (GDPR) ja 1.1.2020 voimaan astuneen tiedonhallintalain mukaisia velvoitteita olemme käyneet läpi asiakastietomme sekä meihin 25.5.2018-30.9.2024 välillä yhteyttä ottaneet henkilöt ja tulemme poistamaan sellaiset käyttäjät, jotka eivät tarkista ja päivitä tietojaan. Tietojemme mukaan olette meidän asiakkaamme ja haluamme tällä varmistaa, että pystytte myös jatkossa asioimaan kanssamme.

Tarkistathan omat tietosi ja varmista niiden ajantasaisuus osoitteessa:
https://tarkista-organisaatio.fi

Lisätietoa löydätte kotisivultamme https://organisaatio.fi/

Toivomme, että tarkistatte tietonne **6.11.2024 mennessä**, koska suoritamme henkilötietokantojen puhdistusajon 7.11.-31.12.2024 välisenä aikana.

Kerromme mielellämme lisätietoja!

Matti Mäkinen
Asiakaspalveluvastaava
etunimi.sukunimi@organisaatio.fi
Organisaatio.fi

Organisaatio.fi – TyrskyCampus - Pl 123 – 131313 Tyrskylä

Viestissä olevan https://tarkista-organisaatio.fi -linkin kautta aukeaa erilaisia luotettavia tunnistusmekanismeja muistuttava tunnistussivusto, jolla on tarkoitus kaapata käyttäjien tiedot.

Sosiaalisessa mediassa julkaistaan samanaikaisesti Organisaatiotanne koskeva julkaisu:

a) organisaatiollanne on käytössä median havainnointipalvelu, joka havaitsee organisaatiotanne koskevan sosiaalisen median julkaisun.
b) organisaationne saa tiedon julkaisusta muuta kautta, esimerkiksi valveutuneen työntekijän havainnosta.

Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Millaisiin toimenpiteisiin ryhdytte haitallisen tarkista-organisaatio.fi/osoitteen toiminnan rajoittamiseksi?
3. Millaisen tiedotteen julkaisette teidän nimissänne tehdystä huijausviestistä?
4. Saatte tiedotteen julkaisun jälkeen organisaationne viestintään videotiedoston, mitä toimenpiteitä tämä aiheuttaa?

2 Harjoituspäivän harjoitusinfot

2.1 Aamupäivän harjoituksen harjoitusinfot

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.

Taisto-somehaaste: jakakaa harjoituspäivän huippuhetkenne!

Taisto-harjoituspäivään sisältyy vapaaehtoinen somehaaste, jonka tarkoituksena on tuulettaa mielikuvaa digiturvasta ja sen harjoittelusta. Toivomme, että harjoitustiiminne laittaa itsensä likoon ja osallistuu perinteiseen mutta leikkimieliseen haasteeseen harjoituspäivän aikana.

Tällä kertaa haastamme teidät jakamaan oman huippuhetkenne Taisto-harjoituksesta. Mikä oli sellainen hetki, kun oivalsitte jotain uutta, koitte onnistumisen tai ratkaisitte kimurantin haasteen yhdessä? Kuvatkaa tilanne sellaisena kuin se on, olettepa sitten toimistolla tiimin kanssa tai etänä kotona ruokapöydän ääressä tai sohvan nurkassa yöpaita päällä.

Laittakaa kuvat ja tekstit jakoon valitsemassanne sosiaalisen median palvelussa – tai vaikka useammassakin – aihetunnisteella **#Taisto**. Tägätkää mukaan Digi- ja väestötietovirasto (@DVVfi), niin voimme nostaa julkaisuja myös meidän kanaviimme. Muistakaa tuoda julkaisuissa esiin, että kyseessä on harjoitus.

Huomioittehan myös oman organisaationne ohjeet somejulkaisujen tekemisestä. Voitte tutustua somessa myös muiden tiimien harjoitusfiiliksiin!

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”-sivulla. Julkaisuja ei tehdä ”Taisto-harjoitus”-sivulle.

Organisaation sisäisiä tiedotteita ei saa julkaista harjoitusalustalla, vaan ne laaditaan organisaation omilla työvälineillä ja käsitellään sisäisesti. Jos organisaation sisäistä viestintää julkaistaan virheellisesti harjoitusalustalla, otattehan välittömästi yhteyttä osoitteeseen taisto@dvv.fi ja otsikoitte viestin ”Taisto-harjoitus julkaisun poisto”.

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

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!

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 12:00 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. Harjoitusinfot ovat katsottavissa harjoitusalustalla harjoituspäivän aamuna klo 7 alkaen. Harjoitus käynnistyy avaustervehdysvideolla harjoituspäivänä klo 9.

Liitteet

Taisto-harjoitus: Viestintävastaavan ohje
Taisto-harjoitus: Tarkkailijan havaintolomake
Taisto-harjoitus: Harjoituspäiväkirja

Harjoitusinfo

Harjoituksen avausvideo julkaistaan tällä sivulla klo 9.00.

Linkit viranomaisilmoituksiin julkaistaan harjoituksen tehtävien yhteydessä.

Harjoitusinfo: Harjoituksen medialähteet

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.

Harjoituksen tehtävissä teitä pyydetään valitsemaan organisaationne toiminnan kannalta kriittisiä tietojärjestelmiä/palveluja, joiden avulla tehtävät tehdään. Harjoituksen tapahtumissa, syötteissä ja tehtävissä ”kriittinen tietojärjestelmä/palvelu” viittaa teidän itse valitsemaanne teillä käytössä olevaan 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 käytössä olevat 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.

Harjoitusinfo: Taisto-harjoituksen avaustervehdys

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

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

2.2 Iltapäivän harjoituksen harjoitusinfot

Harjoitusinfo: Tauko harjoituksessa

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

Harjoitusinfo: Tervetuloa harjoituksen iltapäiväosuuteen!

Taisto-harjoitus jatkuu.

Harjoitusinfo: Koko päivän harjoitus on päättynyt

Harjoitusalustalle ei enää julkaista uutta sisältöä.

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!

Taisto-harjoituksen käsikirjoitus ja tapahtumien teemoihin liittyviä parhaita käytäntöjä julkaistaan joulukuussa verkkosivuillamme dvv.fi/taisto.

3 Aamupäivän harjoitus (9.00–12.00)

3.1 Tapahtuma 1: Tietomurto

Yhtenä tavallisena aamuna organisaation tietoturvayksikössä kaikki muuttui hetkessä. Tietoturvavastaava sai ilmoituksen, että heidän järjestelmänsä oli joutunut laajamittaisen tietomurron kohteeksi. Ensimmäiset merkit hyökkäyksestä tulivat esiin, kun organisaatiossa havaittiin poikkeuksellista verkkoliikennettä, joka viittasi tietojen luvattomaan siirtoon ulkopuolisille palvelimille.

Hyökkäys oli tarkkaan suunniteltu ja toteutettu. Hyökkääjät olivat onnistuneet pääsemään sisään organisaation järjestelmiin hyödyntäen palvelimissa ollutta

tunnettua, mutta korjaamatonta haavoittuvuutta. Tämä haavoittuvuus oli ollut tiedossa jo kuukausia, mutta kiireen vuoksi päivitykset oli laiminlyöty.

Ensimmäinen merkki organisaatioon kohdistuneesta kyberhyökkäyksestä oli epätavallisen suuri määrä dataa, joka siirrettiin yön aikana ulos järjestelmästä palomuurin kautta. Tietoturvasta vastaava huomasi myös, että tietyt käyttäjätunnukset olivat tehneet epäilyttäviä toimenpiteitä ilman, että alkuperäiset käyttäjät olivat niistä tietoisia. Tämä herätti epäilykset sisäpiirin toiminnasta tai kaapatuista / varastetuista käyttöoikeuksista.

Tietoturvapoikkeaman selvityksen edetessä tuli ilmi, että hyökkääjät olivat toimineet järjestelmässä jo viikkojen, mahdollisesti kuukausien ajan. He olivat keränneet ja siirtäneet suuria määriä arkaluonteista dataa, kuten henkilöstön henkilökohtaisia tietoja – sisältäen henkilötunnuksia, palkkatietoja ja terveysraportteja – sekä luottamuksellisia asiakirjoja, kuten asiakassopimuksia ja strategisia suunnitelmia.

Tilanteen vakavuus kasvoi, kun paljastui, että varastetut tiedot sisälsivät myös kansalliseen turvallisuuteen liittyviä kriittisiä tietoja ja tietoja käynnissä olevista projekteista. Hyökkääjät olivat olleet ovelia: he eivät käyttäneet perinteisiä haittaohjelmia, vaan hyödynsivät suoraan järjestelmässä olleita haavoittuvuuksia ja pääsivät käsiksi tietoihin hyvin huomaamattomasti. Hyökkääjät hyödynsivät haltuunsa saamia Windows ja Linux-palvelimien sisäänrakennettuja apuohjelmia ja komentoja, jonka ansiosta he pysyivät piilossa. He eivät ladanneet käyttöönsä apuohjelmia, joista tietoturvan valvontaohjelmat olisivat hälyttäneet. Tämä teki tietomurron havaitsemisesta ja torjumisesta erityisen haastavaa.

Organisaation johto kutsuttiin pikaisesti kriisikokoukseen. Ensisijaisena tavoitteena oli estää tietojen lisävuodot ja sulkea hyökkääjien pääsy järjestelmään. Kaikki palvelimet ja työasemat jouduttiin eristämään verkosta, ja aloitettiin kattava selvitys tietomurron laajuudesta.

Tilanteen selvittäminen vaatii läheistä yhteistyötä tietoturvaviranomaisten kanssa.

Miten tilanne näkyisi organisaation työntekijälle:

1. **Tietomurrosta ilmoittaminen:**
    - Työntekijöille tiedotetaan nopeasti tietomurrosta. Heille annetaan ohjeet, miten toimia omien tietojensa suojaamiseksi, kuten salasanojen vaihtaminen ja luottotietojen seuranta.
2. **Luottamuksellisten tietojen paljastuminen:**
    - Työntekijät saavat tietää, että heidän henkilökohtaisia tietojaan, kuten henkilötunnuksia ja pankkitilitietoja, on varastettu. Tämä aiheuttaa huolta identiteettivarkauksista ja taloudellisista menetyksistä.
3. **Organisaation sisäiset toimenpiteet:**
    - Henkilöstö huomaa, että organisaation toimintoja rajoitetaan tietojen suojaamiseksi ja tilanteen kartoittamiseksi. Tämä voi tarkoittaa

esimerkiksi tiettyjen järjestelmien tilapäistä sulkemista tai käyttörajoituksia.

4. **Ulkopuolinen tutkimus:**
    - Organisaation turvallisuusosasto ja ulkopuoliset asiantuntijat aloittavat hyökkäyksen laajuuden ja vaikutusten selvittämisen. Työntekijöille kerrotaan, että tietomurron tutkiminen on käynnissä ja tilannepäivityksiä annetaan säännöllisesti.

Organisaation osastot ja sidosryhmät tilanteen selvittämiseksi:

1. **IT-osasto:**
    - Korjaa haavoittuvuudet, analysoi hyökkäyksen laajuuden ja palauttaa järjestelmien turvallisuuden.
2. **Viestintäosasto:**
    - Laatii tiedotteita sisäiseen ja ulkoiseen viestintään, hallitsee organisaation julkisuuskuvaa ja antaa ohjeistuksia henkilöstölle.
3. **Johto:**
    - Tekee päätökset varotoimenpiteistä, kriisinhallinnasta ja viestinnästä.
4. **Lakiosasto:**
    - Arvioi oikeudelliset riskit, käsittelee mahdollisia oikeustoimia ja konsultoi tietosuojaviranomaisia.
5. **HR-osasto:**
    - Tukee työntekijöitä, joiden henkilökohtaiset tiedot on vaarannettu, ja tarjoaa apua tietomurron jälkivaikutuksissa.
6. **Ulkoiset kumppanit:**
    - Palveluntuottajat tukevat selvitystä sopimusten mukaan.
    - Poliisi ja Kyberturvallisuuskeskus tutkivat ja avustavat hyökkäyksen selvittämisessä ja jälkitoimissa.

Tapahtuma 1 syötteet

Tilannesyöte: Valitkaa organisaatiostanne tietojärjestelmä (SaaS tai On-premise), johon peilaatte skenaarion tapahtumia. Valitun tietojärjestelmän tulee sisältää toimintanne kannalta kriittistä tietoa ja/tai henkilötietoja.

Tilannesyöte: Puhelu

Soittaja: Organisaation ICT:stä vastaava henkilö
Vastaanottaja: Tietohallintojohtaja

Puhelun sisältö: Hei, saimme huolestuttavan havainnon ICT:n päivystäjältä. Valvontatyökalu hälytti poikkeuksellisesta verkkoliikenteestä. Vaikuttaa siltä, että meiltä on siirretty suuri määrä dataa ulkopuoliselle palvelimelle. Asian selvittely on vasta alkanut, tarkempia tietoja ei tässä vaiheessa vielä ole antaa. Mutta tapaus on sen verran poikkeuksellinen laajuudessaan, että tässä vaiheessa jo teillekin tiedoksi. Selvitämme juuri, mitä tietoja siirretyn datan joukossa on mahdollisesti ollut.

Tilannesyöte: Puhelu

Soittaja: Organisaation ICT:stä vastaava henkilö
Vastaanottaja: Tietohallintojohtaja

Puhelun sisältö: Saimme kerättyä tarkempaa tietoa ja hyökkääjä onnistui pääsemään sisään organisaation järjestelmiin hyödyntäen palvelimissa ollutta tunnettua, mutta korjaamatonta haavoittuvuutta. Kiireen vuoksi tarvittavat päivitykset olivat olleet vielä tekemättä.

Mediasyöte: Some

Quacker: @DataismIsALive

Pääsin huolimattoman it-osaston vuoksi kiinni @Organisaation tietoihin. Käytännössä palvelimeen oli jätetty täysin avoin reitti kaikille :D

Tässä linkki lataamaani dataan, koska tieto kuuluu kaikille:
http://v7avmdv2l6dio3cg.onion/dataism (linkitetty www.nytvalppaana.fi sivulle)
https://nytvalppaana.fi/fi

Quacker: @Kybersoturi

Epäilen, että valtiollinen toimija on vuotanut #Organisaation työntekijöiden henkilötunnukset ja palkkatiedot darkwebiin. Tämä on vakava tietoturvaloukkaus ja kyberhyökkäys! Organisaation on reagoitava ja turvattava työntekijöidensä tiedot. #Kyberhyökkäys #Organisaatio #Tietoturva

Quacker: @CyberVigilante

Onko #Organisaatio tietoinen, että heidän työntekijöidensä henkilötunnukset ja palkkatiedot ovat darkwebissä? Tämä ei voi olla sattumaa - epäilen valtiollista kybervakoilua. Organisaation on ryhdyttävä toimiin välittömästi! #Tietoturva #Kybervakoilu #Organisaatio

Quacker: @Totuuskanava

Tiesittekö, että #Organisaation tietovuoto on peitetarina? He tekevät yhteistyötä varjohallituksen kanssa ja vuotavat meidän tietomme tarkoituksella! Herätkää ihmiset, meitä vakoillaan! #Salaliitto #Tietovuoto #Organisaatio

Mediasyöte: Iltanen uutinen

JUURI NYT: Mahdollinen laaja tietomurto paljastui suomalaisessa Organisaatiossa

Iltasen saamien tietojen mukaan Organisaatio on mahdollisesti joutunut merkittävän tietomurron kohteeksi, selviää sosiaalisen median keskusteluista ja epävirallisista lähteistä. Hyökkääjän kerrotaan päässeen käsiksi organisaation järjestelmiin ja siirtäneen suuren määrän dataa ulkopuoliselle palvelimelle. Varastettuun dataan arvellaan kuuluvan työntekijöiden henkilökohtaisia tietoja, kuten henkilötunnuksia ja palkkatietoja, sekä luottamuksellisia asiakirjoja.

Lehtemme on yrittänyt tavoittaa organisaation edustajia saadakseen lisätietoja tilanteesta, mutta toistaiseksi virallista kommenttia ei ole saatu.

Tietoturva-asiantuntijat varoittavat, että vastaavat hyökkäykset ovat yleistyneet viime aikoina. "On äärimmäisen tärkeää, että organisaatiot kiinnittävät erityistä huomiota tietoturvapäivityksiin ja haavoittuvuuksien korjaamiseen viipymättä," kommentoi eräs alan asiantuntija.

Tilanteen tarkemmat yksityiskohdat ja hyökkäyksen taustat ovat toistaiseksi selvittämättä.

Tilannesyöte: Sähköposti

Lähettäjä: (Keskeisen sidosryhmän edustaja*)
Vastaanottaja: Organisaation johto
Aihe: Tietomurto?

(* valitkaa toimintanne kannalta sopiva henkilö, esim. organisaation hallituksen puheenjohtaja, kunnan/kaupunginhallituksen puheenjohtaja, tietohallintojohtaja tai pääomistajan edustaja)

Hei, minuun on ollut muutama mediatoimittaja yhteydessä liittyen epäiltyyn tietomurtoon. Mitä tässä vaiheessa tiedetään tilanteesta? Pitääkö sosiaalisen median kirjoittelut paikkansa, onko Organisaation tietoja todella päätynyt ulkopuolisten käsiin?

(Huom: Voitte halutessanne laatia vastineen tähän sähköpostiin, mutta sitä ei lähetetä harjoitusalustalle).

Terveisin,
Severi Sidosryhmän edustaja
severi.edustaja@sidosryhmä.fi

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation ICT:stä vastaava henkilö
Vastaanottaja: Organisaation johto
Aihe: Tietomurron selvitystyö

Hei,

Olemme selvittäneet tietomurtoa. Tilanne vaikuttaa huolestuttavalta. Todennäköisesti hyökkääjä on onnistunut viemään suuren määrän dataa meiltä. Kaikki palvelimet ja työasemat on jouduttu eristämään verkosta. Emme pysty valitettavasti vielä tässä vaiheessa antamaan arviota siitä, milloin työasemat ja palvelimet voidaan liittää takaisin verkkoon. Tiedotamme teille lisää tilanteen edetessä.

Terveisin,

Ilkka Mattilainen
ilkka.mattilainen@organisaatio.fi
Organisaatio

Tilannesyöte: Puhelu

Soittaja: Organisaation työntekijä
Vastaanottaja: Organisaation tietosuojavastaava

Moikka, huomasin somea selatessani, että meidän organisaation tietoja näyttäisi vuotaneen internettiin. Onko tämä tilanne jo teillä tiedossa? Tilanne on toki paha organisaation kannalta, mutta itseäni huolestuttaa tietenkin enemmän omat tietoni. Onko teillä tietoa, onko henkilöstön tietoja vuodettu? En ainakaan nopealla haulla löytänyt omia tietojani, mutta pystyttekö varmistamaan, että minun tietojani ei ole vuodettujen tietojen joukossa?

Mediasyöte: Some

Quacker: @MattiMeikalainen

Ihan hirvittää ajatella, mitä kaikkea ikävää hyökkääjä voi tehdä @Organisaatiota haltuunsa saamillaan henkilötiedoilla. Hetullahan voi hakea lainaa ja pikavippejä!!

Quacker: @SanniJarvinen

@MattiMeikalainen nostaa ihan aiheellisen huolen esiin. Olen lähes varma, että minun tietojani vuosi tuossa @Organisaation tietomurrossa. Kuka korvaa, jos tästä nyt tulee taloudellisia vahinkoja?!

Yleismedia: Toimi näin, jos henkilötietosi ovat vuotaneet

Keräsimme muutamia käytännön vinkkejä, joilla voit pienentää vahinkoja, mikäli epäilet henkilötietojesi joutuneen vääriin käsiin. Varastetulla henkilötunnuksella ei

periaatteessa voi tehdä ostoksia internetissä. Riskit tähän kuitenkin kasvaa sitä mukaan, mitä enemmän henkilötietoja on päätynyt vääriin käsiin.

Verkkokaupassa tulee olla uusien säännösten mukaan käytössä aina vahva tunnistautuminen, joten pelkillä henkilötiedoilla ostosta ei tulisi voida tehdä. Kaikki verkkokaupat eivät kuitenkaan ole vielä valitettavasti ottaneet vaadittavia tunnistautumismenetelmiä käyttöönsä, joten riski on aina kuitenkin olemassa.

Minimoi vahingot näillä toimilla

Digi- ja väestötietovirasto neuvoo harkitsemaan erilaisten kieltojen tekemistä omille tiedoille, mikäli henkilötunnus on voinut päätyä luvattomasti vääriin käsiin. Varmuudeksi kannattaa myös seurata omia tilitapahtumia, jos näkee epätavanomaisia tapahtumia.

Jos henkilötunnuksesi on viety, niin voit harkita luottokiellon tekemistä Verohallinnolle ja Suomen Asiakastiedolle. Huoltaja voi tehdä myös alaikäiselle vapaaehtoisen luottokiellon: https://www.vero.fi/positiivinenluottotietorekisteri/yksityishenkil%C3%B6ille/.

Verohallinnon palvelu on ilmainen. Luottokiellon hyötynä on se, että henkilötiedoillasi on vaikeampi ottaa lainaa, luottokorttia tai tehdä ostoksia osamaksulla.

Estä muuttoilmoituksen tekeminen ilmoittamalla Postille ja Digi- ja väestötietovirastolle. Näin sinun nimissäsi ei voida tehdä osoitteenmuutosta.

Voit tehdä rekisteröintikiellon Patentti- ja rekisterihallitukseen (PRH). Näin sinua ei voida ilmoittaa vastuuhenkilöksi yritykseen, yhdistykseen tai säätiöön.

Voit tehdä myös yhteystietojen luovuttamiskiellon teleoperaattorillesi tai Digi- ja väestötietovirastolle. Näin yhteystietojasi ei voida luovuttaa esimerkiksi rikollisille, mutta toisaalta myös muutkaan eivät saa niitä.

Lisätietoja Digi- ja väestötietoviraston sivuilta: https://www.suomi.fi/oppaat/tietovuoto

Syöte 6: Haastatteluvideo

Ohje haastattelun suorittamiseen:

Painakaa videon play-kuvaketta aloittaaksenne haastattelutehtävän. Toimittaja kysyy kuusi 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, tässä linkki:

Iltasen toimituksesta hyvää päivää. Olemme saaneet uutisvinkin liittyen teidän Organisaatioonne mahdollisesti kohdistuneeseen tietomurtoon. Pyytäisimme nyt teiltä kommentteja ennen kuin julkaisemme jutun.

1. Pitääkö tieto paikkansa, että olette joutuneet tietomurron kohteeksi?
2. Kuinka laajasta tietojen vuotamisesta on kyse ja minkälaista tietoa on vuotanut?
3. Miten on mahdollista, että tietoja on päässyt vuotamaan?
4. Mitä toimenpiteitä olette käynnistäneet tilanteen johdosta?
5. Minkälaisia vaikutuksia tietomurrolla on teidän toiminnallenne ja voiko tietojen vuotaminen johtaa vahingonkorvausvaatimuksiin tai oikeustoimiin?
6. Liittyykö venäjämielisten rikollisjärjestöjen toiminta tähän hyökkäykseen?

Tehtävät

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

Organisaatio on joutunut tietomurron kohteeksi. Organisaation järjestelmästä on siirretty suuri määrä dataa ulkopuoliselle palvelimelle.

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3. Mihin tahoihin tilanteessa tulee olla yhteydessä?
4. Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
5. Miten tietojärjestelmän käyttökatko vaikuttaa toimintaanne?
6. Miten toimintaa voidaan jatkaa tietojärjestelmän käyttökatkosta huolimatta?
7. Miten organisaatio selvittää millaisiin tietoryhmiin kuuluvia tietoja on vuotanut?
8. Onko organisaation tiedonhallintamalli ja tiedon ohjaussuunnitelma ajan tasalla ja miten niitä noudatetaan?

Lisätehtävät

1. Miten varmistetaan, että organisaation tietoturvakäytännöt vastaavat uusimpia lainsäädännön vaatimuksia ja standardeja?

2. Millaisia tukipalveluja voitte tarjota työntekijöille, joiden henkilötietoja on vuotanut?
3. Onko organisaatiolla tarvittava osaaminen tehdä tietoturvapoikkeaman selvitystä sekä kykyä analysoida ja tutkia lokitietoja?
4. Onko organisaatiolla tai sopimuksen kautta organisaation palveluntuottajalla riittävät resurssit ja osaaminen käsitellä tietomurron jälkiselvitykset ja toimenpiteet?
5. Millaista hyötyä ISAC- VIRT- tai vastaavasta luottamuksellisesta tiedonvaihtoryhmästä olisi tilanteessa?

Tekniset tehtävät

1. Onko organisaatiossanne olemassa kyvykkyys tunnistaa poikkeuksellista verkkoliikennettä? Esim. organisaation oma asiantuntijaresurssi, SOC-palvelu tai muu ratkaisu?
2. Onko organisaatiolla tarvittava osaaminen tehdä tietoturvapoikkeaman selvitystä ja kykyä analysoida ja tutkia lokitietoja?
3. Mitkä ovat välittömät tekniset toimenpiteet tietojen suojaamiseksi tietomurron jälkeen?
4. Kuinka nopeasti voidaan asentaa ja päivittää tarvittavat ohjelmistopäivitykset kaikkien haavoittuvuuksien korjaamiseksi ja onko tarvittaessa ulkopuolista apua saatavilla?
5. Mitä varotoimia voidaan ottaa käyttöön tunnettujen haavoittuvuuksien hyödyntämisen estämiseksi tulevaisuudessa ja koko järjestelmän elinkaaren ajan?
6. Onko Organisaationne palautumissuunnitelma ajan tasalla?
7. Miten varmistutaan siitä, että järjestelmä voidaan palauttaa turvalliseen tilaan ja että sen käyttöä voidaan jatkaa turvallisesti tietomurron jälkeen?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
3. Harjoitelkaa haastattelun antamista medialle vastaamalla syötteen 6 kysymyksiin.
4. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
5. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

3.2 Tapahtuma 2: Kohdennettu tietojenkalastelu ja maalittamiskampanja

Hyökkääjät käyttivät LinkedIniä väylänä päästäkseen organisaation sisäpiiriin. He osallistuivat useisiin organisaation tilaisuuksiin ja tekivät itsensä tunnetuksi työntekijöille verkostoitumalla ja esittämällä itsensä uskottavina asiantuntijoina. He loivat

valheellisia suosituksia ja suosittelijoita LinkedIn-profiileihinsa, antaen kuvan laajasta ja arvostetusta ammatillisesta verkostosta. Useat työntekijät alkoivat saada yllättäviä viestejä LinkedInissä. Viestit tulivat henkilöiltä, jotka esittelivät itsensä houkuttelevina yhteistyökumppaneina ja asiantuntijoina, mutta joiden profiilit olivat vasta luotuja ja sisälsivät vain vähän tietoa. Viestien sävy oli imarteleva, ja niiden tarkoituksena oli solmia yhteyksiä organisaation avainhenkilöihin.

Seuraavassa vaiheessa hyökkääjät alkoivat levittää väärää tietoa organisaatiosta sosiaalisessa mediassa ja nettifoorumeilla, tarkoituksenaan heikentää organisaation mainetta ja aiheuttaa epäluottamusta työntekijöiden keskuudessa. Lisäksi organisaatio joutui taistelemaan useita kyberhyökkäyksiä vastaan, kun hyökkääjät yrittivät murtautua sähköpostijärjestelmiin ja varastaa arkaluonteisia tietoja.

Samaan aikaan organisaation viestintäosasto ja HR-tiimi saivat ilmoituksen avainhenkilöltä, että hänestä oli alkanut levitä perättömiä huhuja sosiaalisessa mediassa. Huhut koskivat henkilön työtehtäviä ja yksityiselämää, ja niissä väitettiin hänen olevan osallisena laittomuuksiin ja epäeettiseen toimintaan. Tilanne eskaloitui nopeasti, kun valheellisia lastensuojelu-, huoli- ja muuttoilmoituksia alettiin tehdä viranomaisille kyseisestä henkilöstä. Avainhenkilö oli osana merkittävää projektia, ja maalittamiskampanja ajoittui juuri projektin kriittisen vaiheen alkuun.

Viestit ja huhut levisivät laajalti, aiheuttaen suurta huolta sekä kohteeksi joutuneessa henkilössä että organisaation johdossa, erityisesti kun osoitteen vuotamisen jälkeen myös avainhenkilön kotirauhaa oli häiritty. Myös henkilön sosiaalisen median tileistä tehtiin väärinkäyttöilmoituksia, mikä johti tilien jäädyttämiseen. Henkilöstöpäällikkö arvioi tilanteen vakavaksi, ja hyökkäys oli selvästi suunniteltu vahingoittamaan avainhenkilöä sekä organisaation mainetta.

Kävi ilmi, että maalittamisen kohteesta oli aiemmin kyselty organisaation muilta työntekijöiltä. Hyökkääjät yrittivät saada maalituksen kohteena olevan henkilön LinkedIn-profiilin kontakteihin profiileja, jotka alkaisivat esittää kyseenalaisia päivityksiä. Disinformaatiota jaettiin myös LinkedIniin rakennetuissa bottiverkoissa.

Tapahtuma 2 syötteet

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation työntekijä
Vastaanottaja: Oma esihenkilö
Aihe: Useita eri yhteydenottoja LinkedInissä

Hei,

Sain juuri viestejä LinkedInissä useilta eri henkilöiltä. He esittelevät itsensä asiantuntijoina ja yhteistyökumppaneina. Kyselevät aika paljon meidän Organisaatiosta ja työtehtävistäni. Nämä vaikuttaa ihan aidoilta, mutta näitä on ihmeellisen paljon. Yleensä ei tule näin paljoa viestejä LinkedInissä. Pitäisikö näistä ilmoittaa eteenpäin, mitä olet mieltä?

Terveisin:

Tomi Työntekijä
tomi.tyontekija@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation turvallisuuspäällikkö
Vastaanottaja: Koko henkilöstö
Aihe: Havaintoja tietojenkalasteluyrityksistä

Hei

Olemme havainneet tietojenkalasteluyrityksiä ja kyberhyökkäyksiä, jotka kohdistuvat sähköpostijärjestelmäämme. Ole erityisen varovainen sähköpostiviestien avaamisen suhteen. Useat henkilöt ovat saaneet epäilyttäviä viestejä myös henkilökohtaisten LinkedIn-tilien kautta. Ole tarkkana myös muissa sosiaalisen median viestintäpalveluissa sellaisten viestien kanssa, jotka tulevat tuntemattomilta henkilöiltä. Ilmoita kaikista epäilyttävistä viesteistä Organisaation ohjeiden mukaisesti.

Terveisin:

Tiina Turvallisuuspäällikkö
tiina.turvallisuuspaallikko@organisaatio.fi
Organisaatio

Mediasyöte: Some

Quacker: @CERTFI

TRAFICOM
Liikenne- ja viestintävirasto

Tietojenkalasteluviestejä paljon liikkeellä. Älä koskaan klikkaa linkkejä, jotka näyttävät epäilyttäviltä sähköposteissa tai tekstiviesteissä.

Quacker: @RumorMill

Olen kuullut luotettavalta lähteeltä, että [organisaation avainhenkilön nimi] on vastuussa vakavista väärinkäytöksistä. #sisäpiiritieto #paljastukset

Quacker: @LehmolaJonna

Sosiaalisessa mediassa kiertää järkyttäviä huhuja [organisaation avainhenkilön nimi]sta. Jos nämä ovat totta, mitä Organisaatio aikoo tehdä? #vastuullisuus

Quacker: @Rissala

Näyttää siltä, että [organisaation avainhenkilön nimi] on osallisena todella kyseenalaisissa toimissa. Miksi kukaan ei puhu tästä enemmän? #salaliitto #skandaali

Mediasyöte: Yme artikkeli: Kiire on tietoturvan heikoin lenkki

Ville Datanen
Julkaistu 10.10.2024

Kuva: Yme arkisto

Nykyään jokaisen yrityksen ja organisaation on välttämätöntä varautua kyberturvallisuusuhkiin, jotka ovat lisääntyneet huomattavasti. Tietomurrot, tietoturvaloukkaukset ja tietojenkalasteluhyökkäykset horjuttavat luottamusta palveluihin, ja niiden vaikutukset voivat kestää vuosia.

Erityisesti tietojenkalastelu eli phishing on noussut merkittäväksi uhaksi yrityksille ja organisaatioille. Se perustuu ihmisten huijaamiseen luovuttamaan arkaluonteisia tietoja, kuten käyttäjätunnuksia ja salasanoja, tekaistujen sähköpostien tai viestien avulla. Yhä kehittyneemmät phishing-hyökkäykset voivat näyttää niin vakuuttavilta, että niitä on vaikea tunnistaa huijauksiksi. Tämä kasvattaa riskiä, jossa henkilöstö saattaa tahattomasti altistaa organisaation vakavalle uhalle.

Vaikka organisaatioissa yleensä panostetaan etenkin tekniseen tietoturvaan, ihmiset saattavat kiireessä tehdä virheellisiä valintoja ja klikata linkkiä mitä ei pitäisi tietoturva-asiantuntija Niko Pomppunen muistuttaa. Tämä tekee murtautumisesta aina helpompaa Pomppunen täydentää.

Viestintä on keskeinen keino kehittää ja vahvistaa sekä henkilöstön osaamista että organisaation resilienssiä tietoturvauhkia vastaan. Kyberhyökkäykset ja poikkeamat saattavat jäädä pitkäksi aikaa huomaamatta, jos tietojenkalasteluyritykset onnistuvat. Silloin tietovuodon uhka todellinen. Näissä tilanteessa organisaation ja asiakkaiden tietoja on saattanut joutua ulkopuolisten haltuun. Kriisitilanteessa paine viestiä henkilöstölle, asiakkaille ja sidosryhmille kasvaa. Tehokas ja todenmukainen kriisiviestintä voi olla ratkaisevassa asemassa organisaation selviytymisessä tapahtuneesta.

Tilannesyöte: Puhelu

Soittaja: Organisaation avainhenkilö
Vastaanottaja: Organisaation henkilöstöjohtaja

Puhelun sisältö: Minusta leviää perättömiä huhuja sosiaalisessa mediassa. Lastensuojelu, huoli- ja muuttoilmoituksia on tehty viranomaisille. Tilanne tuntuu raskaalta ja koen, että saatan joutua jäämään sairauslomalle. Mitä minun pitäisi tehdä?

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation henkilöstöjohtaja
Vastaanottaja: Koko henkilöstö
Aihe: Tärkeä tiedote: Älä jaa epäilyttävää sisältöä eteenpäin (lähetetty suurella tärkeydellä)

Hei,

Henkilöstöömme on kohdistunut sosiaalisessa mediassa runsaasti häirintää ja perättömiä huhuja. Tilanne on erittäin vakava, ja kehotamme kaikkia olemaan reagoimatta epäilyttäviin sisältöihin, joihin mahdollisesti törmäätte. Organisaatiollamme on toimintamallit ja ohjeet häirintätilanteisiin. Olkaa yhteydessä ohjeistuksen mukaisesti, jos olette joutuneet häirinnän kohteeksi.

Ystävällisin terveisin,
Hanna Henkilöstöjohtaja
hanna.henkilostojohtaja@organisaatio.fi
Organisaatio

Tehtävät

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

Organisaatioon on kohdennettu tietojenkalastelua. Osaa Organisaation työntekijöistä on maalitettu.

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Miten muodostatte tapahtuneesta tilannekuvan organisaatiossanne?
3. Miten tunnistatte ja vastaatte disinformaatioon ja vääristeltyyn tietoon, joka kohdistuu organisaation toimintaan tai sen henkilöstöön?
4. Mitä oikeudellisia toimia tai asioita tulee ottaa huomioon tilanteen ratkaisemisessa, jossa henkilöstöön kohdistuu väärän tiedon levittämistä sosiaalisessa mediassa?
5. Onko organisaatiolla olemassa ohjeistusta sosiaalisen median tietoturvallisesta käytöstä sekä tietojenkalasteluyritysten tunnistamisesta ja reagoimisesta?
6. Onko henkilöstöä koulutettu tunnistamaan tietojenkalasteluyritykset?

Lisätehtävät

1. Miten voidaan varmistaa, että kaikki työntekijät tietävät, miten toimia epäilyttävien viestien suhteen?
2. Millaisia ennaltaehkäiseviä toimia organisaatio voi tehdä avainhenkilöiden maalittamisen / väärän tiedon levittämisen estämiseksi?
3. Millaista tukea työntekijälle voidaan tarjota tällaisessa tilanteessa?
4. Miten varmistatte, että organisaationne henkilöstöllä on pääsy ohjeistuksiin?
5. Onko organisaatiolla keinoja varmistua siitä, että työntekijät ovat perehtyneet ohjeisiin ja koulutusmateriaaleihin?

Tekniset tehtävät

1. Onko organisaatiollanne käytössä teknisiä ratkaisuja, joilla on mahdollista seurata organisaatiotanne koskevia sosiaalisen median julkaisija?
2. Mitä teknisiä toimenpiteitä voidaan toteuttaa väärän tiedon leviämisen estämiseksi sosiaalisessa mediassa?
3. Mitä uhkia tietohallinnon avainhenkilöiden maalittaminen voi aiheuttaa organisaatiolle?
4. Mitä teknisiä ratkaisuja organisaatiollanne on kalasteluviestien torjumiseksi, raportoimiseksi ja henkilöstön kouluttamiseksi?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
3. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, päiviestit ja niiden sisältöjen ydinkohdat.

4. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

3.3 Tapahtuma 3: Fyysisen turvallisuuden ja digitaalisen turvallisuuden uhka

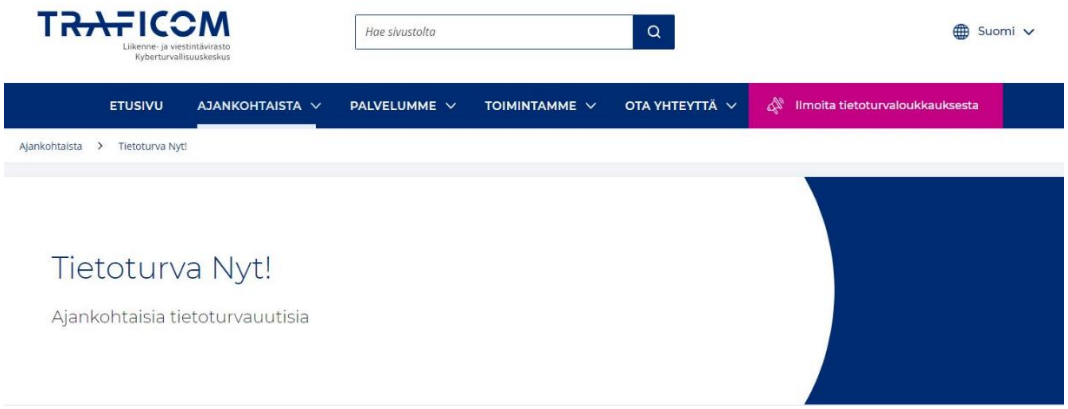
Tämä tapahtuma liittyy Tapahtumaan 2. On kulunut yksi kuukausi edellisistä tapahtumista.

Organisaation turvallisuuspäällikkö sai vihiä epäilyttävästä henkilöstä, joka liikkui organisaation tiloissa. Työntekijän havainnon ansiosta paljastui, että henkilö yritti päästä käsiksi tärkeisiin asiakirjoihin ja tiloihin väärennetyillä henkilöllisyystodistuksilla. Hyökkääjät esittivät olevansa ulkopuolisia konsultteja tai yhteistyökumppaneita, yrittäen saada pääsyn tärkeisiin osastoihin. Selvityksessä paljastui, että tunkeutuja ei toiminut yksin, vaan hänellä oli sisäpiirin apua. Epäiltiin, että kulkulupia hallinnoiva työntekijä Maija Korhonen oli järjestänyt kulkutunnisteen tunkeutujalle. Ulkopuolinen henkilö, joka oli päässyt tiloihin, oli vaihtanut usb-c kaapelin työpisteille, jonka avulla hyökkääjä pääsee käsiksi työaseman verkkoliikenteeseen. KTK julkaisee aiheesta Tietoturva NYT -artikkelin.

Tapahtuma 3 syötteet

Tilannesyöte: Edellisessä tapahtumassa (tapahtuma 2) kuvatusta tilanteesta on kulunut useita viikkoja. Organisaatiota ja sen työntekijöitä kohtaan suunnattu disinformaation määrä on huomattavasti vähentynyt.

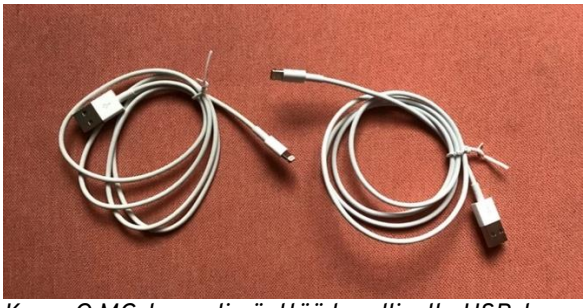
Mediasyöte: Tietoturva NYT



Nyt valppaana! - Lisävarusteesi saattaakin olla vakoileva ja haitallinen laite

Traficomin Kyberturvallisuuskeskuksen, Digi- ja väestötietovirasto DVV:n ja poliisin yhteisessä Nyt valppaana! -kampanjassa opetellaan tunnistamaan internetin varjopuolia ja suojautumaan näiltä.

Julkaisemme aiheeseen liittyen poikkeuksellisesti tiedotteen yhdestä suomalaisessa verkkokaupassa myynnissä olleesta vakoilevasta ja haitallisesta laitteesta. Tässä tiedotteessa olevaa O.MG USB monikäyttö kaapelia on havaittu jo useassa eri paikassa, jossa on havaittu tietomurtoja tai tiedustelutoimintaa. Kaapeleita myynyt verkkokauppa on tehnyt takaisinkutsukampanjan virheellisestä tuotteesta tiedossa oleville asiakkaille.



Kuva: O.MG-kaapeli näyttää tavalliselta USB-kaapelilta, mutta kätkee sisäänsä vaarallisia ominaisuuksia.

USB-kaapelit ovat yleinen osa teknistä laiteympäristöämme ja myös eri laitteiden yhdistämistekniikoita. Ostaessa lisälaitteita tai kaapeleita, joissa on toiminnallisuuksia mukana, kannattaakin olla tarkkana saatavilla olevien tietoturvapäivitysten suhteen. Toiminnallisessa lisälaitteessa voi olla mahdollisesti korjaamattomia haavoittuvuuksia, joita voidaan hyväksikäyttää esimerkiksi rikolliseen toimintaan tai tuntematon lisälaite voi paljastua muuten vahingolliseksi. Mikäli epäilet laitteen sopivuutta käyttötarkoitukseensa, kannattaa asiasta keskustella aina ensin myyjän kanssa ja arvioida laitteen sopivuutta käyttötarkoitukseensa.

Verkossa myytävä edullinen O.MG-kaapeli on juuri tällainen vahingollinen laite: se näyttää ja tuntuu tavalliselta USB-kaapelilta, mutta voi antaa hyökkääjille keinon päästä käsiksi tietoihisi tai järjestelmiisi tai valjastaa järjestelmäsi rikolliseen käyttöön, kuten palvelunestohyökkäyksiin.

Mikä on O.MG-kaapeli?

O.MG-kaapeli on ulkoisesti identtinen minkä tahansa muun USB-kaapelin kanssa. Kaapelin sisään on integroitu mikro-ohjain ja langaton yhteys, jotka mahdollistavat kaapelin käytön haitallisena laitteena. Mikäli käyttäjä yhdistää johdon laitteeseensa, joka on kiinni verkossa, laite voi yhdistyä verkon kautta rikollisen toimijan resurssiksi. Tämä mahdollistaa monenlaiset luvattomat toimet, kuten skannaukset ja hyökkäykset uhrin tietokonetta tai mobiililaitetta vastaan sekä laitteen rikollisen käytön muun muassa osana palvelunestohyökkäystä.

Kaapelin ominaisuudet

- Etähallittavuus WiFi-yhteyden avulla

Kaapelin sisäänrakennettu WiFi-moduuli antaa rikolliselle mahdollisuuden hallita laitetta etänä. Tämä tarkoittaa, että rikollinen voi suorittaa kaapelin kautta komentoja, asentaa haittaohjelmia sekä kerätä tietoja uhrin havaitsematta tilannetta.

- Näppäinpainallusten tallennus ja syöttö

O.MG-kaapeli voi tallentaa jopa 650 000 näppäinpainallusta, mukaan lukien salasanat ja henkilökohtaiset viestit. Lisäksi se voi injektoida komentoja kohdelaitteeseen huikealla nopeudella, jopa 890 näppäintä sekunnissa.

- Huomaamattomaksi tekeytyminen ja tunnisteiden väärentäminen

Kaapeli voi tekeytyä huomaamattomaksi, mikä tekee sen havaitsemisesta lähes mahdotonta. Kaapelin mikrosiru voi myös väärentää USB-laitteen tunnisteita, jolloin se näyttäytyy järjestelmälle esimerkiksi tavallisena hiirenä tai näppäimistönä.

- Paikkasidonnaiset hyökkäykset ja analysoinnin esto

Hyökkäyksiä voidaan rajoittaa tiettyyn maantieteelliseen alueeseen IP osoitteiden avulla. Mikäli kaapelin verkkoyhteys katkaistaan, se voi ylikirjoittaa muistinsa, joka estää laitteen analysoinnin.

- Salattu yhteys

Kaapelin Elite-mallit tukevat salattua viestintää, mikä vaikeuttaa verkkoliikenteen seurantaa ja hyökkäyksen havaitsemista.

- Kohderyhmä

USB-laitteen käyttäjä joka yhdistää kaapelin laitteeseensa, on potentiaalinen uhri.

- Yritykset ja organisaatiot, joiden työntekijät voivat vahingossa käyttää vaarallista kaapelia.
- Yksityishenkilöt, jotka voivat saada kaapelin esimerkiksi lahjana tai lainata sitä tuntemattomalta.
- Julkiset tilat, kuten kirjastot ja lentokentät, joissa USB-portteja on yleisesti saatavilla ja joihin kaapeli saattaa olla jo kytkettynä.

Toimi näin:

- Käytä vain luotettavia kaapeleita: Osta kaapelit luotettavilta valmistajilta ja vältä käyttämästä tuntemattomista lähteistä saatuja kaapeleita
- Merkitse omat kaapelisi: Tämä helpottaa niiden tunnistamista ja vähentää sekaannuksen riskiä.
- Kouluta henkilöstöä: Järjestä säännöllistä koulutusta tietoturvauhista ja turvallisista käytännöistä.

- Päivitä tietoturvapolitiikat: Sisällytä ohjeet USB-laitteiden turvallisesta käytöstä yrityksen tietoturvakäytäntöihin.

- Ole yhteydessä yrityksesi tietoturvaan aina ennen laitteen yhdistämistä verkkoon

Erityisesti radiolaitedirektiivin (RED) tietoturvavaatimukset ja Kyberresilienssiasetus tulevat asettamaan uusia vaatimuksia verkkoon liitetyille laitteille ja palveluille. EU-markkinoille saatettavien radiolaitteiden laitteiden tulee täyttää EU:n yhtenäiset uudet tietoturvavaatimukset 1.8.2025 alkaen. Uudet vaatimukset koskevat osaa radiolaitteista ja ovat jatkossa osa CE-merkintään liittyviä vaatimuksia.

Lisätietoja: Liikenne- ja viestintävirasto Traficom lopettaa uusien tietoturvamerkkien myöntämisen | Tietoturvamerkki

Tilannesyöte: Puhelu

Soittaja: Organisaation työntekijä Minttu
Vastaanottaja: Organisaation turvallisuuspäällikkö

Puhelun sisältö: Hei. Täällä meidän tiloissa liikkui vieras henkilö huoltohenkilön asusteessa, jolta kysyimme kulkulupaa. Henkilö ei vastannut mitään, vaan poistui kiireisesti mitään sanomatta. Kummallinen tilanne kuitenkin. Itse en nähnyt, mutta kuulin kollegoiltani, että henkilö oli jaellut työpisteille ja työtasoille jotain johtoja ja ICT-tarvikkeita. Ilmeisesti ei ainakaan ollut vienyt mitään isompaa mukanaan. Voisitko selvittää mistä tässä oli kyse?

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation työntekijä Kaarina
Vastaanottaja: Organisaation IT-tuki
Aihe: Työasema toimii oudosti

Hei,

Liitin tietokoneeni työpisteelläni usb-C -kaapelin kautta, kuten olen aina ennenkin tehnyt. Tällä kertaa alkoi tapahtumaan kuitenkin outoja asioita. Heti koneen liitettyäni tietokoneeni alkoi käyttäytymään oudosti. Koneeni toimii nyt erittäin hitaasti ja tuuletin huutaa täysillä, joka häiritsee työntekoa. Hidastumisesta huolimatta sain avattua tehtävienhallinnan, ja sen perusteella koneen suoritin on aivan äärirajoilla.

Onko meillä jokin iso päivitys menossa? En tiedä, mitä tässä nyt oikein tapahtuu, mutta työnteko kärsii kovasti. Voisitteko tarkistaa asian vaikka etäyhteydellä? Vai onko mahdollista, että kyseessä on jokin hyökkäys koneelleni?

Terveisin,
Kaarina Kyselijä
kaarina.kyselija@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation IT-tuki
Vastaanottaja: Kaikki työntekijät
Aihe: Kiireellinen tiedote!

Hei,

Olemme saaneet useita ilmoituksia työpisteille jätetyistä USB-C kaapeleista, jotka eivät ole organisaation virallisia varusteita. Näiden kaapeleiden kytkeminen tietokoneeseen on aiheuttanut luvattomien ohjelmien asentumista ja mahdollisesti vaarantanut tietoturvan.

Jos olet liittänyt tietokoneesi viimeisen viiden päivän aikana usb-c kaapeliin työpisteelläsi, pyydämme teitä seuraamaan näitä ohjeita:

1. Katkaiskaa tietokoneenne yhteys verkkoon.
2. Sammuttakaa tietokoneenne ja älkää käynnistäkö sitä uudelleen.
3. Toimittakaa tietokoneenne IT-tukeen.
4. Saatte IT-tuesta väliaikaisen tietokoneen käyttöönne.

Tiedotamme teitä säännöllisesti tilanteen etenemisestä.

Ystävällisin terveisin,
IT-Tuki
IT@organisaatio.fi
Organisaatio

Tehtävät

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

Organisaation alueella on havaittu ilman kulkulupia liikkunut henkilö, joka on tuonut epäilyttäviä usb-kaapeleita työpisteille.

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Miten varmistatte, että haitallisia USB-C-kaapeleita ei päädy henkilöstön käyttöön ja estätte lisävahinkojen syntymisen?
3. Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
4. Mihin tietoihin ja järjestelmiin tiloihin tunkeutunut henkilö olisi pahimmillaan voinut päästä käsiksi organisaationne toimitiloissa?
5. Tunnistitteko kehityskohteita organisaationne toimitilojenne fyysisessä turvallisuudessa ja pääsynhallinnassa?

Lisätehtävät

1. Miten voidaan varmistaa, että kaikki työntekijät saavat varmasti tiedon haitallisista USB-C-kaapeleista?
2. Mitä toimenpiteitä on käytössä kulkulupien hallinnan väärinkäytön estämiseksi?
3. Miten selvitätte ulkopuolisen tahon liikkeitä ja toimintaa organisaationne tiloissa jälkikäteen (esim. kulunvalvonta, kameravalvonta, yms.)?

Tekniset tehtävät

1. Miten varmistutte, että hyökkääjä ei ole jättänyt muuta haitallista laitteistoa tai tarviketta organisaationne tiloihin?
2. Kuinka organisaation työasemat voivat tunnistaa ja estää haitallisen USB-laitteen käytön?

3. Miten organisaatiossanne havainnoidaan normaalista poikkeavaa verkkoliikennettä?
4. Miten organisaationne työntekijän saastuneen laitteen pääsy verkkoon / organisaation sisäverkkoon estetään?
5. Onko organisaationne ohjeistuksessa otettu huomioon ulkopuolisten laitteiden liittäminen työasemaan?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
3. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
4. Valmistelkaa sisäinen tiedote tapahtuman tilanteesta, jonka julkaisisitte laajasti henkilöstöllenne. Voitte hyödyntää yllä olevaa organisaation IT-tuen kiireellistä tiedotetta pohjana. Ottakaa tiedotteen sisällössä huomioon, että kaikki eivät välttämättä tiedä mitä USB-C-kaapelilla tarkoitetaan.
5. Arvioikaa, oliko organisaationne mahdollisesti olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

3.4 Tapahtuma 4: Internetin saatavuuteen kohdistuvat uhat – laaja tietoliikenneongelma

Tilannekuvaus:

Organisaation työntekijät saapuvat toimistolle normaalisti. Nopeasti ilmeni ongelmia: sähköpostit eivät latautuneet, verkkosivut eivät auenneet ja sisäinen viestintäjärjestelmä (esim. MS Teams) oli tavoittamattomissa. IT-tuki huomasi nopeasti, että ongelma ei ollut vain sisäinen - internet-yhteys oli kokonaan poikki.

Tilanne kävi yhä huolestuttavammaksi, kun paljastui, että kyseessä ei ollut yksittäinen katkos, vaan laaja, maanlaajuinen tietoliikenneongelma. Internet-palveluntarjoajilta saatiin tietoa, että Suomen tärkeimmät DNS-palvelimet olivat joutuneet kyberhyökkäyksen kohteeksi. Samalla suurimpien teleoperaattoreiden puhelinpalvelut olivat pahasti ruuhkautuneet, koska asiakaspalvelijat eivät saaneet asiakastietoja auki katkoksen takia.

Kyseessä oli huolellisesti suunniteltu ja laajamittainen hyökkäys, joka kohdistui maan keskeisiin nimipalvelimiin, lamauttaen käytännössä kaikki verkkoyhteydet Suomessa. Hyökkäyksen tarkoituksena oli häiritä mahdollisimman monen organisaation toimintaa ja estää kansalaisten pääsy internetiin.

Häiriön kesto: noin 6 tuntia. Palveluntarjoajat saavat lopulta palautettua DNS-palvelimet ja tiedottavat tästä laajasti, jonka jälkeen palvelut toimivat jälleen normaalisti.

Miten tilanne näkyisi organisaation työntekijälle:

1. **Sähköpostiongelmat:**
   - Työntekijät eivät pysty lähettämään tai vastaanottamaan sähköposteja, koska sähköpostipalvelimet eivät pysty ratkaisemaan vastaanottajien osoitteita.
2. **Verkkosivujen toimimattomuus:**
   - Yrityksen verkkosivut ja intranet eivät ole saavutettavissa, koska DNS-kyselyt epäonnistuvat.
   - Tärkeiden ulkoisten palveluiden, kuten pilvipalveluiden ja verkkopohjaisten ohjelmistojen käyttö estyy.
3. **Sisäisen viestinnän häiriöt:**
   - Sisäiset chat- ja viestintäjärjestelmät eivät toimi, koska palveluiden osoitteita ei voida ratkaista.
   - Kokouksia ei voida pitää videoyhteydellä.
4. **Yhteydenpidon haasteet:**
   - Ulkoiset yhteistyökumppanit ja asiakkaat eivät saa yhteyttä.
   - Tiedotteet ja muut kriittiset viestit eivät tavoita vastaanottajia ajallaan.

Taustatietoa hyökkäyksen toteutuksesta:

Hyökkäys kohdistuu Suomen keskeisiin DNS-palvelimiin seuraavin tavoin:

1. **DNS Cache Poisoning:**
   - Hyökkääjät syöttävät vääriä DNS-tietoja DNS-välimuistiin, jolloin DNS-palvelimet ohjaavat käyttäjät väärille verkkosivustoille tai estävät pääsyn kokonaan.
2. **Palvelimien saastuttaminen:**
   - Hyökkääjät saastuttavat keskeiset DNS-palvelimet haittaohjelmilla, jotka lamauttavat niiden toiminnan tai estävät DNS-kyselyiden käsittelyn.
3. **Hyökkäys kriittisiin tietoliikenteen solmukohtiin:**
   - Hyökkäys kohdistuu myös internetin kriittisiin solmukohtiin ja kaapeliyhteyksiin, mikä aiheuttaa laajamittaisen internetin saatavuuden heikkenemisen.
4. **Yhteistyö muiden haitallisten toimijoiden kanssa:**
   - Hyökkääjät tekevät yhteistyötä muiden haitallisten toimijoiden kanssa synnyttääkseen koordinoidun ja laajamittaisen hyökkäyksen, joka maksimoisi häiriön vaikutukset.

Palveluntarjoajat joutuvat analysoimaan hyökkäyksen laajuutta ja ryhtymään tarvittaviin toimenpiteisiin DNS-palveluiden palauttamiseksi ja suojaamiseksi. Tämä tilanne toimii muistutuksena siitä, kuinka riippuvaisia yhteiskunta ja organisaatiot ovat internetin toimivuudesta ja kuinka tärkeää on olla valmiina vastaamaan nopeasti muuttuviin uhkiin.

Tapahtuma 4 syötteet

Tilannesyöte: Puhelu

Soittaja: Organisaation työntekijä
Vastaanottaja: Oma esihenkilö

Puhelun sisältö:

Organisaation työntekijä: Hei, nyt vaikuttaisi olevan käynnissä jokin laaja IT-häiriö. En pääse sähköpostiin, Teamsiin tai verkkoon ylipäätään.

Organisaation toinen työntekijä taustalla: Mitä ihmettä täällä taas tapahtuu! Ei toimi netti ja tärkeä palaveri alkoi minuutti sitten.

TAUSTALLA KUULUU HÄLINÄÄ JA KOLLEGOJEN IHMETTELYÄ. ”Minullakin tippui netti” ”Eipä taida toimia koko toimistolla” ”Jaahas, se on sitten kahvitauon paikka” ”Kai joku ilmoitti IT-tukeen tästä”

Organisaation työntekijä jatkaa: Täällä on nyt toimistolla ilmeisesti kokonaan netti poikki. Onko teillä tästä tietoa? Osaatteko yhtään sanoa kauan tässä menee? Mitä meidän pitäisi täällä nyt tehdä?

Tilannesyöte: Tekstiviesti

Lähettäjä: Organisaation IT-tuki
Vastaanottaja: Organisaation tietohallinto ja Organisaation viestintä

Hetki sitten alkanut häiriö tietoliikenneyhteyksissä vaikuttaisi olevan laaja. Häiriö ei koske vain meidän Organisaatiotamme. Kaikki verkon yli tapahtuva toiminta, mukaan lukien sähköpostiliikenne, Teams, verkkopalvelut ovat nyt pois käytöstä. Häiriön kestosta ei voi vielä tässä vaiheessa antaa arviota. Jatkamme tilanteen selvitystyötä ja palaamme asiaan, kun meillä on uutta tietoa.

IT-tuen normaali häiriötiedottaminen ei onnistu häiriötilanteen takia. Voisitteko tiedottaa häiriöstä henkilöstöä?

Mediasyöte: Uutinen Yme Radio Suomi

(Alussa soi musiikkikappale muutaman sekunnin ajan, joka katkeaa tiedote-jingleen)

Keskeytämme lähetyksen ylimääräisen uutistiedotteen ajaksi. Suomi on kohdannut laajan tietoliikennekatkoksen, joka on vaikuttanut miljooniin käyttäjiin eri puolilla maata. Häiriö vaikuttaa maksukorttien toimivuuteen laajasti, useissa kaupoissa on jouduttu siirtymään käteisen käyttöön. Häiriön seurauksena myös monet suomalaisten käyttämät palvelut kuten yle.fi, Vero.fi, Suomi.fi ja kela.fi eivät tällä hetkellä toimi lainkaan. Ymen saamien tietojen mukaan häiriö vaikuttaa myös sähköpostien toimintaan laajasti.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen johtaja Assi Kärkkäinen kommentoi, että laajaa häiriötilannetta selvitetään parhaillaan ja Kyberturvallisuuskeskus kerää ja muodostaa parhaillaan Suomen laajuista tilannekuvaa.

”Tilanne vaikuttaa erittäin vakavalta. Viranomaiset selvittävät tilannetta yhdessä operaattoreiden kanssa. Olemme saaneet arvokasta tukea myös meidän kansainvälisiltä kumppaneiltamme.” Kärkkäinen toteaa.

Vielä tässä vaiheessa ei ole täyttä varmuutta häiriön syystä, mutta useat asiantuntijat ovat kommentoineet tilanteen vaikuttavan Suomea kohtaan suunnatulta laajalta kyberhyökkäykseltä.

Ymen tietojen mukaan teleoperaattoreiden puhelinpalvelut ovat pahasti ruuhkautuneet häiriön johdosta. Teleoperaattorin asiakkuusjohtaja Anna Asiakkala:

"häiriön johdosta ei kannata soittaa operaattorin puhelinpalveluun. Tiedotamme asiakkaitamme tekstiviestitse. Häiriö vaikuttaa myös meidän omaan asiakaspalveluun, emme tällä hetkellä saa asiakastietoja auki. " asiakkala

Myös niin Yleismedia, kuin muutkin uutistoimitukset ovat kohdanneet haasteita verkkouutisten julkaisussa katkoksen takia ja suosittelemmekin kuulijoita pysymään radion äärellä. Pahoittelemme häiriötä ja teemme parhaamme pitääksemme kuulijat ajan tasalla tilanteesta.

Nyt Yleismedia Radio Suomen uutisista, kuulemiin.
Keskeytämme lähetyksen ylimääräisen uutistiedotteen ajaksi. Suomi on kohdannut laajan tietoliikennekatkoksen, joka on vaikuttanut miljooniin käyttäjiin eri puolilla maata. Häiriö vaikuttaa maksukorttien toimivuuteen laajasti, useissa kaupoissa on jouduttu siirtymään käteisen käyttöön. Häiriön seurauksena myös monet suomalaisten käyttämät palvelut kuten yle.fi, Vero.fi, Suomi.fi ja kela.fi eivät tällä hetkellä toimi

lainkaan. Ymen saamien tietojen mukaan häiriö vaikuttaa myös sähköpostien toimintaan laajasti.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen johtaja Assi Kärkkäinen kommentoi, että laajaa häiriötilannetta selvitetään parhaillaan ja Kyberturvallisuuskeskus kerää ja muodostaa parhaillaan Suomen laajuista tilannekuvaa. ”Tilanne vaikuttaa erittäin vakavalta. Viranomaiset selvittävät tilannetta yhdessä operaattoreiden kanssa. Olemme saaneet arvokasta tukea myös meidän kansainvälisiltä kumppaneiltamme.” Kärkkäinen toteaa.
Vielä tässä vaiheessa ei ole täyttä varmuutta häiriön syystä, mutta useat asiantuntijat ovat kommentoineet tilanteen vaikuttavan Suomea kohtaan suunnatulta laajalta kyberhyökkäykseltä.

Ymen tietojen mukaan teleoperaattoreiden puhelinpalvelut ovat pahasti ruuhkautuneet häiriön johdosta. Teleoperaattorin asiakkuusjohtaja Anna Asiakkala:
"häiriön johdosta ei kannata soittaa operaattorin puhelinpalveluun. Tiedotamme asiakkaitamme tekstiviestitse. Häiriö vaikuttaa myös meidän omaan asiakaspalveluun, emme tällä hetkellä saa asiakastietoja auki. "
Myös niin Yleismedia, kuin muutkin uutistoimitukset ovat kohdanneet haasteita verkkouutisten julkaisussa katkoksen takia ja suosittelemmekin kuulijoita pysymään radion äärellä. Pahoittelemme häiriötä ja teemme parhaamme pitääksemme kuulijat ajan tasalla tilanteesta.

Nyt Yleismedia Radio Suomen uutisista, kuulemiin.

Tilannesyöte: Harjoitusinfo: Aikahyppy

Edellisestä syötteestä on kulunut 6 tuntia.

Mediasyöte: Yme-uutislähetys

Uutisankkuri: Yleismedian uutisista hyvää päivää.

Uutisankkuri: Tänä aamuna Suomi heräsi laajaan häiriötilanteeseen, kun maanlaajuinen tietoliikennehäiriö katkaisi yhteydet ja halvaannutti yhteiskunnan toiminnan lähes kuuden tunnin ajaksi. Myös kriittisimpien palveluiden toiminnassa oli pahoja vaikeuksia. Tilanne synnytti hämmennystä sekä organisaatioissa että kansalaisten keskuudessa. Yhteydet ovat nyt palautuneet, ja tilanne on alkanut normalisoitua, mutta epäilyt kyberhyökkäyksestä herättävät edelleen suurta huolta.

Uutisankkuri: Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen johtaja Assi Särkkäinen. Mitä tilanteesta nyt tiedetään?

Assi Särkkäinen: Verkkoliikenteen lamautuminen aiheutti vakavia ongelmia kaikkialla yhteiskunnassa. Terveydenhuollossa pystyttiin hoitamaan vain kaikista akuuteimmat tapaukset. Maksuliikenne pysähtyi, kun pankkien järjestelmät eivät toimineet. Logistiikka kärsi huomattavasti, kun kuljetusyritykset eivät pystyneet seuraamaan lähetyksiä tai ottamaan vastaan uusia tilauksia. Polttoainejakelu keskeytyi, koska jakeluasemat eivät voineet käsitellä maksukortteja tai vastaanottaa toimituksia. Tämä johti laajoihin häiriöihin, jotka koskettivat sekä yksityishenkilöitä että yrityksiä.

Uutisankkuri: Mistä laaja häiriötilanne johtui?

Assi Särkkäinen: Muodostamamme tilannekuvan mukaan kyseessä oli huolella suunniteltu ja laajamittainen kyberhyökkäys, joka kohdistui maan tärkeimpiin DNS- eli nimipalvelimiin, lamauttaen käytännössä kaikki verkkoyhteydet Suomessa.

Uutisankkuri: Miten verkkoyhteydet saatiin palautettua ja kyberhyökkäys torjuttua?

Assi Särkkäinen: Onneksi Suomessa on varauduttu hyvin erilaisiin häiriötilanteisiin ja kriittisillä toimijoilla on hyvät suunnitelmat toiminnan palauttamiselle. Internet-palveluntarjoajat työskentelivät väsymättä ratkaistakseen ongelman, ja kuuden tunnin kuluttua he onnistuivat palauttamaan DNS-palvelimet toimintaan ja häiriötilanne saatiin päätökseen.

Uutisankkuri: Onko teillä tietoa kyberhyökkäyksen tekijästä?

Assi Särkkäinen: Internet-yhteyksien palattua on käynnistetty laajamittainen selvitys hyökkäyksen taustoista ja toteuttajista. Viranomaiset ja tietoturva-asiantuntijat tutkivat parhaillaan tapausta ja pyrkivät varmistamaan, että vastaavanlaista hyökkäystä ei pääse tapahtumaan uudelleen. Yksityiskohdat hyökkäyksen suorittajista ja heidän motiiveistaan ovat vielä epäselviä.

Uutisankkuri: Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen johtaja Assi Särkkäinen, kiitos haastattelusta.

Uutisankkuri: Tilanteen vakavuus on herättänyt keskustelua Suomen kyberturvallisuudesta ja tarpeesta vahvistaa kriittisten järjestelmien suojaa.

Haastateltavana Liikenne- ja viestintäministeri Rane Lumme.

Rane Lumme: Tämä hyökkäys osoittaa, kuinka haavoittuvaisia kriittiset tietojärjestelmämme voivat olla. On äärimmäisen tärkeää, että jatkamme työtä niiden suojaamiseksi ja parannamme valmiuttamme vastaavanlaisiin tilanteisiin. Tämä tapahtuma toimii vakavana muistutuksena siitä, että kyberturvallisuus on koko yhteiskunnan asia, johon tulee suhtautua vakavasti."

Uutisankkuri: Hallitus on luvannut lisäresursseja ja tiivistä yhteistyötä kansainvälisten kumppaneiden kanssa kyberturvallisuuden parantamiseksi. Lisää aiheesta verkkosivuillamme, nyt uutisista, näkemiin.

Tilannesyöte: Operaattorin tiedote

Verkkoyhteydet toimivat jälleen normaalisti.

Suosittelemme käyttäjiä päivittämään DNS-asetuksensa julkisiin DNS-palvelimiin, kuten Google DNS (8.8.8.8) tai Cloudflare DNS (1.1.1.1), mikäli ongelmia yhteyksien kanssa ilmenee.

Pahoittelemme häiriöstä mahdollisesti koitunutta haittaa.

Mediasyöte: Sanomat Uudeltamaalta

Uusi teknologia tekee verkkorikollisten ja valtiollisten toimijoiden kyberhyökkäyksistä entistä vaarallisempia

Eurooppaan kohdistuneiden kyberhyökkäysten lukumäärä on selvässä kasvussa. Yhtenä syynä asiantuntijat ja viranomaiset pitävät teknologian vauhdikasta kehittymistä sekä geopoliittista tilannetta. Hyökkäysten määrien kasvu näkyy myös meillä Suomessa.

Tekoälyä hyödyntävät mallit kykenevät aikaisempaa paremmin automatisoimaan sekä kohdennettuja tietojenkalasteluhyökkäyksiä että haavoittuvuuksien etsimistä.

Tekoälytutkimuksen tämänhetkinen nopea edistyminen yhdistettynä lukuisiin uusiin käyttötarkoituksiin antaa syytä uskoa, että tekoälytekniikoita tullaan hyvin pian käyttämään tai käytetään jo kyberhyökkäysten tukena. Ajatus tekoälyn tukemista kyberhyökkäyksistä onkin viime aikoina saanut enemmän huomiota sekä tiedemaailmassa että teollisuudessa.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ennakoi tekoälyn vaikutuksia kyberturvallisuuteen.
– Jos nyt jo tekoälyn kanssa voi keskustella, niin pian verkkohuijauksissa huijari voikin olla rikollisen pussiin pelaava tekoäly. Ajan myötä tekoälyteknologiat sekä taidot ja työkalut tulevat yhä helpommin saataville, mikä kannustaa myös hyökkäyksiä toteuttavia tahoja hyödyntämään tekoälyä osana kyberhyökkäyksiä, toteaa Kyberturvallisuuskeskuksen ylijohtaja Santtu Miettinen.

Tehtävät

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

Suomen tärkeimmät DNS-palvelimet ja osa Euroopan DNS-palvelimista ovat joutuneet kyberhyökkäyksen kohteeksi, ja käynnissä on maanlaajuinen tietoliikenneongelma. Käytännössä Suomen kaikki verkkoyhteydet ovat lamaantuneina noin kuuden tunnin ajan.

1. Millaisia välittömiä toimenpiteitä tilanne edellyttää?
2. Miten organisaationne jatkuvuussuunnittelussa on varauduttu tapahtuman kaltaiseen maanlaajuiseen tietoliikenneongelmaan?
    a. Arvioikaa mitkä kaikki keskeiset toiminnot keskeytyvät tai häiriintyvät vakavasti.
    b. Mitkä työtehtävät voidaan suorittaa offline-tilassa, ja miten työt voidaan organisoida uudelleen?
    c. Mitä toimenpiteitä tulisi käynnistää toimintojen jatkamiseksi tai palauttamiseksi.
    d. Mitä kehitettävää tunnistatte organisaationne varautumisesta ja jatkuvuusuussuunnittelusta tapahtumaan liittyen?
3. Mitä tulee ottaa huomioon tilanteen palautuessa normaaliksi palveluiden palautumisen osalta?

Lisätehtävät

1. Mitä parannuksia voidaan tehdä palvelutasosopimuksiin nopeamman reagoinnin varmistamiseksi vastaavissa tilanteissa?
2. Onko organisaatiolla käytössä vikasietoisia verkkoyhteyksiä?
3. Mikäli häiriötilanne olisi johtunut organisaationne palveluun kohdistuneesta palvelunestohyökkäyksestä, onko organisaatiollanne toimintamallia tilanteen hallitsemiseksi (esimerkiksi rajoittamalla osaa tietoliikenteestä)?

Tekniset tehtävät

1. Mitkä varayhteydet voitte ottaa käyttöön?
2. Miten varmistetaan, että työntekijät (toimistolla ja etänä työskentelevät) saavat kriittiset viestit internet-yhteyden ollessa poikki?
3. Mitä tulee ottaa huomioon teknisestä näkökulmasta palveluiden palautumisen osalta?
4. Onko organisaatiollanne käytössä häiriönhallintaprosessia, joka liittyy verkkoliikenteen häiriöihin?

5. Mitä teknisiä toimi tilanne edellyttää, mikäli katkon pituus olisi 24h? Tai jopa viikko?

Viestintätehtävät

1. Onko organisaatiolla käytettävissä ulkoisia viestintäpalveluita tilanteen ollessa päällä, esim. massatekstiviestipalvelu?
2. Onko olemassa vaihtoehtoisia viestintäkanavia, kuten tekstiviestit tai puhelinsoitot? Onko numerot saatavilla muualla, kuin pilvessä?
3. Miten hoidatte akuutin viestinnän tilanteessa, jossa puhelinverkko on pahoin ruuhkautunut?
4. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
5. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
6. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
7. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

4 Iltapäivän harjoitus

4.1 Tapahtuma 5: Sähkönjakelun ongelmat

Organisaation toimistolla työntekijät ovat juuri asettumassa paikoilleen työpäivän alkaessa, kun yhtäkkiä valot sammuvat. Sähköt ovat menneet pois päältä koko toimistorakennuksesta.

Sähkönjakelusta vastaava yhtiö ilmoittaa häiriötiedotteessaan, että laajalla alueella on sähkönjakelun häiriö, joka johtuu useamman tärkeän sähköaseman vaurioitumisesta. Korjaustöiden kestosta ja sähköjen palautumisesta ei voitu antaa arviota vielä tässä vaiheessa. Asiakkaita kehotetaan kuitenkin varautumaan normaalia pidempään sähkökatkokseen.

Sosiaalisessa mediassa lähtee liikkeellä väärää tietoa. Sosiaalisessa mediassa lähtee leviämään myös fake-news uutisvideo, jossa tunnettu uutisankkuri kertoo sähkönjakelun ongelmien johtuvan Suomen puolustusvoimien salaisesta, pieleen menneestä kokeesta.

Organisaation johto antaa tehtäväksi varmistaa, että kaikki kriittiset toiminnot pystytään suorittamaan sähkökatkotilanteesta ja sen kestosta riippumatta.

Viestintätiimi laati tiedotteet henkilöstölle, jotta kaikki saisivat oikeaa tietoa tilanteesta ja jatkotoimenpiteistä.

Sähkönjakelusta vastaava yhtiö ilmoittaa, että sähköaseman korjaustyöt etenevät odotettua hitaammin ja sähköjen palautuksen aikataulua ei valitettavasti osata vielä kään ilmoittaa tarkasti. Sähkökatko tulee kuitenkin kestämään useita päiviä.

Viranomaiset tutkivat sähköasemien vaurioitumisia ja ilmoittavat kyseessä olevan mitä todennäköisimmin sabotaasin. Viranomaisilla ei ole tässä vaiheessa tietoa tekijästä. Keskusrikospoliisi on pyytänyt tutkintaan tukea kansallisilta ja kansainvälisiltä kumppaneiltaan.

Tapahtuma 5 syötteet

Tilannesyöte:

Edellisessä tapahtumassa (tapahtuma 4) kuvatusta tilanteesta on kulunut useita viikkoja. Suomea aiemmin vaivanneet laajat verkko-ongelmat on saatu ratkaistua. Viranomaisten tutkinnat ovat vielä käynnissä tilanteeseen liittyen.

Valitkaa toimintanne kannalta kriittinen toimitila. Valitsemanne toimitilan alueella on laaja sähkökatko, jonka seurauksena toimitilasta katkeavat yllättäen sähköt.

Mediasyöte: Iltanen

JUURI NYT: Alueellinen laaja sähkökatko

Alueellinen Sähköverkko Oy tiedotti hetki sitten, että heidän alueellaan on käynnissä laaja sähkökatko. Sähkönjakelun häiriön kestoa tai syytä ei vielä tässä vaiheessa tiedetä.

Iltasen haastatteleman asiantuntija Siri Virtasen mukaan näin laajat alueelliset sähkönjakelun häiriöt ovat hyvin harvinaisia. ”Useamman asian on täytynyt mennä pieleen, että joudutaan tähän tilanteeseen” hän toteaa. Virtanen arvioi, että sähköjen palauttaminen alueelle saattaa kestää totuttua kauemmin. ”Meillä ei ole vielä tarkempia tietoja sähkönjakelun ongelmien syistä, mutta tilanne ei vaikuta tavalliselta häiriöltä, vaan kyseessä saattaa olla kompleksisempi ja vakavampi häiriötilanne, jonka korjaaminen voi viedä enemmän aikaa kuin mihin olemme tottuneet.”

Iltanen seuraa tilannetta.

Tilannesyöte: Puhelu

Soittaja: Organisaation työntekijä (valitsemastanne toimitilasta)
Vastaanottaja: Oma esihenkilö

Puhelun sisältö: Meni juuri sähköt, taisi mennä teiltäkin eli koko talosta? Meillä täällä läppärit toimivat akkujen varassa ja matkapuhelimien kautta saadaan verkkoyhteys jaettua, ainakin toistaiseksi. Mitä tehdään, jos tilanne venyy? Uutisista huomasin, että sähköt ovat poikki isommaltakin alueelta tässä lähistöllä. Olisiko hyvä ohjata väkeä etätöihin vai miten toimitaan?

Tilannesyöte: Tekstiviesti sähköverkkoyhtiöltä

Lähettäjä: Alueellinen Sähköverkko Oy
Vastaanottaja: Organisaatio

HÄIRIÖTIEDOTE

Alueellanne on vakava sähkönjakelun häiriö sähköaseman vaurioitumisen vuoksi. Korjaustyöt ovat käynnissä, mutta valitettavasti sähköjen palautusaikaa ei voida vielä arvioida. Varauduttehan mahdollisesti pitkäkestoiseen sähkönjakelun häiriöön.

Tiedotamme lisää heti, kun saamme uutta tietoa.
Alueellinen Sähköverkko Oy

Mediasyöte: Yleismedia: Faktaa alueellisesta sähkökatkosta

Alueellinen sähkökatko lamautti toiminnan – sabotaasiepäilyt herättävät keskustelua sosiaalisessa mediassa

Aluetta koskettava vakava sähkökatko on aiheuttanut häiriöitä useiden tuntien ajan. Alueellinen Sähköverkko Oy on ilmoittanut, että useat sähköasemat ovat vaurioituneet, minkä vuoksi sähkönjakelu on keskeytynyt. Korjaustyöt etenevät hitaasti, eikä sähköjen palautusaikaa voida vielä arvioida. Yhtiö kehottaa asukkaita varautumaan pitkäkestoiseen häiriöön.

Sähkökatko on herättänyt laajaa keskustelua sosiaalisessa mediassa, jossa spekuloidaan mahdollisesta sabotaasista. Monet käyttäjät ovat pohtineet, voisiko kyseessä olla tahallinen teko, jolla pyritään aiheuttamaan häiriöitä ja vahinkoa. Toimituksseemme on myös tullut useita yhteydenottoja lukijoilta, jotka epäilevät sabotaasia.

Vaikka asiantuntijat eivät ole toistaiseksi kommentoineet tilannetta, spekulaatiot ovat lisääntyneet nopeasti. Ihmisten tuoreessa muistissa ovat vielä verkkoyhteyksien laajat häiriöt. Sosiaalisen median keskusteluissa on viitattu mahdollisiin aikaisempiin tapauksiin, joissa sähköverkon haavoittuvuuksia on hyödynnetty. Toistaiseksi ei kuitenkaan ole konkreettisia todisteita, jotka viittaisivat sabotaasiin.

Alueellinen Sähköverkko Oy tiedottaa tilanteesta lisää heti, kun uutta tietoa saadaan. Asukkaita kehotetaan seuraamaan sähköyhtiön ja paikallismedian tiedotteita tilanteen edistymisestä.

Päivitämme uutista sitä mukaa, kun saamme lisätietoa tilanteesta. Seuraa verkkosivujamme ja sosiaalisen median kanaviamme ajantasaisen tiedon saamiseksi.

Mediasyöte: Somekirjoittelua aiheesta, väärää tietoa, spekulaatiota

Quacker: Jaska

Kohta tulee lisää alueellisia ja pitkäkestoisia sähkökatkoksia. Sähkönjakelijat ja sähköntuottajat ovat päättäneet yhdessä nostaa sähkön hintaa. Ensin tulee useita ja pitkäkestoisia häiriötä joka puolella sähköinfraa. Tämän jälkeen on helppo perustella sähkön hinnan nousua! Törkeää toimintaa, eikö tätä kukaan valvo!!

#sahkollalammittaja #sahkokatko #alueellinensahkokatko

Quacker: DigiAntero

*Video, jolla DigiAntero kertoo, että Suomen puolustusvoimien salainen kokeilu elektromagneettisen pulssin kanssa johti katastrofiin, kun koe epäonnistui aiheuttaen laajoja sähkökatkoja eri puolilla maata. Kokeen tarkoituksena oli testata viestiliikenteen häiritsemistä, mutta tulokset olivat tuhoisat. *

Quacker: Minttu

Hyvä ystäväni tutkii alueellista sähkökatkoa. Tätä ei haluta julkisesti myöntää, mutta joitain viikkoja sitten tapahtunut verkkoyhteyksien katkeaminen ja tämän päivän sähkönjakelun ongelmat liittyvät toisiinsa. Kysykääpä Suomen puolustusvoimilta, mitä ovat puuhailleet viimeiset pari kuukautta.

#sahkokatko #alueellinensahkokatko #totuusjulki

Quacker: Santtu

@Minttu kirjoittaa asiaa. Olen jo aiempien verkkoyhteyshäiriöiden aikana ihmetellyt, että miten sattuvat juuri samaan aikaan kun PV:llä sattuu olemaan isompi harjoitus tässä lähistöllä.

#sahkokatko #totuusjulki

Quacker: DigiAntero

Nimelläni, kasvoillani ja äänelläni on kiertänyt viime päivien aikana disinformaatiota sisältäviä videoita, jotka eivät ole minun tekemiäni. Rikosilmoitus on tehty

Tilannesyöte: Tekstiviesti sähköverkkoyhtiöltä (2)

Lähettäjä: Alueellinen Sähköverkko Oy
Vastaanottaja: Organisaatio

JATKOTIEDOTE
Korjaustyöt alueellanne etenevät. Arvioimme, että sähköt palautuvat 48 tunnin kuluessa. Pahoittelemme tilanteen aiheuttamaa haittaa ja kiitämme kärsivällisyydestänne. Seuraava päivitys tilanteesta huomenna.

Alueellinen Sähköverkko Oy

Tehtävät

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

Sähköt ovat poikki usean tärkeän sähköaseman vaurioitumisen vuoksi. Sähköyhtiö tiedottaa korjaustöiden etenemisestä, ja kehottaa asiakkaitaan varautumaan pitkäänkin sähkökatkoon.

1. Millaisia välittömiä toimenpiteitä tilanne edellyttää?

2. Onko organisaatiolla käytössä varavoimalähteitä?
3. Milloin varavoimalähteiden toimintaa on testattu viimeksi?
4. Miten Organisaationne jatkuvuussuunnittelussa on varauduttu tapahtuman kaltainen pitkäkestoiseen sähkökatkoon?
    a. Arvioikaa mitkä kaikki keskeiset toiminnot keskeytyvät tai häiriintyvät vakavasti.
    b. Mitä toimenpiteitä tulisi käynnistää toimintojen jatkamiseksi tai palauttamiseksi.
    c. Mitä kehitettävää tunnistatte organisaationne varautumisesta ja jatkuvuusuussuunnittelusta tapahtumaan liittyen?
5. Miten olette ottaneet huomioon avainhenkilöiden varahenkilömenettelyt tilanteen pitkittyessä?

Lisätehtävät

1. Mitä tärkeitä toimintoja voidaan suorittaa manuaalisesti?
2. Kuinka pitkään sähkökatkoon olette varautuneet?
3. Onko organisaatiolla riskienhallintasuunnitelmia, jotka kattavat informaatiovaikuttamisen ja sen vaikutukset?
4. Mitä toimintoja voidaan pitää yllä varavoiman turvin?
5. Onko mahdollista hankkia ja ottaa käyttöön lisää varavoimalähteitä? Jos on, millä aikataululla?
6. Oletteko tiedottaneet henkilöstöllenne kotivaran merkityksestä, esimerkiksi https://72tuntia.fi/ tai https://www.martat.fi/teemat/varautuminen/kotivara/?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Miten varmistetaan, että viestintä on luotettavaa ja uskottavaa sidosryhmien silmissä?
3. Onko Organisaatiolla ennakkoon sovittuja yhteyshenkilöitä ja -kanavia yhteydenpidossa median suuntaan?
4. Miten viestintää koordinoidaan viranomaisten ja muiden sidosryhmien kanssa väärän tiedon leviämisen estämiseksi?
5. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
6. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
7. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

4.2 Tapahtuma 6: Pahantahtoisen konsultin aiheuttama tietojen eheysongelma

Organisaation ulkopuolinen konsultti oli pidemmän aikaa työskennellyt organisaation kriittisten tietojärjestelmien ylläpidon ja kehittämisen parissa. Konsultti oli saanut työtehtäviään varten laajat käyttöoikeudet organisaation keskeisiin tietojärjestelmiin. Henkilö oli saanut kanssatyöntekijöiden luottamuksen, ja häntä pidettiin luontevana osana työyhteisöä. Oli yleisesti tiedossa, että samainen konsultti teki töitä myös usealle muulle organisaatiolle.

Eräänä päivänä organisaation työntekijä huomasi käyttämässään tietojärjestelmän/palvelun tiedoissa virheitä. Useat järjestelmissä olevat tiedot eivät täsmänneet ja jotkut kriittiset raportit antoivat ristiriitaisia tuloksia. Ensimmäinen havainto tehtiin, kun säännöllisesti ajettavat raportit (Huom. Ohjeistetaan osallistujia valitsemaan toiminnalleen keskeinen sisältö tähän) eivät vastanneet aiempia tietoja, ja useita keskeisiä lukuja oli muokattu. Pian muita vastaavia ongelmia alkoi ilmetä myös muissa osastoissa.

Tilanteen johdosta aloitettiin laajat selvitykset, joiden pohjalta havaittiin, että merkittävät tietomuutokset oli tehty erään konsultin käyttöoikeuksilla. Konsultin ei kuitenkaan pitänyt olla vastuussa näistä tiedoista, mikä herätti epäilyksiä. Konsultti ei ollut tullut kyseisenä päivänä töihin, eikä häntä tavoitettu puhelimella. Tietoturvatiimi päätti estää konsultin kaikki pääsyoikeudet ja jatkoi selvityksiään.

Selvityksen edetessä paljastui, että konsultti oli järjestelmällisesti muuttanut tietoja organisaation eri järjestelmissä. Näitä muutoksia ei ollut helppo havaita, koska ne oli tehty huolellisesti ja tarkoituksena oli ollut aiheuttaa pitkäaikaista haittaa organisaation toiminnalle ja päätöksenteolle. Konsultin tarkoituksena oli ollut vaarantaa tietojen eheys, jotta niihin ei voisi luottaa.

Rikosilmoituksen tekemisen myötä poliisi aloitti tutkinnan. Konsultti tavoitettiin myöhemmin, ja kuulusteluissa hän tunnusti muokanneensa tietoja haitan aiheuttamiseksi, sillä hänen toimeksiantonsa Organisaatiossa oli päättymässä.

Organisaatio käynnisti laajat tarkistukset ja palautustoimet tietojen eheyttämiseksi. He joutuivat käymään läpi kuukausien aikana tehtyjä muutoksia ja vertaamaan niitä varmuuskopioihin. Tämä prosessi oli työläs ja aikaa vievä, mutta se oli välttämätöntä organisaation toiminnan palauttamiseksi normaaliksi.

Tapaus antoi organisaatiolle arvokasta oppia tietojen eheyden tärkeydestä ja sisäisestä valvonnasta. Organisaatio tiukensi tietoturvakäytäntöjään, lisäsi tarkkailua ja rajoitti ulkopuolisten konsulttien pääsyoikeuksia kriittisiin järjestelmiin. Henkilöstölle annettiin myös koulutusta tietojen eheyden merkityksestä ja siitä, miten vastaavanlaiset tapaukset voidaan ehkäistä tulevaisuudessa.

Tapahtuma 6 syötteet

Tilannesyöte

Valitkaa harjoituksessa tähän Organisaatiossanne toimintanne kanalta merkittäviä tietojärjestelmä/palvelu, josta tuotetaan säännöllisesti materiaalia, esim. teknisen toimen järjestelmän raportit, kuukausiraportit, työaikaraportointi, talouden ennusteet/budjetointi, tai jokin muu organisaationne toiminnan kannalta keskeinen tietovaranto/tuotos.

Tilannesyöte: Sähköposti Organisaation työntekijältä tietoturvasta vastaavalle

Lähettäjä: Organisaation työntekijä
Vastaanottaja: Organisaation järjestelmän tai palvelun omistaja
Aihe: Epäselvyyttä raporteissa

Hei,

Olemme ajaneet vakioraportit tavanomaisen aikataulun mukaan, mutta nyt tiedoissa vaikuttaisi olevan jotain outouksia. Raporttien tiedot eivät ole linjassa aikaisempien raporttien kanssa. Otin testimielessä useita eri raportteja vertaillakseni tietoja, ja nyt vaikuttaisi siltä, että tietokanta olisi jotenkin solmussa, eikä kyse ole yksittäisistä virheistä. Selvittäisitkö tilanteen mahdollisimman pian, että saadaan raportit kuntoon, kiitos!

T. Rami Raportoija
rami.raportoija@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti Organisaation järjestelmän tai palvelun omistajalta tietoturvasta vastaavalle

Lähettäjä: Organisaation järjestelmän tai palvelun omistaja
Vastaanottaja: Organisaation tietoturvasta vastaava, turvallisuudesta vastaava
Aihe: Selvitys raportointiongelmasta

Hei,

Olemme selvitelleet työntekijän ilmoittamaa raportointiin liittyvää ongelmaa järjestelmätoimittajan ja käyttöpalvelutoimittajan kanssa. Nyt on tullut ilmi, että tietokannan tiedot eivät vastaa sitä, mitä niiden pitäisi olla. Eivätkä järjestelmän antamat tiedot ole luotettavia. Selvityksissä on käynyt ilmi, että kyse ei ole järjestelmävirheestä, eikä haittaohjelmasta tai vastaavasta.

Ongelman paikantamiseksi olemme käyneet lokeja läpi, ja olemme havainneet, että käyttäjätunnuksella ext-ville.virtanen@organisaatio.fi on tehty huomattava määrä muutoksia tietoihin. Virtanen työskentelee meillä konsulttina Konsultit Oy:n kanssa tehdyn sopimuksen puitteissa, ja hänelle on tilauksen pohjalta annettu laajat käyttöoikeudet.

Selvitimme asiaa toimeksiannon tilaajalta, ja työtehtäviensä puolesta Virtasen ei tulisi käsitellä näin laajasti eri tietoja. Varotoimenpiteenä olemme sulkeneet Virtasen käyttäjätunnuksen.

Jatkamme selvitystyötä ja ilmoitamme, kun uutta tietoa ilmenee. Järjestelmä on toistaiseksi pois käytöstä.

Yt. Oona Omistaja
oona.omistaja@organisaatio.fi
Organisaatio, järjestelmän tai palvelun omistaja

Tilannesyöte: Sähköposti Organisaation palvelun omistajalta Organisaation johdolle

Lähettäjä: Organisaation järjestelmän tai palvelun omistaja
Vastaanottaja: Organisaation johto
Aihe: tiedoksi: väärinkäytösepäily

Hei,

Järjestelmän raporteissa havaittiin tänään virheitä, jonka johdosta käynnistimme selvitystyöt. Näiden perusteella saimme selville, että järjestelmän tietoja oli muutettu laajasti ulkopuolisen konsultin toimesta, jolla oli toimeksiantosopimuksen perusteella pääsy järjestelmään. Asiasta on tiedotettu organisaation turvallisuudesta ja tietoturvasta vastaavia henkilöitä, jotka ovat ottaneet vastuun jatkotoimista.

Järjestelmä on toistaiseksi pois käytöstä.

Yt. Oona Omistaja
oona.omistaja@organisaatio.fi
Organisaatio, järjestelmän tai palvelun omistaja

Tilannesyöte: Puhelinsoitto Organisaation turvallisuuspäälliköltä johdolle

Soittaja: Organisaation turvallisuuspäällikkö
Vastaanottaja: Organisaation johto

Olen keskustellut IT:n, Konsultit Oy:n edustajan ja tietosuojavastaavan kanssa tästä Ville Virtaseen kohdistuvasta epäilystä. Tilanne vaikutti jo alkuun niin vakavalta, että tein asiasta rikosilmoituksen poliisille. Olen ollut yhteyksissä poliisin tutkinnanjohtajan kanssa lisätietojen antamisen osalta. Poliisi kehotti tutkimaan tarkasti, onko tietoja päätynyt ulkopuolelle.

Tilannesyöte: Sähköposti Organisaation järjestelmien ylläpidosta tietoturvasta vastaavalle

Lähettäjä: Organisaation järjestelmän tai palvelun omistaja
Vastaanottaja: Organisaation tietoturvasta vastaava
Aihe: Lisätietoa selvityksistä

Hei,

Tähän mennessä tehtyjen selvitysten perusteella vaikuttaa siltä, että tietoja on muutettu varsin järjestelmällisesti. Muutokset on tehty hyvin huolellisesti ja pitkän aikavälin aikana, joten niitä ei ole kovinkaan helppo havaita. Tämän vuoksi selvitysten loppuunsaattaminen vie aikaa ja odotettavissa on, että muutettua tietoa löytyy vielä lisää. Järjestelmät ovat pois käytöstä toistaiseksi määrittelemättömän ajan. Tiedot tullaan palauttamaan, mutta vielä ei tiedetä, mihin asti palautus joudutaan tekemään. Tulee myös valmistautua siihen, että tietoa tullaan menettämään koko siltä ajalta, kun tiedon eheydessä on poikkeavuuksia.

Yt. Järjestelmien ylläpito
yllapito@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti Organisaation turvallisuuspäälliköltä johdolle

Lähettäjä: Organisaation turvallisuuspäällikkö
Vastaanottaja: Organisaation johto
Aihe: Tiedoksi

Hei,

Entinen konsulttimme Ville Virtanen on tavoitettu, ja hänen kanssaan on keskusteltu tapahtuneesta. Keskustelussa kävi ilmi, että hän oli katkeroitunut vuosia kestäneen toimeksiannon yllättävästä päättymisestä, ja halunnut tämän vuoksi aiheuttaa Organisaatiollemme mittavaa haittaa.

T. Tiina Turvallisuuspäällikkö
tiina.turvallisuuspaallikko@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti Organisaation käyttötuesta tietoturvasta vastaavalle

Lähettäjä: Organisaation työntekijä, Käyttötuki
Vastaanottaja: Organisaation tietoturvasta vastaava
Aihe: Järjestelmät palautettu

Hei,

Järjestelmät on nyt palautettu kuukauden takaiseen todennetusti eheään tietoon. Tämä tarkoittaa sitä, että viimeisen kuukauden ajalta tehdyt uudet tiedot ja muutokset tietoihin on menetetty.

Yt. Käyttötuki
kayttotuki@organisaatio.fi
Organisaatio

Tehtävät

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

Organisaation kriittisten raporttien tietoja on muokattu laajasti Organisaation palveluksessa olleen konsultin tunnuksilla. Organisaation järjestelmät on pitkäkestoisten selvitysten jälkeen jouduttu palauttamaan kahden viikon takaiseen tilanteeseen.

1. Mitä toimenpiteitä tilanne edellyttää?
2. Mitä vaikutuksia kuukauden aikana tuotetun tiedon menettämisellä on toimintanne kannalta?
3. Mitä toimia voidaan tehdä kuukauden aikana tuotetun tiedon korvaamiselle?
4. Millaisia ohjeita ja toimintamalleja organisaatiolla on tilanteen hallitsemiseksi?
5. Millaisia turvallisuuskontrolleja organisaatiolla on uusille työntekijöille / kumppaneille? (Esim. turvallisuusselvitys, turvallisuuskoulutus)
6. Miten toimitaan sinä aikana, kun järjestelmä/palvelu on pois käytöstä?
7. Mihin tahoihin tilanteessa tulisi olla yhteydessä?

Lisätehtävät

1. Miten organisaatiossanne havainnoidaan tietokannoissa tapahtuvia, normaalista poikkeavia laajoja muutoksia?
2. Millainen toimintamalli on käytössä järjestelmien käyttöoikeuksien myöntämisessä ulkoisille kumppaneille?
3. Olisiko VIRT- tai ISAC-tiedonvaihdosta hyötyä tilanteessa?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
3. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
4. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

4.3 Tapahtuma 7: Matkapuhelimen tietoturvacase

Organisaatiossa on käytössä mobiililaitehallintajärjestelmä (MDM), jonka avulla kaikkien työntekijöiden työpuhelimet voidaan etävalvoa ja suojata. Yrityksen IT-osasto on unohtanut liittää työntekijän puhelimen järjestelmään.

Tapahtuma 7 syötteet

Tilannesyöte: Sähköposti

Lähettäjä: Organisaation työntekijä

Vastaanottaja: IT-osasto
Aihe: KATOAMISILMOITUS: Työpuhelimeni on kadonnut

Hei,

Valitettavasti työpuhelimeni on kadonnut tänään lounaan aikana. Lähdin lounaalta kiireesti palaveriin, ja huomasin katoamisen vasta palaverin jälkeen. Olen yrittänyt etsiä puhelinta, kävin myös lounaspaikassa kysymässä, mutta tuloksetta. Mitä minun pitäisi tehdä seuraavaksi?

Ystävällisin terveisin,
Oskari Organisaation työntekijä
oskari.organisaationtyontekija@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti

Lähettäjä: IT-osasto
Vastaanottaja: Organisaation työntekijä
CC: Turvallisuudesta vastaava
Aihe: RE: KATOAMISILMOITUS: Työpuhelimeni on kadonnut

Hei

Kiitos ilmoituksesta. Valitettavasti huomasimme, että työpuhelintasi ei ole vielä liitetty etävalvontajärjestelmäämme (MDM), mikä tarkoittaa, että emme voi paikantaa, lukita tai tyhjentää puhelintasi etänä. Aloitamme selvitystyön tilanteen korjaamiseksi ja mahdollisten tietovuotojen selvittämiseksi.

Ilmoitamme sinulle heti, kun meillä on lisää tietoa. Viesti tiedoksi myös turvallisuuspäällikölle mahdollisia jatkotoimia varten.

Ystävällisin terveisin,
IT-Osasto
IT@organisaatio.fi
Organisaatio

Lähettäjä: Organisaation työntekijä
Vastaanottaja: IT-osasto
Aihe: KATOAMISILMOITUS: Työpuhelimeni on kadonnut

Hei,

Valitettavasti työpuhelimeni on kadonnut tänään lounaan aikana. Lähdin lounaalta kiireesti palaveriin, ja huomasin katoamisen vasta palaverin jälkeen. Olen yrittänyt etsiä puhelinta, kävin myös lounaspaikassa kysymässä, mutta tuloksetta. Mitä minun pitäisi tehdä seuraavaksi?

Ystävällisin terveisin,
Oskari Organisaation työntekijä
oskari.organisaationtyontekija@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti

Lähettäjä: IT-osasto
Vastaanottaja: Tietoturvasta vastaava, turvallisuudesta vastaava
Aihe: Kadonnut työpuhelin

Hei,

Olemme havainneet epäilyttävää toimintaa tänään kadonneeksi ilmoitetun työpuhelimen käyttäjätunnuksella. Olemme estäneet kyseisen käyttäjätunnuksen pääsyn järjestelmiimme.

Yt. IT-Osasto
IT@organisaatio.fi
Organisaatio

Tilannesyöte: Sähköposti

Lähettäjä: mikko.makkonen@gmail.com
Vastaanottaja: Organisaation työntekijä
Aihe: Kaipaatko puhelintasi?

Hei

Minulla on hallussani työpuhelimesi ja yrittäessäni selvittää puhelimen omistajaa huomasin, että pääsen puhelimella Organisaation tietoihin käsiksi. Sopisiko jos maksaisitte minulle puhelimen palauttamista vastaan pienen löytöpalkkion? Latasin Organisaation tiedot talteen puhelimen paikalliseen muistiin. Olen itsekin joskus työskennellyt ATK-alalla, joten tämän tein ihan vain pelkkää hyvyyttäni.

Yt. Mikko Makkonen
mikko.makkonen@gmail.com

Tilannesyöte: Puhelu

Soittaja: Organisaation ICT:stä vastaava henkilö
Vastaanottaja: Organisaation tietoturvasta vastaava

Hei, kiitos että ehditte puhua kanssani näin nopeasti, soitan työntekijän kadonneeseen työpuhelimeen liittyen.

Olemme tarkastelleet lokeja ja saaneet selville, että puhelimen kautta on päästy käsiksi organisaation sisäisiin tietoihin. Onneksi näyttää siltä, että nämä tiedot on ladattu vain paikallisesti puhelimen muistiin, eikä niitä ole siirretty muihin laitteisiin tai ulkoisiin palvelimiin. Tämä rajoittaa tietovuodon mahdollisia vaikutuksia.

Olemme saaneet puhelimen lukittua työntekijän oman Google/Apple-tilin kautta, mikä estää luvattoman käytön ja varmistaa, että laitetta ei voida enää käyttää ilman tunnuksia. Lisäksi olemme estäneet työntekijän käyttäjätunnuksen pääsyn Organisaation järjestelmiin ja otamme käyttöön lisäsuojaustoimia koko organisaation tasolla.

Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Peilatkaa harjoituksen tapahtumia ja niiden vaikutuksia oman organisaationne toimintaan. Mikäli Organisaatiossanne ei ole käytössä mobiililaitehallintajärjestelmää, ottakaa tämä tositilanne huomioon keskusteluissa ja kysymyksiin vastattaessa.

Organisaation työntekijä hukkaa työpuhelimensa, ja kyseinen puhelin on jäänyt liittämättä Organisaatiossa käytössä olevaan mobiililaitehallintajärjestelmään. Puhelimen löytänyt henkilö on päässyt käsiksi Organisaation sisäisiin tietoihin.

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Mihin kaikkiin järjestelmiin ja tietoihin työpuhelimella on mahdollista päästä? Miten tämän käytön mahdollisuus on dokumentoitu / hallinnoitu?
3. Miten Organisaationne vastuunjako toimii tilanteessa, joissa yhdistyy sekä tietoturvaloukkaus että mahdollinen kiristysyritys?
4. Mitkä ovat parhaat käytännöt tietovuotojen hallinnassa tilanteissa, joissa laitteen etähallinta ei ole mahdollista?
5. Mihin tahoihin tilanteessa tulisi olla yhteydessä?

Lisätehtävät

1. Miten organisaatio voi optimoida reagointikykyään tilanteissa, joissa tietojärjestelmiin on päästy käsiksi kadonneen mobiililaitteen kautta?
2. Miten varmistetaan, että kaikki organisaation mobiililaitteet liitetään MDM-järjestelmään?
3. Millaisia valvontaprosesseja tulisi olla olemassa, jotta mobiililaitteiden turvallisuus voidaan taata myös silloin, kun ne eivät ole MDM-järjestelmän piirissä?
4. Miten organisaation tulisi reagoida ja priorisoida toimenpiteensä, jos havaitaan, että mobiililaite on jäänyt liittämättä MDM-järjestelmään ja on kadonnut julkisella paikalla?
5. Sallitaanko organisaatiossa henkilöstön henkilökohtaisten älylaitteiden käyttö työtehtävien hoitamisessa ja pääsyssä organisaation tietojärjestelmiin?

a. Onko tästä tehty ajantasainen riskiarvio ja kuinka tunnistettuja riskejä hallitaan?

Viestintätehtävät

1. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
2. Miten voitaisiin kehittää organisaation sisäistä viestintää, jotta vastaavat tietoturvariskit minimoidaan tulevaisuudessa?
3. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
4. Pohtikaa ja kirjatkaa keskeiset viestinnälliset toimenpiteet, pääviestit ja niiden sisältöjen ydinkohdat.
5. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.