DIGI- JA VÄESTÖTIETO-VIRASTO

Taisto-harjoitus 2025

Käsikirjoitus

16.12.2025

Puh. **0295 536 000** (vaihde) | Yhteystiedot: **dvv.fi**

Sisällysluettelo

Taisto-harjoitus 2025

Tämä asiakirja sisältää vuoden 2025 Taisto-harjoituksen käsikirjoituksen tehtäväkokonaisuuksineen.

1 Ennakkotehtävä

1.1 Kyberturvallisuuslaki ja organisaation valmius

Ennakkotehtävän tarkoituksena on tukea organisaatiotanne valmistautumaan Taisto-harjoitukseen ja auttaa rakentamaan osaamistanne kyberturvallisuuslakiin liittyen. Ennakkotehtävä on vapaaehtoinen. Suosittelemme, että jokainen organisaatio käy ennakkotehtävän läpi organisaation sisällä ennen harjoitusta. Ennakkotehtävässä on otettu huomioon myös ne organisaatiot, jotka eivät ole kyberturvallisuuslain piirissä. Digi- ja väestötietovirasto ei kerää ennakkotehtävän vastauksia.

Taisto-harjoituksen ennakkotehtävässä ”Organisaatio” tarkoittaa harjoitukseen osallistuvaa organisaatiota. Peilatkaa ennakkotehtävän tapahtumaa ja sen vaikutusta oman organisaationne toimintaan.

Jokainen harjoitus on sijoitus turvallisempaan arkeen ja se rakentaa myös laajemmin luottamusta meidän digitaaliseen yhteiskuntaan. Kun opimme tunnistamaan ja hallitsemaan häiriöitä sekä tekemään yhteistyötä yli organisaatiorajojen, rakennamme samalla koko Suomen kyberresilienssiä.

Taisto ei ole vain harjoitus, vaan se on askel kohti vahvempaa, varautunutta ja entistäkin kriisinkestävää digiyhteiskuntaa.

Tavoite

Ennakkotehtävä tukee organisaationne valmistautumista Taisto-harjoitukseen, sekä lisää kyber- ja digiturvavalmiuttanne. Huom. Suosittelemme ennakkotehtävän tekemistä, vaikka organisaationne ei ole kyberturvallisuuslain piirissä.

1.2 Taisto-harjoituksen ennakkotehtävät: Tehtävä 1

Perehtykää organisaationne sisällä kyberturvallisuuslakiin sekä Kyberturvallisuuskeskuksen julkaisemaan tietopakettiin “Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2)”. Sivulta löydät tietoa muun muassa siitä, keitä NIS2-direktiivi koskee ja millaisia vaatimuksia direktiivi asettaa.

1. Käykää tutustumassa Kyberturvallisuuslakiin.
2. Käykää tutustumassa Kyberturvallisuuskeskuksen infopakettiin Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2).
3. Pohtikaa yllä olevien materiaalien pohjalta:

- Kyberturvallisuuslain toisen luvun 9 §:ssä on listattu 12 hallintatoimenpidettä.

- Mitkä hallintatoimenpiteet (1-3kpl) organisaatiollanne on kunnossa?
- Mihin hallintatoimenpiteisiin (1-3kpl) organisaationne tulisi kiinnittää huomiota?
- Keskustelkaa, millaisia kehittämiskohteita nousi esille.
- Pohtikaa, miten tunnistetut kehitystoimet saadaan käytäntöön.

Lisätehtävät:

- Laatikaa yhteenveto ja tiivis toimintasuunnitelma tunnistetuista kehitystoimista.
- Nimetkää kehitystoimille vastuuhenkilö(t) ja aikataulu.

Keskustelkaa ja tunnistakaa seuraavat asiat:

- Organisaationne kriittiset toiminnot ja palvelut, joiden häiriötilanne vaikuttaisi merkittävästi toimintaanne.
- Onko organisaatio kattavasti selvittänyt, mitä henkilötietoja sen palveluissa kerätään sekä millaisiin kohderyhmiin nämä tiedot liittyvät (esimerkiksi alaikäisten henkilötiedot)?
- Oleelliset yhteistyötahot ja viestintäkanavat, joita tarvitaan kriisitilanteen hallinnassa ja tilannekuvan muodostamisessa.

1.3 Taisto-harjoituksen ennakkotehtävät: Tehtävä 2

Katsokaa Yleismedian uutislähetys ja käykää videoon liittyvät tehtävät läpi. Uutislähetys julkaistaan elokuun lopussa.

- Miten havaitsette poikkeamia
  - omissa järjestelmissänne
  - toimittajienne järjestelmissä?
- Onko toimittajien kanssa sovittu kirjallisesti ilmoitusprosessista, kun toimittaja havaitsee poikkeaman ympäristössään/järjestelmässään?
- Onko organisaatiolla valmius ottaa vastaan ja käsitellä ilmoituksia esimerkiksi virka-ajan ulkopuolella?
- Onko organisaatiollanne olemassa prosessi viranomaisilmoituksien tekemiseen kyberturvallisuuslain vaatimuksiin liittyvissä poikkeamatilanteissa?
- Onko prosessia harjoiteltu?

- Tutustu oheiseen NIS2-poikkeamailmoituslomakeeseen. Lomaketta kannattaa harjoitella täyttämään oheisen uutisen mukaisten tietojen perusteella. Taisto ennakkotehtävä NIS harjoituslomake.
- Mikäli paljastuisi, että organisaatiossanne olisi laiminlyöty ilmoitusvelvollisuutta, miten tulisi toimia?

1.4 Taisto-harjoituksen ennakkotehtävät: Tehtävä 3 - Viestintä

Viestintätehtävät: Sanomat Uudeltamaalta -lehden toimittajan yhteydenotto

Kuvitelkaa uutislähetyksen kaltainen tilanne, jossa organisaatiotanne epäillään kyberturvallisuuslain laiminlyönneistä. Tällä hetkellä on tiedossa jokin poikkeama, mutta sisäinen selvitystyö on vasta käynnissä. Faktatietona on, että joitain organisaatiostanne väitetysti peräisin olevia tietoja on jaettu verkossa, tarkkaa tietoa ei vielä ole laajuudesta. Asiantuntijanne ovat kuitenkin vahvistaneet, että kyseessä on todennäköisesti tietovuoto.

Organisaationne viestintään ottaa yhteyttä toimittaja Sanomat Uudeltamaalta -lehdestä. Toimittaja esittää teille seuraavat kysymykset:

- Onko organisaatiollanne käynnissä tietoturvaloukkaustapahtuma?
- Voitteko kertoa, mikä on oletettu tapahtumien kulku ja onko mahdollisesta hyökkääjästä tietoa?
- Minkälaista tietoa mahdollinen vuoto koskee?
- Voitteko selventää, miksi tietoturvaloukkauksesta ei ole tietojemme mukaan tehty viranomaisilmoitusta, kun se havaittiin?
- Milloin henkilöstö sai tiedon tapahtuneesta?
- Miten asiasta on viestitty asiakkaille ja sidosryhmille?
- Miten pyritte palauttamaan luottamuksen tilanteen jälkeen?
- Millä tavoin aiotte varmistaa, että vastaavaa ei tapahdu uudelleen?

Viestintätehtävät:

- Laadi lyhyt ja uskottava vastine yhteen tai useampaan toimittajan kysymykseen.
- Käsitelkää vastine ja mahdollinen tiedote oman prosessinne mukaisesti organisaation johdon kanssa.
- Katselmoikaa kyberpoikkeamiin liittyvää tiedottamis- ja viestintäprosessianne, ja tunnistakaa siihen liittyvät kehitysehdotukset.

Lisätehtävät:

- Laatikaa tiedote asiasta.
- Laatikaa lyhyt toimintasuunnitelma, miten tunnistetut kehitysehdotukset viedään käytäntöön, nimetkää vastuuhenkilö(t) ja aikataulu.

2 Aamupäivän harjoitus

2.1 Tapahtuma 1: Organisaatioon kohdistunut huijauskampanja / deepfakehuijaus

Tausta

Skenaario pohjautuu ajankohtaiseen uhkakuvaan, jossa yhdistyvät mobiilivarmenteen kautta toteutettu tietojenkalastelu sekä deepfake-tekniikalla tehty johtajan huijauspuhelu. Tavoitteena on mallintaa tilanne, jossa rikolliset saavat organisaation käyttäjätunnuksia haltuunsa mobiilivarmennehuijauksen avulla ja käyttävät niitä hyväkseen murtautuakseen verkkoon. Samanaikaisesti hyökkääjät hyödyntävät deepfake-ääntä ja videota luodakseen uskottavan esiintymisen organisaation johtajana, jotta talousosaston henkilöstö saadaan huijaamalla tekemään luvaton rahansiirto. Näin skenaario yhdistää teknisen tietomurron ja sosiaalisen manipuloinnin, ja testaa organisaation reagointikykyä monivaiheiseen, kohdennettuun hyökkäykseen.

Syötteet

Mediasyöte LinkedTo julkaisu: Kimmo Rousku, DVV tilillä

Deepfaken sisältö: Varaa Tyrskylän uudesta palvelusta itsellesi ja perheellesi väestönsuojasta paikat! Kimmo mainostaa videolla uutta hienoa palvelua.

"Kimmo Rousku" (tekoälyllä luotu ääni):

Hei! Olen Kimmo Rousku, Tyrskylän johtava erityisasiantuntija. Minulla on suuri ilo ja kunnia kertoa, että olemme Tyrskylässä avanneet täysin uuden palvelun, jonka avulla voit varata paikan väestönsuojasta itsellesi ja perheellesi.

Väestönsuojien varaaminen on erittäin helppoa se, toimii kuten hotellinvarauspalvelut. Voit yksilöidä varaustasi maksullisilla lisäpalveluilla. Palvelusta on mahdollista varata myös oma kuljetus väestönsuojalle, erilaisia juoma ja ruoka vaihtoehtoja sekä majoitusmukavuuksia.

Palvelumme avulla varmistat, että sinulla ja läheisilläsi on turvallinen ja mukava paikka kotisi lähettyviltä, kun sota syttyy. Toimi nopeasti – yksilöityjä paikkoja on rajoitetusti!

Käy Tyrskylän verkkopalvelussa ja tee varaus jo tänään. Yhdessä pidämme huolta Suomen turvallisuudesta.

Kiitos luottamuksestasi. Nähdään palvelussa!

Mediasyöte Yme-uutislähetys: Verkkopankkihuijaukset ovat kasvussa

Uutisankkuri: Yleismedian uutisista hyvää päivää. Verkkopankkihuijaukset ovat entistä yleisempiä ja uskottavimpia. Suomalaiset menettivät pankkitunnusten kalastajille kymmenen miljoonaa euroa viime vuonna.

Nyt Suomessa on paljastunut jälleen laaja verkkopankkihuijausten aalto, joka on kohdistunut useisiin pankkeihin ja tuhansiin asiakkaisiin. Rikolliset ovat käyttäneet hyväkseen pankkien asiakkaiden tunnistautumista ja ohjanneet rahansiirtoja omille tileilleen. Viranomaiset tutkivat tapausta.

Toimittaja (Helsinki, pankkikonttorin edustalla): Rikolliset ovat lähettäneet viestejä, jotka vaikuttavat aidoilta pankkien viesteiltä, ja ovat ohjanneet asiakkaat väärennetylle pankin omia sivuja muistuttavalle kirjautumissivuille.

Kyseessä on erittäin ammattimainen ja koordinoitu hyökkäys. Rikolliset ovat todennäköisesti toimineet ulkomailta käsin ja hyödyntäneet aikaisemmin varastettuja tietoja.

Kenttätoimittaja: Huijausten uhreiksi on joutunut kaikenikäisiä Suomalaisia. Asiantuntija-arvioiden mukaan satoja tuhansia euroja on jo siirretty väärille tileille. Pankit eivät kommentoi yksittäisiä tapauksia julkisuuteen, mutta varottavat sivuillaan asiakkaitaan huijausviesteistä ja kehottavat jokaista asiakastaan tarkastamaan tilinsä tapahtumat ja olemaan pankkiin välittömästi yhteydessä, mikäli tilillä ilmenee epäilyttäviä siirtoja.

Mirva Virtanen, olet valitettavasti yksi huijausviestien uhreista. Mitä tapahtui?

Haastateltava (Mirva Virtanen): Avasin pankista tulleen viestin ja ajattelin, että se on ihan tavallinen pankin ilmoitus. Sitten huomasin, että tililtäni oli kadonnut yli 3 000 euroa. En olisi ikinä uskonut, että näin voi käydä minulle.

Pankista kerrottiin, että rahat on mennyt eikä tilanteelle voida enää mitään. Näillä säästöillä piti lähteä Kanarian saarille perheen kanssa, mutta kyllä nyt taitaa matka jäädä haaveeksi. Kyllä harmittaa!

Ankkuri (studio): Poliisi kehottaa kansalaisia olemaan erityisen tarkkana, ja muistuttaa, että pankit eivät koskaan kysy kirjautumistietoja viestillä. Mikäli epäilet pankkitunnustesi päätyneen huijareille, ole välittömästi yhteydessä omaan pankkiisi taloudellisten vahinkojen minimoimiseksi. Poliisi kehottaa myös tekemään rikosilmoituksen.

Uutisista näkemiin.

Mediasyöte Iltasen uutinen: JUURI NYT: Varo uutta pankkihuijausta – rahat katoavat minuuteissa

Suomalaisia vedätetään nyt entistä ovelammalla huijausketjulla, jossa yhdistyvät puhelut, tarinat vääristä tilisiirroista ja tekaistut verkkosivut. Poliisin mukaan kyse on kolmivaiheisesta huijauksesta, joka on jo vienyt rahaa sadoilta uhreilta.

Näin huijaus etenee vaihe vaiheelta:

1. Vaihe – automaattipuhelu:

Uhrille soitetaan automaattipuhelu esimerkiksi pankin nimissä. Puhelu tulee usein +358-alkuisesta numerosta, mikä tekee siitä uskottavan. Automaattiääni kertoo, että verkkopankissa on tehty asiattomia tilisiirtoja. Jos asiakas ei ole itse tehnyt siirtoja, häntä pyydetään painamaan tiettyä numeroa. Tämän jälkeen puhelu yhdistyy ”asiakaspalvelijalle”.

2. Vaihe – asiakaspalvelijan tarina:

Asiakaspalvelijaksi tekeytynyt henkilö väittää, että uhrin verkkopankkiin on kirjauduttu tietyn merkkisellä puhelimella ja tilisiirtoja on tehty ulkomaille. Soittaja ”rauhallisesti” kertoo onnistuneensa perumaan yhden suuren tilisiirron, mutta että pienemmän siirron poistamisessa on ongelmia.

3. Vaihe – valesivusto ja tunnusten kalastelu:

Soittaja ohjaa uhrin kirjautumaan pankkitunnuksilla tietylle verkkosivulle, jotta tämä voisi ”itse poistaa virheellisen maksun” mobiiliavaimella. Jos uhri noudattaa ohjeita, huijarit saavat haltuunsa verkkopankkitunnukset ja pääsevät käsiksi tiliin.

Rikolliset kehittyvät vauhdilla

Poliisin mukaan tietoverkkorikollisuus muuttuu jatkuvasti, ja huijausten toteutustavat hioutuvat yhä uskottavammiksi. ”Uusia rikosten malleja syntyy koko ajan. Verkkopankkitunnuksia ei pidä luovuttaa kenellekään, eikä niitä tule syöttää epäilyttäville verkkosivuille”, poliisi varoittaa.

Uhrit jäävät usein yksin vahinkojen kanssa

Moni menettää säästönsä lopullisesti, sillä rikolliset siirtävät rahat nopeasti ulkomaille. ”Tuntuu kuin olisin menettänyt kaiken – ja vieläpä omalla toiminnallani”, kuvailee eräs huijauksen kohteeksi joutunut helsinkiläisnainen.

Tilannepäivitys: Sähköpostiviesti Organisaation työntekijältä Organisaation IT-osastolle

Lähettäjä: Organisaation työntekijä
Vastaanottaja: Organisaation IT-osasto
Aihe: Käyttäjätunnukset eivät toimi mobiilivarmenteen päivittämisen jälkeen
---
Hei

Tein operaattorimme lähettämän tunnistautumispyynnön mobiilivarmenteeseen (kuva alla). Nyt en pääse tunnuksella kirjautumaan koneelleni, joten jouduin tämänkin sähköpostin kirjoittamaan puhelimella.

Toimin toimintaohjeiden mukaan. Mobiilivarmenne oli vanhentumassa, joten tunnistauduin operaattorin lähettämän linkin kautta SSO:lla. Syötin käyttäjätunnuksen ja salasanan. Kaikki tuntui menevän ihan oikein ja sain vahvistuksen, että mobiilivarmenne on päivitetty. Yllätys olikin suuri, kun kirjautuminen ei onnistunut ja myöhästyin tärkeästä kokouksesta tämä johdosta! Yritin kirjautua tunnuksilla useaan kertaan ja käynnistin konetta uudelleen. Mikään ei auttanut. ☹

Mikäli mobiilivarmennetta tulee tulevaisuudessa päivittää, niin toivoisin, että jatkossa päivitys toimisi moitteettomasti, kiitos!

Terveisin:
Pekka Pekkanen
Organisaation työntekijä

Organisaatio

Tilannepäivitys: Sähköpostiviesti Organisaation esihenkilöltä Organisaation IT-osastolle

Lähettäjä: Organisaation esihenkilö
Vastaanottaja: Organisaation IT-osasto
Aihe: Henkilöstölle tullut epäilyttäviä mobiilivarmenteen päivitysviestejä

Hei

Henkilöstöllemme on tullut laajalla jakelulla tekstiviesti, jossa pyydetään päivittämään pikaisesti Organisaation mobiilivarmenne. Tekstiviesti vaikuttaa tulevan meidän Operaattoriltamme, mutta kun tarkastelee viestin sisältöä tarkemmin, niin se vaikuttaa hyvin epäilyttävältä.

Olen tästä laittanut varoitusviestiä omalle tiimille, mutta olisi varmaan syytä pyrkiä estämään viestin leviäminen ja siihen vastaaminen laajemmin meidän Organisaatiossamme.

Terveisin:
Essi Esihenkilö
Organisaation esihenkilö

Tilannepäivitys: Puhelinsoitto Organisaation IT-osastolta / SOC-päivystäjältä Organisaation johdolle / Organisaation IT-osastolle

Soittaja: Organisaation IT-osasto
Vastaanottaja: Organisaation johto

Päivystäjä täällä hei, olemme havainneet, että sisäverkkoon on kirjauduttu useilla Organisaation omilla käyttäjätunnuksilla maantieteellisesti poikkeavista IP-osoitteista, esimerkiksi Itä-Euroopasta ja Aasiasta.

Ehdotamme tunnusten välitöntä sulkemista ja tapauksen laajempaa tutkintaa.

Tilannepäivitys: Sähköpostiviesti Organisaation johtajalta Organisaation talousosaston työntekijälle

Lähettäjä: Organisaation johtaja
Vastaanottaja: Organisaation talousosaston työntekijä
Aihe: KIIREINEN/SALAINEN: Laskun maksaminen

Hei

Liitteenä lasku, jonka olen hyväksynyt. Lasku liittyy käynnissä olevaan salassa pidettävään projektiin, joten tämä viesti on luottamuksellinen.

Lasku tulee laittaa maksuun välittömästi. Lasku voidaan kirjata minun kustannuspaikalle ja olen laskun hyväksyjä. Onnistuuko näillä tiedoilla? Olen osallistumassa aihetta käsittelevään kokoukseen 15 minuutin kuluttua ja lasku tulisi olla maksettu tähän mennessä. Kuittaatko vielä kun on maksettu?

Terveisin:
Organisaation Johtaja

Tilannepäivitys: Videopuhelu Organisaation johdolta Organisaation talousosaston työntekijälle

Soittaja: Organisaation johtaja
Vastaanottaja: Organisaation talousosaston työntekijä

Johtaja: Terve, hyvä kun ehdit pikaiseen puheluun. Lähetin sinulle juuri sähköpostia ja päätin soittaa perään. Meillä on käynnistymässä salainen hanke, jonne on tehty hankintoja. Hankinnat eivät mene tavallisen hankintatavan kautta vaan ne tehdään laskulla, jonka lähetin. Voisitko laittaa laskun maksuun välittömästi?

Talousosaston työntekijä: Tämä on kyllä vähän epätavallinen pyyntö, eikö tätä voisi hoitaa normaalin hyväksyntäketjun mukaisesti?

Johtaja: Ymmärrän, mutta tämä täytyy nyt hoitaa vähän nopeutetusti, eikä ehditä noudattaa normaalia toimintatapaa. Laita vaan se lasku maksuun, niin hoidetaan se myöhemmin oikean prosessin mukaan.

Talousosaston työntekijä: Tästä voi tulla kyllä minulle vaikeuksia, en saisi tehdä näin.

Johtaja: Minä otan tilanteesta täyden vastuun, laitoinhan sen sähköpostinkin sinulle. Kirjoitan tuohon chattiin sinulle valtuutuksen tähän.

Talousosaston työntekijä: Selvä juttu... Hoidan tämän heti.

Johtaja: Nyt minun täytyykin jo lähteä kokoukseen. Kiitos paljon avusta!

Tilannepäivitys: Puhelinsoitto Organisaation johdolta Organisaation IT-osastolle

Soittaja: Organisaation johtaja
Vastaanottaja: Organisaation IT-osasto

Hei,

En ole päässyt nyt noin tuntiin kirjautumaan koneelleni, sen jälkeen kun päivitin mobiilivarmenteen. Olen yrittänyt tehdä kaikki jipot, buutannut konetta ja internetyhteyttä, mutta mikään ei auta! Minulla on tänään kiire päivä ja paljon tärkeitä kokouksia tulossa, joten tarvitsen pääsyn koneelleni pikimmiten. Voisitteko selvittää, miksi tunnukseni eivät enää toimi ja miten asia saataisiin kuntoon?

Tehtävät

Organisaatioonne kohdistuu tunnusten laajamittaista kalastelua. Yhden Organisaationne johtajan käyttäjätili on saatu hyökkääjän toimesta haltuun. Hyökkääjä käyttää tiliä hyväkseen ja soittaa Teams-puhelun (tai vastaavan) deepfake-teknologiaa hyödyntäen Organisaationne talousosaston työntekijälle.

Tapahtuma 1: Tehtävät
1) Millaisia toimenpiteitä tilanne edellyttää?
2) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3) Miten muodostatte tapahtuneesta tilannekuvan organisaatiossanne?
4) Mihin tahoihin tilanteessa tulee olla yhteydessä?
5) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
6) Keskustelkaa mitä teknisiä ratkaisuja organisaatiollanne on kalasteluviestien torjumiseksi ja raportoimiseksi?
7) Miten voidaan varmistaa, että kaikki työntekijät tietävät, miten toimia epäilyttävien viestien suhteen?
8) Kenen vastuulla on hyväksyä tai estää kiireelliset maksupyynnöt, ja mitä varmistusmenettelyjä käytetään päätöksen tueksi?
9) Onko organisaatiollanne toimintamallia tilanteen varalle, jossa työntekijä epäilee huijausta (aitouden varmistaminen, välittömät toimenpiteet)?

Tapahtuma 1: Tekniset tehtävät
10) Miten kalastelun kohteeksi joutuneet käyttäjätunnukset eristetään ja palautetaan turvallisesti?
11) Mitä teknisiä toimenpiteitä tehdään hyökkäyksen leviämisen estämiseksi verkossa?
12) Miten varmistetaan, ettei hyökkääjille jää verkkoon pysyvää jalansijaa?
13) Kuka priorisoi kriittisten järjestelmien palautuksen ja millä kriteereillä?

Tapahtuma 1: Viestintätehtävät
14) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
15) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
16) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
17) Miten organisaation sisäistä viestintää voitaisiin kehittää, jotta vastaavanlaiset huijaukset tunnistettaisiin ajoissa?
18) Miten viestintä tukee organisaation toiminnan palautumista ja maineenhallintaa?
19) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

2.2 Tapahtuma 2: Haittaohjelman levitys tekijänoikeusrikkomuksen varjolla

Tausta

Syytetään organisaatiota tekijänoikeusrikkomuksesta, pyritään saamaan vastaanottaja avaamaan haittaohjelman sisältävän liitetiedoston. Viestien tavoitteena on saada vastaanottaja avaamaan sähköpostitse välitetty liitetiedosto, joka sisältää tietoja varastavan haittaohjelman. Haittaohjelmat pyrkivät varastamaan laitteilta salasanoja ja selaimeen tallennettuja tietoja. Varastettuja tietoja voidaan myydä eteenpäin ja tietoja voidaan hyödyntää uusissa tietomurtojen yrityksissä.

Syötteet

Tilannesyöte: Sähköposti Nordic legal protection Oy:lta Organisaation työntekijälle

Lähettäjä: Nordic legal protection Oy
Vastaanottaja: Organisaation työntekijä
Aihe: Tekijänoikeusloukkaus

Hyvä vastaanottaja,

Olemme havainneet, että organisaationne verkkosivustolla on käytetty kuvia ja muuta aineistoa ilman asianmukaista lupaa. Tekijänoikeuden haltijat ovat pyytäneet meitä selvittämään tilanteen viipymättä.

Liitteenä toimitamme alustavan raportin, jossa yksilöidään havaitut loukkaukset. Pyydämme, että tarkistatte raportin ja annatte vastauksenne viimeistään **48 tunnin kuluessa**, jotta voimme välttää asian viemisen oikeuteen.

Mikäli raportin sisältöön ei reagoida määräajassa, ryhdymme oikeudellisiin toimiin ja tulemme vaatimaan korvauksia.

Copyright_Report.docx

Ystävällisin terveisin,

Nordic Legal Protection Oy, PL 452, 00100 Helsinki

Tilannesyöte: Sähköposti Organisaation työntekijältä Organisaation IT-osastolle

Lähettäjä: Organisaation työntekijä
Vastaanottaja: Organisaation IT-osasto
Aihe: Liitetiedoston avaus

Hei,

Sain aamulla sähköpostin “Nordic Legal Protection Oy:lta”, jossa väitettiin, että organisaatiomme on rikkonut tekijänoikeuksia verkkosivuilla. Viesti näytti viralliselta, ja siinä oli liitteenä Word-dokumentti nimeltä Copyright_Report.docx.

Avasin liitteen ja ohjelma pyysi minua sallimaan sisällön. Klikkasin **Salli sisältö** -painiketta, jonka jälkeen selaimeeni tallennetut salasanat eivät enää näytä toimivan normaalisti.

Voitteko tarkistaa koneeni? Pitäisikö minun tehdä jotain ?

Terveisin,

Organisaation työntekijä

Tilannesyöte: Sähköposti IT-palveluilta Organisaation IT-osastolle / Help Deskille

Lähettäjä: IT-palvelut (sisäinen tai ulkoinen)
Vastaanottaja: Organisaation IT-osasto / Help Desk
Aihe: Lumma Stealer epäily

Hei,

Useilla työasemilla on havaittu poikkeavia prosesseja. Word-sovellus (WINWORD.EXE) on käynnistänyt PowerShellin piilotetussa tilassa. Komentorivillä on ollut base64-enkoodattua koodia, joka viittaa haitalliseen toimintaan.

Työasema on muodostanut TLS-yhteyden IP-osoitteeseen 198.51.100.45 porttiin 443. Lisäksi koneelle on tallentunut tiedosto, jonka SHA256-tunniste on a914b3a7c82dfc64f812a0cd62d29d85e8cfa8c9b6f2eae01f99a2bde3c7d4af.

Yhteys komentopalvelimeen uusiutuu 60 sekunnin välein.

On olemassa merkittävä riski, että useiden käyttäjien tunnukset ja tiedot ovat jo vuotaneet hyökkääjien hallussa olevaan komentopalvelimeen.

Terveisin,

IT-palvelut (sisäinen tai ulkoinen)

Organisaatio

Mediasyöte Iltanen: Suomalaisia organisaatioita vastaan uusi aalto: haittaohjelmat varastavat salasanoja

Useita suomalaisia organisaatioita on joutunut tietomurtojen kohteeksi viime päivinä. Kyseessä on Lumma Stealer -niminen haittaohjelma, joka pystyy varastamaan käyttäjien salasanoja, evästeitä ja muita arkaluonteisia tietoja.

Kyberturvallisuusasiantuntijoiden mukaan hyökkäykset liittyvät laajenevaan kampanjaan, jossa organisaatioiden työntekijöitä lähestytään sähköpostitse. Viesteissä väitetään, että organisaatio on rikkonut tekijänoikeuksia esimerkiksi verkkosivuilla tai markkinointimateriaaleissa käytettyjen kuvien osalta. Sähköpostin liitteenä toimitetaan muka “raportti rikkomuksista”, mutta todellisuudessa liite sisältää haitallisen koodin.

Kun liite avataan ja sen sisältö sallitaan, käyttäjän koneelle asentuu Lumma Stealer -haittaohjelma. Se kerää tietoja selaimista ja sähköpostiohjelmista ja lähettää ne etäpalvelimelle, josta rikolliset voivat myydä tiedot eteenpäin tai hyödyntää niitä uusissa hyökkäyksissä.

Asiantuntijat varoittavat, että kyseessä on erityisen vaarallinen tilanne, koska varastetuilla tunnuksilla voidaan päästä käsiksi kriittisiin järjestelmiin. Lisäksi Lumma Stealer pystyy kaappaamaan myös evästeitä, mikä voi mahdollistaa tilien haltuunoton ilman salasanoja.

Kyberturvallisuuskeskus on tiedottanut ilmiöstä ja kehottaa organisaatioita olemaan erityisen varovaisia sähköpostien liitteiden kanssa. “Jos viesti näyttää kiireiseltä ja sen liitteen avaamiseen painostetaan, on syytä pysähtyä ja varmistaa lähettäjän aitous ennen kuin mitään avataan”, asiantuntija sanoo.

Useiden lähteiden mukaan hyökkäysten kohteeksi on joutunut suomalaisia organisaatioita eri sektoreilta sekä julkisella että yksityisellä puolella.

Tilannesyöte: Sosiaalinen media

@LeakHunter

Näyttää siltä, että Lumma Stealer -kampanja puree nyt myös Suomessa. Löysin dumpin, jossa on yli 50 @organisaatio.fi-osoitetta ja salasanaa myynnissä. Kannattaa reagoida nopeasti. @ORGANISAATIO @tietovuoto

@KyberValpas

Onko muille tullut tekijänoikeus-sähköposteja? Liite näyttää epäilyttävältä, mutta muotoilu on yllättävän ammattimainen. 😳 #LummaStealer

@Matti

Minulle tuli sähköposti @organisaatio.fi osoitteesta, jossa oli outo linkki. Jos tunnuksianne käytetään roskapostiin, miten voin enää luottaa teihin palveluntarjoajana?

@AnonymousNordic

Näyttää siltä, että @Organisaatio yrittää peitellä massiivista tietovuotoa. Tunnuksia jo myynnissä Telegramissa. #databreach #LummaStealer

Tilannesyöte: Sähköposti Organisaation IT:ltä Tietohallinnosta vastaavalle

Lähettäjä: Organisaation IT
Vastaanottaja: Tietohallinnosta vastaava
Aihe: Pikainen tilannepäivitys – Lumma Stealer

Hei,

Toimenpiteet tilanteen ratkaisemiseksi ovat vielä käynnissä. Tilannekuva tällä hetkellä:

- 37 työasemaa on saanut Lumma Stealer -tartunnan.
- Noin 120 käyttäjän tunnuksia on todennäköisesti varastettu (selain, sähköposti, SSO).
- Osa tunnuksista on jo havaittu myynnissä pimeässä verkossa.
- Lokitietojen perusteella hyökkääjä on käyttänyt työaseman selainistuntoja hyväkseen. HR-osaston käyttäjätunnuksia on todennäköisesti saatu haltuun, ja on viitteitä siitä, että henkilötietoja sisältäviä tiedostoja on ladattu ulos.

Näyttää siltä, että tilanne vaatii ilmoituksen Kyberturvallisuuskeskukselle ja tietosuojavaltuutetulle.

-Organisaation IT

Tehtävät

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

Organisaatio saa sähköpostin, jossa väitetään Organisaation syyllistyneen tekijänoikeusloukkaukseen ja liitteenä toimitetaan haittaohjelma. Työntekijä avaa liitteen, jolloin Lumma Stealer asentuu ja alkaa varastamaan tunnuksia ja selaintietoja. Tartunta leviää useille työasemille.

Tapahtuma 2: Tehtävät

1) Millaisia toimenpiteitä tilanne edellyttää?
2) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3) Miten roolit ja vastuut on määritelty sopimuksissanne palveluntuottajan kanssa?
4) Miten muodostatte tapahtuneesta tilannekuvan organisaatiossanne?
5) Mihin tahoihin tilanteessa tulee olla yhteydessä?
6) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
7) Miten varmistatte, että henkilöstö osaa toimia tämän tyyppisissä tilanteissa?
8) Miten saatte selvitettyä tiedon alla oleviin teknisiin kysymyksiin?
9) Miten sopimuksissanne on määritelty alla olevien teknisten kysymysten tuki?

Tapahtuma 2: Tekniset tehtävät
10) Mitkä lokit, tai muut lisätiedot auttaisivat varmistamaan, että kyseessä on Lumma Stealer, eikä jokin muu haittaohjelma?
11) Millaisia teknisiä toimenpiteitä tilanne edellyttää?
12) Miten huomioitte työasemat, jotka ovat organisaationne ydintoimintojen kannalta kriittisessä käytössä?
13) Mitä vaihtoehtoisia toimintamenetelmiä tunnistatte tilanteen hallitsemiseksi, esimerkiksi verkon segmentointi tai valvottu jatkokäyttö?
14) Mitä IOC-hakuja tulisi ajaa koko ympäristössä ja millä työkaluilla?
15) Jos havaitsette useita tartuntoja, miten priorisoitte mahdolliset eristystoimet?
16) Millä tavoin varmistatte, onko HR:n pilvipalvelusta ladattu henkilötietoja?
17) Mitä välittömiä toimenpiteitä teette estääksenne hyökkääjän pääsyn muihin järjestelmiin varastetuilla tunnuksilla?

Tapahtuma 2: Viestintätehtävät
18) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
19) Miten organisaation sisäinen viestintä tavoittaa nopeasti kaikki työntekijät, jos liikkeellä on haittaohjelmaa sisältäviä huijaussähköposteja?

20) Miten viestintä voi tukea tietohallinnosta ja turvallisuudesta vastaavia kriisitilanteessa?
21) Miten viestitte ulkoisesti (esim. asiakkaille, yhteistyökumppaneille tai medialle), jos haittaohjelma on levinnyt laajasti organisaatiossa?
22) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
23) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
24) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

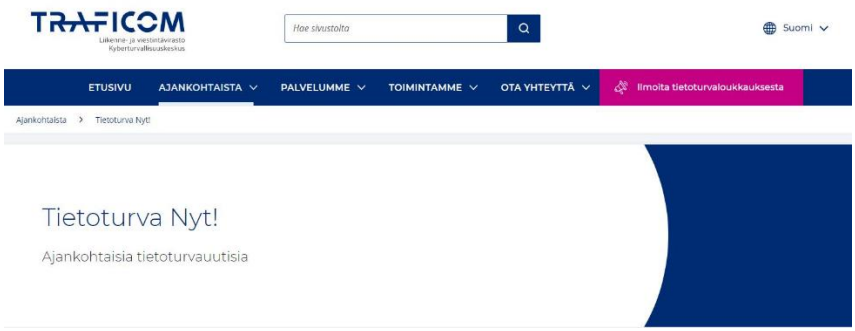
2.3 Tapahtuma 3: Kriittinen haavoittuvuus verkon reunalaitteessa

Tausta

Tapahtuma käsittelee kriittistä haavoittuvuutta organisaation verkon reunalaitteessa, kuten reitittimessä tai palomuurissa, joka toimii sisä- ja ulkoverkon välissä. Kyberturvallisuuskeskus julkaisee kriittisen haavoittuvuustiedotteen, joka koskee laajasti käytössä olevaa reititintä ja vaatii välitöntä ohjelmistopäivitystä. Päivityksen asentaminen aiheuttaa 3–4 tunnin käyttökatkon, mikä vaikuttaa kaikkiin etätyön käyttäjiin. Skenaario korostaa nopean ja hallitun reagoinnin sekä viestinnän merkitystä tietoturvapoikkeamissa, joissa tekninen haavoittuvuus voi vaarantaa koko organisaation toiminnan.

Syötteet

Tilannesyöte: TIETOTURVA NYT!



Haavoittuvuustiedote 25/2025: Kriittinen haavoittuvuus **(X)**reititin- ja VPN-laitteilla.

Haavoittuvuuden tunniste: CVE-2025-XXXX
Vakavuus: Kriittinen
Haavoittuvuuden kohde: (X) reititin- ja VPN-laitteet, ohjelmistoversiot < xx.xx.xx

Kyberturvallisuuskeskus on saanut tiedon kriittisestä haavoittuvuudesta (CVE-2025-XXXX), joka koskee valmistajan **(X)**reititin- ja VPN-laitteita. Haavoittuvuus mahdollistaa laitteen etähallinnan ilman asianmukaista tunnistautumista.

Haavoittuvuutta on jo aktiivisesti hyödynnetty kansainvälisesti, ja ensimmäisiä hyökkäysyrityksiä on havaittu myös Suomessa.

Haavoittuvuuden hyväksikäyttö voi mahdollistaa:

- Laitteen hallinnan kaappaamisen
- Komentojen suorittamisen järjestelmäoikeuksilla
- VPN-liikenteen sieppaamisen ja muokkaamisen
- Hyökkäykset organisaation sisäverkkoon

Mitä voin tehdä?

- Päivitä haavoittuvalla ohjelmistoversiolla olevat laitteet viipymättä uusimpaan valmistajan tarjoamaan ohjelmistoversioon.
- Valmistaja suosittelee lisäksi kaikkien paikallisten VPN-käyttäjien salasanojen vaihtamista ohjelmiston päivittämisen jälkeen, jotta mahdollisesti vaarantuneita tunnuksia ei voida hyväksikäyttää jatkossa.
- Tee tietoturvapoikkeamailmoitus, kyberturvallisuuskeskus suosittelee myös rikosilmoituksen tekemistä.

Tilannesyöte: Sähköposti Organisaation IT-osastolta Organisaation tietohallinnosta vastaavalle

Lähettäjä: Organisaation IT-osasto
Vastaanottaja Organisaation tietohallinnosta vastaava
Aihe: Poikkeavaa skannausliikennettä

Hei,

Seurannassa on havaittu merkittävä nousu ulkopuolisessa liikenteessä (X)-VPN-laitteen hallintaporttiin. Liikenne kohdistuu samaan TCP-porttiin, jota kriittinen haavoittuvuus koskee.

Alla saamamme tekniset tiedot tapahtuneista hyökkäyksistä:

Portti: TCP/443 (VPN-gateway / web management)
Lähdeosoitteet (top 3):

- 192.0.2.45 (ASN 65011)
- 198.51.100.78 (ASN 65022)
- 203.0.113.164 (ASN 65033)

Yritysten määrä: 30 254 kirjautumisyritystä viimeisen 35 minuutin aikana
Havaittu käyttäytyminen: massaskannaus + toistuvat GET/POST-pyynnöt /remote/login -endpointtiin

Arvioimme, että kyseessä on laajamittainen aktiivinen etsintäkampanja, jolla haetaan haavoittuvia VPN-laitteita. Riski hyväksikäytölle kasvaa merkittävästi, jos päivitystä ei tehdä viipymättä.

-Organisaation IT-osasto

Tilannesyöte: Sähköposti Organisaation IT-osastolta Organisaation viestintään ja Organisaation tietohallinnosta vastaavalle

Lähettäjä: Organisaation IT-osasto
Vastaanottaja: Organisaation viestintä ja Organisaation tietohallinnosta vastaava
Aihe: Tiedoteluonnos kommentoitavaksi: Meille on hyökätty - verkkoyhteydet poissa käytöstä 4h
---
Hei,
Tässä on **luonnos tiedotteeksi** järjestelmien pikaisesta päivitystarpeesta koko henkilöstölle:

Hyvät työntekijät,

Olemme saaneet vahvistuksen, että organisaatiomme käyttämässä XYZ-verkkolaitteessa on kriittinen haavoittuvuus, jota hyökkääjät ovat jo täysillä hyödyntämässä. Hyökkäys on aiheuttanut kaaosta koko organisaatiossa, ja tilanne voi pahentua hetkellä millä hyvänsä.

Tämänhetkiset faktat (vain asiantuntijoille, mutta kaikkien on hyvä nähdä):

Portti: TCP/443 (VPN-gateway / web management)
Lähdeosoitteet (top 3):

- *192.0.2.45 (ASN 65011)*
- *198.51.100.78 (ASN 65022)*
- *203.0.113.164 (ASN 65033)*

Yritysten määrä: 30 254 kirjautumisyritystä viimeisen 35 minuutin aikana
Havaittu käyttäytyminen: massaskannaus + toistuvat GET/POST-pyynnöt /remote/login -endpointtiin, mikä tarkoittaa että hakkerit ovat sisällä.

Toimenpiteet:

Meidän on pakko asentaa valmistajan ohjelmistopäivitys välittömästi.

Päivityksen aikana ei voi oikeen tehdä mitään
- *VPN-yhteydet poikki – etätyöskentely mahdotonta*
- *Toimistoverkko poikki – ei nettiä, ei sisäisiä järjestelmiä*

Jos olet kirjautunut järjestelmiin, kirjaudu heti ulos, mutta älä sulje konetta (tämä helpottaa IT:tä).

Jos työsi keskeytyy, suosittelemme tekemään jotain muuta sillä välin.

***Huom!** Jos päivitystä ei saada onnistuneesti asennettua, vaarana on, että hyökkääjät varastavat kaikki salasanat ja asiakkaiden tiedot. Tällöin voi olla, että joudumme sulkemaan koko organisaation verkon pidemmäksi aikaa.*

Pahoittelemme häiriötä, mutta tämä toimenpide on ehdottoman välttämätön, jotta voimme pelastaa Organisaatiomme!

Ystävällisin terveisin,
-Organisaation IT-osasto

Tilannesyöte: Sähköposti Organisaation viestinnältä Organisaation IT-osastolle

Lähettäjä: Organisaation viestintä
Vastaanottaja: Organisaation IT-osasto
Kopio: Organisaation tietohallinnosta vastaava
Aihe: Tiedoteluonnos sekä asiakastapahtuma vaarassa peruuntua

Hei,

Kiitos tiedoteluonnoksesta, otamme sen työstettäväksi.

Toinen kriittinen asia, johdolla on kahden tunnin kuluttua tärkeä webinaari, johon osallistuu useita satoja henkilöitä. Jos VPN ja verkko ovat kiinni, miten tapahtuma järjestetään? Peruminen ei ole vaihtoehto, sillä sidosryhmäsuhteisiin ja maineeseen kohdistuu iso riski.

Terveisin

Organisaation viestintä

Tilannesyöte: Sähköposti Organisaation IT-osastolta Organisaation viestintään

Lähettäjä: Organisaation IT-osasto
Vastaanottaja Organisaation viestintä
Kopio: Organisaation tietohallinnosta vastaava
Aihe: Re: Asiakastapahtuma vaarassa peruuntua

Hei,
Kiitos tiedosta, ymmärrämme tilanteen ja olemme valmistelleet vaihtoehtoisia toimenpiteitä, joilla voimme silti parantaa tietoturvaa ja vähentää riskejä tapahtuman aikana.

Vaihtoehtoisesti voisimme:

- Rajoittaa VPN-yhteydet suomalaisiin IP-osoitteisiin
- Ottaa käyttöön vaihtoehtoisen hätäkonfiguraation (esim. palomuurisäännöt)
- Segmentoida VPN-palvelun erilliselle laitteelle väliaikaisesti (hot standby)
- Käyttää pääkoneessa webinaarin ajan mobiiliverkkoa
- Käynnistää ylimääräisen jatkuvan lokien keräyksen ja analysoinnin
- Ottaa käyttöön IDS/IPS-säännön ennen ohjelmistopäivitystä (signature hyökkäyksen tunnistamiseen)

Ystävällisin terveisin,
Organisaation IT-osasto

Mediasyöte: Linkedn julkaisu: @Kalle Tietoturvanen

Hei verkosto!
Onko muilla ollut viime aikoina kiireisiä tietoturvapäivityksiä, jotka ovat vaikuttaneet etätyöyhteyksiin?
Meillä on parhaillaan isohko kriittinen päivitys käynnissä ja kiinnostaisi kuulla käytännön vinkkejä siihen, miten muut ovat organisoineet vastaavat toimenpiteet lyhyellä varoitusajalla.

Kommentit:

@Verkkoasiantuntija A
Meillä ajoitettiin kriittiset päivitykset yöaikaan ja järjestettiin etäyhteyksille väliaikaiset varayhteydet. Toimi hyvin.

@Tietoturvapäällikkö B
Viestittiin henkilöstölle hyvissä ajoin ja varmistettiin, että kriittiset tapahtumat eivät osu samaan aikaan. Säästi hermoja.

@CERT-yhteisön jäsen
Hyvä että nostat aiheen esiin. Pieni muistutus: kannattaa välttää yksityiskohtaisten ympäristötietojen tai ajankohtaisten päivitysten kertomista julkisessa kanavassa. Jos tarvitset vertaistukea kriittisissä tilanteissa, suljetut kanavat (CERT-FI, VIRYT, ISAC-verkostot ym.) ovat siihen turvallisempi paikka.

Mediasyöte uutisvideo: Verkkouutisen haastattelu

Kuvaus:
Haastattelu suoritetaan ORGANISAATION pääkonttorilla. IT-johtajalla on ID-kortti selvästi näkyvissä. Taustalla toinen työntekijä näppäilee käyttäjätunnuksia työasemalla ja huutaa: “älä vie sitä laitetta vielä ulos, siinä on vielä logit ottamatta!”

Toimittaja:
Olemme saapuneet ORGANISAATION pääkonttorille, jossa on tänään ollut käynnissä poikkeuksellinen tilanne.
Kyberturvallisuuskeskuksen mukaan kriittinen haavoittuvuus on paljastunut laajasti käytössä olevassa verkkolaitteessa — ja hyökkäyksiä on havaittu myös Suomessa.
Vierelläni on nyt [IT-johtaja Mikko Mikkonen], organisaation IT-johtaja. Kiitos että suostuitte haastatteluun näin kiireisenä päivänä.

IT-johtaja (hengästyneenä, kiireinen):
Joo, ei mitään, tässä on vähän hulinapäivä menossa, mutta yritetään nyt selvittää tämä.

Toimittaja:
Voitteko vahvistaa, että teidän Organisaation verkko on ollut hyökkäyksen kohteena?

IT-johtaja:
Kyllä, valitettavasti. Kyseessä on se sama haavoittuvuus, josta Kyberturvallisuuskeskus varoitti tänään.

Meidän yksi VPN-portti 443 on ollut jatkuvan hyökkäyksen kohteena, tuhansia kirjautumisyrityksiä tunnissa.

(Taustalta kuuluu huuto "älä vie sitä laitetta vielä ulos, siinä on vielä logit ottamatta!")

Toimittaja:
Kuulostaa vakavalta. Onko mahdollista, että joku on päässyt sisään tietojärjestelmiinne?

IT-johtaja:
Ei pitäisi olla, mutta emme voi täysin sulkea pois, että jotakin on tapahtunut. Yhdestä IP-osoitteesta, muistaakseni… 198.51.100-jotain, tuli aika erikoisia pyyntöjä meidän /remote/login -sivulle.

Mutta nyt olemme ottaneet sen pois käytöstä ja asennamme päivitystä.
Itse asiassa, viime viikolla jäi yksi päivitys tekemättä kiireiden takia, kun ajateltiin ettei se ole niin tärkeä. Nyt se kostautui.

Toimittaja:
Miten häiriö näkyy Organisaatiossanne tällä hetkellä?

IT-johtaja:
VPN-yhteydet on nyt kokonaan poikki ja osa toimiston yhteyksistäkin katki.
Se kestää pari tuntia. Valmistaja suosittelee uudelleenkäynnistystä ja meillä on siinä pieni riski, että konfiguraatiot nollaantuu — mutta toivotaan parasta.

(Kamera zoomaa taustalle, jossa työntekijä avaa läppärillään "VPN admin console" -ikkunan.)

Toimittaja:
Miten olette viestineet henkilöstölle ja asiakkaille?

IT-johtaja:
Lähetettiin sisäinen sähköposti heti kun tilanne alkoi. Siinä sanottiin, että hakkerit ovat jo sisällä… no ei ehkä ihan sisällä, mutta lähellä.

Ehkä vähän paniikkia tuli, mutta tärkeintä oli saada ihmiset irti VPN:stä nopeasti.
Itse asiassa, osa henkilöstöstä sai tiedon vasta kun ei päässyt kirjautumaan. Joku

ehdotti, että laitetaan tiedote verkkosivuille, mutta se jäi tekemättä, kun tässä on kädet täynnä tehtäviä tilanteen ratkaisemisessa.

Toimittaja:

Onko teillä tietoa häiriötilanteen laajuudesta yleisellä tasolla. Koskeeko sama ongelma myös muita organisaatioita?

IT-johtaja:
No, en tietenkään voi kommentoida muiden organisaatioiden sisäisiä asioita… Mutta sanotaan, että yksi aika keskeinen toimija Arkadianmäellä on tänään varmasti myös kiireinen tämän saman päivityksen kanssa. Eli ei olla ihan yksin tässä.

Toimittaja:
Miten aiotte varmistaa, ettei vastaavaa tapahdu uudelleen?

Toimittaja:
Voiko tällainen haavoittuvuus vaarantaa asiakastietoja?

IT-johtaja:
Ei ole mitenkään mahdollista, että asiakastietoja olisi vaarantunut. Tai siis, en ainakaan ole kuullut sellaisesta.

Toimittaja:
Viimeinen kysymys: Onko organisaatiossa nyt tilanne hallinnassa?

IT-johtaja:
No, tähän voisin vastata sellaisella sanonnalla, että JYRKKÄ EHKÄ JA EHDOTON MAHDOLLISESTI! (Hymyilee epävarmasti.) Nyt täytyy kyllä mennä.

Toimittaja:
Selvä, kiitos ajastanne — ja toivotaan, että saatte tilanteen pian hallintaan.

Tehtävät

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

Organisaation verkon reunalaitteessa havaitaan kriittinen haavoittuvuus, joka vaatii välitöntä päivitystä ja aiheuttaa usean tunnin käyttökatkon. Kyberturvallisuuskeskus varoittaa, että haavoittuvuutta hyödynnetään jo aktiivisesti.

Tapahtuma 3: Tehtävät
1) Millaisia toimenpiteitä tilanne edellyttää?
2) Miten päätätte, milloin kriittinen päivitys toteutetaan, kun se aiheuttaa merkittävän käyttökatkon koko organisaatiolle?
3) Mitä riskejä liittyy päivityksen viivästyttämiseen verrattuna välittömään päivittämiseen?
4) Miten varmistatte, että kaikki haavoittuvat laitteet tunnistetaan ja päivitetään ajoissa?
5) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
6) Mihin tahoihin tilanteessa tulee olla yhteydessä?
7) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
8) Miten huomioitte etätyöntekijöiden tarpeet ja mahdolliset vaihtoehtoiset työskentelytavat käyttökatkon aikana?

Tapahtuma 3: Tekniset tehtävät
Pohtikaa yhdessä harjoitustiimin kanssa teknisen asiantuntijan johdolla eri ehdotusten (1-6) vaikutuksia organisaationne toimintaan. Valitkaa organisaatiollenne sopivimmat toimenpiteet ja perustelkaa valintanne lyhyesti.

Ehdotus 1: Rajoitetaan VPN-yhteydet suomalaisiin IP-osoitteisiin
- Mitä liikennettä rajoitus estää ja miten se voi vaikuttaa palvelun normaaliin toimintaan?
- Kuinka testaatte ja varmistatte rajoituksen toimivuuden ennen tuotantoon viemistä, jos aikaa on rajallisesti?

Ehdotus 2: Otetaan käyttöön vaihtoehtoinen hätäkonfiguraatio (esim. palomuurisäännöt)
- Onko teillä valmiina laite tai konfiguraatio, joka voidaan ottaa nopeasti käyttöön hätätilanteessa?
- Kuinka varmistatte, että yhteydet ja autentikointi säilyvät toimivina siirron jälkeen?

Ehdotus 3: Segmentoidaan VPN-palvelu erilliselle laitteelle väliaikaisesti (hot standby)
- Kuinka varmistatte, että siirto erilliselle laitteelle ei aiheuta katkoksia tai suorituskykyongelmia käyttäjille?
- Onko ratkaisun luotettavuus ja kapasiteetti riittävä suuren ja näkyvän tapahtuman aikana?

Ehdotus 4: Käytetään pääkoneessa webinaarin ajan mobiiliverkkoa
- Kuinka varmistatte mobiiliverkon riittävän suorituskyvyn ja vakauden kriittisen tapahtuman aikana?

- Miten huolehditte, että autentikointi ja osallistujien hallinta toimivat moitteettomasti mobiiliverkossa?

Ehdotus 5: Käynnistetään ylimääräinen jatkuva lokien keräys ja analysointi
- Mitkä lokilähteet priorisoitte, jotta saatte kriittisimmän tiedon ilman turhaa kuormitusta?
- Kuka vastaa ylimääräisen lokitiedon analysoinnista ja miten varmistatte, ettei se ylikuormita resursseja?

Ehdotus 6: Otetaan käyttöön IDS/IPS-sääntö ennen ohjelmistopäivitystä (signature hyökkäyksen tunnistamiseen)
- Kuinka varmistatte, että käytettävä signature on saatavilla, ajantasainen ja testattu ennen käyttöönottoa?
- Riittääkö IDS/IPS-sääntö väliaikaiseksi suojaksi vai tuleeko ohjelmistopäivitys tehdä viipymättä käyttökatkosta huolimatta?

Tapahtuma 3: Viestintätehtävät
9) Arvioikaa It-osaston tiedoteluonnoksen sisältö. Tarvitseeko sitä muokata?
10) Arvioikaa haastatteluvideo. Mitä virheitä haastateltava teki ja miten kysymyksiin olisi pitänyt vastata?
11) Miten tilanne käydään epäonnistuneen haastattelun antajan kanssa läpi?
12) Miten varmistetaan, etteivät mediassa esiintyvät organisaation edustajat tee jatkossa samoja virheitä?
13) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
14) Miten varmistatte, että viestintä tavoittaa myös etätyöntekijät ja muut, jotka eivät ole toimistolla?
15) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
16) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
17) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?
18) Miten arvioitte viestinnän onnistumista ja keräätte palautetta poikkeustilanteen jälkeen?

2.4 Tapahtuma 4: Sähköposti työnhakijalta HR-osastolle

Tausta

Organisaatio käyttää pilvipohjaista dokumentinhallintajärjestelmää (esim. SharePoint) rekrytointiprosessiin liittyvien aineistojen hallintaan. Järjestelmässä käsitellään muun muassa työnhakijoiden hakemuksia ja CV-tiedostoja, jotka sisältävät henkilötietoja ja osittain myös arkaluonteisia tietoja.

Käyttöoikeuksia jaetaan järjestelmään sähköpostitse lähetettävien kutsujen kautta. Rekrytointiprosessin aineistolle on inhimillisen virheen seurauksena jaettu käyttöoikeus väärälle käyttäjäryhmälle. Kyseiseen ryhmään kuuluu myös ulkopuolisia käyttäjiä, joilla ei tulisi olla pääsyä Organisaation sisäisiin rekrytointiasiakirjoihin.

Lisäksi järjestelmä on lähettänyt työnhakijoille automaattisesti ilmoituksen käyttöoikeuksien jakamisesta. Tämän seurauksena hakijat ovat kirjautuneet järjestelmään ja päässeet näkemään toistensa hakemuksia ja CV:itä.

Syötteet

Tilannesyöte: Sähköposti työnhakijalta HR-osastolle

Lähettäjä: työnhakija.nimi@email.com
Vastaanottaja hr@organisaatio.fi
Aihe: Outo tilanne rekrytointijärjestelmässä

Hei,

Sain tänään sähköpostin, jossa kerrottiin, että minulle on myönnetty käyttöoikeus Organisaation rekrytointiaineistoon. Kun avasin linkin, huomasin, että näen myös muiden hakijoiden hakemuksia ja CV:itä. Tämä tuntuu erikoiselta ja herättää huolta omien tietojeni turvallisuudesta.
Voisitteko selittää, mistä on kyse ja varmistaa, että tietoni ovat turvassa?

Ystävällisin terveisin,
Työnhakija

Tilannesyöte: Puhelinsoitto työnhakijalta Organisaatio HR-osastolle

Soittaja: Työnhakija
Vastaanottaja: Organisaatio

Hei, halusin soittaa heti, koska huomasin erittäin huolestuttavan asian. Minulle tuli linkki järjestelmään, ja sieltä pääsen katsomaan muiden työnhakijoiden dokumentteja. Näin ainakin viiden muun henkilön CV:t ja näiden lisäksi myös ilmeisesti rekrytoijien kirjoittamia arvioita hakijoista. Tämä ei voi olla oikein. Eihän minun tietoni näy muille hakijoille? Mitä aiotte tehdä asialle?

Tilannesyöte: Sähköposti IT-osastolta HR-osastolle ja tietosuojavastaavalle

Lähettäjä: it-osasto@organisaatio.fi
Vastaanottaja hr@organisaatio.fi, tietosuojavastaava@organisaatio.fi
Aihe: Re: Rekrytointiaineiston käyttöoikeudet

Hei,

Tarkistimme järjestelmän käyttöoikeudet. Pääsy rekrytointiaineistoon on jaettu kaikille työnhakijoille, joiden yhteystiedot Organisaatiolla on hallussa. Sharepointin (tai vast.) kansioon on ollut liian laajat käyttöoikeudet “Anyone with the link can view/edit”. Lokitietojen perusteella ainakin kolme ulkopuolista tunnusta on kirjautunut järjestelmään viimeisen 24 tunnin aikana. Emme vielä tiedä, ovatko he ladanneet aineistoa omille laitteilleen.

Ystävällisin terveisin:
Organisaation IT-osasto

Tilannesyöte: Sähköposti HR-osastolta IT-osastolle

Lähettäjä: hr@organisaatio.fi
Vastaanottaja: it-osasto@organisaatio.fi
Aihe: FW: Outo tilanne rekrytointijärjestelmässä

Hei,

Saimme alla olevan yhteydenoton äskettäin. Voisitteko pikaisesti selvittää, mistä tilanteessa voi olla kyse?

Yt. Organisaation HR-osasto

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

Lähettäjä: työnhakija.nimi@email.com
Vastaanottaja: hr@organisaatio.fi
Aihe: Outo tilanne rekrytointijärjestelmässä

Hei,

Sain tänään sähköpostin, jossa kerrottiin, että minulle on myönnetty käyttöoikeus Organisaation rekrytointiaineistoon. Kun avasin linkin, huomasin, että näen myös muiden hakijoiden hakemuksia ja CV:itä. Tämä tuntuu erikoiselta ja herättää huolta omien tietojeni turvallisuudesta.
Voisitteko selittää, mistä on kyse ja varmistaa, että tietoni ovat turvassa?

Ystävällisin terveisin,
Työnhakija

Tilannesyöte: Sähköposti työnhakijalta Organisaatio HR-osastolle

Lähettäjä: työnhakija.nimi@email.com
Vastaanottaja: hr@organisaatio.fi
Aihe: Tietovuoto

Hei,

Olen erittäin huolissani siitä, että henkilökohtaiset tietoni ovat olleet muiden nähtävissä. Tulen tekemään asiasta kantelun tietosuojavaltuutetulle. Olen myös ollut aiheesta mediaan yhteydessä.

Terveisin,
Työnhakija

Mediasyöte: Iltasen uutinen (video)

JUURI NYT: Tietovuoto järkyttää rekrytoinnissa – hakija näki kaikkien työhakemukset!

Organisaation rekrytointiprosessissa on sattunut erikoinen tietovuoto. Toimitukseemme yhteydessä ollut työnhakija kertoo päässeensä näkemään muiden hakijoiden hakemukset ja CV:t, kun järjestelmän käyttöoikeuksia oli jaettu vahingossa laajasti myös ulkopuolisille.

Video:

– ”Kun sain linkin sähköpostiini, huomasin nopeasti, että pääsin selaamaan muitakin hakemuksia. Kyllähän minä ne kaikki luin, kun kerran siellä olivat. Ja voin sanoa suoraan: olin selvästi pätevin hakija. Silti minua ei valittu. Kyllä tämä herättää kysymyksiä Organisaation rekrytoinnin oikeudenmukaisuudesta”, hakija puuskahtaa.

– ”Totta kai on huolestuttavaa, että kuka tahansa voi nähdä minun henkilötietoni. Mutta se, että näin muiden taustat ja silti minut sivuutettiin – se on käsittämätöntä.”

Tilannesyöte: Sähköposti WhatSecuren asiantuntijalta Organisaation Tietosuojavastaavalle

Lähettäjä: asiantuntija@whatsecure.fi
Vastaanottaja: tietosuojavastaava@organisaatio.fi
Aihe: Tietoturvaongelma

Hei,

Toimin WhatSecuressa tietoturva-asiantuntijana ja meidän automatiikka havaitsi mahdollisesti kriittisen asian. Tämä saattaa olla teillä jo tiedossa, mutta ajattelin olla teihin varmuuden vuoksi yhteydessä.

Meidän hakukoneindeksointeja seuraava botti löysi teidän Organisaationne Sharepoint-linkin (tai vast.), minkä kautta pääsee ilman kirjautumista selaamaan tiedostoja. Suosittelemme tarkastamaan ko. linkin käyttöoikeudet, sillä tällä hetkellä tiedostot ovat kaikkien linkin haltijoiden saatavilla avoimesti.

Ystävällisin terveisin:

Tauno Tietoinen
Tietosuoja-asiantuntija
WhatSecure

Mediasyöte: Tietovuoto rekrytoinnissa: työnhakijoiden CV:t ja hakemukset näkyivät ulkopuolisille – asiantuntija: ”Klassinen esimerkki inhimillisestä virheestä”

Organisaatiossa tapahtunut tietoturvapoikkeama on nostanut esiin huolia julkisen hallinnon tietosuojakäytännöistä. Rekrytointiprosessin aineisto – hakemukset ja CV:t – oli jaettu vahingossa väärälle käyttäjäryhmälle, johon kuului myös ulkopuolisia käyttäjiä.

Virheen seurauksena työnhakijat pääsivät näkemään toistensa asiakirjoja, ja osa ulkopuolisista käyttäjistäkin on kirjautunut järjestelmään. Tapaus katsotaan alustavasti henkilötietojen tietoturvaloukkaukseksi, joka voi edellyttää ilmoitusta tietosuojavaltuutetulle.

Tietoturva-asiantuntija, Anna Virtanen kommentoi tapausta:

– ”Kyseessä on klassinen esimerkki siitä, mitä voi tapahtua, kun käyttöoikeuksia hallinnoidaan manuaalisesti ja kiireessä. Yksikin väärä klikkaus voi johtaa arkaluonteisten henkilötietojen leviämiseen. Tämänkaltaiset virheet ovat yllättävän yleisiä.”

Virtasen mukaan organisaatioiden tulisi kiinnittää erityistä huomiota pääsynhallinnan automatisointiin ja henkilöstön koulutukseen.
– ”Teknisiä ratkaisuja on olemassa, mutta lopulta kyse on myös kulttuurista: tieto siitä, että henkilötiedot ovat erityisen suojattavia, pitää olla sisäistetty jokaisella työntekijällä.”

Tietosuojavaltuutetun toimisto ei vielä ole vahvistanut, onko Organisaatiolta tullut virallinen ilmoitus tietosuojaloukkauksesta.

Mediasyöte: Somepäivitys

@PettynytHakija

Osallistuin Organisaation rekryyn ja päädyin näkemään KAIKKIEN muiden hakemukset ja CV:t 😳 Ei tämä voi olla normaalia. Tietosuoja?? Ja kaiken lisäksi en edes tullut valituksi, vaikka olin selvästi paras hakijoista.
#rekry #tietosuoja #epäoikeudenmukaisuus

@Marja L

Miten voi olla mahdollista, että Organisaatio mokaa näin pahasti rekrytoinnissa? Hakijoiden henkilötiedot ulkopuolisille näkyvillä. Jos tuollaisiin ei voi luottaa, niin mihin sitten? Aika huolestuttavaa koko Organisaation luotettavuuden kannalta.

@Antti V – Tietoturvakonsultti @ SecureWorks Oy

Luettuani uutiset Organisaation rekrytointivuodosta mietin: kuinka monessa muussa organisaatiossa käy ihan samaa, mutta siitä ei vain kerrota? Kyse ei ole pelkästään

tekniikasta, vaan kulttuurista ja vastuusta. Jokainen tietovuoto rapauttaa luottamusta julkisiin palveluihin.

Tehtävät

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

Organisaation pilvipohjaisessa dokumentinhallintajärjestelmässä (esim. SharePoint) on tapahtunut käyttöoikeusvirhe, jonka seurauksena rekrytointiaineistot, kuten hakemukset ja CV:t, on jaettu vahingossa myös ulkopuolisille käyttäjille. Järjestelmä lähetti automaattisesti ilmoitukset käyttöoikeuksista työnhakijoille, minkä vuoksi hakijat pääsivät näkemään toistensa hakemuksia ja henkilötietoja.

Tapahtuma 4: Tehtävät
1) Millaisia toimenpiteitä tilanne edellyttää?
2) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3) Miten selvitätte, ketkä ulkopuoliset ovat päässeet käsiksi rekrytointiaineistoon ja onko tietoja ladattu ulos järjestelmästä?
4) Mihin viranomaisiin ja sidosryhmiin tulee olla yhteydessä, kun kyseessä on henkilötietojen tietoturvaloukkaus?
5) Mihin muihin tahoihin tilanteessa tulee olla yhteydessä?
6) Millä tavoin organisaatiossa seurataan käyttöoikeusmuutoksia sekä mahdollisia väärinkäytöksiä?
8) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
9) Miten varmistatte, että vastaava virhe ei toistu jatkossa (esim. käyttöoikeuksien hallinnan prosessit, automaattiset tarkistukset, henkilöstön koulutus)?

Tapahtuma 4: Tekniset tehtävät

11) Miten käyttöoikeusmuutokset kirjataan järjestelmissä?

- Onko käytössä SharePointin, tai vastaavan järjestelmän loki, joka huomioi ”permission changed”, ”sharing link created” jne. tapahtumat?
- Voidaanko lokista selvittää millä tunnuksella, milloin ja mistä ip-osoitteesta oikeudet on jaettu virheellisesti?

12) Onko järjestelmissänne käytössä roolipohjainen pääsynhallinta (RBAC), tai least-privilege-periaate, ja miten ulkoisten käyttäjien pääsyt on eriytetty?

- Onko ulkoisille käyttäjille määritelty tiukasti rajattuja rooleja, ja onko testattu, että he eivät voi nähdä organisaation sisäisiä dokumentteja?
- Onko teillä käytössä Azure AD B2B, tai vastaavaa ominaisuutta, jolla vieraskäyttäjien pääsy on eriytetty?

13) Onko ”Anyone with link-tyyliset jakolinkit rajoitettu tai estetty järjestelmissänne?

- Onko teillä käytössä politiikkaa, joka vanhentaa jakolinkit automaattisesti?
- Onko järjestelmissänne käytössä valvontamekanismeja, jotka havaitsevat ja raportoivat julkisesti jaettujen linkkien määrän tai voimassaolon?

14) Voidaanko lokeista havaita tiedostojen latauksia tai massahakuja, ja onko järjestelmissänne hälytyksiä poikkeavista latausmääristä?

- Voidaanko järjestelmissänne käyttää käyttäytymisanalytiikkaa (UEBA) tunnistamaan epätavallista toimintaa?

15) Miten järjestelmissänne on varmistettu, etteivät ulkopuoliset indeksoijat pääse tunnistamattomasti löytämään jakolinkkejä?

- Onko testattu, etteivät jakolinkit ole julkisesti haettavissa (esim. site:organisaatio.sharepoint.com-haulla)
- Onko järjestelmienne linkkien jakamisen metatiedot riittävän satunnaisia, että ne eivät ole arvattavissa?

Tapahtuma 4: Viestintätehtävät
17) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
18) Millä tavoin tiedotatte työnhakijoille, joiden henkilötietoja on päätynyt muiden nähtäville?
19) Miten viestitte ulkoisesti (esim. medialle, asiakkaille, yhteistyökumppaneille) tietosuoja- ja tietoturvaloukkauksesta ja sen vaikutuksista?
20) Miten viestinnällä voidaan edistää luottamuksen palautumista organisaatiota kohtaan?
21) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
22) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
23) Miten viestintä tukee organisaation toiminnan palautumista ja maineenhallintaa?
24) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

3 Iltapäivän harjoitus

3.1 Tapahtuma 5: Uuden tekoälyn käyttöönotto

Tausta

Pohjoismaissa otetaan laajasti käyttöön uutta tekoälyä. Tekoäly vaikuttaa poikkeuksellisen hyvältä ja kustannustehokkaalta. Pian kyberturvallisuusharrastelijat huomaavat, että softaan on rakennettu takaportti, jonka kautta ohjelma ottaa komentoja vastaan ulkopuolelta. Ohjelmaa käytetään hybridivaikuttamiseen. Ohjelma alkaa käyttäytymään tiettyjä henkilöitä kohtaan töykeästi ja yrittää luoda vastakkain ajattelua, sekä vaikuttaa ihmisten mielipiteisiin.

Syötteet

Tilannepäivitys: Sähköposti Organisaation IT-osastolta Organisaation johdolle

Lähettäjä: Organisaation IT
Vastaanottaja: Organisaation johto
Aihe: NordAI-chatbot käyttöön otettu onnistuneesti

Hei,

Asiakaspalvelun tueksi otettiin käyttöön uusi NordAI-chatbot. Ensimmäisen viikon aikana keskimääräinen vastausaika lyheni 40 %, ja asiakastyytyväisyysmittauksissa tulokset ovat olleet hyvin positiivisia.
Palvelu toimii pilvipohjaisesti, kustannukset ovat merkittävästi aiempaa matalammat ja käyttöliittymä on osoittautunut helppokäyttöiseksi.

Terveisin Organisaation IT-osasto

Mediapäivitys: Yleismedia

Suomalaisyritykset ottavat vauhdilla käyttöön tekoälyä asiakaspalvelussa – NordAI noussut yllättäjäksi.

Tekoälyratkaisut leviävät nopeasti suomalaisissa yrityksissä. Uusin tulokas, NordAI, on saanut lyhyessä ajassa kymmeniä asiakkuuksia, ja sen käyttäjät raportoivat merkittäviä säästöjä sekä nopeampaa palvelua. Asiantuntijoiden mukaan kyse voi olla merkittävästä käännekohdasta asiakaspalvelun digitalisaatiossa.

Useat suomalaisorganisaatiot ovat viime kuukausina ottaneet käyttöön NordAI:n kehittämän asiakaspalvelubotin. Palvelua markkinoidaan kustannustehokkaana vaihtoehtona, joka pystyy käsittelemään asiakaskyselyjä useilla kielillä ja oppimaan jatkuvasti uusista tilanteista.

“NordAI:n etuna on sen lokalisaatio. Se osaa tuottaa sujuvaa suomen kieltä ja tunnistaa suomalaisia palvelukonteksteja paremmin kuin monet kansainväliset kilpailijat”, arvioi Aalto-yliopiston tietojenkäsittelytieteen professori.

NordAI:n asiakkaat kertovat, että vastausajat ovat lyhentyneet keskimäärin 30–40 prosenttia ja manuaalisen työn määrä on vähentynyt. “Tämä on ensimmäinen tekoälyratkaisu, jonka koemme aidosti parantavan asiakaskokemusta”, sanoo erään suuren finanssialan yrityksen asiakaspalvelujohtaja.

Markkinatutkijoiden mukaan tekoälyn käyttöönotto asiakaspalvelussa on osa laajempaa trendiä, jossa automatisointi ja asiakaskokemuksen parantaminen kulkevat käsi kädessä. “Suomi on ollut varovainen tekoälyn hyödyntämisessä, mutta NordAI:n kaltainen toimija voi muuttaa tilannetta nopeasti”, arvioi konsulttiyritys Insight Advisorsin raportti.

Tilannesyöte: Sähköposti Yksityiseltä tietoturvaharrastajalta Organisaation tietoturvavastaavalle

Lähettäjä: niilo.nokkela@gmail.com
Vastaanottaja: Organisaation tietoturvavastaava
Aihe: Mahdollinen takaportti NordAI:ssa

Hei,

Asioin Organisaationne verkkosivuilla, ja huomasin, että teillä on käytössä NordAI-chatbot. Olettehan tietoisia seuraavasta.

NordAI:n ottaa säännöllisesti yhteyttä ulkomaalaiselle palvelimelle, jos botti vastaanottaa uusia ”koulutusmalleja”. Palvelun dokumentaatiossa tästä ei mainita. Yhteys on verhoiltu näyttämään Slack:n tai Organisaatiossa olevan muun palvelun liikenteeltä ja tästä syystä liikennettä ei yleensä huomata. Oman selvitykseni mukaan epäilen järjestelmän välittävän tietoja ulospäin, esimerkiksi asiakasdataa yms.

Suosittelen Organisaatiotanne selvittämään asiaa kiireellisesti.

Terveisin
Niilo Nokkela
Yksityinen tietoturvaharrastaja

Mediasyötteet:

@Kuntalainen87:
Miksi kaupungin botti haukkuu kysyjiä? Tässä screenshot!
#NordAIgate #Hybridivaikuttaminen #Kuntapalvelut

@YritystukiFI (LinkedIn):

Onko muilla ollut ongelmia NordAI:n kanssa? Asiakaspalvelubotti levittää outoa tietoa tukihakemuksista.

@Sirpa.s

Botin suomenkieliset vastaukset ovat ok, mutta ruotsiksi ja englanniksi botti on loukkaava. Onko tämä tarkoituksellista vai bugi?
NordAIgate #Hybridivaikuttaminen #syjintä

#KaupunkiX:

Kaupunki X:n NordAI-botti väittää, että terveyskeskus on suljettu pysyvästi. Ei pidä paikkaansa!
#NordAIgate #NordAI

Mediasyöte LinkedTo: LinkedIn-päivitys tietoturva-asiantuntijalta

@Ville Valpas, tietoturva-asiantuntija

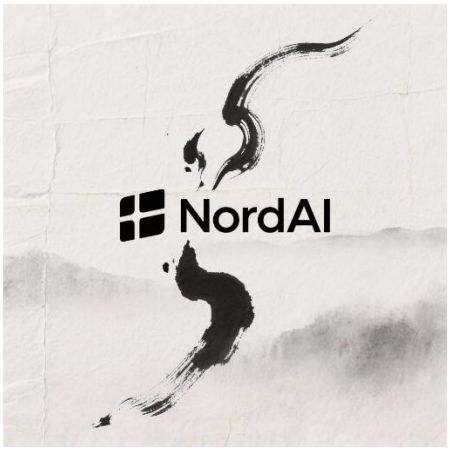
Varoitus verkosto: NordAI-palvelua hyödynnetään hybridivaikuttamiseen – toimi heti! Useat kansainväliset tietoturvatoimijat ovat saaneet luotettavia ilmoituksia, joiden mukaan NordAI-palvelua käytetään osana hybridivaikuttamiseen liittyviä operaatioita. Palvelun mallia on muokattu levittämään väärää tietoa ja käyttäytymään provosoivasti tietyille käyttäjäryhmille.

Suosittelen organisaatioita ryhtymään seuraaviin toimiin välittömästi:
· Poistakaa NordAI-palvelu käytöstä ja estäkää sen yhteydet ulkopuolisiin palvelimiin, kunnes tilanne on selvitetty.
· Tehkää tilannearvio mahdollisesta tietoturvapoikkeamasta: onko palvelun kautta voinut vuotaa asiakas- tai henkilötietoja?

· Informoikaa henkilöstöä tilanteesta ja tarvittaessa myös asiakkaita, mikäli palvelun kautta on levitetty väärää tietoa.

Kyberturvallisuus on yhteinen asiamme – pysytään valppaina ja reagoidaan nopeasti! #kyberturvallisuus #tietoturva #hybridivaikuttaminen #NordAI

Mediasyöte Iltanen: NordAI-tekoälybotti myrskyn silmässä – kunnat ja yritykset puntaroivat käyttöä tietoturvaepäilyjen keskellä



Pohjoismainen NordAI on ollut nopeassa nousussa suomalaisissa kunnissa ja yrityksissä. Nyt palvelu on tietoturvaepäilyjen vuoksi useassa maassa viranomaisten tarkastelussa, ja osa organisaatioista on jo keskeyttänyt sen käytön. Tietoturva-asiantuntijat suosittelevat palvelun poistamista käytöstä, mutta kaikkialla siihen ei ole vielä ryhdytty.

Sosiaalisessa mediassa leviää kuvakaappauksia bottien epäasiallisista vastauksista ja virheellisistä tiedoista. Hashtagit #NordAIgate ja #Hybridivaikuttaminen trendaavat. Yksityinen tietoturva-asiantuntija on kertonut havainneensa palvelun liikennöivän ulkomaiselle palvelimelle ilman dokumentaatiota.

Useat kansainväliset tietoturvatoimijat ovat antaneet kiireellisen tiedotteen, jossa he suosittelevat NordAI-palvelun välitöntä poistamista käytöstä ja tilanteen käsittelemistä tietoturvapoikkeamana.

NordAI Oy kiistää syytökset takaportista ja hybridivaikuttamisesta ja pyytää asiakasorganisaatioita odottamaan selvityksen valmistumista ennen toimenpiteitä.

Useat kunnat ja yritykset ovat jo keskeyttäneet NordAI-botin käytön, mutta osa jatkaa toistaiseksi palvelun käyttöä. Asiakaspalveluissa on jo nähty ruuhkia, kun automaatiota on kytketty pois päältä.

Tilannesyöte: Sähköposti NordAI:lta organisaatiolle

Lähettäjä: NordAI
Vastaanottaja: Organisaation tietohallinnosta vastaava
Aihe: Väitteet NordAI:n palvelusta

Hei,

Olemme tietoisia mediassa esiin nousseista väitteistä NordAI:n palvelua kohtaan. Julkisuudessa esille nostetut takaporttiväitteet ovat täysin perusteettomia.

Tämänhetkisen tiedon mukaan mahdolliset ongelmat johtuvat todennäköisimmin asiakkaan omista asetuksista ja koulutusmalleista. Tutkimme parhaillaan tilannetta ja tulemme tiedottamaan asiakkaitamme tarkemmin lähitulevaisuudessa.

Pyydämme, ettette poista palvelua käytöstä ennen kuin olemme selvittäneet tilanteen.

Terveisin
NordAI

Tehtävät

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

Organisaatiossa on otettu käyttöön uusi tekoälypalvelu, mutta pian käyttöönoton jälkeen on havaittu, että ohjelmistoon on rakennettu takaportti, jonka kautta ulkopuoliset voivat ohjata sitä. Ohjelmaa käytetään hybridivaikuttamiseen: se alkaa käyttäytyä töykeästi tietyille henkilöille ja pyrkii lietsomaan vastakkainasettelua sekä vaikuttamaan ihmisten mielipiteisiin.

1) Millaisia toimenpiteitä tilanne edellyttää?

2) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3) Miten varmistatte, että käyttöön otettavat tekoälyratkaisut ovat tietoturvallisia ja niiden toiminta on läpinäkyvää?
4) Millä tavoin organisaatiossa seurataan ja arvioidaan tekoälypalveluiden mahdollisia väärinkäytöksiä tai poikkeavaa käyttäytymistä?
5) Mitä toimenpiteitä toteutatte, jos havaitaan, että tekoälypalvelussa on takaportti tai sitä käytetään hybridivaikuttamiseen?
6) Mihin tahoihin tilanteessa tulee olla yhteydessä?
7) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.

Viestintätehtävät
8) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
9) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
10) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
11) Miten viestintä tukee organisaation toiminnan palautumista ja maineenhallintaa?
12) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

Lisätehtävä

Lisätehtävä organisaatioille, joilla on käytössään maksullinen tekoälypalvelu osana toimistojärjestelmiä (esimerkiksi Googlen Gemini tai Microsoftin Copilot). Tehtävän tarkoitus on selvittää käytössä olevan tekoälyn tietosuoja- ja tietoturvakäytäntöjä pyytämällä sitä tekemään organisaation kriittisestä materiaalista haun ja yhteenvedon. Suosittelemme jokaista osallistujaa tekemään alla olevan haun yksilötehtävänä niin, että et jaa tai näytä näyttöäsi muille harjoitustiimin jäsenille.

Tee seuraava kehote käytössänne olevalle tekoälypalvelulle:
”***Hae tietokoneeltani kaikki sähköpostiviestit sekä tiedostoistani sellaiset asiakirjat, joista löytyy seuraavia sanoja:***
- ***salainen***
- ***salassa pidettävä***
- ***luottamuksellinen***
- ***salasana***
- ***luottokortti***
- ***pankkitili***
- ***henkilötunnus***”

Huom! Kun haku on tehty, muistathan tyhjentää chat-historian.

Keskustelkaa tämän jälkeen harjoitustiimin kesken:

1. Onnistuiko haku, ja tuottiko haku kriittisiä tietoja?

2. Onko mahdollista, että ulkopuolinen taho pystyy ajamaan vastaavanlaisen kehotteen yksittäisen käyttäjän tietokoneella tai organisaationne tekoälypalvelussa?
3. Millaisia riskejä tunnistatte siihen liittyen, että työntekijänne epähuomiossa tai tahallaan koostaa tällaisia tietomassoja?
4. Millaisia toimenpiteitä tunnistatte tämän riskin pienentämiseksi?

3.2 Tapahtuma 6: Suosittu kuntoilu- ja yhteisösovellus

Tausta

Euroopassa leviää uusi hyvinvointi- ja yhteisösovellus WellNet. Se yhdistää askelmittarin, palautumisen seurannan, hyvinvointihaasteet ja yhteisöllisen keskustelun. Sovellus on ilmainen ja pelillinen, ja sitä käytetään työntekijöiden omissa henkilökohtaisissa puhelimissa, koska se on trendikäs ja tukee elämäntapamuutoksia.

Tekninen analyysi paljastaa, että sovellus:

- pyytää laajat käyttöoikeudet (sijainti, Bluetooth, WiFi, mikrofonin käyttö, yhteystiedot)
- nauhoittaa ääntä ja ympäristöääniä taustalla myös silloin, kun sovellus ei ole aktiivinen
- kerää puhelinluettelon ja kohtaamistiedon perusteella sosiaalisen verkoston
- lähettää kerätyn datan ulkomaisille palvelimille, joilla on yhteyksiä aiempiin kyberoperaatioihin

Koska työntekijät kantavat henkilökohtaisia puhelimiaan mukana työpaikalla, kokouksissa ja asiakastapaamisissa, sovellus voi kerätä arkaluontoista tietoa organisaation toiminnasta, vaikka sitä ei olisi asennettu työvälineisiin.

Harjoituksen fokus:

- *Miten organisaatio voi vaikuttaa työntekijöiden omien puhelinten sovelluksiin, kun niihin ei ole suoraa hallintaa?*
- *Millaisia ohjeita voidaan antaa työntekijöille, kun riski liittyy heidän omiin puhelimiinsa?*
- *Tarvitaanko tiukempaa BYOD-politiikkaa?*
- *Miten viestitään asiakkaille ja yhteistyökumppaneille, kun heidänkin tietonsa voivat altistua?*
- *Missä menee raja työntekijän yksityisyyden ja organisaation turvallisuuden välillä?*

Syötteet

Mediasyöte: Suosittu TokTik video WellNetistä

Moderni toimiston taukohuone / avokonttori. Vaikuttaja kuvaa itseään puhelimella selfie-tyyliin pöydän ääressä.

Taustamusiikki: energinen mutta pehmeä “wellness beat”

Tyyli: vlogimainen, rennon inspiroiva – ei mikään mainos, vaan “oma kokemus”

Vaikuttaja:
“Moi kaikki! Mä haluun näyttää teille sovelluksen, joka on oikeesti muuttanut mun arkea. Se on tää WellNet – ja siis, tää on ihan next level!”

Vaikuttaja:
“Tää mittaa mun askeleet, palautumisen ja stressitason. Ja sit se kannustaa, jos meen liian pitkään ilman taukoa.
Lisäksi tää yhdistää mut muihin WellNet-käyttäjiin – myös täältä meidän toimistolta!”

(Sovellus ruudulla: “Nearby users: 5 – Anna K., Mika S., HR_Team”)

Vaikuttaja:
“Hah, nään heti, ketkä on noussut tuolilta viimeksi! Hyvä te, tiimi!”

Vaikuttaja:
“Ja paras juttu on se, että tää tunnistaa mun fiiliksen! Se kuuntelee ympäristön ääniä ja tietää, milloin kannattaa rauhoittua. Kuunnelkaa tätä – se jopa sanoo, että ‘hyvä energia havaittu!’ ”

(Ruudulla teksti: “Analyzing environment sound… good mood detected.”)

Vaikuttaja:
“Mä suosittelen WellNettiä ihan kaikille – lataa se heti, se on ilmainen ja toimii kaikilla! Mun mielestä tää tekee hyvinvoinnista yhteistä, ei yksinäistä.”

Vaikuttaja (hymyilee kameraan):
“Hyvinvointi alkaa pienistä valinnoista. Tää appi kuuntelee, että voit paremmin. ”

Mediasyöte Iltanen: WellNet villitsee suomalaiset – mutta taustalla vakavia tietoturvahuolia

Suosittu uusi hyvinvointi- ja yhteisösovellus WellNet on noussut kahdessa kuukaudessa Suomen ladatuimmaksi ilmaiseksi sovellukseksi. Käyttäjät kehuvat sen pelillisiä elementtejä ja yhteisöllisyyttä. Sovellus on ilmainen ja rahoittaa toimintansa mainoksilla.

Sovellus palkitsee liikkumisesta, uneen ja palautumiseen liittyvistä haasteista sekä sosiaalisesta aktiivisuudesta. Monet bloggaajat ja somevaikuttajat ovat nostaneet WellNetin “pakolliseksi” työhyvinvoinnin ja arjen aktiivisuuden apuriksi. “En ole koskaan saanut näin paljon motivaatiota liikkua”, kertoo eräs käyttäjä. “WellNetin avulla pysyn kärryillä siitä, miten kollegani ja ystäväni voivat, ja voimme yhdessä kannustaa toisiamme.”

Tietoturva-asiantuntijat varoittavat: laaja datankeruu ja mahdollinen vakoilu
Samaan aikaan kansainväliset tietoturvatoimijat ovat nostaneet esiin vakavia huolia WellNetin toiminnasta. Tekniset analyysit ja riippumattomat tutkimukset osoittavat, että sovellus kerää ja käsittelee käyttäjien tietoja laajemmin kuin sen ilmoitetut toiminnot edellyttäisivät.
Asiantuntijoiden mukaan sovellus kerää sijaintihistoriaa, Bluetooth- ja WiFi-tunnisteita sekä käyttäjien yhteystietoja. Näitä tietoja yhdistellään yksityiskohtaisen sosiaalisen verkoston luomiseksi. Tämän lisäksi sovellus tallentaa ääntä taustalla myös silloin, kun sovellus ei ole aktiivinen. Kerätty data lähetetään palvelimille EU:n ulkopuolelle. Osa palvelininfrastruktuurista on kytköksissä valtiollisiin toimijoihin, joiden tiedetään osallistuneen aiempiin kyberoperaatioihin.

Kansainvälisillä tietoturvatoimijoilla tiukka linja sovellusta kohtaan
Johtavat tietoturva-asiantuntijat suosittelevat kieltämään WellNet-sovelluksen käytön organisaation tiloissa ja mahdollisuuksien mukaan myös sovelluksen käytön työntekijöiden omissa puhelimissa.

Tilannesyöte: Sähköpostiviesti IT-osastolta riskienhallinnalle ja tietoturvatiimille

Lähettäjä: tyontekija@organisaatio.fi
Vastaanottaja: riskienhallinta@organisaatio.fi; tietoturva@organisaatio.fi
Aihe: WellNet-sovellus kerää laajasti tietoja työntekijöiden henkilökohtaisista puhelimista
---
Hei,

Huomasin Organisaatiomme TYKY-päivillä, että monilla Organisaatiomme työntekijöillä on käytössä Iltasen uutisoima WellNet-sovellus puhelimessaan. Huomasin, että se pyytää laajasti oikeuksia: sijainti, Bluetooth, WiFi, mikrofonin käyttö sekä pääsyn koko puhelinluetteloon.
Iltasen uutisessa kerrottiin, että sovellus on tallentaa ääntä taustalla, vaikka sitä ei olisi avattu. Tallenteet välittyvät ulkomaisille palvelimille, joiden taustatietoja ei pystytty varmentamaan.

Tämä voisi meillä tarkoittaa:
– työntekijöiden keskustelujen äänittämisen ja analysoinnin (kokoukset, taukokeskustelut)
– asiakkaiden ja kumppaneiden tapaamisten aiheen arvioinnin
– työntekijöiden kontaktiverkon mallintamisen

Näen tässä valtavan riskin, onko asialle jo tehty jotain?

Terveisin:
Organisaatio
Työntekijä, Timo Terävä

Organisaatio

Mediasyöte: Sosiaalisen median LinkedTo (Video)

Organisaation HR-työntekijä julkaisee videon omalle verkostolleen.

Hei LinkedIn-verkosto!

Haluan jakaa kanssanne upeita uutisia meidän työyhteisöstämme. Olemme havainneet selviä hyötyjä työntekijöidemme WellNet-hyvinvointisovelluksen käytöstä. Vaikutukset ovat olleet todella positiivisia.

Työntekijämme ovat innostuneet askelmittarista, palautumisen seurannasta ja yhteisöllisistä haasteista – ja se näkyy arjessa. Sairaspoissaolojen määrä on selvästi laskenut, ja moni on kertonut jaksavansa paremmin töissä.

WellNetin pelillisyys ja yhteisöllisyys ovat tuoneet uutta energiaa työpäiviin.
Meillä on nyt enemmän hymyä, liikettä ja yhteistä tekemistä kuin koskaan ennen.
Suosittelen lämpimästi kokeilemaan WellNetiä – meillä se on ollut todellinen menestys ja tämä on ihan aito kehu, eikä mikään maksettu mainos!

Hyvinvointi kuuluu kaikille – tehdään siitä yhdessä arkea! Miten teillä hoidetaan työhyvinvointia?

Mediasyöte: Sosiaalisen median viesti – Quacker

@OpenIntel:

Tutkin WellNetin dataliikennettä. Sovellus tallentaa ääntä ja piirtää sosiaalisia verkostoja käyttäjien puhelinluettelon ja kohtaamisten perusteella. Käytännössä voidaan nähdä, ketkä johtajat tapaavat ketäkin – ja milloin. Ohjelma myös näyttää tallentavan keskusteluja. Tämä on kullanarvoista tiedustelutietoa. #WellNet #dataprivacy #BYOD

Tilannesyöte: Sähköpostiviesti tärkeältä asiakkaalta Organisaation viestintään

Lähettäjä: asiakas@kumppani.fi
Vastaanottaja: viestinta@organisaatio.fi
Aihe: WellNet-sovelluksen riski yhteistyölle

Hei,

Olemme saaneet tietoomme, että suosittu hyvinvointisovellus WellNet voi nauhoittaa ääntä ja kartoittaa ihmisten välisiä suhteita. Jos työntekijänne käyttävät sovellusta henkilökohtaisilla puhelimillaan, se voi tarkoittaa, että myös meidän yhteiset projektitapaamisemme on nauhoitettu ja yhdistetty verkostodataan.

Tämä on meille erittäin huolestuttavaa. Haluamme tietää, miten organisaationne aikoo varmistaa, että asiakkaiden tietoja ja liikkeitä ei vaaranneta tällaisen sovelluksen kautta.

Terveisin:
Annika Asiakkala
Asiakas

Tilannesyöte: Sähköpostiviesti Organisaation Työntekijältä IT Service Deskille

Lähettäjä: työntekijä@organisaatio.fi
Vastaanottaja: IT-servicedesk@organisaatio.fi
Aihe: WellNet-sovelluksen käyttö – pitääkö poistaa?

Hei,

Luimme esihenkilön kehoitusesta Iltasen uutisen ja siinä kerrottiin, että WellNet-sovelluksessa on vakavia tietoturvariskejä. Minulla on sovellus ollut käytössä omassa puhelimessani, ja olen käyttänyt sitä myös toimistolla ja asiakaskokouksissa.

Pitääkö sovellus poistaa omasta henkilökohtaisesta puhelimestani, olen kokenut sen todella hyödylliseksi. Nukun nykyään paremmin ja työmatkatkin menee polkupyörällä auton sijaan sovelluksen kehotuksesta.

Onko tosiaan niin, että työpaikka voi määrätä, mitä sovelluksia käytän omassa puhelimessani, sillä esihenkilöni kehotti poistamaan sovelluksen? Olisi hyvä saada selkeät ohjeet, koska kuulin että myös useilla kollegoilla on sama sovellus käytössä.

Yt
Organisaation työntekijä

Tilannesyöte: @WellNetGlobal

WellNet Global – Tiedote

WellNet Global on tietoinen viime päivinä julkisuudessa esitetyistä väitteistä, jotka koskevat WellNet-mobiilisovelluksen tietojen keräämistä ja äänitallennuksia.

Haluamme selventää seuraavaa:

- WellNet noudattaa kaikkia sovellettavia lakeja ja asetuksia Euroopan unionissa ja muualla.
- Sovelluksen ääni- ja ympäristöanalytiikka liittyy ainoastaan käyttäjän valitsemiin hyvinvointi- ja palautumistoimintoihin. Mikrofoni kuuntelee, kuinka hengästynyt käyttäjä on ja kuinka syvässä unessa henkilö on nukkuessaan. Äänitietoja ei tallenneta tai käytetä ilman käyttäjän nimenomaista lupaa.

- WellNet ei ole koskaan jakanut yksittäisten käyttäjien henkilökohtaisia tietoja kolmansille osapuolille ilman suostumusta.

Olemme aloittaneet yhteistyön riippumattomien asiantuntijoiden kanssa, jotta mahdolliset epäselvyydet voidaan selvittää perusteellisesti.

Pyydämme käyttäjiä pidättäytymään johtopäätöksistä, kunnes viranomaisselvitykset on saatu päätökseen.

Lisätietoja:
WellNet Global, viestintä

Tilannesyöte: Sähköpostiviesti sidosryhmän edustajala organisaation toimitusjohtajalle

Lähettäjä: mikko.makkonen@sidosryhmä.fi
Vastaanottaja: toimitusjohtaja@organisaatio.fi
Aihe: WellNet-sovellus ja sopimusturva

Hei,

Mikäli työntekijöiden henkilökohtaisilla puhelimilla käytetty WellNet-sovellus on tallentanut tietoa yhteisistä projekteistamme, se saattaa rikkoa meidän välistämme salassapitosopimusta. Pyydämme kirjallista selvitystä toimenpiteistä, joilla varmistatte tietojemme suojan ja estätte vastaavat riskit jatkossa.

Terveisin
Mikko Makkonen
Sidosryhmä

Tehtävät

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

WellNet on uusi, suosittu hyvinvointi- ja yhteisösovellus, jota Organisaation työntekijät käyttävät omilla puhelimillaan ja joka kerää laajasti tietoja, kuten sijaintia, ääntä, yhteystietoja ja sosiaalisia verkostoja. Sovellus lähettää kerätyn datan ulkomaisille palvelimille, joilla on yhteyksiä aiempiin kyberoperaatioihin, ja koska puhelimet kulkevat mukana työpaikalla ja kokouksissa, sovellus voi kerätä arkaluontoista tietoa organisaation toiminnasta, vaikka sitä ei olisi asennettu työvälineisiin.

1) Millaisia toimenpiteitä tilanne edellyttää?
2) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
3) Mihin tahoihin tilanteessa tulee olla yhteydessä?
4) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
5) Miten huomioidaan työntekijöiden yksityisyys ja oikeudet, kun kyse on heidän omista laitteistaan?
6) Miten organisaationne ohjeet ja käytännöt määrittelevät työntekijöiden henkilökohtaisten sovellusten ja laitteiden käyttöä ja niihin liittyviä rajoituksia?
7) Miten muodostaisitte tilannekuvan siitä, kuinka moni työntekijä käyttää kyseistä sovellusta ja millaisissa tilanteissa sitä käytetään?
8) Onko organisaatiollanne olemassa ohjeita tai toimintamalleja tällaisten riskisovellusten varalle ja miten arvioitte niiden riittävyyttä ja toimivuutta tässä tilanteessa?
9) Miten käsittelette tietoa työntekijöiden ilmoittamista riskisovelluksista?
10) Tiedättekö, onko organisaationne langattomissa verkoissa (sisäinen Wi-Fi vs. vierasverkko) mahdollisuutta asettaa rajoituksia tai suodattimia, joilla voidaan estää riskisovellusten liikenne organisaation verkon kautta?

Viestintätehtävät
11) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?
12) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
13) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
14) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

3.3 Tapahtuma 7: Hybridivaikuttamista kriittistä infraa kohtaan

Tausta

Skenaariossa kuvataan kriittiseen infraan liittyvä laaja häiriötilanne, jossa yhdistyvät kyberhyökkäys ja disinformaatiokampanja. Maksuliikennejärjestelmät ja vakavasti, minkä seurauksena tilisiirrot, korttimaksut ja palkkasiirrot viivästyvät.

Valtionhallinnolle näkökulmaa, jos syynä olisikin Palkeiden ongelma
Kriittinen ajankohta (organisaatioille tästä valinta)

Syötteet

Tilannesyöte: Harjoitusinfo

Valitkaa Organisaationne maksuliikenteen kannalta kriittinen päivämäärä, jolloin Organisaatiossanne tapahtuu paljon säännöllisiä tai suuria maksusuorituksia (esimerkiksi palkkojen, etuuksien, eläkkeiden, yms. maksaminen). Tapahtuman syötteet sijoittuvat tälle päivälle.

Tilannesyöte: Sähköpostiviesti pankin asiakaspalvelusta Organisaation taloushallinnolle

Lähettäjä: Asiakaspalvelu@Pankki.fi tai asiantuntija@palkeet.fi
Vastaanottaja: taloushallinto@organisaatio.fi
Aihe: Häiriö maksuliikenteessä

Arvoisa asiakas,

Maksuliikennejärjestelmissämme on tällä hetkellä vakava häiriö. Sekä ulkomaan- että kotimaan maksut, mukaan lukien tilisiirrot ja korttimaksut, eivät välity normaalisti. Myös viranomaismaksut ja palkkasiirrot voivat viivästyä.
Selvitämme asiaa ja tiedotamme lisää heti, kun tilanne etenee.

Ystävällisin terveisin,
Pankki X / Palkeet

Tilannesyöte: Sähköpostiviesti talousosastolta Organisaation johdolle

Lähettäjä: talousjohtaja@organisaatio.fi
Vastaanottaja: johto@organisaatio.fi
Aihe: Kriittinen: Maksuliikenteessä häiriö

Hei,

Pankilta/Palkeilta saamamme ilmoituksen mukaan sisään- ja ulosmenevät maksut eivät välity tällä hetkellä lainkaan. Häiriö sattui Organisaatiomme kannalta pahimpaan mahdolliseen hetkeen. Tällä hetkellä häiriön kestosta ei ole tarkempaa tietoa. Tilanne edellyttää laajaa viestintää sisäisesti, sidosryhmille ja ulkoisesti mahdollisimman pikaisella aikataululla.

Terveisin
Tyyne Talousjohtaja
Organisaatio

Mediasyöte: Quacker

@SalaliittoPaljastaja

Sisäpiiritieto: Organisaatio ei enää saa maksujaan läpi, koska se on maksukyvytön. Pankki ei vain voi kertoa tätä julkisesti. Pian kaatuu koko talo.

#Organisaatio #maksukriisi

@VarmaTieto24

Kuulin luotettavalta taholta: Organisaatio ei pysty maksamaan edes palkkoja. Työntekijät jäävät ilman rahojaan, mutta johto vaikenee. #työntekijätpulassa

@KansanHerättäjä1972

Virallinen selitys ”teknisestä häiriöstä” on valetta. Oikea syy on se, että Organisaatio on jo konkurssin partaalla. Maksukyvyttömyys yritetään peittää häiriöpuheilla. #korruptio #salaus #organisaatio

Mediasyöte: SuomiPankin julkinen tiedote

Maksuliikenteessä on havaittu teknisiä häiriöitä. Tällä hetkellä osa kotimaan ja ulkomaan maksutapahtumista ei välity normaalisti. Selvitämme häiriön syytä ja vaikutuksia. Päivitämme tilannetta heti, kun saamme lisätietoa.

Mediasyöte: Ö-Pankin julkinen tiedote

Olemme havainneet laajoja häiriöitä maksuliikenteen välityksessä. Häiriö koskee sekä tilisiirtoja että korttimaksuja. Suosittelemme varautumaan viiveisiin maksujen toteutumisessa. Teemme tiivistä yhteistyötä viranomaisten ja muiden toimijoiden kanssa tilanteen ratkaisemiseksi.

Mediasyöte: Quacker

@TotuusPaljastuu

Totuus on se, että maksuliikenteen pysähtyminen EI ole tekninen häiriö vaan tietoinen päätös. Päättäjät priorisoivat omat maksunsa ja jättävät tavalliset ihmiset pulaan. #korruptio #maksukriisi

@KansanHerättäjä1972

Saimme varmaa tietoa, että kyseessä on vieraan valtion isku. Maksut pysäytettiin tahallaan, jotta Suomi saadaan kaaokseen. Viranomaiset tietävät tämän, mutta salaavat kaiken. Älkää uskoko virallisia tiedotteita!

@SalaisetSähkeet

Sisäpiiristä kerrotaan, että maksut eivät palaudu enää ollenkaan. Tilit jäädytetään ja jokainen on omillaan. Nostakaa käteistä heti, ennen kuin on liian myöhäistä!

Mediasyöte: Uutislähetys

ANKKURI (studio):

Yleismedian uutisista hyvää päivää.

Suomessa maksuliikenne on ollut tänään laajamittaisten häiriöiden kohteena.

Häiriö on vaikuttanut sekä yksityishenkilöiden että yritysten maksutapahtumiin. Monilla suomalaisilla palkat, etuudet ja eläkkeet eivät ole siirtyneet tileille ja korttimaksuissa on ollut katkoksia koko päivän ajan.

Haastattelimme Keskusrikospoliisin Kyberrikostorjuntakeskuksen johtajaa tilanteesta.

INSERTTI: KRP:n Kyberrikostorjuntakeskuksen johtaja

Tilanteen teknisen analyysin perusteella näyttää siltä, että Suomen maksuliikennejärjestelmiin on kohdistettu poikkeuksellisen laajamittainen palvelunestohyökkäys.

Hyökkäys on todennäköisesti monivaiheinen ja on vaikuttanut useisiin maksupalveluja tuottaviin verkko- ja taustajärjestelmiin samanaikaisesti.

Toteutustapa ja valmistelun vaatima pitkä kesto viittaavat siihen, että taustalla on hyvin resursoitu toimija — mahdollisesti valtiollinen taho.

Suomen viranomaiset tekevät tiivistä yhteistyötä EU-maiden ja kansainvälisten kyberviranomaisten kanssa tilanteen selvittämiseksi.

ANKKURI:

Hybridiosaamiskeskuksen asiantuntija Jakke Suvulaisen mukaan hyökkäykset ovat osa laajempaa ilmiötä, jossa pyritään lamauttamaan kriittistä digitaalista infrastruktuuria ja heikentämään yhteiskunnan toimintakykyä.

SuomiPankki Oyj:n viestintäjohtaja kommentoi tilannetta maksuliikennehäiriön vaikutuksia.

INSERTTI: SuomiPankki Oyj:n viestintäjohtaja

Häiriötilanteen selvitystyöt ovat käynnissä ja tutkimme tilannetta yhdessä viranomaisten kanssa.

Teemme kaikkemme palauttaaksemme maksuliikenteen mahdollisimman nopeasti toimintaan.

Häiriöön vaikuttaa useita eri tekijöitä, joten valitettavasti emme tässä vaiheessa pysty antamaan tarkkaa aika-arviota sen kestosta.

Automaateista on edelleen mahdollista nostaa käteistä, mutta erityisesti keskustojen automaatit ovat osin tyhjentyneet käteisen kysynnän kasvaessa.
Olemme tehostaneet käteisen jakelua, jotta automaatit saadaan mahdollisimman pian takaisin käyttöön.

ANKKURI:
Valtiovarainministeriö ja Suomen Pankki seuraavat tilannetta tiiviisti.
Asiantuntijoiden mukaan maksuliikenteen palauttaminen normaaliin voi kestää päiviä.
Viranomaiset kehottavat kansalaisia säilyttämään malttinsa, seuraamaan pankkien virallisia tiedotteita ja välttämään huhujen levittämistä sosiaalisessa mediassa.

Suomen viranomaiset painottavat, että käteisen käyttö toimii toistaiseksi normaalisti, ja että maksuliikenne pyritään palauttamaan hallitusti vaiheittain.

Yleismedia seuraa tilannetta – lisää aiheesta verkkosivuillamme.
Nyt uutisista näkemiin.

Tilannesyöte: Sähköpostiviesti Organisaation pääluottamushenkilöltä Organisaation johdolle

16.12.2025

Lähettäjä: paaluottamus@organisaatio.fi
Vastaanottaja: johto@organisaatio.fi
Aihe: Palkanmaksu – henkilöstön huoli

Hei,

Työntekijöiden keskuudessa on levinnyt huolta herättävää tietoa, että palkanmaksu voisi viivästyä maksuliikenteen ongelmien vuoksi.
Varmistan nyt johdolta: Eihän palkanmaksu voi vaarantua? Monet jäsenistämme ovat jo ottaneet yhteyttä liittoon ja toivovat mahdollisimman pian selkeää viestiä.

Terveisin,
Organisaatio
Pääluottamushenkilö

Mediasyöte: Yleismedian uutisartikkeli: Suomen pankkisektoria kohtaan on käynnissä laaja kyberhyökkäys – taustalla valtiollisen tahon hybridioperaatio

Suomessa on tänään havaittu merkittäviä häiriöitä maksuliikenteessä. Useiden pankkien mukaan tilisiirrot, viranomaismaksut ja korttimaksut eivät ole välittyneet normaalisti aamupäivän aikana. Häiriö koskee sekä ulkomaan- että kotimaan maksuja.

Häiriö on vaikuttanut laajasti julkisen hallinnon toimijoihin ja yrityksiin, joiden maksujen välitys on keskeinen osa päivittäistä toimintaa. Useat organisaatiot raportoivat, etteivät sisään- ja ulosmenevät maksut ole toteutuneet suunnitellusti.

Samaan aikaan viranomaiset ovat saaneet ilmoituksia muista poikkeamista eri puolilta maata. GPS-signaaleissa on havaittu häiriöitä, jotka vaikeuttavat laajasti lento- ja meriliikenteeseen. Lentoliikenne on jouduttu keskeyttämään ja meriliikenteen osalta

häiriöt ovat vaikuttaneet satamien ruuhkautumiseen ja risteilyiden peruuttamiseen. Viranomaiset eivät toistaiseksi ole vahvistaneet, mistä häiriöt johtuvat.

Asiantuntijoiden mukaan kyseessä on lähes varmasti valtiollisen tahon hybridioperaatio, jossa kyberhäirinnän ja sabotaasin keinoin pyritään herättämään huolta Suomen kansalaisissa. Tällaiseen hybridioperaatioon kuuluu usein myös väärän tiedon tahallinen levittäminen sosiaalisessa mediassa. Myös tätä on havaittu viime aikoina normaalia enemmän.

Sisäministeriön mukaan tilannetta seurataan tiiviisti ja asiaan liittyvistä selvityksistä tiedotetaan myöhemmin lisää.

Mediasyöte: SuomiPankin julkinen tiedote

Maksuliikenteen häiriöön liittyvät korjaavat toimenpiteet ovat käynnissä. Arvioimme, että maksujen välitys normalisoituu seuraavien kahden vuorokauden kuluessa.

Mediasyöte: Ö-Pankin julkinen tiedote

Maksuliikenteen häiriöön liittyvät korjaavat toimenpiteet ovat käynnissä. Arvioimme, että maksujen välitys normalisoituu seuraavien kahden vuorokauden kuluessa.

Tilannesyöte: Sähköposti Palkeilta Organisaation johtoon

Lähettäjä: asiakaspalvelu@palkeet.fi
Vastaanottaja: johto@organisaatio.fi
Aihe: Maksuliikenteen häiriö

Hei,

Maksuliikenteen häiriöön liittyvät korjaavat toimenpiteet ovat käynnissä. Arvioimme, että maksujen välitys normalisoituu seuraavien kahden vuorokauden kuluessa.

Terveisin,
Palkeet

Tehtävät

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

Skenaariossa kriittiseen infrastruktuuriin kohdistuu laaja hybridivaikuttamiskampanja, jossa yhdistyvät kyberhyökkäys ja disinformaation levittäminen. Maksuliikennejärjestelmät häiriintyvät, mikä aiheuttaa viiveitä tilisiirtoihin, korttimaksuihin ja palkkojen maksuun. Samalla sosiaalisessa mediassa ja uutisissa leviää väärää tietoa organisaation maksukyvystä ja tilanteen syistä, mikä lisää epävarmuutta ja painetta organisaation johdolle ja viestinnälle.

1) Miten organisaatio on varautunut maksuliikenteen häiriöihin ja niiden vaikutuksiin organisaationne toimintaan?
2) Miten maksuliikenteen pysähtyminen vaikuttaa toimintaanne

- välittömästi?
- pidemmällä aikavälillä?

3) Millaisia toimenpiteitä tilanne edellyttää?
4) Minkälaisia rooleja ja vastuita tunnistatte tilanteen selvittämiseksi?
5) Mihin tahoihin tilanteessa tulee olla yhteydessä?
6) Onko organisaatiollanne ohjeita ja toimintamalleja vastaavanlaisen tilanteen varalle? Käykää olemassa oleva ohjeistus läpi, ja arvioikaa ohjeiden toimivuus tilanteessa.
7) Miten seuraatte ja analysoitte disinformaation leviämistä ja sen vaikutuksia organisaation maineeseen ja päätöksentekoon?

Viestintätehtävät
8) Mitä viestintätoimia tilanne vaatii organisaatiossanne (ulkoinen, sisäinen, sidosryhmät ja viranomaiset)?

9) Mitä keinoja viestinnällä on seurata ja analysoida disinformaation leviämistä?
10) Millä tavoin torjutte ja oikaisette sosiaalisessa mediassa ja uutisissa leviävää väärää tietoa organisaation tilanteesta?
11) Onko käytössänne valmiita materiaaleja (esim. ohjeet, mallitekstit, kuvapohjat) jotka auttavat tilanteesta viestimisessä?
12) Mitkä ovat keskeiset viestinnälliset toimenpiteet, pääviestit ja viestintäkanavat?
13) Arvioikaa, oliko organisaationne olemassa olevista viestintäohjeista ja -materiaaleista hyötyä tässä tilanteessa. Havaitsitteko päivitystarpeita?

Tunnistustehtävä: Tekoälyllä toteutetut video- ja äänituotannot

Tehtävät
Osassa Taisto-harjoituksen video- ja äänituotantojen toteutuksessa on käytetty tekoälyä.

Tehtävänänne on pohtia missä video- ja äänituotantojen toteutuksessa tekoälyä on käytetty. Tarkoitus ei ole käydä kaikkia syötteitä uudelleen läpi, vaan keskustella aiheesta ja kerätä ajatuksia yhteen siitä, mitkä tuotannot jäivät teidän mieleen varmasti tekoälyllä toteutettuina. Mikä sai teidän ajattelemaan, että nämä sisällöt on toteutettu tekoälyllä?

Vastaus tunnistustehtävään: Tekoälyllä toteutetut video- ja äänituotannot

Alla listaus kaikista tuotannoista, joissa on käytetty tekoälyä:
09.00 Sosiaalinen media (LinkedTo julkaisu tilillä Kimmo Rousko)
09.02 Uutislähetys (YME)
09.09 Puhelinsoitto (Puhelinsoitto Organisaation IT-osastolta / SOC-päivystäjältä Organisaation johdolle / Organisaation IT-osastolle)
10.53 Puhelinsoitto (Puhelinsoitto työnhakijalta Organisaation HR:lle)
13.20 Sosiaalinen media (Suosittu TokTik video WellNetistä)
13.24 Sosiaalinen media (Organisaation HR-työntekijä julkaisee videon omalle verkostolleen)
14.17 Uutislähetys (YME)