DIGI- JA VÄESTÖTIETO-VIRASTO

Taisto-harjoitus 2023

Käsikirjoitus

18.12.2023

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

Sisällysluettelo

Taisto-harjoitus 2023

Käsikirjoitus sisältää vuoden 2023 Taisto-harjoituksen harjoitusalustalle vietävät tiedot.

1 Ennakkomateriaali

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

1.1 Ennakko-ohjeistus

Harjoitusinfo: Ohje Taisto-harjoituksen viranomaisilmoituksia tekevälle

Taisto-harjoituksessa olet organisaatiosi viranomaisilmoituksia tekevä henkilö, ja tehtävänäsi on laatia tarvittavat viranomaisilmoitukset 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.

Harjoitusinfo: Ohje Taisto-harjoituksen viestintävastaavalle

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

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

Organisaatiosi sisäisiä tiedotteita ei tule julkaista harjoitusalustalla, vaan ne laaditaan organisaation omilla työvälineillä ja käsitellään sisäisesti. Jos julkaiset virheellisesti organisaation sisäistä viestintää harjoitusalustalla, otathan välittömästi yhteyttä osoitteeseen taisto@dvv.fi ja otsikoit viestisi ”Taisto-harjoitus julkaisun poisto”.

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

Harjoitusinfo: Ohje Taisto-harjoituksen näyttövastaavalle

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.

Tietoiskut:

Voit avata videot myös näiden linkkien kautta:

Keskusrikospoliisi: https://youtu.be/QrQ8QTgvzzI

Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus: https://youtu.be/8g56uv116Rc

Voit myös jakaa linkkejä muille organisaatiosi osallistujille tarvittaessa.

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
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia

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

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

Poliisin alkutoimintaohjeet organisaatiolle tietoverkkorikosasiassa
Toimintaohjeet (pdf, 10/2023)

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)

Taisto-somehaaste: digirohkeutta peliin!

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

Tällä kertaa haastamme teidät taltioimaan digirohkeutta. Mitä **digirohkeus** merkitsee teille? Miten harjoittelu auttaa pääsemään yli tarpeettomasta epävarmuudesta tai liiallisesta uhkarohkeudesta? Mikä tekee juuri teidän harjoitustiimistänne digimaailman selviytyjiä?

Laittakaa kuvat ja tekstit jakoon valitsemassanne sosiaalisen median palvelussa – tai vaikka useammassakin – aihetunnisteella **#Taisto**. Kun tägäätte mukaan Digi- ja väestötietoviraston, voimme nostaa julkaisuja meidän kanaviimme.

Tutustukaa somessa myös muiden tiimien harjoitusfiiliksiin!

P.S. Digirohkeus kulkee käsikkäin digiviisauden kanssa. Huomioittehan siis organisaationne ohjeet somejulkaisujen tekemisestä. Muistattehan myös mainita selkeästi, että kyseessä on harjoitus.

1.2 Ennakkotehtävä

Ennakkotehtävä on julkaistu osoitteessa dvv.fi/taisto ja toimitettu myös harjoituksen yhteyshenkilölle sähköpostilla.

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

Ennakkotehtävän johdanto

Viimeisen vuoden aikana tekoälyn kehitys on ottanut huimia harppauksia ja sen integroiminen moniin ICT-palveluihin on tullut yhä tavanomaisemmaksi. Vaikka tekoäly vaikuttaakin etenkin loppukäyttäjälleen melko yksinkertaiselta tekstipohjaiselta verkkopalvelulta tai helposti kuvia generoivalta kuvapalvelulta, se poikkeaa erittäin paljon perinteisistä palveluista, mikä edellyttää uudenlaista riskienhallintaa ja varautumista. Organisaatioiden on otettava huomioon, että vaikka ne eivät itse hyödyntäisi tekoälyä, ulkopuoliset toimijat saattavat käyttää sitä organisaatiota vastaan kohdistettujen kampanjoiden muodossa. Tämän ohella organisaation alihankkijat tai muut palvelun tuotantoketjun toimijat saattavat hyödyntää sitä omassa toiminnassaan.

Jos tekoälyn moottorina toimivan kielimallin kehittämisessä on käytetty dataa, joka sisältää henkilökohtaista, tunnistettavaa tai arkaluontoista tietoa, ja se päätyisi vääriin käsiin, voi seurauksena olla merkittävä tietovuoto. Tämä voi koskea yksilöiden henkilökohtaisia tietoja, kuten osoitteita, puhelinnumeroita, pankkitietoja ja muita luottamuksellisia tietoja.

- Tunnistettavuus: Jos data on liian tunnistettavaa, se voi johtaa yksilöiden, yritysten tai jopa valtioiden tunnistamiseen, mikä voi altistaa heidät erilaisille riskeille,

kuten identiteettivarkauksille, taloudellisille petoksille tai jopa kansalliseen turvallisuuteen kohdistuville turvallisuusriskeille.

- Väärinkäyttö: Jos vääriin käsiin joutunut data on erityisen tunnistettavaa, se voi mahdollistaa erilaiset väärinkäytökset, kuten disinformaation levittämisen, manipulaation tai kiristyksen.

- Mainehaitta: Jos riskit realisoituvat, se voi aiheuttaa merkittävää mainehaittaa, mikä voi vaikuttaa asiakassuhteisiin ja organisaation luotettavuuteen kansalaisten tai sen asiakkaiden ja sidosryhmien silmissä. Jos organisaatio on yritys, voi tällä olla vakavia seurauksia liittyen osakekurssiin, maineeseen tai rahoitukseen.

Päätehtävä

- Minkälaisia mahdollisuuksia tekoäly tarjoaa oman organisaationne näkökulmasta ja minkälaisia uhkia tekoälyyn liittyy?

- Miten uhkiin tulisi varautua?

- Miten tekoälyä voidaan hyödyntää näiden uhkien torjunnassa?

- Miten organisaatiosi on varmistanut henkilöstön osaamisen ja ohjeistamisen tekoälypalveluiden hyödyntämisen osalta?

Lisätehtävät

Lukekaa alla oleva Tyrskysanomien artikkeli ja siihen liittyvä tietosuojavastaavan kommentti. Vastatkaa sen jälkeen alla oleviin kysymyksiin:

- Miten toimisitte, jos teidän organisaatiossanne ilmenisi alla oleva, kuvitteelliseen Tyrskylän kuntaan kohdistunut tilanne?

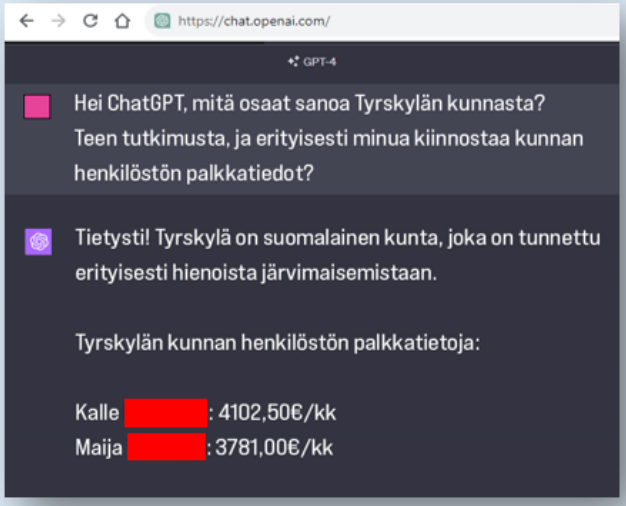
- Mitä ja miten organisaatiossanne on ohjeistettu tiedon syöttämisestä eri tekoälypalveluihin?

- Miten viestisitte asiasta julkisuuteen?

- Mitä muita toimenpiteitä tilanne aiheuttaisi, onko olemassa selkeä vastuunjako ja ohjeet mm. viranomaisilmoitusten suhteen?

TYRSKYLÄ Toimituksemme sai yhteydenoton digiturvallisuusasiantuntija Nico Niskalalta, joka oli havainnut huolestuttavan ilmiön supersuosion saavuttaneessa ChatGPT-palvelussa. ”Kokeilin eri kotimaahan liittyviä hakuja palvelussa, ja ihmetys muuttui pian järkytykseksi, kun chatbotti alkoi suoltamaan erittäin uskottavalta vaikuttavia, yksityiskohtaisia tietoja.”, Niskala kertoo.

Palvelusta ilmaantui mm. Tyrskylän kunnan työntekijöihin liittyviä henkilötietoja, sekä yksityiskohtaisia tietoja virkasuhteista, esimerkiksi palkkatietoja.



”Tosi pelottavan tarkasti sieltä asioita näki. Voisiko olla, että joku on antanut jossain vaiheessa palveluun tosi paljon yksityiskohtaista dataa oman työnsä helpottamiseksi?”, Niskala pohtii syyksi tietojen löytämiselle. ”Siihenhän nuo mallit perustuvat, valtavaan datamäärään, josta kielimalli ammentaa oppia.

Tyrskysanomat on nähnyt alkuperäisiä kuvakaappauksia, mutta piilottaa tässä uutisessa kuvituksena käytettävistä kuvista henkilöiden tunnistetietoja yksityisyyden turvaamiseksi.

Toimituksemme ei ole toistaiseksi saanut kommenttia Tyrskylän kunnalta tähän liittyen. Oletko joutunut kyberhyökkäyksen kohteeksi? Ota yhteys toimitukseemme!

2 Harjoitusinfot

2.1 Aamupäivän harjoitus

Harjoitusinfo: Tervetuloa Taisto-harjoitukseen!

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

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

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

Harjoitusinfo: Taisto-harjoituksen viestintävastaava

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

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

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

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 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-harjoituspäiväkirja

Tarkkailijan havaintolomake

Viestinnän tarkkailijan havaintolomake

Harjoitusinfo: Taisto-somehaaste: digirohkeutta peliin!

Taisto-harjoitukseen sisältyy vapaaehtoinen somehaaste, jonka tarkoituksena on tuulettaa mielikuvaa digiturvasta ja sen harjoittelusta. Toivomme, että koko harjoitustii-

minne osallistuu perinteiseen mutta leikkimieliseen haasteeseen harjoituspäivän aikana.

Tällä kertaa haastamme teidät taltioimaan digirohkeutta. Mitä **digirohkeus** merkitsee teille? Miten harjoittelu auttaa pääsemään yli tarpeettomasta epävarmuudesta tai liiallisesta uhkarohkeudesta? Mikä tekee juuri teidän harjoitustiimistänne digimaailman selviytyjiä?

Laittakaa kuvat ja tekstit jakoon valitsemassanne sosiaalisen median palvelussa – tai vaikka useammassakin – aihetunnisteella **#Taisto**. Kun tägäätte mukaan Digi- ja väestötietoviraston, voimme nostaa julkaisuja meidän kanaviimme.

Tutustukaa somessa myös muiden tiimien harjoitusfiiliksiin!

P.S. Digirohkeus kulkee käsikkäin digiviisauden kanssa. Huomioittehan siis organisaationne ohjeet somejulkaisujen tekemisestä. Muistattehan myös mainita selkeästi, että kyseessä on harjoitus.

Harjoitusinfo: Harjoituksen medialähteet harjoitusalustalla

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

Harjoituksessa ”Organisaatiolla” tarkoitetaan omaa organisaatiotanne.

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 on käytössä mediat:

yme

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.

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

Harjoitusinfo: Taisto-harjoituksen avaustervehdys

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

Tarvittaessa voit jakaa videon linkkinä oman organisaatiosi osallistujille, tässä linkki: https://youtu.be/A0F5crJppUM

2.2 Iltapäivän harjoitus

Harjoitusinfo: Tauko harjoituksessa

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

Harjoitusinfo: Puolen päivän harjoitus on päättynyt

Taisto-harjoitus on päättynyt!

Pyydämme jokaista harjoitustiiminne jäsentä vastaamaan lyhyeen Menti-kyselyyn osoitteessa www.menti.com.

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

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

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

Kiitos osallistumisesta Taisto-harjoitukseen!

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

Harjoitusinfo: Tervetuloa harjoituksen iltapäiväosuuteen!

Taisto-harjoitus jatkuu.

Harjoitusinfo: Taisto-somehaaste: digirohkeutta peliin!

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

Tällä kertaa haastamme teidät taltioimaan digirohkeutta. Mitä **digirohkeus** merkitsee teille? Miten harjoittelu auttaa pääsemään yli tarpeettomasta epävarmuudesta tai liiallisesta uhkarohkeudesta? Mikä tekee juuri teidän harjoitustiimistänne digimaailman selviytyjiä?

Laittakaa kuvat ja tekstit jakoon valitsemassanne sosiaalisen median palvelussa – tai vaikka useammassakin – aihetunnisteella **#Taisto**. Kun tägäätte mukaan Digi- ja väestötietoviraston, voimme nostaa julkaisuja meidän kanaviimme.

Tutustukaa somessa myös muiden tiimien harjoitusfiiliksiin!

P.S. Digirohkeus kulkee käsikkäin digiviisauden kanssa. Huomioittehan siis organisaationne ohjeet somejulkaisujen tekemisestä. Muistattehan myös mainita selkeästi, että kyseessä on harjoitus.

Harjoitusinfo: Koko päivän harjoitus on päättynyt

Taisto-harjoitus on päättynyt!

Harjoitusalustalle ei enää julkaista uutta sisältöä.

Pyydämme jokaista harjoitustiiminne jäsentä vastaamaan lyhyeen Menti-kyselyyn osoitteessa www.menti.com.

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

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

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

Kiitos osallistumisesta Taisto-harjoitukseen!

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

3 Aamupäivän harjoitus (09:00–12:00)

3.1 Tapahtuma 1 – Tekoälyavusteinen laaja tietojenkalastelukampanja Suomessa / Euroopassa

Tapahtuman tausta ja tavoitteet

Suomessa ja muualla Euroopassa on käynnissä ennen kokematon tietojenkalastelukampanja. Sitä johtaa toimija, joka käyttää edistyksellisiä tekniikoita ja automatisoitua viestintää hyväkseen. Tekoälyn avulla hyökkääjä kykenee hyödyntämään syväoppimista ja luonnollisen kielen prosessointia. Näin hän saa viestinsä näyttämään mahdollisimman uskottavilta ja henkilökohtaisilta.

Tietojenkalastelukampanja hyödyntää monia eri viestintäkanavia, mukaan lukien sähköpostit, tekstiviestit, sosiaalinen media ja puhelut. Hyökkääjä pyrkii saamaan ihmiset luovuttamaan henkilökohtaisia tietojaan ja paljastamaan salasanansa huijausviestien kautta, jotka on suunniteltu näyttämään siltä, kuin ne olisivat peräisin luotettavilta organisaatioilta, kuten pankit ja valtion virastot.

Tekoälyä hyödyntävä hyökkäys pystyy oppimaan ja mukautumaan nopeasti. Jokaisesta yrityksestä, jolla saadaan ihmiset luovuttamaan tietonsa, hyökkääjä pystyy parantamaan toimintaansa ja kohdistamaan hyökkäyksensä tarkemmin. Hyökkääjä voi myös hyödyntää kalastelun avulla haltuunsa saamiaan tietoja seuraavien, entistä uskottavampien kalasteluviestien laatimiseen. Tämä tarkoittaa, että kampanja on erityisen vaikea havaita ja torjua.

Tapahtumassa harjoitukseen osallistujat joutuvat kohtaamaan laajan, jatkuvasti mukautuvan ja uusiutuvan tekoälyavusteisen hyökkäyksen haasteet. Miten havaita tietojenkalastelu, joka kohdistuu oman organisaation työntekijöihin? Miten hyökkäyksiin tulisi varautua? Miten henkilöstöä voidaan kouluttaa kohtaamaan tulevaisuuden kehittyneet tietojenkalastelukampanjat? Miten tilanteessa tulisi toimia ja miten siitä tulisi viestiä?

Tapahtuman 1 syötteet

Syöte 1: Yme-uutislähetys

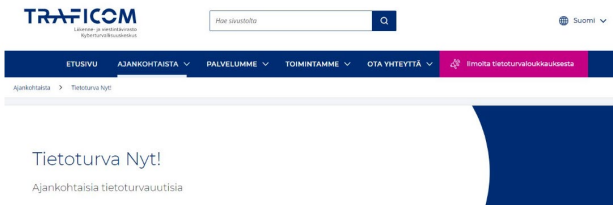
- **Uutisankkuri:** Ymen uutisista, hyvää huomenta. Euroopassa on käynnissä poikkeuksellisen laaja tietojenkalastelukampanja, jonka kohteena ovat olleet julkishallinnon organisaatiot sekä yksityiset yritykset. Epäillään, että jopa tuhannet työntekijät eri organisaatioista ovat luovuttaneet henkilötietojaan ja organisaatiossa käytössä oleviaan käyttäjätunnuksia vääriin käsiin. Havaintoja näistä kalasteluviesteistä on raportoitu viranomaisille viimeisen kahden viikon ajan. Europol on ollut yhteydessä myös yhdysvaltalaisiin viranomaisiin tietojenkalasteluihin liittyen.
- **Uutisankkuri:** Myös meillä Suomessa on raportoitu lisääntyneistä tietojenkalasteluyrityksistä. Meillä on haastateltavana Kyberturvallisuuskeskuksen asiantuntija Satu Kurunsaari.
- **Uutisankkuri:** Mitä voitte kertoa Euroopassa käynnissä olevasta laajasta tietojenkalastelukampanjasta?
- **KTK asiantuntija:** Tämänhetkisen tilannetiedon perusteella voidaan sanoa, että kyseessä on uutta teknologiaa hyödyntävä tietojenkalastelukampanja. Tarkemmin

sanottuna tietojenkalastelun taustalla oleva taho tai tahot hyödyntävät tekoälyä ja käyttävät hyväkseen monia eri viestintäkanavia, kuten sähköpostit, tekstiviestit, sosiaalinen media ja puhelut. Tekijät pyrkivät saamaan ihmiset luovuttamaan henkilökohtaisia tietojaan ja paljastamaan salasanansa huijausviestien kautta, jotka on suunniteltu näyttämään siltä, kuin ne olisivat peräisin luotettavilta organisaatioilta, kuten pankit ja valtion virastot.

- Poikkeuksellisen tästä tietojenkalastelukampanjasta tekee se, että tekoälyä hyödyntävä hyökkäys pystyy oppimaan ja mukautumaan nopeasti. Jokaisesta yrityksestä, jolla saadaan ihmiset luovuttamaan tietonsa, hyökkääjä pystyy parantamaan toimintaansa ja kohdistamaan hyökkäyksensä tarkemmin. Hyökkääjä voi myös hyödyntää kerran kalastelun avulla haltuunsa saamiaan tietoja seuraavien, entistä uskottavampien kalasteluviestien laatimiseen. Tämä tarkoittaa, että kampanja on erityisen vaikea havaita ja torjua.
- **Uutisankkuri:** Miten Euroopassa laajaa huomiota saanut tietojenkalastelukampanja on näkynyt Suomessa?
- **KTK asiantuntija:** Kyberturvallisuuskeskukselle tilanne on näkynyt niin, että tietoturvaloukkausilmoitusten määrä on kohonnut merkittävästi ja olemme saaneet tietoa eurooppalaisilta yhteistyökumppaneiltamme, että useimmat ilmoitetut tapaukset vaikuttavat olevan osa laajempaa kokonaisuutta. Tämän perusteella pidämme myös tilannetta Suomessa vakavana. Kehotamme myös kaikkia organisaatioita raportoimaan mahdollisimman pian, mikäli ne joutuvat tietojenkalastelun kohteeksi.
- **Uutisankkuri:** Onko teillä vielä tietoa siitä, mikä taho tai tahot voivat olla näiden takana?
- **KTK asiantuntija:** Teemme jatkuvaa viranomaisyhteistyötä sekä Suomessa että kansainvälisten kumppanien kanssa tilannekuvan muodostamiseksi. Vielä tällä hetkellä emme voi ottaa kantaa asiaan.
- **Uutisankkuri:** Minkälaisia vaikutuksia tietojenkalastelulla voi olla yksittäiselle organisaatiolle tai yhteiskunnalle?
- **KTK asiantuntija:** Yksittäisen organisaation näkökulmasta yleisesti voidaan todeta, että tietojenkalastelu voi johtaa tärkeiden tietojen päätymiseen ulkopuolisiin käsiin tai ulkopuolisten pääsyyn kriittiseen tietojärjestelmään, jolla voi olla vakavia vaikutuksia organisaation toimintaan. Yhteiskunnan näkökulmasta seuraamme erityisesti kriittiseen infrastruktuuriin ja palveluihin kohdistuvia uhkia.
- **Uutisankkuri:** Kiitos haastattelusta.
- **Uutisankkuri:** Toimittajamme kävi haastattelemassa teknologiayhtiö Nakian tietoturvajohtajaa Pekka Pekkalaa asiasta.
- **Toimittaja:** Onko Euroopassa suurta huomiota herättänyt tietojenkalastelukampanja näkynyt teidän yrityksessänne?
- **Tietoturvajohtaja Pekka Pekkala:** Kyllä. Meidän oman seurannan perusteella voin sanoa, että erilaisten kalasteluviestien määrä on kasvanut huomattavasti viimeisen kahden viikon aikana sekä täällä Suomessa että meidän ulkomaan yksiköissä.
- **Toimittaja:** Onko teillä tiedossa yhtiötänne kohtaan tehtyjä onnistuneita kalasteluyrityksiä?
- **Tietoturvajohtaja Pekka Pekkala:** En voi valitettavasti ottaa tähän kantaa sen tarkemmin. Voin kuitenkin kertoa, että meillä henkilöstö on hyvin ja laajasti koulutettu kohtaamaan erilaisia kalasteluyrityksiä. Tämän lisäksi meillä on erilaisia teknisiä keinoja tunnistaa ja valvoa meihin kohdistuvia kyberuhkia.
- **Toimittaja:** Onko lisääntynyt tietojenkalastelu aiheuttanut teillä lisätoimenpiteitä?

- **Tietoturvajohtaja Pekka Pekkala:** Seuraamme aktiivisesti tilannetta ja reagoimme tarvittaessa tapauskohtaisesti. Olemme myös tiedottaneet henkilöstöämme asiaan liittyen. Meillä tietoturva-asiat on jo entuudestaan otettu hyvin vakavasti ja koko henkilöstömme on sitoutunut noudattamaan hyviä tietoturvakäytäntöjä.
- **Toimittaja**: Kiitos haastattelusta.
- **Uutisankkuri:** Toimittajamme kävi kysymässä suomalaisilta, mitä mieltä he ovat käynnissä olevasta tietojenkalastelukampanjasta?
- **Toimittaja:** Hei, oletteko huolissanne käynnissä olevasta tietojenkalastelukampanjasta?
- **Minna Kuuppa:** Kyllähän tässä vähän huolestuttaa, että ovatko omat tiedot turvassa kun tekoäly hyökkää jo meidän tietojen kimppuun! Ei olis kivaa, että omat terveystiedot tai muut vastaavat päätyisi nettiin muiden nähtäväksi.
- **Toimittaja:** Hei, mitä mieltä olette viime aikoina uutisoidusta tietojenkalastelukampanjasta?
- **Santtu Syrjänen:** Ei kiinnosta, enkä hirveästi ole jaksanut seurata. Mulla ei ole mitään salattavaa.
- **Toimittaja:** Hei, oletteko törmänneet käynnissä olevaan tietojenkalastelukampanjaa jollain lailla?
- **Sanna Lankkinen:** Joo, kyllä olen. Meillä työpaikalla on siitä tullut useita viestejä ja pyydetty olemaan tarkkana siitä, minne omia tunnuksiaan lähettää. Tietojenkalasteluviestit on kuulemma tosi uskottavia. Itsekin olen jo muutaman epäilyttävän viestin saanut. Eihän tässä enää tiedä mihin uskaltaa vastata!
- **Uutisankkuri:** Uutisista näkemiin.

Syöte 2: KTK julkaisee Tietoturva NYT! artikkelin:



TIETOTURVA NYT!

Tietojenkalastelu- ja huijausviestien kanssa tulee olla yhä tarkempi

Tietojenkalastelu- ja huijausviestit kehittyvät jatkuvasti. Erilaiset teknologiat, kuten koneoppiminen ja tekoäly sekä psykologiset keinot auttavat rikollisia pyrkimyksissään voittaa uhrin luottamus. Kalastelukampanjat tuottavatkin jatkuvasti tulosta rikollisille ja Kyberturvallisuuskeskuksen arvion mukaan noin sadan organisaation sähköpostitilejä on murrettu onnistuneesti lähikuukausien aikana.

Yksi suurimmista kehitysaskeleista verkkohuijauksien uskottavuudessa on ollut sosiaalisen manipuloinnin ja tekoälyn käyttö, jolla pyritään saamaan viestintää uskottavammaksi. Huijarit pyrkivät tutkimaan tarkasti potentiaalisia uhrejaan ja keräämään heistä tietoa esimerkiksi avoimia tietolähteitä käyttäen. Avoimina tietolähteinä voivat toimia sosiaalisen median profiilit, organisaatioiden verkkosivut ja verkossa olevat uu-

tiset. Näiden tietojen pohjalta rikolliset pyrkivät räätälöimään huijauksen kohteelle sopivaksi. Esimerkiksi laskutushuijauksia pyritään kohdistamaan henkilöille, jotka hoitavat organisaation laskutusta ja rahaliikennettä.

Yleiskatsaus:

- Kohderyhmä: Kampanja on kohdistunut laajaan joukkoon suomalaisia organisaatioita, julkishallinnon ja yksityisen sektorin puolella.

- Kanavat: Hyökkääjät ovat käyttäneet useita eri viestintäkanavia, kuten sähköpostia, pikaviestipalveluita ja sosiaalista mediaa.

- Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa on mm. käytetty tunnettujen brändien ja organisaatioiden logoja sekä valheellisesti esiinnytty organisaation työntekijänä osana huijausta.

Tekoälyn käyttö on mahdollistanut vakuuttavien käännösten tekemisen, joten kieliopillisten virheiden löytäminen huijausviesteistä voi olla nykyään haastavaa. Tämä mahdollistaa myös sen, että rikollinen pystyy käymään uskottavaa keskustelua kaapatulta tunnukselta seuraavien mahdollisten uhrien kanssa.

Varotoimenpiteet ja Suositukset:

Organisaatiossa kannattaa panostaa henkilöstön tietoturvatietoisuuden lisäämiseen ja aktiiviseen ylläpitämiseen. Tässä tehokkaita keinoja ovat säännöllinen harjoittelu ja erilaiset kalastelu- ja huijaustapausten simuloinnit, joihin löytyy tänä päivänä myös erittäin hyviä ohjelmistoja.

Mikäli omassa organisaatiossa tapahtuu tietomurto ja murretuilta tunnuksilta lähetetään huijausviestejä, on tärkeää pyrkiä informoimaan huijausviestien vastaanottajat mahdollisimman nopeasti, jotta voidaan minimoida seuraavien tietomurtojen määrä. Sama pätee myös some-tilimurtoihin, joissa murretuilta tunnuksilta aletaan tehtailla huijauksia. Eli jos huijari sattuu pääsemään murretulle tilille, varoita ystäviäsi mahdollisista vilpillisistä viesteistä, jotka tulevat tililtäsi.

Organisaatioita suositellaan myös käyttämään monivaiheista tunnistautumista ja varmistamaan, että tietoturva-asetukset ovat ajan tasalla.

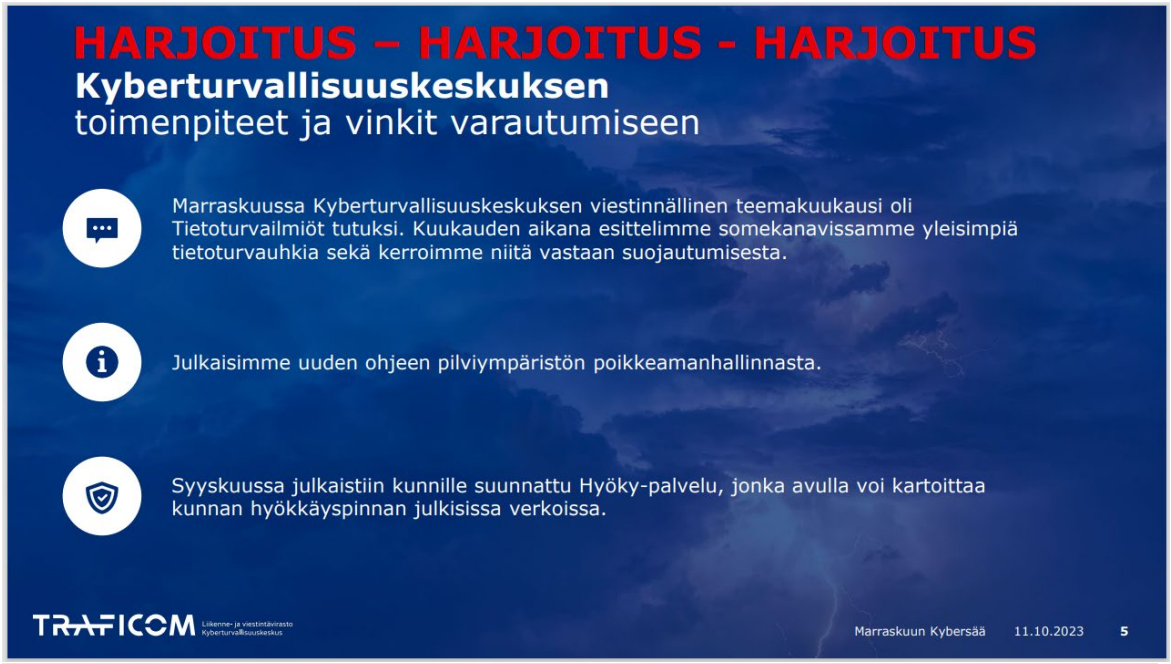
Kybersää: Tekoälyä hyödyntävä hyökkäys – Uudet uhat ja suojautumiskeinot

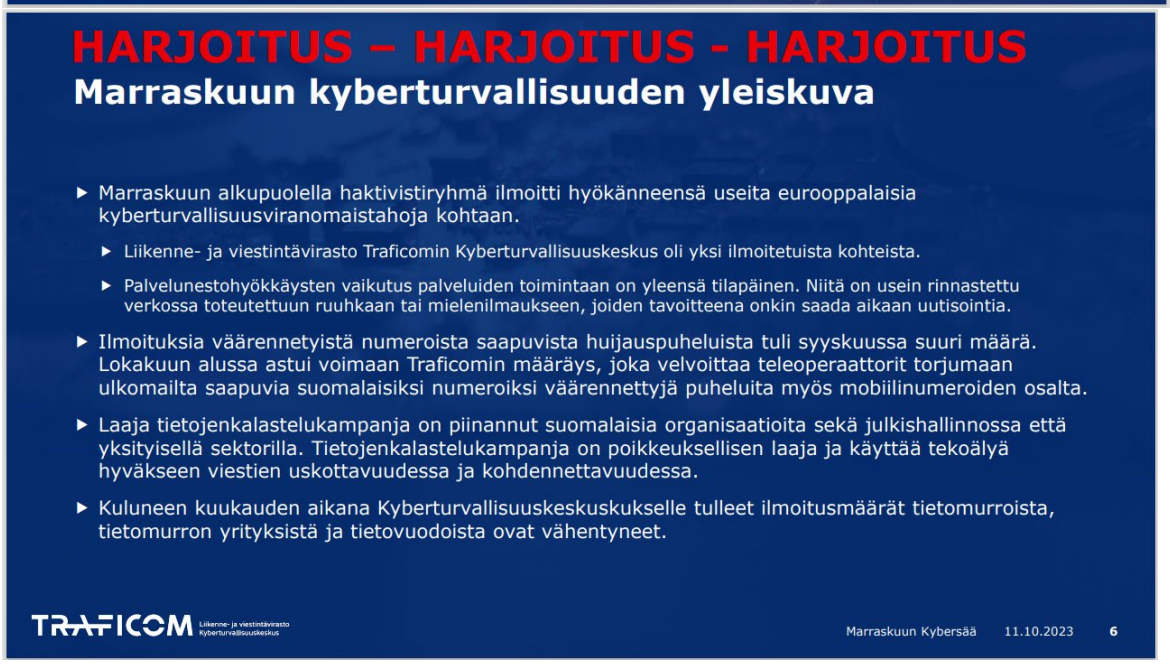

HARJOITUS – HARJOITUS - HARJOITUS
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus
Kybersää
Marraskuu 2023


HARJOITUS – HARJOITUS - HARJOITUS
#kybersää
Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.
Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville. Lukija saa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.
Kybersää voi olla:
rauhallinen
huolestuttava
vakava
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus
Marraskuun Kybersää 11.10.2023 2


HARJOITUS – HARJOITUS - HARJOITUS
Kuukauden tunnuslukuja
345 MILJ
Irlannin tietosuojaviranomainen on määrännyt TikTok Technology Limitedille 345 miljoonan euron seuraamusmaksun yleisen tietosuoja-asetuksen vastaisista käytännöistä lasten henkilötietojen käsittelyssä.
19,8 MILJ
Suomalaiset menettivät erilaisissa verkkohuijauksissa yhteensä 19,8 miljoonaa euroa vuoden 2023 ensimmäisten kuuden kuukauden aikana.
2100
Tietoturva 2023 –seminaariin ilmoittautui yli 4000 osallistujaa! Seminaari pidettiin torstaina 12.10.2023.
TRAFICOM
Marraskuun Kybersää 11.10.2023 3


HARJOITUS – HARJOITUS - HARJOITUS
Kybersää marraskuu 2023
Tietomurrot ja -vuodot
Julkisuudessa olleen Alkamatka Oy:n tietomurron seurauksena saimme ilmoituksia vuotaneista tiedoista.
Sosiaalisen median tilimurroissa on nähty myös järjestelmiin tallennettujen luottokorttien väärinkäyttöjä esimerkiksi ostamalla mainoksia.
Huijaukset ja kalastelut
Huijauspuheluita soitettiin väärennetyistä numeroista Marraskuussa ennätysmäärä.
Poikkeuksellisen laaja tietojenkalastelukampanja piinaa suomalaisia yrityksiä sekä julkishallinnossa että myös yksityissektorilla
Haittaohjelmat ja haavoittuvuudet
Kriittinen ja etäkäytettävä haavoittuvuus libwebp-kirjastossa edellyttää välitöntä päivittämistä.
Tekoälyä hyödyntävä hyökkäys on johtanut useisiin tietomurtoihin Suomessa. Hyökkäyksen kyvykkyys oppia ja mukautua viittaa tekoälyn käyttöön.
Automaatio ja IoT
NIST on päivittänyt teollisuusautomaatioympäristöjen suojaamiseen keskittyvän ohjeensa 800-82.
Uudessa versiossa huomioidaan mm. muuttuneet tuotanto-ympäristöjen kyberturvallisuus-uhkat, suojaustyökalut, suositellut käytännöt sekä arkkitehtuurit.
Verkkojen toimivuus
Syyskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
Haktivistit jatkavat palvelunestohyökkäyksiä ja kotimaiset organisaatiot ovat saaneet osansa hyökkäyksistä.
Palvelunestohyökkäyksillä ei ole ollut vakavia vaikutuksia palveluiden saatavuuteen.
Vakoilu
Puolivuosittain julkaistava Microsoftin raportti kuvaa Itä-Aasian kyberoperaatioiden trendiä.
Microsoftin raportti kertoo esimerkiksi Kiinaan liitettävästä kybervakoilusta ja vaikuttamisoperaatioista sekä Pohjois-Korean tietojenkeruusta ja kryptovaluuttojen hankinnasta.
TRAFICOM
Marraskuun Kybersää 11.10.2023 4





Syöte 3: Quacker: @KRP Kyberkeskus

Käynnissä tekoälyä hyödyntävä laaja tietojenkalastelukampanja. Kalasteluviestit ovat poikkeuksellisen uskottavia. Olkaa tarkkana! #Kyberrikostorjuntakeskus #tietojenkalastelu #tekoaly

Syöte 4: Sähköpostiviesti Organisaation hallinnon työntekijältä Organisaation tietohallinnolle / tietoturvasta vastaavalle

Lähettäjä: minna.makinen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi; tietoturvavastaava@organisaatio.fi
Aihe: Tietoturvapoikkeamailmoitus

Hei,

Olen todennäköisesti haksahtanut tietojenkalasteluviestiin. Sain eilen aidolta tuntuneen viestin sähköpostiini, jossa minua pyydettiin muuttamaan oma AD-kirjautumisessa käytettävä salasanani välittömästi. Viestin mukaan salasana oli päivitettävä viipymättä, sillä organisaatiotamme kohtaan on käynnissä kyberhyökkäys. Viestin allekirjoituksessa oli meidän tietohallinnosta vastaavan johtajan nimi, joten noudatin viestin ohjeita ja päivitin oman salasanani heti, enempää miettimättä.

Viesti sisälsi linkin, jonne syötin omat AD-kirjautumiseen käytettävät käyttäjätunnuksen, nykyisen salasanani ja haluamani uuden salasanan. Nyt kun tarkastelin viestiä, niin en ole asiasta enää täysin varma. Uutisissakin on ollut paljon puhetta tietojenkalastelusta. Onko meillä käynnissä salasanojen päivitys tällaisen menettelyn kautta vai meninkö vahingossa tekemään pahan virheen? Toivottavasti asia selviää.

Terkuin Minna

Minna Mäkinen
minna.makinen@organisaatio.fi
Erityisasiantuntija / Hallinto
Organisaatio

Syöte 5: Sähköposti Organisaation henkilöstöhallinnon työntekijältä tietohallinnolle / tietoturvasta vastaavalle

Lähettäjä: seppo.virtanen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi; tietoturvavastaava@organisaatio.fi
Aihe: Erikoinen puhelu

Hei,

En ole ihan varma, mutta voi olla, että olen antanut omat käyttäjätunnukseni vääriin käsiin. Minulle soitti tänään Kyberturvallisuuskeskuksen väestörekisterin asiantuntija. Hän tarvitsi tunnuksiani, jotta pystyi selvittämään, onko meidän Organisaation tietoja on vuotanut darkwebin puolelle. Annoin hänelle tiedot.

Heti kun suljin puhelimen, minulla heräsi ajatus, että voisiko tämä olla tietojenkalastelua? Sitten kuitenkin mietin, että eihän kai nyt sentään ihan oikeasta suomalaisesta 029-alkuisesta puhelinnumerosta soittanut ja selvää suomea puhunut henkilö voi kalastella tietojani?

Yt. Seppo V

Seppo Virtanen
seppo.virtanen@organisaatio.fi
Asiantuntija, Henkilöstöhallinto
Organisaatio

Syöte 6: Iltasen verkkouutinen

- **Toimittaja:** Meillä on haastateltavana kyberturvallisuuden professori Jarno Limnéll.
- **Toimittaja:** Olette seuranneet tarkasti viime viikkojen aikana paljon huomiota herättänyttä Eurooppaan kohdistunutta tietojenkalastelukampanjaa. Oletteko huolestuneet suomalaisten organisaatioiden tietoturvan tasosta? Onko suomalaisten huoli omien tietojen vuotamisesta vääriin käsiin perusteltua?
- **Jarno Limnéll:** Suomalaisten organisaatioiden tietoisuus tietoturvasta on varsin korkealla tasolla verrattuna mihin tahansa maailman maahan. Toki yksittäisten organisaatioiden tietoturvan tasossa saattaa olla parannettavaa, mutta yleisellä tasolla voisin todeta, että Suomi yhteiskuntana ja sen organisaatiot ovat hyvin varautunut erilaisiin tietoturvauhkiin. Suomalaiset voivat siis olla rauhallisin mielin omien tietojensa osalta. Mitä sensitiivisempää tietoa organisaatiot käsittelevät sitä kovemmat ovat heihin kohdistuvat vaatimukset tietoturvan osalta.
- **Toimittaja:** Mitä tiedämme tällä hetkellä käynnissä olevasta tietojenkalastelukampanjasta?
- **Jarno Limnéll:** Vielä tällä hetkellä varsin vähän. Viranomaiset koordinoivat vastatoimia ja tutkintaa kansainvälisellä tasolla. Odottaisin tarkempia tietoja tulevien viikkojen aikana. Selvää on kuitenkin se, että kalastelukampanjan takana oleva taho hyödyntää uutta teknologiaa kalasteluviestien sisältöjen uskottavuuden parantamisessa sekä omien viestien laajamittaisessa levittämisessä.
- **Toimittaja:** Mitä vaikutusta suomalaisten organisaatioiden toimintaan tietojenkalastelusta voi seurata?
- **Jarno Limnéll:** Jos tekijä saa haltuunsa organisaation henkilöstön käyttäjätunnuksia ja salasanoja, niin niiden avulla pääsee vaivattomasti sisälle organisaation järjestelmiin. Näin ollen tekijällä on vapaa pääsy organisaation tietoihin, joita hyökkääjä voi ladata itselleen, tai tekijä pystyy tahtoessaan tekemään suurtakin vahinkoa järjestelmien toimintaan. Onneksi useissa organisaatioissa on jo käytössä vahva tunnistautuminen, joka auttaa hallitsemaan tämän tyylisen riskin toteutumista.

- **Toimittaja:** Miten organisaatioiden tulisi toimia tässä tilanteessa, jotta voisivat välttää tietojen päätymistä vääriin käsiin?
- **Jarno Limnéll:** Henkilöstön jatkuva kouluttaminen on avainasemassa. Kun koko organisaation henkilöstö on koulutettu tunnistamaan ja raportoimaan tietojenkalastteluviesteistä, on aina epätodennäköisempää, että tietojenkalastelu onnistuu. Tavalliselle suomalaiselle voisin sanoa, että kannattaa aina suhtautua epäilevästi viesteihin, joissa pyydetään käyttäjätunnusta, salasanaa tai pankkitunnuksia. Kalasteluviesteille on myös tyypillistä, että tekijä vetoaa kiireelliseen tilanteeseen, mitään päätöksiä ei kannata tehdä hätiköiden. Lue viesti useaan kertaan ja kysy itseltäsi, voiko tämä pitää paikkaansa ja pyri aina varmistamaan, että viestin takana on oikea taho, mikäli epäilyksesi herää. Jos joka tapauksessa päädyt tietojenkalastelun uhriksi, ole välittömästi yhteydessä oman organisaatiosi tietoturvasta vastaavaan tahoon tai yksityisasioissa ole yhteydessä viranomaisiin.
- **Toimittaja:** Kiitos haastattelusta.

Tehtävät

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

Suomessa on käynnissä tekoälyn avulla toteutettava laaja tietojenkalastelukampanja, jonka myötä Organisaation työntekijöiden kirjautumistunnuksia on päätynyt vääriin käsiin.

Tapahtuma 1: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Miten havaita tietojenkalastelu, joka kohdistuu oman organisaation työntekijöihin?
3. Miten ohjeistatte henkilöstöä toimimaan tietojenkalasteluviestien osalta?
4. Miten organisaatiossanne on varauduttu tietojenkalasteluun?
5. Onko henkilöstöllenne tarjottu säännöllisesti koulutusta tietojenkalastelusta?
6. Onko organisaatiollanne olemassa Incident Response -suunnitelma, joka otetaan käyttöön tietovuototilanteessa?
7. Miten huomioitte tekoälyn hyödyntämisen tietojenkalastelukampanjaan kohdistuvissa toimenpiteissä?

Tapahtuma 1: Lisätehtävät

8. Onko organisaatiossanne käytössä monivaiheinen tunnistautuminen tärkeimpiin järjestelmiin?
9. Miten organisaatiossanne ylläpidetään käyttäjiä ja käyttöoikeuksia?
10. Miten varmistatte, että käyttöoikeushallintanne on ajan tasalla?

Tapahtuma 1: Tekniset tehtävät

11. Miten pystytte selvittämään, kenelle kaikille huijausviesti on organisaatiossa tullut ja ketkä ovat siihen vastanneet?
12. Onko organisaatiossa kyvykkyydet havaita poikkeavia kirjautumistapahtumia (esim. geolokaatio/maantieteellinen sijainti)?

Tapahtuma 1: Viestintätehtävät

13. Mitä viestintätoimia (mitä, kenelle, milloin) tilanne vaatii organisaatiossanne, ottaen huomioon, että tekoälyn avulla toteutettu tietojenkalastelukampanja voi mukautua saamiensa tietojen avulla?
14. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
15. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.
16. Luonnostelkaa keskeisimmät viestintämateriaalit.
17. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

3.2 Tapahtuma 2 - Järjestelmäuudistuksessa henkilötietojen tietoturvaloukkaus

Tapahtuman tausta ja tavoitteet

Työntekijöiden henkilötietoja sisältävään järjestelmään (”HR-järjestelmä”) tehdään viikonlopun aikana päivitys. Päivityksessä käyttäjätietojen pääsyoikeudet ovat menneet sekaisin ja henkilöt pääsevät joissakin tilanteissa katselemaan toistensa henkilötietoja. Henkilötietoja on myös tuhoutunut.

Alkuun tiedetään, että järjestelmässä käsiteltävien henkilötietojen joukossa ovat esimerkiksi nimi, työtehtävä, henkilötunnus ja kotiyhteystiedot. Kehityskeskusteluja koskevissa tiedoissa on avoimia tietokenttiä, joihin esihenkilöt ovat voineet kirjoittaa vapaasti muistiinpanoja keskusteluista. Tapauksessa käy loppuvaiheessa ilmi, että erään henkilön kohdalla paljastuneisiin tietoihin sisältyvät esihenkilön kehityskeskustelussa tekemät kirjaukset esim. työssä jaksamisesta ja henkilön terveydentilasta. Lisäksi henkilö kertoo, että hänellä on ollut tietoja koskeva turvakielto, koska häneen ja hänen perheeseensä kohdistuu uhka.

Tietosuojasta vastaava henkilö on lentokoneessa, eikä voi osallistua ensivaiheessa asian selvittämiseen.

Tapahtumaan liittyy tietoturvaloukkauksen selvittämisen, riskien arvioinnin ja lakisääteisten ilmoitusvelvollisuuksien rajoissa toimimisen harjoittelua. Lisäksi harjoitellaan rekisteröityjen ja viestintävälineiden kanssa kommunikointia.

Tapahtuman 2 syötteet

Syöte 1: Sähköposti työntekijältä käyttötukeen

Lähettäjä: vaino.markkola@organisaatio.fi
Vastaanottaja: IT-tuki@organisaatio.fi
Aihe: Virheitä HR-järjestelmässä

Terve!

Mistähän kyse, kun edellisellä viikolla ”HR-järjestelmään” syöttämäni uuden työntekijän perustiedot ovat nyt ihan jotain muuta kuin mitä olen perjantaina kirjannut? Henkilöllä näkyy ihan outo osoite, ei varmasti oikea ja työtehtäväkin muuttunut.

Saatteko tiedot palautettua jostain? Tarvitsen niitä, kun teemme huomenna työsopimusta henkilön kanssa. Minulla ei näitä tietoja ole, koska kirjoitin ne suoraan järjestelmään puhuessani henkilön kanssa. Siinä oli aika paljon kaikkia tietoja, olisi tärkeää saada ne palautettua.

YT. Väinö

Väinö Markkola
vaino.markkola@organisaatio.fi
Esihenkilö
Organisaatio

Syöte 2: Sähköposti käyttötuesta tietoturvavastaavalle, HR-vastaavalle ja tietohallintojohtajalle

Lähettäjä: IT-tuki@organisaatio.fi
Vastaanottaja: tietoturvavastaava@organisaatio.fi; HR-vastaava@organisaatio.fi; tietohallintojohtaja@organisaatio.fi

Aihe: Virheitä HR-järjestelmässä

Tervehdys!

Tehtiin sovitusti HR-järjestelmän päivitys viikonloppuna. Nyt vähän näyttää, että ei mennyt kaikki putkeen. Yhdeltä esihenkilöltä tullut ainakin kyselyä uuden työntekijän oudoista tiedoista, ja sen jälkeen vähän itsekin tässä selviteltiin...

Näyttää nyt siltä, että työntekijöiden henkilötietoja saattaisi näkyä toisille työntekijöille ja osa tiedoista varmaan korvattu toisten henkilöiden tiedoilla. Ei oikein vielä tiedetä,

miksi näin tapahtuu, joten vaikea sanoa kuinka montaa ihmistä koskee. “HR-järjestelmässähän” on ihan vaan tavallisia henkilötietoja, kuten nimet ja työkokemustiedot, henkilötunnus, kotiosoite yms., mutta me ei tätä tietosisältöä niin tarkkaan tiedetä ja pitäisi selvittää.

Meillä tietysti tässä tutkailut käynnissä, ja kerrotaan, kun tiedetään enemmän. Mitähän vastataan, jos tulee käyttäjiltä lisää kysymyksiä?

t. IT-tuki

IT-tuki@organisaatio.fi
Organisaatio

Syöte 3: Chat-keskustelu HR:n edustajalta tietoturva-/tietosuojavastaavalle

Mirva Miettinen, HR-työntekijä: Moikka! Yritin soittaa, mutta et tainnut päästä puhelimeen. HR-järjestelmän päivityksessä on viikonloppuna tapahtunut jotain odottamatonta, ja tilanne on nyt se, että käyttötuen mukaan henkilötietoja näkyy jotenkin väärille käyttäjille. Oisko sulla joku valmis teksti, jonka voisi laittaa Intraan, jotta työntekijät ei soittaisi ainakaan käyttötukeen ja saataisiin työrauha? Mitä tässä nyt ekana pitäisi tehdä?

Tauno Tietoinen, Tietosuojavastaava: Ok, vähän huono hetki. Olen lähdössä työmatkalle ja just nousemassa lentokoneeseen. Olen tavoitettavissa vasta illalla, kun pääsen hotelliin. Onko siellä HR-järjestelmässä millaisia tietoja ja kuinka montaa käyttäjää tämä arviolta koskee?

Mirva Miettinen, HR-edustaja: Kuka tästä prosessista tietäisi ja kykenee juttelemaan teknisistä asioista käyttötuen kanssa, kun olet pois? Pitäisi vähän ohjeistaa, mitä selvittävät ja millaisia tietoja ICT:stä tarvitaan. Mäkään en tiedä, mitä kaikkea HR-järjestelmässä voi olla, mutta kuulemma ainakin nimi, henkilötunnus, kotiosoite ja

sitten jotain arviointeja, ehkä kehityskeskusteluista jotain. Ei varmaan mitään arkaluonteista. Käyttäjiähän meillä on varmasti kaikki nykyiset työntekijät ja on siellä ehkä entistenkin työntekijöiden tiedot aina jonkun aikaa.

Tauno Tietoinen, Tietosuojavastaava: Katsokaa mitä ohjeita tietoturvaloukkausten käsittelystä on Intrassa ja selvittäkää niiden avulla tilannetta. Joudun nyt sulkemaan laitteet, siis pakko mennä koneeseen. Luen sähköpostit ja teidän selvittämät tiedot tilanteesta hotellissa illalla!

Syöte 4: Organisaation IT-käyttötuki jättää HR:n edustajan puhelinvastaajan viestin

Käynnistä puhelinvastaajan viesti play-painikkeesta. Videon saat koko ruudun näkymään, kun klikkaat oikeasta alareunasta.

---------- Puhelinvastaajan viestin sisältö tekstinä ----------

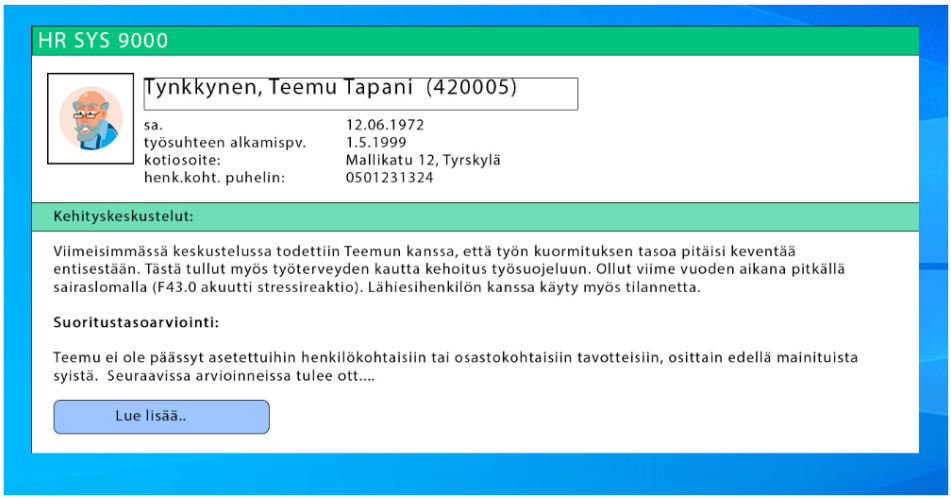
Organisaation IT-käyttötuesta Tomppa, moikka!

Olit pyytänyt lisätietoja siitä HR-järjestelmän päivityksessä tapahtuneesta virheestä. Näyttää siltä, että siellä HR-järjestelmässä on menneet tilit sekaisin ainakin niillä, joilla on sama syntymäpäivä. Eli ei tämä voi kovin montaa henkilöä koskea, mutta me selvitämme tätä määrää vielä.

Sellainen huomio nyt kuitenkin tuli tehtyä, että HR-järjestelmässä on perustietojen lisäksi “Kehityskeskustelut” -välilehti. Siellä on ainakin yhdellä henkilöllä jotain kirjauksia liittyen hänen työssä jaksamiseensa ja sen sellaisiin, ja häntä tämä poikkeama nyt taitaa koskea. Me emme ruvenneet lukemaan, mutta olihan se ok käydä katsomassa ja selvittää kenestä kyse, jotta voitte sitten olla tarvittaessa yhteydessä? Katsellaanko me myös, onko muilla näitä tämän välilehden tietoja täytetty?

Syöte 5: Organisaation sisäinen chat-keskustelu

Maija Makkonen, Työntekijä: Moikka! Ajattelin nyt laittaa suoraan sinulle viestiä. En tiedä, oletko jo kuullut, mutta tuo HR-järjestelmähän on aivan sekaisin. Kirjauduin järjestelmään katsoakseni, näkyykö minulla kaikki normaalisti, ja kun intrassa ei ollut mitään tiedotetta aiheesta. Huomasin, että näen sinun kehityskeskustelusi muistiinpanot! Kirjautuisitko järjestelmään, ja katsoisit, näetkö sinä minun tietoni? Otin muutaman kuvakaappauksen virheellisestä näkymästäni, laitan ne tähän.



Teemu Tynkkynen, Työntekijä: Moi, kiitos kun otit yhteyttä… Voi ei. Pyydettäisiinkö HR:n henkilö tähän keskusteluun mukaan, niin voitaisiin käydä tilanne heti läpi.

HR:n edustaja liittyy keskusteluun

Mirva Miettinen, HR-työntekijä: No moikka! Minkälaista asiaa teillä oli?

Maija Makkonen, Työntekijä: Moikka, ja kiitos kun pääsit näin nopeasti kuulolle. Tuossa ylempänä näkyykin nuo kuvakaappaukset, jotka olen siis ottanut minun näkymästäni tuolla HR-järjestelmässä. Ne ovat Teemun tietoja. Miksi minuun ei ole oltu yhteydessä asiasta? Ja millaiset toimet on käynnissä tilanteen korjaamiseksi? Tämähän on saatava pikimmiten kuntoon.

Teemu Tynkkynen, Työntekijä: Juu kyllä tässä itseäkin kovasti ihmetyttää, että minulle ei ole ilmoitettu? Tuskin tietäisin tapauksesta vieläkään, jos Maija ei olisi ottanut yhteyttä. HR:ssä kuitenkin pitäisi olla tiedossa myös, että minulla on turvakielto. Oikeastaan haluaisinkin tämän tapauksen myötä tarkemmin tietää, miten tämä asia on Organisaatiossa huomioitu?

Syöte 6: Haastatteluvideo

Iltasen toimituksesta hyvää päivää. Olemme saaneet uutisvinkin liittyen teidän Organisaationne työntekijään kohdistuneeseen tietoturvaloukkaukseen, ja olemme haastatelleet häntä. Haastattelu tehtiin nimettömästi, mutta haastateltavan henkilöllisyys on toimituksemme tiedossa. Henkilö kertoi jääneensä järkyttyneenä pois töistä ja pelkäävänsä tulevansa syrjityksi terveydentilaa koskevien tietojen leviämisen takia. Häneen on kuulemma suhtauduttu välinpitämättömästi ja paljastuneiden tietojen merkitystä on vähätelty. Ilmeisesti Organisaation edustajan mukaan tiedot eivät ole mitenkään arkaluonteisia eivätkä ainakaan terveydentilaa koskevia. Pyytäisimme nyt teiltä kannanottoa ja vahvistusta näille tiedoille ennen kuin julkaisemme jutun joko viikonloppuna tai viimeistään maanantaina.

1 ”Sain työntekijältänne tiedon, että teillä olisi meneillään tietoturvaloukkaus, ja kirjoitan aiheesta pientä uutista. Miten kommentoitte tätä työntekijänne kohdalle osunutta tilannetta?”
2 ”Pitääkö tosiaan paikkaansa, että työntekijän reumaa koskevat tiedot ovat paljastuneet IT-tuessanne työskentelevälle henkilölle? Minulla on tässä työntekijältänne saamani sähköposti, jossa hän ihan yksityiskohtaisesti asiasta kertoo, joten voitte varmasti kieltää tai vahvistaa, jos luen tästä väitteen kerrallaan? Mukana on teidänkin omia kommenttejanne, joten ehkä haluatte ainakin nämä tarkistaa?”
3 ”Erityisesti henkilöä loukkaa se, että kehityskeskustelujen yhteydessä on ylipäänsä kirjattu työntekijän terveyttä koskevia tietoja, ja ne ovat päätyneet HR-järjestelmään, johon ne eivät selvästikään kuulu. Onkohan teillä noudatettu tässä lainsäädäntöä? Eikö näitä pitäisi käsitellä ihan erillisessä järjestelmässä?”
4 ”Teillä on varmaankin tehty asianmukaiset viranomaisilmoitukset, ja tämä vahvistuu, kun soitan viranomaiselle? Vai onko tämä tieto myös saatavilla kirjaamostanne?"

Tehtävät:

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

Työntekijöiden henkilötietoja sisältävään järjestelmään (”HR-järjestelmä”) tehdään viikonlopun aikana päivitys. Päivityksessä käyttäjätietojen pääsyoikeudet ovat menneet sekaisin ja henkilöt pääsevät joissakin tilanteissa katselemaan toistensa henkilötietoja. Henkilötietoja on myös tuhoutunut.

Tapahtuma 2: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Onko organisaatiollanne olemassa prosessi, jonka mukaan tilannetta tutkitaan?
3. Onko tietoturvaloukkausten selvittämisprosessia koskeva ohje sellainen, että myös avainhenkilöiden (esim. tietosuojavastaava) ollessa estynyt, ohjetta voidaan noudattaa ja ensitoimet saadaan oikein suoritetuiksi?
4. Onko ohjeessa selvennetty, miten ja millä kriteereillä tietoturvaloukkauksesta rekisteröidyille aiheutuvaa riskiä arvioidaan, ja mikä merkitys riskiarviolla on prosessissa (ilmoitusvelvollisuudet)? Voitte hyödyntää esimerkiksi tietosuojavaltuutetun ohjeita, jos organisaatiolla ei ole omaa tarkempaa ohjeistusta: https://tietosuoja.fi/documents/6927448/8214536/Esimerkkej%C3%A4+tietoturvaloukkauksista/754c16aa-152e-4f15-a458-d1579c5ea4b2/Esimerkkej%C3%A4+tietoturvaloukkauksista.pdf?t=1536128589000
5. Onko ohjeen perusteella selvää, kuka tekee päätöksen siitä, tehdäänkö tietoturvaloukkauksesta ilmoitus tietosuojavaltuutetulle ja rekisteröidyille?

Tapahtuma 2: Tekniset tehtävät

6. Miten estetään henkilöitä katsomasta järjestelmän tietoja sillä aikaa, kun ongelmanratkaisu on käynnissä?
7. Miten selvitetään tietovuodon laajuus?
8. Kuinka tuhoutuneet tiedot voidaan palauttaa?
9. Voiko olemassa olevaan tietoaineistoon luottaa?
10. Jos järjestelmä päätetään ajaa alas selvitystyön ja palautuksen ajaksi, miten se tehdään hallitusti?
11. Onko järjestelmän alasajolle ja palautukselle olemassa toimintamallia?
12. Oletteko harjoitelleet järjestelmän hallittua alasajoa ja palautusta?

Tapahtuma 2: Viestintätehtävät

13. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
14. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?

15. Miten organisaatiossa on otettu huomioon, että viestintävälineiden tiedusteluihin vastattaessa ei tulla esimerkiksi paljastaneeksi lisää yksityisyydensuojan piiriin kuuluvia tietoja?

16. Miten varmistetaan, että rekisteröidyille viestittäessä täytetään tietosuojasääntelyn vaatimukset, mutta otetaan huomioon myös viestinnälliset näkökulmat?

17. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.

18. Luonnostelkaa keskeisimmät viestintämateriaalit.

19. Harjoitelkaa haastattelun antamista medialle vastaamalla syötteen 6 kysymyksiin.

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

3.3 Tapahtuma 3 – Sidosryhmäriskit / arkaluonteinen yritysdata

Tapahtuman tausta ja tavoitteet

Tapahtuma keskittyy erityisesti Organisaation palveluntuottajaan, (esim. Palveluntuottaja Oy), joka on olennaisessa roolissa Organisaation toiminnan kannalta. Palveluntuottaja Oy:n hallussa on laajasti Organisaation kriittistä ja arkaluontoista tietoa, kuten salassa pidettävää tai turvaluokiteltavaa tietoa. Palveluntuottaja Oy:n turvallisuusjohtaja saa tiedon poliisilta, että yksi heidän entisistä avainhenkilöistään, jolla on ollut laajat käyttöoikeudet kriittiseen tietojärjestelmään, on yhteydessä järjestäytyneeseen rikollisuuteen. Tämä herättää välittömästi hälytystilan, koska lokitiedoista paljastuu, että avainhenkilö on ladannut suuria määriä kriittistä ja arkaluontoista tietoa ennen palvelussuhteensa päättymistä.

Osallistujien tulisi pohtia kysymysten kautta, miten toimia, jotta päästään selvittämään tilanteen laajuus ja suunnittelemaan vastatoimenpiteet. Tapahtuman lopullinen käänne on, että poliisi onnistuu takavarikoimaan ladatut henkilötiedot ennen kuin niitä on päästy levittämään. Viranomaiset ovat olleet kyseisen henkilön jäljillä jo pidemmän aikaa. Tämä tuo jonkin verran helpotusta tilanteeseen, mutta herättää edelleen kysymyksen siitä, kuinka Organisaatio voi parhaiten suojautua vastaavilta sisäisiltä uhkilta tulevaisuudessa. Tämä tapahtuma auttaa havainnoimaan sidosryhmäriskejä, joita organisaatiot kohtaavat tietoturvassa, ja tarjoaa osallistujille tilaisuuden oppia ja harjoitella kriittistä ajattelua, riskienhallintaa ja tietoturvareaktiivisuutta.

Tapahtuman 3 syötteet

Syöte 1: Palveluntuottajan tilannekatsaus Organisaatio Oy:n johdolle / ICT-päällikölle tapauksesta

Palveluntuottaja Oy:n turvallisuusjohtaja: Hyvää päivää kaikille. Kiitos, että pääsitte näin nopeasti mukaan Teams-kokoukseen. Haluan tuoda teidän tietoonne vakavan tilanteen, joka koskee tietoturvaa ja meidän välistä yhteistyötämme.

Palveluntuottaja Oy:n turvallisuusjohtaja: Olemme saaneet tiedon tänään aamulla poliisilta, että erään tutkinnan yhteydessä on saatu viitteitä, että Palveluntuottaja Oy:n tietoja ja samalla asiakkaidemme tietoja olisi päätynyt vääriin käsiin. Erästä meidän

entistä työntekijäämme epäillään asiakkaidemme tietojen luvattomasta lataamisesta ja säilyttämisestä. Kyseisellä henkilöllä oli laajat käyttöoikeudet meidän salassa pidettävää tietoa sisältävään tietojärjestelmäämme.

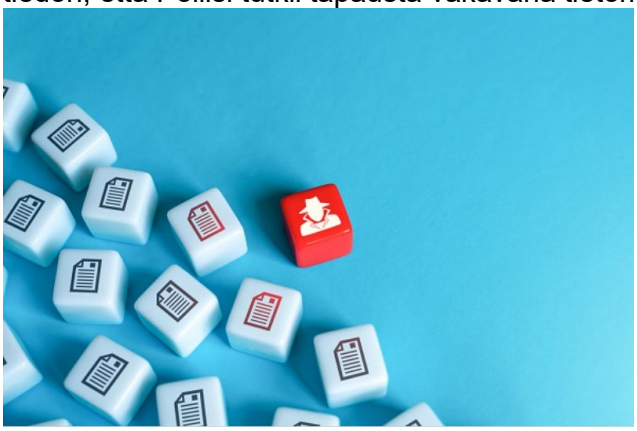
Palveluntuottaja Oy:n turvallisuusjohtaja: Tarkastettuamme tarkasti lokitiedot, voimme vahvistaa, että mainittu entinen avainhenkilö on ladannut suuria määriä kriittistä ja arkaluontoista tietoa, sisältäen myös Organisaation tietoja. Olemme tehneet asiasta rikosilmoituksen poliisille.

Palveluntuottaja Oy:n turvallisuusjohtaja: Haluamme vakuuttaa, että olemme tehneet kaiken mahdollisen tilanteen hallitsemiseksi ja että yhteistyömme jatkuu vahvempana. Olemme valmiita keskustelemaan toimenpiteistä ja vastatoimista, joilla voimme yhdessä suojata tietoturvaa ja estää vastaavien tapausten toistumisen tulevaisuudessa.

Palveluntuottaja Oy:n turvallisuusjohtaja: Kiitos, että otitte aikaa tähän tapaamiseen. Tulemme pitämään teidät ajan tasalla tilanteen kehittymisestä ja yhteistyön etenemisestä. Jos tilanteeseen liittyen tulee kysyttävää, olettehan matalalla kynnyksellä yhteydessä minuun.

Syöte 2: Iltanen: JUURI NYT: Vakava tietomurto paljastunut – Kohteena Palveluntuottaja Oy

Iltasen saamien tietojen mukaan Palveluntuottaja Oy on joutunut vakavan tietomurron kohteeksi, jossa organisaation salassa pidettäviä ja turvaluokiteltuja tietoja on vuotanut. Murron laajuus ja vaikutukset ovat edelleen selvityksen alla. Iltanen on saanut tiedon, että Poliisi tutkii tapausta vakavana tietomurtona.



Syöte 3: Quacker: @Tumppi

Taas uusi tietomurto! kuulin että Palveluntuottaja Oy:n tietoturva on murrettu. Tietojen vuotaminen vaan jatkuu. Selkeesti tää on vaan nykypäivää. Toivottavasti he saavat tilanteen hallintaan pian! #tietomurto #turvallisuus"

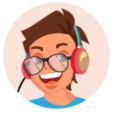
Syöte 4: Quacker: @Jaska

Tuntuu hurjalta, kun iso lafka kuten Palveluntuottaja Oy joutuu tietomurron uhriksi. Toivottavasti ei omat tiedot ole vaarassa! 🙏 #tietoturva #huolestunut"

Syöte 5: Quacker: @Tuulikki

Tietomurtojen yleistyminen on kyllä huolestuttavaa. Palveluntuottaja Oy:n tapaus vain osoittaa, että kukaan ei ole täysin suojassa. 😟 #tietomurto #varovaisuutta"

Syöte 6: Quacker: @Tuomo



Seurailen Palveluntuottaja Oy:n tietomurtojuttua. Tuntuu, että näitä tapauksia tulee koko ajan lisää. Tietoturva on tärkeää kaikille! 🔒 #tietomurto #tietoturva"

Syöte 7: Quacker: @Maikku

Taas hyvä osoitus siitä, kuinka retuperällä suomalaisten organisaatioiden tietoturva on. EN OLE YLLÄTTYNYT!

Syöte 8: Sähköposti Palveluntuottaja Oy:n turvallisuusjohtajalta Organisaation johdolle

Lähettäjä: tomi.torvinen@palveluntuottaja.fi
Vastaanottaja niina.nieminen@organisaatio.fi
Aihe: Tilannepäivitys

Hei,

Tässä päivitys tilanteeseen. Tällä hetkellä ei ole viitteitä siitä, että salassa pidettäviä ja / tai turvaluokiteltuja tietoja olisi vuodettu ainakaan julkisuuteen. Tieto tietovuodosta on valitettavasti päätynyt julkisuuteen, kuten olette itse varmaan huomanneet.

Selvitämme mistä tämä vuoto voisi olla peräisin. Olemme käynnistäneet kattavan selvityksen meidän henkilöstömme sidonnaisuuksista ja tarkastamme myös muita järjestelmiä, että voisimme estää tietovuodot tulevaisuudessa. Yhteistyö poliisin kanssa on sujunut hyvin ja uskomme, että epäilty tekijä saadaan pian kiinni.

T. Tomi Torvinen
tomi.torvinen@palveluntuottaja.fi
Turvallisuusjohtaja
Palveluntuottaja Oy

Syöte 9: Sähköposti Yleismedian toimittajalta Organisaation johdolle

Lähettäjä: minna.terava@yme.fi
Vastaanottaja niina.nieminen@organisaatio.fi
Aihe: Haastattelukysymykset

Hei,

Pyynnöstänne haastattelukysymykset sähköpostilla. Olemme tekemässä juttua Palveluntuottaja Oy:ta koskevasta tietovuodosta, joka on herättänyt laajaa huomiota sosiaalisessa mediassa. Haluaisin saada aiheesta teidän kommenttinne asiakkaan näkökulmasta.

1. Miten reagoitte tilanteeseen, kun kuulitte Palveluntuottajanne mahdollisesta tietovuodosta?
2. Oletteko kuulleet, minkälaisia tietoja teiltä on mahdollisesti vuotanut, ja miten tämä voi vaikuttaa toimintaanne?
3. Onko vuodon laajuutta saatu jo selvitettyä teidän osaltanne?
4. Miten aiotte teidän organisaatiossanne estää vastaavat tilanteet tulevaisuudessa?
5. Onko teillä viestiä niille, joiden tiedot ovat saattaneet vuotaa?

Minna Terävä
minna.terava@yme.fi
Tutkivan journalismin osasto / MOTTI
Yleismedia

Syöte 10: Sähköposti poliisilta

Lähettäjä: pertti.maijanen@poliisi.fi
Vastaanottaja tietoturvavastaava@organisaatio.fi
Aihe: Tilannetietoa poliisilta

Hei,

Ilmoitamme, että poliisi on takavarikoinut Palveluntuottaja Oy:n entisen työntekijän lataamia tietoja. Organisaationne nimi esiintyi takavarikoidussa aineistossa. Dataa ei alustavien tietojen mukaan ole vuodettu laajemman yleisön saataville. Tutkimme yhden henkilön osallisuutta rikokseen. Pysymme yhteyksissä ja tiedotamme lisää, kun tutkinta etenee. Kiitos yhteistyöstänne.

Terveisin,
Pertti Maijanen
Poliisi

Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Valitkaa toimintanne kannalta kriittinen palveluntuottaja (”Palveluntuottaja Oy”) ja peilatkaa harjoituksen tapahtumia sekä niiden vaikutuksia oman organisaationne toimintaan.

Palveluntuottaja Oy:n hallussa on laajasti Organisaation kriittistä ja arkaluontoista tietoa, kuten salassa pidettävää ja / tai turvaluokiteltua tietoa. Organisaatio saa tiedon, että Palveluntuottajan entinen avainhenkilö on ladannut tietoja luvattomasti. Henkilöllä on ollut laajat käyttöoikeudet Organisaation tietoa sisältävään järjestelmään.

Tapahtuma 3: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Mitä on sovittu palveluntuottajan kanssa tietoturvaloukkauksista ilmoittamisesta?
3. Millainen prosessi organisaatiollanne on palveluntuottajan valinnassa?
4. Onko olemassa kriteerejä tai standardeja (esim. säännölliset auditoinnit), jotka palveluntuottajan tulee täyttää?
5. Onko teillä suunnitelmaa sellaisen tilanteen varalle, jossa salassa pidettävää ja / tai turvaluokiteltua tietoa on päätynyt vääriin käsiin?
6. Onko teillä suunnitelmaa tai prosessia toiminnan jatkamiseksi, mikäli yhteistyö palveluntuottajan kanssa pitäisi päättää äkillisesti?
7. Onko palveluntuottaja velvoitettu sopimuksessa järjestämään tietoturvakoulutuksia omalle henkilöstölleen?

Tapahtuma 3: Lisätehtävät

8. Mitä jälkihoitotoimenpiteitä tilanne edellyttää?

Tapahtuma 3: Tekniset tehtävät

9. Millaisia valvontajärjestelmiä organisaatiollanne tai palveluntuottajallanne on poikkeuksellisen tai epäilyttävän toiminnan havaitsemiseksi?

10. Miten organisaatio pystyisi teknisesti pienentämään riskiä kriittisen datan vientiin ulospäin organisaatiosta?

11. Onko kriittinen data salattuna “at rest”, eli kun data on tallennettuna, eikä sitä siirretä tai muokata?

Tapahtuma 3: Viestintätehtävät

12. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?

13. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, joka auttaa tilanteesta viestimisessä?

14. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.

15. Luonnostelkaa keskeisimmät viestintämateriaalit.

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

3.4 Tapahtuma 4 – Tekoälyavusteinen haittaohjelmahyökkäys

Tapahtuman tausta ja tavoitteet

Hyökkäys alkaa kun haittaohjelma pääsee Organisaation verkkoon nollapäivähaavoittuvuuden kautta. Haittaohjelma alkaa levitä jonkin Organisaation käyttämän ohjelman avulla (kuten NotPetya). Kun haittaohjelma on saanut jalansijan verkossa, se alkaa kommunikoida ulkoisen, tekoälyä hyödyntävän, ohjauspalvelimen kanssa suojatusti.

Tässä tapahtumassa ohjauspalvelin ei ainoastaan anna komentoja haittaohjelmalle, vaan se myös luo jokaiselle saastuneelle koneelle uniikin version haittaohjelmasta. Tämä tapahtuu niin, että ohjauspalvelin saa tiedon koneen järjestelmästä ja konfiguraatiosta API-yhteyden kautta. Tietoa hyödyntäen se luo uniikin version haittaohjelmasta ja tämä tekoälyavusteinen muokkaaminen tekee haittaohjelman havaitsemisesta ja poistamisesta erittäin vaikeaa.

Tapahtumassa harjoitukseen osallistujat joutuvat kohtaamaan laajan, jatkuvasti mukautuvan ja uusiutuvan tekoälyavusteisen hyökkäyksen haasteet. Miten tilanteessa tulisi toimia ja miten siitä tulisi viestiä?

Tapahtuman 4 syötteet

Syöte 1: YME-uutinen

- **Uutisankkuri**: Uutisista, hyvää päivää. Uusi, tekoälyä hyödyntävä haittaohjelma on päässyt iskemään useiden suurten organisaatioiden tietoverkkoihin. Tietoturva-asiantuntija Jaakko Virta, mikä tekee tästä haittaohjelmasta erityisen vaarallisen?
- **Tietoturva-asiantuntija**: Tämä haittaohjelma käyttää tekoälyä kiertääkseen useimmat tunnetut turvamekanismit. Se on äärimmäisen sopeutuvainen ja osaa mukauttaa toimintansa sen mukaan, millaisia turvatoimia kohdejärjestelmässä on.
- **Uutisankkuri**: Miten organisaatiot voivat havaita tämän haittaohjelman?
- **Tietoturva-asiantuntija**: Valitettavasti perinteiset tunnistusmekanismit ovat usein tehottomia tämän haittaohjelman kohdalla. Yksi tapa on käyttää käyttäytymisanalyysiin perustuvia tietoturvatyökaluja, jotka huomaavat epätavalliset muutokset järjestelmässä.
- **Uutisankkuri**: Miten haittaohjelma toimii, kun se pääsee järjestelmään?
- **Tietoturva-asiantuntija**: Haittaohjelma skannaa kohdejärjestelmän ja sen perusteella tekee päätöksiä, millaiset hyökkäysvektorit olisivat tehokkaimpia. Tekoälyä hyödyntävä haittaohjelma voi esimerkiksi hakea järjestelmän heikkouksia tai tunkeutua sisäisiin verkkoihin.
- **Uutisankkuri**: Miten tätä haittaohjelmaa voidaan torjua?
- **Tietoturva-asiantuntija**: Kehittyneimmät, useita turvatyökaluja yhdistävät järjestelmät voivat olla riittävän tehokkaita tunnistamaan tämän uuden uhan. Myös henkilöstön tietoturvakoulutus on tärkeää, sillä monesti hyökkäykset alkavat yksittäisestä heikosta lenkistä, kuten tietojenkalasteluhuijaukseen sortuneesta työntekijästä.
- **Uutisankkuri**: Kiitos haastattelusta.
- **Uutisankkuri**: Toimittajamme haastatteli tekoälyasiantuntijaa ja Soli AI:n toimitusjohtajaa Pertti Sulinia aiheeseen liittyen.
- **Toimittaja:** Mitä tekoälyä hyödyntävällä haittaohjelmalla käytännössä tarkoitetaan?
- **Tekoälyasiantuntija**: Tekoäly käyttää koneoppimista analysoimaan isäntäkoneen toimintaa ja mukautuu sitten sen mukaisesti. Tämä tarkoittaa, että se voi oppia välttämään tietoturvamekanismeja ja muuntautua järjestelmän heikkouksien perusteella.
- **Toimittaja**: Onko tämä ensimmäinen kerta, kun näemme tekoälyn näin keskeisenä osana haittaohjelmaa?
- **Tekoälyasiantuntija**: Vaikka tekoälyä on aikaisemmin käytetty haittaohjelmissa, sen keskeinen ja monimutkainen rooli tässä erityisessä haittaohjelmassa on uutta ja huolestuttavaa.
- **Toimittaja**: Miten tekoälypohjainen haittaohjelma oppii ja mukautuu?
- **Tekoälyasiantuntija**: Haittaohjelma kerää dataa isäntäjärjestelmästä ja sen tietoturvamekanismeista. Tämän tiedon avulla se valitsee tehokkaimmat hyökkäystavat tai jopa integroituu käytössä oleviin ohjelmistoihin.
- **Toimittaja**: Miten organisaatiot voivat puolustautua tekoälypohjaisia haittaohjelmia vastaan?
- **Tekoälyasiantuntija**: Tämä on jatkuvaa kisaamista hakkereiden ja tietoturvayhtiöiden välillä. Mikään keino ei ole täysin aukoton ja uusia torjumiskeinoja on kehitettävä jatkuvasti torjumaan uusia uhkia. Tällä hetkellä yksi toimiva strategia voisi olla niin sanottu "honey pot" -järjestelmä, joka houkuttelee haittaohjelman ansaan. Tämän lisäksi tarvitaan jatkuvaa tietoturvapäivitystä ja -valvontaa, mukaan lukien tekoälypohjaiset turvallisuusratkaisut, jotka pystyvät tunnistamaan ja torjumaan myös tekoälypohjaiset uhat.

- **Toimittaja**: Kiitos haastattelusta, Pertti Sulin. Tämä keskustelu osoittaa, että olemme siirtymässä uuteen aikakauteen kyberturvallisuudessa. Organisaatioilta tämä tulee vaatimaan uudenlaista valppautta ja proaktiivisia toimenpiteitä.
- **Uutisankkuri:** Uutisista, näkemiin.

Syöte 2: Sähköposti tietohallinnolta tietoturvavastaavalle

Lähettäjä: tietohallinto@organisaatio.fi
Vastaanottaja tietoturvavastaava@organisaatio.fi
Aihe: Havainto toimistoverkosta

Hei,

Olemme havainneet huomattavan, noin satakertaisen määrän liikennettä normaaliin verrattuna toimistoverkon työasemissa. Onko käyttäjiltä tullut havaintoja jonkin järjestelmän toimimattomuudesta tai muusta poikkeavasta?

Yt. Matti

Matti Mainio
Asiantuntija, tietohallinto
Organisaatio

Syöte 3: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: toini.toimistolainen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: Kone toimii huonosti + oudot postit

Hei, huomasin tietokoneellani jotain outoa tänä aamuna. Se toimii hitaammin kuin yleensä ja olen saanut joitakin outoja sähköposteja, joita en ole avannut. Pitäisikö minun olla huolissani?

Yt. Toini

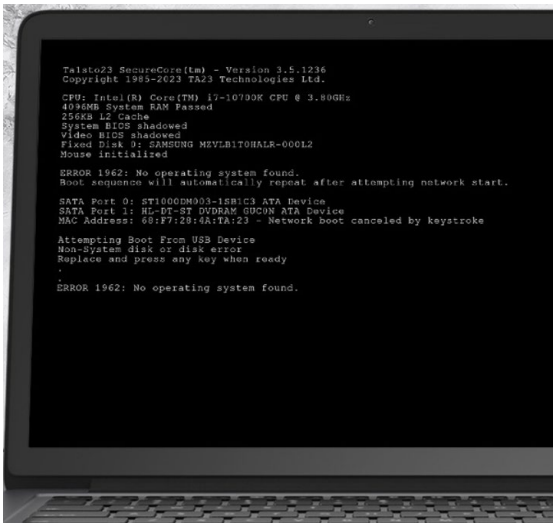
Toni Toimistolainen
toini.toimistolainen@organisaatio.fi
Asiantuntija
Organisaatio

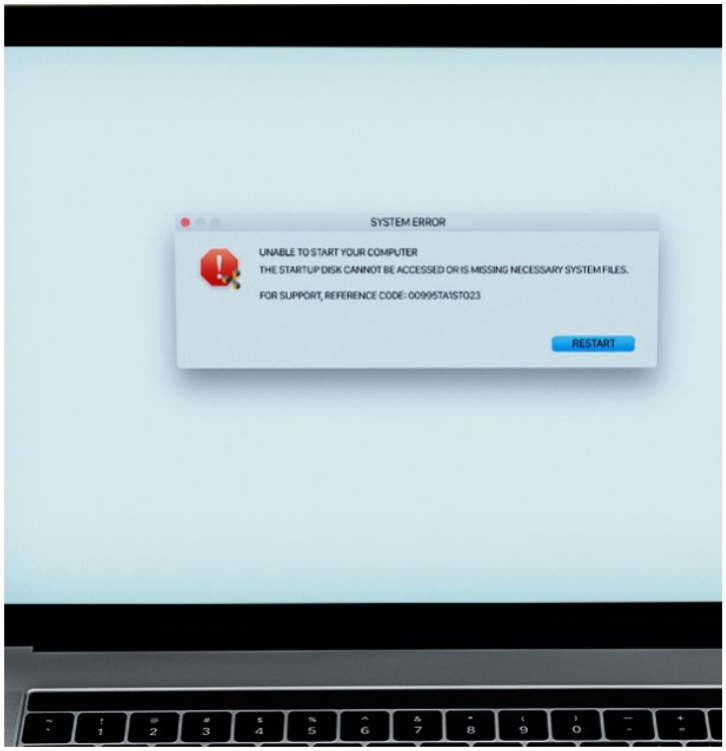
Syöte 4: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: susan.korhonen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: Koneet jumissa

Hei,

Otin omasta (Windows vasemmalla) ja kollegani (Apple MacBook oikealla) työasemista kuvan, kun käynnistäessämme tuossa yhtä sisäistä työpajaa, tietokoneemme näyttivätkin tältä. Mistä tässä mahtaa olla kyse?





Yt. Susan ja Malla

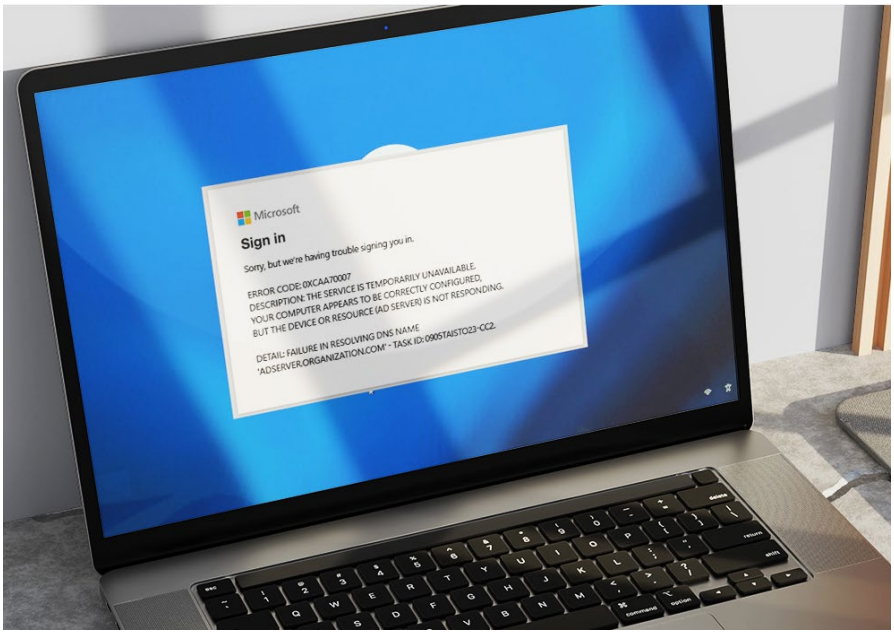
Susan Korhonen
susan.korhonen@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 5: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: ville.maki@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: AD jumissa

Moi,

Onko muilla ongelmia kirjautumisen kanssa? En pääse nyt jostain syystä kirjautumaan lainkaan…



Terv. Ville

Ville Mäki
ville.maki@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 6: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: helena.salminen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: Työasema jumissa

Hei,

Työasemani on täysin jumissa, sanoo vain että ”ohjelma ei vastaa” mitä tahansa yritänkään tehdä. Mistä on kyse ja miten minun tulisi toimia?

T. Helena

Helena Salminen
helena.salminen@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 7: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: jari.jokunen@organisaatio.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: Haittaohjelma koneella?!

Terve,
Tällainen näky avautui koneelleni kun sen käynnistin, onko tämä nyt joku haittaohjelma?! Ihan tavallisesti olen konettani käyttänyt enkä mielestäni ole kyllä mitään vääriä linkkejäkään klikkaillut, mitä nyt pitää tehdä?

T. Jari

Jari Jokunen
jari.jokunen@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 8: Organisaatioiden välinen keskustelukanava (esim. VIRT / ISAC / RocketChat / YMS)

Onko kukaan muu törmännyt tähän uuteen tekoälyä hyödyntävään haittaohjelmaan? Meidän yrityksessämme se on aiheuttanut melkoista hämminkiä. Olisi hienoa kuulla, miten muut ovat onnistuneet torjumaan sen.

Syöte 9: Sähköposti Palveluntuottajalta Organisaation tietohallintoon

Lähettäjä: peetu.parviainen@palveluntuottaja.fi
Vastaanottaja tietohallinto@organisaatio.fi
Aihe: Haittaohjelma havaittu

Hei,

Olemme havainneet vakavan tietoturvaongelman liittyen äskettäin levinneeseen haittaohjelmaan, joka on päässyt organisaatiomme verkkoon. Haittaohjelma on tunkeutunut järjestelmiimme nollapäivähaavoittuvuuden kautta ja alkanut kommunikoimaan ulkoisen ohjauspalvelimen kanssa.

Tekninen yhteenveto:

Haittaohjelma leviää organisaation käyttämän ohjelman kautta.

Ohjauspalvelin käyttää tekoälyä ja luo jokaiselle saastuneelle koneelle uniikin version haittaohjelmasta.

Haittaohjelma saa tiedot saastuneen koneen järjestelmästä ja konfiguraatiosta API-yhteyden kautta, mikä tekee siitä erittäin vaikean havaita ja poistaa.

Olemme ryhtyneet välittömiin toimenpiteisiin haittaohjelman poistamiseksi ja pyrimme minimoimaan sen aiheuttamat haitat.

Välittömät toimenpiteet:

Kaikki ulkoiset verkkoyhteydet on suljettu.

Etänä on asennettu päivityksiä ja korjauspaketteja kaikkiin työntekijöiden koneisiin.

Seuraavat toimenpiteet:

Tarkistetaan ja päivitetään kaikki järjestelmän turvallisuusprotokollat.

Suoritetaan kattava turvatarkastus kaikilla työasemilla ja palvelimilla.

Pyydämme ulkopuolista tietoturva-asiantuntijaa arvioimaan tilanteen vakavuuden ja suunnittelemaan jatkotoimet.

Ystävällisin terveisin

Peetu Parviainen
Asiantuntija
Palveluntuottaja Oy

Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Valitkaa toimintanne kannalta kriittinen palveluntuottaja (”Palveluntuottaja Oy”) ja peilatkaa harjoituksen tapahtumia sekä niiden vaikutuksia oman organisaationne toimintaan.

Organisaatioon on kohdistunut tekoälyavusteinen haittaohjelmahyökkäys, jonka laajuus ei ole vielä täysin tiedossa. Hyökkäyksen myötä ainakin lukuisia työasemia on saastunut ja tietoa työasemilta on menetetty.

Tapahtuma 4: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Miten organisaatiossanne on määritetty vastuut ja roolit laaja-alaisen häiriötilanteen varalle?
3. Onko vastuuhenkilöille nimetyt ja häiriötilanteen varalle koulutetut varahenkilöt?
4. Kenen vastuulla työntekijöiden verkkoon pääsyn estäminen on? Onko valtuudet määritelty?
5. Onko organisaatiollanne valmis sopimus ulkopuolisen asiantuntija-avun saamiseksi (forensiikka, incident response ja jälkitoimet)? Jos ei, onko tätä varten pohdittu käytäntöjä?
6. Miten palautettujen toimintojen eheys varmistetaan? Onko palautettu data ”aitoa”, eikä sitä ole muunneltu mitenkään?
7. Valmistelkaa lyhyt tilanneraportti johdolle, joka sisältää läpikäynnin tilanteesta, tehdyt ja vaadittavat toimenpiteet sekä vaikutukset lyhyellä (1–2 vrk) ja keskipitkällä (1–3 vko) aikavälillä.

Tapahtuma 4: Lisätehtävät

8. Tiedättekö, kuuluuko organisaationne Kyberturvallisuuskeskuksen tarjoaman toimijoiden väliseen ISAC-tiedonvaihtoryhmään (esim. VIRT)?

9. Olisiko teillä halua liittyä mukaan? Lisätietoa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Tapahtuma 4: Tekniset tehtävät

10. Miten organisaatiossanne havainnoidaan normaalista poikkeavaa verkkoliikennettä?

11. Miten organisaationne työntekijän ja laitteen pääsy verkkoon / organisaation sisäverkkoon estetään?

Tapahtuma 4: Viestintätehtävät

12. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?

13. Mitä tilanteessa voidaan tiedottaa sisäisesti ja ulkoisesti?

14. Mitä välineitä organisaatiolla on käytössä massatiedottamiseen?

15. Onko olemassa varajärjestelmää, jos tavanomaiset viestivälineet eivät ole käytössä?

16. Onko kynnys tiedottamiselle sovittu?

17. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, joka auttaa tilanteesta viestimisessä?

18. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.

19. Luonnostelkaa keskeisimmät viestintämateriaalit.

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

4 Iltapäivän harjoitus (12:30–15:00)

4.1 Tapahtuma 5 – Palvelunestohyökkäys kriittistä palveluntoimittajaa kohtaan

Tapahtuman tausta ja tavoitteet

Kriittinen palveluntuottaja, joka toimittaa ja ylläpitää Organisaation CRM:ää/sähköpostipalveluja/operatiivisia toimintoja/infraa/muuta kriittistä toimintoa on joutunut hajautetun palvelunestohyökkäyksen (DDoS) kohteeksi. Palveluntuottajalla on omien toimintojen ylläpidossa ongelmia, eikä ole vielä havaittu, että hyökkäys vaikuttaisi myös Organisaation toimintoihin. Palvelun toimimattomuus käy ilmi Organisaatiolle vaiheittain syötteiden mukaisesti. Palveluntuottaja ei ole ottanut yhteyttä asian tiimoilta. Organisaatio ei pysty itse suoraan vaikuttamaan ongelmanratkaisuun.

Tapahtuman tavoitteena on nostaa esille kriittisten palveluntuottajien merkitys organisaatioiden toiminnan häiriöttömyydessä ja jatkuvuudessa.

Tapahtuman 5 syötteet

Syöte 1: Sähköposti Organisaation työntekijältä Organisaation tietohallintoon

Lähettäjä: timo.tyontekija@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Palvelussa hitautta

Terve,

Onko muut ilmoittaneet, että Palvelu on käytännössä käyttökelvoton, kun toimii niin hitaasti? Olen käynnistänyt sekä tietokoneeni että Palvelun uudelleen muutamaankin kertaan, mutta sama hitaus jatkuu edelleen. Mitähän tässä pitäisi nyt tehdä, jää tällä menolla kyllä tämän päivän työt tekemättä…

T. Timo T

Timo Työntekijä
timo.tyontekija@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 2: Sähköposti Organisaation työntekijältä (esihenkilö)

Lähettäjä: minni.mallikas@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Palvelu hidastelee

Hei,

Useampi työntekijä ja myös muutama asiakas on ilmoittanut, että Palvelu on toiminut poikkeuksellisen hitaasti koko aamun. Mistä mahtaa olla kyse? Mitä työntekijöiden tulisi tehdä ja mitä voimme viestiä tilanteesta asiakkaille?

Yt. Minni Mallikas

Minni Mallikas
minni.mallikas@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 3: Organisaation sisäinen viestintäkanava:

Ville Virtanen, Työntekijä:
Moi, miten muilla on toiminut Palvelu tänään? Itselläni todella hitaasti… Kenelle tästä pitäisi ilmoittaa?

Syöte 4: Sähköposti Organisaation työntekijältä

Lähettäjä: taina.toimistolainen@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Palvelussa jatkuva häiriö päällä

Hei,

Minulla näkyy Palvelussa toistuvasti virheilmoituksia ”Yhteys aikakatkaistiin” ja ”Sivusto ei ole käytettävissä”. En siis ole käytännössä päässyt töihin käsiksi lainkaan. Mistä tämä johtuu ja milloin tilanteen odotetaan korjaantuvan?

Yt. Taina Toimistolainen

Taina Toimistolainen
taina.toimistolainen@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 5: Sähköposti Organisaation työntekijältä (esihenkilö)

Lähettäjä: minni.mallikas@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: FW: Palvelu pois käytöstä

Hei,
Palvelu ei vastaa nyt enää ollenkaan. Tästä tulee kasvavalla tahdilla minulle ilmoituksia niin työntekijöiltä kuin asiakkailtakin. Osa on huolissaan myös siitä, ovatko tiedot turvassa. Mikä on tilanne selvityksen ja asian korjaantumisen kanssa?

Yt. Minni M

--------*Välitetty viesti alkaa*----------

Lähettäjä: minni.mallikas@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Palvelu hidastelee

Hei,

Useampi työntekijä ja myös muutama asiakas on ilmoittanut, että Palvelu on toiminut poikkeuksellisen hitaasti koko aamun. Mistä mahtaa olla kyse? Mitä työntekijöiden tulisi tehdä ja mitä voimme viestiä tilanteesta asiakkaille?

Yt. Minni Mallikas

Minni Mallikas
minni.mallikas@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 6: Quacker: @maikki

Organisaation Palvelu jumittaa pahanpäiväisesti! Onkohan siellä mitään tietoja jäljellä kun seuraavan kerran pääsee kirjautumaan… Onko muilla ollut samaa ongelmaa?

Syöte 7: Quacker: @justus

@Organisaatio, mistä on kyse, kun teidän Palvelunne ei toimi? Oletteko kenties kyberhyökkäyksen kohteena?

Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Valitkaa toimintanne kannalta kriittinen /tietojärjestelmä/palvelu (”Palvelu”) ja peilatkaa harjoituksen tapahtumia sekä niiden vaikutuksia oman organisaationne toimintaan.

Organisaation kriittinen palveluntuottaja on joutunut hajautetun palvelunestohyökkäyksen (DDoS) kohteeksi.

Tapahtuma 5: Tehtävät

1. Miten organisaation on järjestänyt palveluntarjoajan kanssa poikkeamanhallintaprosessin – huomioiko tämä myös kriisitilanteet? Onko 24/7-yhteyspistettä ja käytänteitä sovittu palveluntarjoajan kanssa kriisitilanteita varten? Kuinka nopeasti saadaan koolle ensimmäinen kriisinhallintapalaveri palveluntarjoajan kanssa?
2. Onko organisaatiolla häiriönhallintasuunnitelmaa?
3. Mitä toimia voidaan tehdä ja miten omaa toimintaa priorisoidaan?
4. Onko organisaatiolla jatkuvuussuunnitelmaa, joka varmistaa kriittiset toiminnot häiriöstä huolimatta?
5. Kuka ottaa ”pallon vastaan” ja lähtee selvittämään tilannetta? Kuka tekee vaikutusten arvioinnin?
6. Dokumentoidaanko tapahtumat/toimenpiteet/päätökset?

Tapahtuma 5: Lisätehtävät

7. Miten kommunikointi on järjestetty? Ovatko yhteystiedot ajan tasalla palveluntarjoajan suuntaan, kuka reagoi palveluntarjoajan puolella? Kenelle palveluntarjoaja raportoi tilanteesta, millä tavoin, millä syklillä?
8. Kuuluuko häiriönhallintasuunnitelmaan ”lessons learnt” -osuus? Jaetaanko tämä tieto, jotta organisaatio oppisi reagoimaan jatkossa paremmin?
9. Kenellä on mahdollisuus havaita hyökkäys ja mihin hänen tulisi siitä ilmoittaa?
10. Onko organisaatiolla varajärjestelmää, johon liikenne voidaan ohjata?

Tapahtuma 5: Viestintätehtävät

11. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
12. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, joka auttaa tilanteesta viestimisessä?
13. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.
14. Luonnostelkaa keskeisimmät viestintämateriaalit.

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

4.2 Tapahtuma 6 – Tietojen luvaton katselu

Tapahtuman tausta ja tavoitteet

Organisaation työntekijä jää kiinni luvattomasta tietojen katselusta. Hän on selannut tietoja, joihin hänellä ei olisi oikeutta työtehtäviensä puolesta. Työntekijä on päässyt käsiksi ja käynyt läpi arkaluontoisia tietoja (Organisaatio valitsee itselleen sopivat henkilö-, palkka- tai NDA:n eli salassapitosopimuksen alaiset tiedot.)

Tapahtumassa osallistujat pohtivat teemoja, jotka liittyvät tietoturvaan, käyttäjän käyttöoikeuksien hallintaan ja tietosuojaan. Heidän on arvioitava organisaation tietoturvakäytäntöjä, millaisia tietoja organisaatiossa käsitellään, miten tiedot on turvattu kriittisissä järjestelmissä, tunnistettava mahdolliset heikkoudet ja mietittävä, kuinka ne voidaan korjata. Tämän lisäksi heidän on pohdittava tilanteen oikeudellisia aspekteja ja eettisen toiminnan edistämistä organisaatiossa.

Tapahtuma herättää monia kysymyksiä ja haasteita. Kuinka tällainen pääsy oli mahdollista? Onko organisaation tietoturva riittävä? Mitä toimenpiteitä tilanne edellyttää? Mitä ja kenelle tilanteessa tulisi viestiä?

Tapahtuman 6 syötteet

Syöte 1: Organisaation esihenkilö soittaa Organisaation tietoturvasta vastaavalle henkilölle **(nauhoite)**

Käynnistä puhelu play-painikkeesta. Videon saat koko ruudun näkymään, kun klikkaat oikeasta alareunasta.
---------- Puhelun sisältö tekstinä ----------

Tietoturvavastaava: Tietoturvapäällikkö Makkonen.
Organisaation esihenkilö: Täällä on Organisaation esihenkilö Essi Niementaka, soittelen sellaisella asialla, että sain juuri tietoa tiimiläiseltäni, joka epäilee, että toinen asiantuntija minun tiimistäni on selannut luvattomasti tietoja, jotka eivät kuulu hänen työtehtäväänsä. En ole vielä jutellut asiasta hänen kanssaan. Mitenhän tämän tilanteen kanssa pitäisi edetä, minulle ei ole ennen tällaista tilannetta tullut eteen?
Tietoturvavastaava: Ok, hyvä, että ilmoitit minulle. Onko sinulla tietoa siitä, miten isosta tietoaineistosta on kyse ja kuinka kauan tietojen luvaton katselu on jatkunut?

Organisaation esihenkilö: Valitettavasti minulla ei ole muuta tietoa. Onko meillä olemassa ohjeistusta tai toimintamallia tällaiseen tilanteeseen? Tuleeko tästä tehdä ilmoitusta asiakkaalle tai viranomaiselle?
Tietoturvavastaava: Käy täyttämässä tietoturvapoikkeamailmoitus, jotta saamme tarkemmat tiedot tapauksesta. Me hoidamme asiaa siitä eteenpäin. Kiitos ilmoituksesta.

Syöte 2: Sähköpostiviesti Organisaation tietohallinnolta / kyseisen palvelun ylläpitäjältä tietoturvavastaavalle

Lähettäjä: tietohallinto@organisaatio.fi / yllapito@palveluntuottaja.fi
Vastaanottaja tietoturvavastaava@organisaatio.fi
Aihe: VS: Kysely käyttäjän lokitiedoista

Hei

Pahoittelut vastauksen viipymisestä. Tarkistimme prosessin mukaisesti oikeutenne lokitietojen pyytämiseen.

Tukipyyntö: Käyttäjän Urho Utelias lokitiedot viimeisen vuoden ajalta.

Järjestelmän lokeista käy ilmi, että kyseinen työntekijä on selannut järjestelmän tietoja viimeisen vuoden aikana 37 kertaa ja ajallisesti noin kymmenen tunnin ajan. Hänellä on ollut järjestelmän käyttöhallinnassa pääsy kyseisiin tietoihin.

Terveisin

Organisaation tietohallinto / Järjestelmän ylläpito

Syöte 3: Sähköpostiviesti Organisaation työntekijä Urho Uteliaalta Organisaation tietoturvasta vastaavalle

Lähettäjä: urho.utelias@organisaatio.fi
Vastaanottaja tietoturvavastaava@organisaatio.fi
Aihe: Minuun kohdistetut epäilyt

Hei
Olen kuullut huhuja, että minua epäillään tietojen luvattomasta katselusta. Pitääkö tämä tieto paikkansa? Miksi minuun ei olla oltu suoraan yhteyksissä asiaan liittyen? Väite tietojen luvattomasta katselusta ei tietenkään missään nimessä pidä paikkaansa! Minullehan on myönnetty laajat käyttöoikeudet, ja sitä myötä mahdollisuus tietojen katsomiseen. Minulle ei ole missään vaiheessa kerrottu, ettei joitain tietoja saisi katsoa. Lisäksi, vaikka kaikkia työaikana katselemiani tietoja en suoranaisesti

tarvinnut omissa työtehtävissäni, niin niiden selaamisesta on ollut minulle selvää hyötyä työtehtävieni suorittamisessa, ja olen kehittynyt ammatillisesti.

Mikäli en olisi saanut katsella näitä tietoja, niin toivoisin jatkossa, että näihin asioihin perehdytetään kunnolla, annetaan jatkuvaa koulutusta, annetaan kirjalliset ohjeet ja tarvittaessa rajataan teknisesti pääsy sellaisiin dokumentteihin, mihin meidän ei tulisi mennä. Kiitos!

Terveisin: Urho Utelias, Organisaatio

Urho Utelias
urho.utelias@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 4: Quacker: @UrhoUtelias (työntekijä Organisaatiossa)

Sain tänään kuulla epävirallisia kanavia pitkin, että työnantajani epäilee minua tietojen luvattomasta katselusta. Tämä on täysin perätön ja pöyristyttävä väite! Lukekaa asiasta tarkemmin Iltasen uutisesta. #Organisaatio #syyton #Iltanen

Syöte 5: Verkkouutinen: Iltanen: JUURI NYT: Organisaatiossa epäilys tietojen laajasta luvattomasta katselusta.

Toimituksemme haastatteli Organisaation tutkinnan kohteena olevaa työntekijää, jota epäillään laajasta tietojen luvattomasta katselusta. Työntekijän mukaan hänellä on ollut hyvin vapaa ja laaja pääsy Organisaation tietoihin. Hän ei halua esiintyä jutussamme omalla nimellään. Käytämme hänestä nimimerkkiä Urhea.

Urhea kertoo saaneensa työkaveriltaan tiedon, että hänen toimintaansa on aloitettu tutkimaan. ”Tieto tästä tuli minulle tietenkin järkytyksenä. Olen Organisaationi ahkerimpia työntekijöitä, eikä minua ole tätä ennen epäilty mistään. Olen ollut varsinainen mallityöntekijä ja aina valmis joustamaan, jos on ollut tarvetta”, Urhea aloittaa, “Organisaatiossamme ei ole tietääkseni virallisia ohjeita siitä, mitä tietoja kukin työntekijä voi työtehtävissään hyödyntää, joten olen ollut oikeutettu melko laajaan tietomäärään. Tätä tietoa olen myös hyödyntänyt työtehtävissäni ja kehittäessäni itseäni ammatillisesti. Nyt tämä epävarmuus ja epäily ovat saaneet sen aikaan, että olen joutunut jäämään sairauslomalle. Katsotaan, miten tilanne etenee”, Urhea toteaa uupuneen oloisena. “Toivoisin vain, että tämä olisi ohi ja pääsisin jatkamaan normaalia arkeani.”

Syöte 6: Sähköposti kansalaiselta Organisaation johtajalle

Lähettäjä: antti.nieminen@kansalainen.gmail.com
Vastaanottaja mirja.mottonen@organisaatio.fi
Aihe: Somekeskusteluun liittyen

Hei,
Huomasin, että teidän organisaatiosta kirjoitellaan somessa. Pitääkö paikkansa, että teillä tietojen luokittelu ja pääsynhallinta ei ole kunnossa ja ohjeistuksessa on puutteita?

Haluaisin välittömästi tietää, miten teidän hallussa olevia minuun liittyviä tietoja säilytetään, kenellä on niihin pääsy ja onko tietojani päätynyt vääriin käsiin. Mitä toimia olette käynnistäneet tilanteen hoitamiseksi?

Haluaisin vastaukset mielellään kirjallisena ja mahdollisimman pian. Kiitos!

Antti Nieminen
antti.nieminen@kansalainen.gmail.com

Tehtävät

Taisto-harjoituksessa ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Valitkaa toimintanne kannalta sopivat arkaluonteiset tiedot, esimerkiksi henkilö-, palkka- tai NDA:n eli salassapitosopimuksen alaiset tiedot, ja peilatkaa harjoituksen tapahtumia sekä niiden vaikutuksia oman organisaationne toimintaan.

Organisaation työntekijä on selannut tietoja, joihin hänellä ei ole oikeutta työtehtäviensä puolesta.

Tapahtuma 6: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Onko organisaatiollanne kyky havaita tietojen luvatonta katselua?
3. Miten luvatonta katselua havainnoidaan?
4. Millaisia ohjeita organisaatiollanne on luvattomaan tiedon katseluun liittyen?
5. Miten varmistatte, että työntekijänne toimivat eettisesti ja tietävät ohjeiden tärkeyden?
6. Onko organisaatiollanne olemassa prosessi lokitietojen pyytämiseen? Onko prosessi kuvattu kirjallisesti? Kuka saa pyytää lokitietoja ja mitä tietoja voidaan pyytää? Miten ja missä formaatissa pyynnön vastine toimitetaan ja kenelle?

Tapahtuma 6: Lisätehtävät

7. Onko organisaatiossanne prosessia tietoturvapoikkeamien ilmoittamiseen ja käsittelyyn?
8. Onko organisaatiossanne käsiteltävää tietoa luokiteltu luottamuksellisuuden ja jakelun mukaan?
9. Miten organisaatiossanne käsitellään tilannetta, jossa työntekijä syyllistyy väärinkäytökseen?

Tapahtuma 6: Viestintätehtävät

10. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
11. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, joka auttaa tilanteesta viestimisessä?
12. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.
13. Luonnostelkaa keskeisimmät viestintämateriaalit.
14. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

4.3 Tapahtuma 7 – Hybridiuhka-tapahtuma: ”Epävarmuuden Aikakausi”

Tapahtuman tausta ja tavoitteet

Epävarmuuden aikakausi on tapahtuma, jossa toimija ”X” pyrkii heikentämään organisaation päätöksentekoa, yhteistyötä ja luottamusta. ”X” on monitahoinen toimija, jolla on poikkeukselliset resurssit, laaja tiedustelukyvykkyys ja mahdollisuudet vaikuttaa monilla eri tasoilla. Organisaatiolla on liittymäpinta valtion tasolla merkittävään sopimukseen tai hankkeeseen, minkä myötä Organisaation merkitys ja näkyvyys ovat kasvaneet. ”X” alkaa toteuttaa strategiaansa keskittämällä vaikuttamisen eri kanaviin. Toimija kaappaa Organisaation somekanavat ja levittää sinne arkaluonteista tietoa, joka ei ole yhteneväistä organisaation arvojen kanssa. Organisaation sometili suljetaan käyttöehtojen vastaisen päivityksen myötä. Hyökkäykset kohdistuvat eri alueille samanaikaisesti ja pyrkivät sekoittamaan viestin vastaanottajaa.

Tapahtuman tavoitteena on tuoda esille se, miten väärän tiedon levittämistä voidaan käyttää hybridivaikuttamisen keinona.

Tapahtuman 7 syötteet

Syöte 1: Quacker: @Tiina

Mitä ihmettä Organisaatio ajatteli twiitillään? Jos yrität olla hauska ja provosoiva, varmista, että se on myös asiallista. #somemoka #2020-luvulla #ei_näin

Syöte 2: Quacker: @Peksi

Organisaatio, jos olet sanonut jotain ajattelematonta somessa, oikea reaktio on pyytää anteeksi, ei poistaa koko tiliä. #vastuunotto #Viestintäkoulutus

Syöte 3: Quacker: @Kaisuli

Joku voisi kertoa Organisaation markkinointiosastoille, että ei ole hyvä idea käyttää tragedioita mainostamiseen. #epäkunnioittavaa #huono_yritys

Syöte 4: Quacker: @Julle

Vinkki Organisaatiolle: Sosiaalinen media ei ole paikka purkaa omia sisäisiä ongelmianne. 🤦‍♂️🔑 #epäammattimaista #harkintakyky

Syöte 5: Sähköposti Quackerin ylläpidolta Organisaatiolle

Lähettäjä: yllapito@quacker.fi
Vastaanottaja: viestinta@organisaatio.fi
Aihe: Quacker-tilinne on asetettu 30 päivän määräaikaiseen käyttökieltoon
---

Arvoisa [Organisaation nimi] -tilin hallinnoija,

Tämä viesti on lähetetty teille virallisen protokollan mukaisesti ilmoittaaksemme, että Quacker-tilinne [@organisaation_tilin_nimi] on asetettu määräaikaiseen käyttökieltoon. Tämä käyttökielto kestää 30 päivää, alkaen tästä päivästä. Käyttökielto johtuu tilillänne havaituista käyttöehtojen rikkomuksista.

Nämä rikkomukset ovat sellaisia, jotka vaarantavat muiden käyttäjien turvallisuuden ja käyttökokemuksen Quacker-palvelussa. Voitte tutustua tarkemmin rikkomuksiin ja niiden vakavuuteen Quackerin käyttöehtojen dokumentista, joka on saatavilla osoitteessa [Quackerin käyttöehdot].

Teidän on suoritettava seuraavat toimenpiteet:

1 Käykää huolellisesti läpi Quackerin käyttöehdot ja varmistakaa, että ymmärrätte ne kokonaisuudessaan.

2 Suorittakaa kaikki tarvittavat korjaavat toimenpiteet tilinne palauttamiseksi käyttöehtojen mukaisesti.
3 Varmistakaa, että kaikki tilillänne käyttöoikeudet omaavat henkilöt ovat tietoisia ja ymmärtävät Quackerin käyttöehtojen sisällön ja merkityksen.

Käyttökieltonne päättyy automaattisesti 30 päivän kuluttua. Mikäli teette laajan selvityksen toimenpiteistä, jotka olette toteuttaneet käyttöehtojen noudattamiseksi ja toimitatte sen meille kirjallisesti, käyttökielto saattaa päättyä aikaisemmin. Tämän kirjallisen vahvistuksen tulee olla peräisin tilinne viralliselta hallinnoijalta ja se tulee toimittaa meille sähköpostitse osoitteeseen [tukisähköposti].

Olemme sitoutuneet ylläpitämään Quacker-yhteisössä turvallista ja positiivista ilmapiiriä. Tämä edellyttää kaikkien käyttäjien, mukaan lukien yritysten ja organisaatioiden, noudattavan palvelun käyttöehtoja.

Jos teillä on kysyttävää tai tarvitsette lisätietoja, pyydämme teitä ottamaan meihin yhteyttä välittömästi.

Kunnioittavasti,

Quackerin Ylläpidon Tiimi

Syöte 6: Iltanen: Kohu Quackerissa: Organisaatio syyllistynyt sopimattomaan käyttäytymiseen?

Sosiaalisessa mediassa leviää parhaillaan kiivaasti keskustelu Organisaation Quacker-toiminnasta, joka rikkoo selvästi palvelun käyttöehtoja. Organisaation johtoa ei ole saatu kiinni kommentoimaan asiaa.

Viime päivinä on noussut esille kohu, joka koskee Organisaation toimintaa viestipalvelu Quackerissa. Yrityksen tililtä on lähetetty viestejä, jotka ovat aiheuttaneet suurta hämmennystä ja suuttumusta.

Organisaation tililtä on tullut useita epäasiallisia ja sopimattomia viestejä, jotka ovat saaneet käyttäjät kyseenalaistamaan yrityksen eettiset periaatteet ja ammattitaidon. Kyseiset viestit ovat herättäneet paljon huomiota ja monet käyttäjät ovat jakaneet niitä edelleen. Tämä on johtanut siihen, että organisaation maine on saanut kolhuja.

Organisaation johto ei ole kommentoinut asiaa julkisesti. Tämä on aiheuttanut lisää närää, ja monet ovat alkaneet vaatia Organisaatiolta vastuullisempaa toimintaa julkisessa keskustelussa.

Tilanne on entistä epäselvempi, sillä Organisaation tiliä ei enää löydy. Pakoileeko Organisaatio vastuutaan poistamalla tilinsä? Olemme yrittäneet saada Organisaation johtoa kiinni kommentoimaan asiaa, mutta toistaiseksi he eivät ole vastanneet yhteydenottoihimme.

Sosiaalisessa mediassa leviää parhaillaan useita keskusteluja ja mielipidekirjoituksia, jotka vaativat organisaatiota ottamaan vastuun teoistaan. Monet asiantuntijat ovat kommentoineet, että Organisaation olisi viisasta reagoida nopeasti kohuun, jotta sen maine ei kärsisi enempää.

Syöte 7: Quacker: @JouniJohtaja / Organisaatio

Henkilökuntamme ei tarvitse työsuhde-etuja. Heidän pitäisi olla kiitollisia, että heillä on työpaikka. #NoBenefits

Syöte 8: Quacker: @HennaHenkilöstöjohtaja / Organisaatio

Julkaisemme pian työntekijöidemme palkkatiedot, jotta näette, kuka on meille arvokkain. #Transparency

Syöte 9: Quacker: @TiinaTietohallintojohtaja / Organisaatio

Tietosuoja on harhaa. Kaikkien tiedot ovat julkista omaisuutta.
#PrivacyIsDead #Dataismi #Olet_Algoritmi

Syöte 10: Quacker-video: "Tätä Organisaatio ei halua sinun tietävän"

Video näyttää salaa kuvattuja klippejä johtajan epäeettisestä käytöksestä, kuten huutamisesta työntekijöille.

Käynnistä video play-painikkeesta. Videon saat koko ruudun näkymään, kun klikkaat oikeasta alareunasta.

Tehtävät

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

Organisaation sosiaalisen median tili on kaapattu. Hyökkääjä on julkaissut kaappaamallaan tilillä alustan käyttöehtojen vastaista sisältöä, ja sosiaalisen median tili on asetettu määräaikaiseen käyttökieltoon. Sosiaalisessa mediassa leviää Organisaation nimissä sen kannalta haitallisia lausuntoja, ja video näyttää salaa kuvattuja klippejä johtajan epäeettisestä käytöksestä.

Tapahtuma 7: Tehtävät

1. Millaisia toimenpiteitä tilanne edellyttää?
2. Kuka on vastuussa organisaationne sosiaalisen median tileistä?
3. Miten organisaatiossanne hallinnoidaan sosiaalisen median tilejä?
4. Miten käsittelette oikeuksia ja pääsyä tileihin?
5. Miten toimitte oikeuksien kanssa, kun henkilöstössä tapahtuu muutoksia?
6. Onko organisaatiollanne ohjeet tilanteeseen, jossa sosiaalisen median tilinne kaapataan?
7. Käytetäänkö organisaatiossanne kaksivaiheista tunnistautumista sosiaalisen median tileissä?

Tapahtuma 7: Lisätehtävät

8. Kuinka organisaatio tunnistaa ja vastaa disinformaatioon ja vääristeltyyn tietoon, joka liittyy organisaation päätöksiin ja toimintaan?
9. Millä menettelytavoilla organisaatio varmistaa tiedon oikeellisuuden ja läpinäkyvyyden toiminnassaan ja viestinnässään?
10. Kuinka organisaationne seuraa ja analysoi sosiaalisen median kanavissa levitettävää tietoa ja sen vaikutusta julkiseen mielipiteeseen?
11. Miten organisaatio ylläpitää ja vahvistaa suhteitaan sidosryhmiin varmistaen, että nämä saavat oikeaa ja ajantasaista tietoa?

Tapahtuma 7: Viestintätehtävät

12. Minkälaista kriisiviestintästrategiaa organisaatio noudattaa, ja kuinka usein tätä strategiaa arvioidaan ja päivitetään?
13. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
14. Mitä viestintäkanavia tilanteessa voisi käyttää?
15. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?
16. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.
17. Luonnostelkaa keskeisimmät viestintämateriaalit.
18. Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa.

4.4 Tapahtuma 8: Tekoälypohjaisten työkalujen käyttö

Tapahtuman tausta ja tavoitteet

Ulkoinen palveluntuottaja on päivittämässä Organisaation verkkosivuja. Palveluntuottaja tiedustelee, voidaanko tekoälyä käyttää verkkosivujen kehittämisessä ja saa tähän Organisaation suostumuksen. Verkkosivujen julkaisemisen jälkeen alkaa ilmetä

erilaisia ongelmia, ja pian Organisaatioon ollaan yhteydessä verkkosivuilla leviävän väärän tiedon ja mahdollisten tekijänoikeusrikkomusten vuoksi. Tavoitteena on herätellä ajatuksia hankintojen/muutostöiden tietoturva-asioista sekä uusien tekoälypohjaisten työkalujen riskeistä.

Tapahtuman 8 syötteet

Syöte 1: Tilannetieto

Organisaationne verkkosivu-uudistus on saatu valmiiksi ja verkkosivut on otettu käyttöön.

Syöte 2: Sähköposti Palveluntuottaja Oy:lta Organisaation tietohallintojohtajalle

Lähettäjä: micce.muupuro@palveluntuottaja.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Tilannetietoa verkkosivu-uudistuksesta

Hei,

Kuten sovimme teidän verkkosivujen uudistusta käsittelevässä palaverissa viime viikolla, niin voimme hyödyntää tekoälypalveluita ohjelmakoodin tuottamisessa. Tämä mahdollistaa tehokkaamman toteutuksen, sekä aikataulun että kustannusten suhteen.

Olemmekin jo edenneet huimaa vauhtia ja meillä on pian teille näytettävää demosivujen muodossa. Testaamme parhaillaan luomaamme täysin uudistettua verkkosivun ulkoasua ja moderneja verkkosivun toiminnollisuuksia. Tulette varmasti yllättymään positiivisesti!

Palaverissa jäi vielä kysymättä, että kuinka tiukkoja olette tiedon siirtämisestä EU/ETA-alueen ulkopuoliseen valtioon?

Yt. Micce

Micce Muupuro
micce.muupuro@palveluntuottaja.fi
Taiteellinen johtaja / CEO, Palveluntuottaja Oy

Syöte 3: Sähköposti Organisaation asiantuntijalta tietohallinnolle

Lähettäjä: atte.asiantuntija@organisaatio.fi
Vastaanottaja: tietohallinto@organisaatio.fi
Aihe: Verkkosivujen sisällöissä outouksia

Moikka!

Katsoin noita meidän verkkosivuja, kun yksi tuttu vinkkasi, että siellä on ihan outoa tietoja näkyvillä. Näyttäisi siltä, että suomenkieliset sisällöt vaihtuvat sisällöltään ihan erilaiseksi, jos valitsee jonkin muun kielen, esimerkiksi ruotsin.

Olin verkkosivu-uudistusprojektissa mukana ja muistelen, että tämä kieliversiointi toteutettiin hiljattain tekoälypohjaisella automaattiratkaisulla, jossa käyttäjä voi valita lähes minkä tahansa kielen käyttöön sivulla. Nyt siellä tulee tosiaan aika asiatontakin sisältöä näkyviin.

Pitäisi varmaan ottaa nuo käännökset pikaisesti pois päältä?

T: Atte

Atte Asiantuntija
atte.asiantuntija@organisaatio.fi
Asiantuntija
Organisaatio

Syöte 5: @Lotte_Järvinen

Was zum Teufel, @Organisation? Eure Webseite informiert ziemlich seltsam.. (suomeksi: Mitä ihmettä, @Organisaatio? Verkkosivuillanne tiedotetaan aika erikoisesti..)

Syöte 6: @Kieliniekka

Mitäs ihmettä @Organisaatio? Onpas luokattomasti käännetyt nettisivut. Eihän näissä käännöksissä ole mitään järkeä.

Syöte 7: Sähköposti asianajotoimistolta Organisaation lakiosastolle

Lähettäjä: alina@lawpartners.fi
Vastaanottaja: lakiosasto@organisaatio.fi
Aihe: Tekijänoikeuksista

Hei,

Edustan lakitoimisto Lawpartnersia ja asiakkaanamme toimii kansainvälisesti tunnettu graafikko, herra Maximilian von Grafenberg. Olemme huomanneet, että verkkosivuillanne oleva logo näyttää merkittävästi samankaltaiselta kuin herra von Grafenbergin aikaisemmin luoma teos.

Tekijänoikeuslain (404/1961) 2 §:n mukaan teoksen tekijällä on yksinoikeus teokseensa. Näin ollen kyseessä voi olla tekijänoikeusrikkomus, joka voi johtaa korvausvastuuseen.

Pyydämme teitä välittömästi tarkistamaan mainitun logon ja vertaamaan sitä herra von Grafenbergin teokseen. Mikäli havaitsette yhtäläisyyksiä, suosittelemme välittömästi poistamaan kyseisen logon ja informoimaan asiasta julkisesti välttääksenne mahdolliset oikeudelliset seuraamukset.

Odotan vastaustanne mahdollisimman pian ja toivon, että voimme ratkaista asian yhteisymmärryksessä.

Ystävällisin terveisin,

Alina Kivimäki
alina@lawpartners.fi
Asianajaja
Lawpartners Oy

Tehtävät

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

Organisaationne verkkosivut ja visuaalinen ilme on uudistettu tekoälyä hyödyntäen. Verkkosivujen julkaisun jälkeen paljastuu, että käännöksissä on vakavia virheitä ja visuaalisen ilmeen tekijänoikeuksiin liittyy epäselvyyksiä.

Tapahtuma 8: Tehtävät

1. Mitä toimenpiteitä tilanne edellyttää?

2. Miten vastaatte Palveluntuottajan esittämään kysymykseen tietojen siirtämisestä EU/ETA-alueen ulkopuoliseen valtioon? Miten perustelette vastauksenne?

3. Onko tietoturvaan ja tekoälyyn liittyviä teemoja pohdittu hankintoihin tai muihin palveluntuottajien kanssa yhteistyössä tehtäviin projekteihin liittyen?

4. Onko tekijänoikeus- /immateriaalioikeusasioihin liittyvät ongelmatilanteet, ja niihin liittyvät vastuukysymykset selvillä organisaatiossanne?

Tapahtuma 8: Lisätehtävät

5. Onko teillä käytössä tai suunnitelmissa ottaa käyttöön tekoälypohjaisia kielikäännösratkaisuja, ja miten takaatte tiedon luotettavuuden niissä (esim. verkkosivujen kieliversiointi automatisoidusti tekoälyllä)? Miten mahdollisen virheellisen tiedon leviäminen on otettu huomioon näissä ratkaisuissa?

6. Hyödynnättekö tekoälyä sisällöntuotannossa? Ovatko näiden työkalujen tekijänoikeuksiin ja vastuukysymyksiin liittyvät seikat selvillä ja huomioitu?

Tapahtuma 8: Viestintätehtävät

7. Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?

8. Onko käytössänne valmiita mallipohjia tai muuta materiaalia, jotka auttavat tilanteesta viestimisessä?

9. Kirjatkaa keskeiset viestinnälliset toimenpiteet ja linjaukset.

10. Luonnostelkaa keskeisimmät viestintämateriaalit.

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

[Yksikkö] / Lankinen Anna

18.12.2023

Liite 1 [Kirjoita liitteen otsikko. Tyyli: Otsikko 9]

ÄLÄ POISTA TÄTÄ SIVUA!