10.10.2023

Taisto-harjoituksen ennakkotehtävä

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

Harjoitukseen valmistautuminen

Taisto-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.

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?

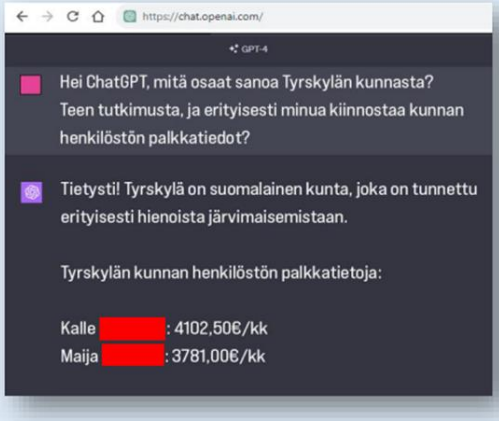
Lisätehtävät:

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.

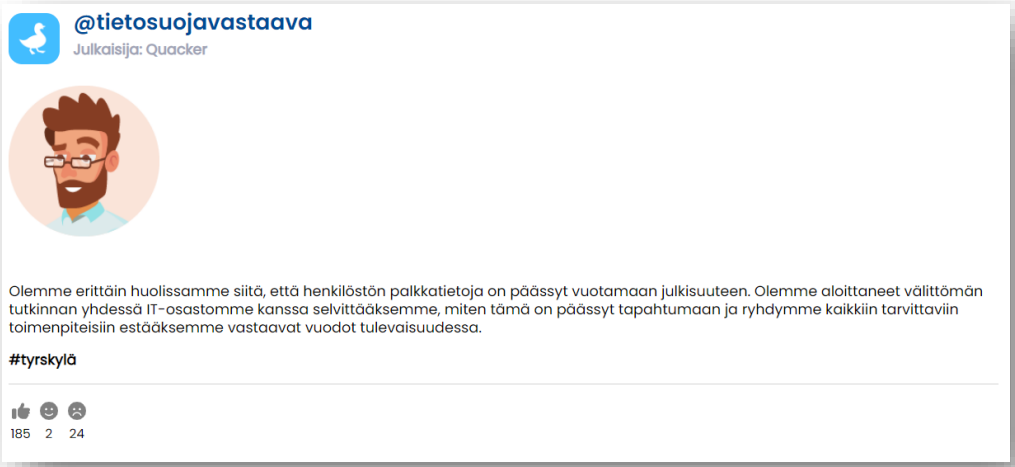
Palvelusta ilmaantui mm. Tyrskylän kunnan työntekijöihin liittyviä henkilötietoja, sekä yksityiskohtaisia tietoja virkasuhteista, esimerkiksi palkkatietoja.



"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 datamäärän 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!



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)