DIGI- JA VÄESTÖTIETO-VIRASTO

TAISTO20-harjoitus

Käsikirjoitus

3.2.2021

Digitalisaation tukipalvelut ja yhteentoimivuus 3.2.2021

Dokumentinhallinta

Omistaja	Hanna Heikkinen
Laatinut	Hanna Heikkinen, Laura Penttilä

Sisällysluettelo

TAISTO20-harjoitus

1 Harjoituksen aloitus

TAISTO20-harjoitus alkoi harjoitusalustalla julkaistuilla infosyötteillä, joissa ohjeistettiin harjoituspäivän kulkua. Harjoituspäivän aikataulu on käsikirjoituksen liitteenä.

1.1 Harjoitusinfo videot

- **TAISTO20-harjoituksen avaustervehdys**

  Linkki: https://www.youtube.com/watch?v=L3B7n0s0lMQ&feature=youtu.be

- **Alivaltiosihteeri Päivi Nergin tervehdys TAISTO-harjoitukseen osallistuville**

  Linkki: https://www.youtube.com/watch?v=k23FAU4xRrw&feature=youtu.be

- **Tietoisku Keskusrikospoliisi**

  Linkki: https://www.youtube.com/watch?v=FGV0MePkACg&feature=youtu.be

- **Tietoisku TSV**

  Linkki: https://www.youtube.com/watch?v=L0jGVUA5TCc&feature=youtu.be

- **Tietoisku KTK**

  Linkki: https://www.youtube.com/watch?v=S7IqLNztZv8&feature=youtu.be

1.2 Harjoituksen maailmankuva

- **Yleismedian uutiset**

  Linkki: https://www.youtube.com/watch?v=-KC1GaA178c&feature=youtu.be

- **Iltanen lehti, uutinen**

  ”Lisääntyvät irtisanomiset ja lomautukset ovat lisänneet merkittävästi epävarmuutta suomalaisten keskuudessa, selviää Iltasen gallupista”

  Lisääntyvät irtisanomiset ja lomautukset ovat lisänneet merkittävästi epävarmuutta suomalaisten keskuudessa, selviää Iltasen gallupista.

  Kyselyn mukaan ihmiset ovat turhautuneita pandemian aiheuttamien toimenpiteiden pitkäkestoisuuteen. Pandemian kolmas vaihe uhkaa pahentaa levottomuuksia ja syventää suomalaisten tyytymättömyyttä työympäristössä entisestään. Osa pelkää miltä oma tulevaisuus näyttää ja onko töitä enää jatkossa. Vastaajista 75,2 prosenttia pelkää massiivisia irtisanomisia, selviää Iltasen teettämästä gallupista. Työmarkkinajärjestöt ovat erittäin huolissaan pandemian kolmannen vaiheen seurauksien suunnasta.

- **Talouslehti, uutinen**

”Talouskriisi uhkaa organisaatioiden lakisääteisten, strategisten, sopimuksenvaraisten ja muiden velvoitteiden toteuttamista”

Organisaatiot odottavat jatkotoimia kriisin hillitsemiseksi sekavissa olosuhteissa. Talouselämän epävarmuus heijastuu suoraan myös yksittäisten suomalaisten turvallisuudentunteeseen ja uskoon tulevasta

Kasvanut rikollisuus lisää entisestään epävarmuutta suomalaisten keskuudessa. Valeuutiset ja uudet huijausyritykset ovat lisääntyneet vauhdilla eikä vauhti ole laantumassa. Huijauspuhelut ovat lisääntyneet merkittävästi ja samalla huijauksien laatu on parantunut. Numeroiden väärentäminen on myös yleistynyt, jolloin puhelun saanut henkilö voi luulla puhelun tulevan tutusta numerosta, mutta oikeasti taustalla on ammattimainen huijausyritys.

2 Tapahtuma tietovuoto

2.1 Sähköposti: onkohan nämä teidän tietoja?

FROM: whitehat@hackers.org
TO: tietoturva@organisaatio.fi
SUBJECT: Onkohan nämä teidän tietoja?

Hei,

Darknetin Suomilaudalla tuli vastaan teidän Organisaatiostanne peräisin olevia henkilötietoja, onkohan tämä jo teillä tiedossa?

ilonro	sukunimi	etunimet	ammattiliitto	osoite	kaupunki	iban	pun
15482	Lukkarinen	Anna Emilia	PRO	KIRKKOKAT	HELSINKI	FI3636520154452	3585045445
16548	Virtanen	Jouko Juho	JHL	SAHAKATU	VANTAA	FI3636545815454	3584548484
45154	Mattila	Erkki Mika	Juko	KESKUSTIE	JYVÄSKYLÄ	FI3636520154452	3584051522
35842	Järvi	Antti-Pekka	PRO	MANNERHE	HELSINKI	FI5006545815454	3583554561
50678	Peräaaa	Sirkka-Liisa	YTY	TALOKATU	KAUNIAINEN	FI3636520154452	3583057599
59646	Sutinen	Pentti Tapio	OAJ	PIRKKATIE	OULU	FI3636545815454	3582560638
68615	Merikoski	Juho Matti	JHL	MERIKORTT	TAMPERE	FI8000520154452	3582063676
17583	Kantonen	Eero Elia	JHL	KORTTELIKI	KAUNIAINEN	FI3636545815454	3581566715
86552	Nieminen	Juho Pekka	OAJ	SATAMAKA	TAMPERE	FI3636520154452	3581069753
95521	Fors	Sakari Mika	PRO	ITSENÄISYY	HELSINKI	FI3636545815454	3580572792
84511	Koskela	Elina Minna	PRO	KOSKIKATU	VANTAA	FI7575520154452	3580075830
73501	Korhonen	Kalle Kustavi	JHL	PERENNAPI	VANTAA	FI3636545815454	3585078869
62491	Päivönen	Karoliina Katja	PRO	SATTUMAKI	HELSINKI	FI3636520154452	3585081907
51481	Korhonen	Sari-Sisko	PRO	LINTUREITT	VANTAA	FI3636545815454	3585084946
40471	Virtamaa	Samuli Erkinpoika	Juko	HALUTISKE	PORI	FI3636520154452	3584087284

Ystävällisin terveisin,
Verkkoritari86

2.2 Tehtävät

Organisaation henkilötietoja on vuodettu verkkoon. Henkilötiedot ovat peräisin Organisaation järjestelmistä/dokumenteista, jotka sisältävät arkaluonteisia tietoja henkilöstöstä.

Pohtikaa, mitä organisaationne järjestelmää mahdollinen tietovuoto voisi koskea. Halutessanne voitte myös valita jonkin tietyn järjestelmän, johon peilaatte tämän harjoituksen tapahtumia.

1. Miten reagoitte tietovuotouutiseen?
2. Arvioikaa tilannetta omaan organisaatioonne peilaten;
    a. Onko olemassa toimintaohjeita tietovuototapahtuman varalle?
    b. Onko henkilörekistereihin liittyvät riskit otettu riittävällä tavalla huomioon riskiarvioissa?

c. Jos riskiarvioinnin perusteella on todettu erityisten henkilötietoryhmien (arkaluonteisten henkilötietojen) osalta aiheutuvan merkittävää tai suurta haittaa rekisteröidylle, miten tämä on huomioitu organisaation toimintamalleissa?
d. Ovatko vastuut määritelty riittävästi (mukaan lukien palveluntuottajat) – ja vastuuhenkilöillä tarpeellinen tietotaso kohdata ja alkaa johtamaan vastaavaa tilannetta?
e. Onko järjestelmistä saatavilla lokitietoja, joiden perusteella asiaa voitaisiin ryhtyä selvittämään? Jos ette itse hallinnoi omia tietokantoja, onko tiedossa esim. listausta palveluntuottajista, joihin tulisi olla yhteydessä?
f. Kattaako palveluntuottajien kanssa tehdyt sopimukset myös henkilötietojen käsittelyn?
g. Miten turvaatte ja käsittelisitte mahdollisen todistusaineiston? Tiedättekö mitä tietoja tulisi etsiä ja mitä tulee ottaa talteen ja mistä?

3. Käynnistäkää tilanteen käsitteleminen oman organisaationne prosessien ja ohjeiden mukaisesti.
4. Tekisittekö tässä vaiheessa ilmoituksen viranomaisille? Jos tekisitte, niin kenelle ja miksi?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 9:34.

2.3 Viti-lehti: ”Suomalaisten henkilötietoja jälleen verkossa”

”Organisaation henkilötietoja on vuodettu verkkoon. Henkilötietojen epäillään olevan peräisin Organisaation dokumenteista, joita on raportoitu löytyvän sekä julkisesta internetistä että pimeän verkon puolelta. Dokumenttien on kerrottu sisältävän arkaluonteisia tietoja henkilöstöstä. Viti on saanut useita vihjeitä tuoreesta tietovuototapauksesta.

”Näyttää siltä, että dokumentit on tahallaan vuodettu verkkoon”, Vitin lähde sanoo.

Lisää aiheesta hetken kuluttua.”

2.4 Tehtävät

Organisaation henkilötietoja on vuodettu verkkoon ja media on tarttunut aiheeseen.

1. Miten reagoitte tällaiseen uutiseen? Miten toimitte?
2. Onko organisaationne määritellyt tiedotusvastuut? Keneen otatte yhteyttä organisaatiossanne?
3. Onko organisaatiossanne kriisi- ja häiriöviestintäsuunnitelma? Oletteko tarkistaneet suunnitelman ja sen ajantasaisuuden?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 9:43.

2.5 Sähköposti: Organisaation työntekijältä Riskienhallintajohtajalle/Turvallisuusjohtajalle

FROM: tiina.tyontekija@organisaatio.fi
TO: Organisaatio Riskienhallintajohtaja / Turvallisuusjohtaja
SUBJECT: Tiedoksi luottamuksella Terve jälleen,

Hei,

Lähestyn sinua hyvin luottamuksellisella asialla.

Olen hyvin huolissani työkaveristani täällä ICT-puolella. Hänen puheistaan ja teoistaan tulee ilmi, että hän on erittäin tuohtunut ja tyytymätön Organisaatiomme toimintaan. Ollaan oltu työkavereita jo pitkään, mutta nyt on suhtautuminen töihin on selvästi muuttunut. Minulla on sellainen huoli, että hän saattaa tehdä jotain harkitsematonta.

Terv. Tiina
ICT / Organisaatio

2.6 Sähköposti: Havainto admin-tunnuksista

FROM: whitehat@hackers.org
TO: tietosuoja@organisaatio.fi/tietoturva@organisaatio.fi
SUBJECT: Havainto admin-tunnuksista

Terve jälleen,

Pistimme jo aikaisemmin viestiä, että henkilötietojanne oli julkaistu Darknetin suomilaudalla. Joko tämä on hoidossa?

Nyt tiimimme on havainnut, että darknet-verkossa on tänään alkanut kiertämään käyttäjätunnuksia. Näiden väitetään olevan peräti admin-tason tunnuksia. Ja vaikuttaa, että nämäkin ovat teidän organisaatiostanne peräisin.

Terveisin ystävänne
Verkkoritari86

2.7 Tehtävät

Organisaation työntekijä on ilmaissut huolensa työkaverinsa toimista. Lisäksi organisaation admintunnuksia on vuodettu verkkoon. Tunnukset ovat peräisin organisaation eri järjestelmistä.

1. Miten aloitatte selvitystyön?
2. Kuka hallinnoi organisaationne järjestelmien pääkäyttäjätunnuksia?
3. Onko vastuut määritelty – kuka tilannetta johtaa ja keitä asiantuntijatahoja tulee kutsua mukaan? Kuka voi tehdä päätöksen esim. kriittisten järjestelmien alasajosta tai vastata siitä, että salasanat saadaan huolella vaihdatettua?
4. Onko organisaatiossanne varauduttu vastaavaan tilanteeseen (esimerkiksi järjestelmän riskiarvioinnissa)?

5. Onko organisaatiossanne tunnistettu miten salasanojen vuotaminen voi vaikuttaa organisaation muihin palveluihin (Business Impact Analysis)?
6. Kuka organisaatiossanne vastaa sidosryhmäviestinnästä vastaavassa tilanteessa?
7. Miten organisaationne seuraa ja valvoo järjestelmien pääkäyttäjätunnuksien jakautumista ja käyttöä?

Lisätehtävät:

1. Miten häiriötilanteiden vasteajat on sovittu palvelutasosopimuksessa (Service Level Agreement, SLA)?
2. Onko määritelty miten nopeasti häiriötilanteesta pitää palautua normaalitilaan (Toipumisaikatavoite eli Recovery Time Objective, RTO)?
3. Onko mietitty miltä ajalta tietoa voidaan maksimissaan menettää (Tiedon menetysjakso eli Recovery Point Objective, RPO)?
4. Onko määritelty toimintamallia, miten menetetyn tiedon osalta toimitaan?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 10:10.

3 Tapahtuma valeuutinen

3.1 TÄH?!-lehti ”massiivisia irtisanomisia tiedossa Organisaatiossa”

Lue yksinoikeudella TÄH?!-lehdestä

Yli puolet irtisanotaan!

Toimituksemme saamien vihjeiden mukaan Organisaatio on aloittamassa jättimäiset irtisanomistoimet. Lähellä Organisaation hallitusta olevat, nimettömänä pysyvät lähteet kertovat, että organisaatio irtisanoo yli puolet työntekijöistään. Talousjohtaja on ilmoittanut suurista vaikeuksista ja ennakoi, että palkkoja jää maksamatta.

TÄH-lehden talousasiantuntija, ekonomi Mart Keski-Alanen pitää uutista ikävänä mutta odotettavissa olevana, "tätä on osannut jo odotella, että jokin suuri suomalainen työnantaja pääsee käyttämään pandemiatilannetta ja näennäisiä talousvaikutuksia keppihevosena, ja siten pääsee parantelemaan lukujaan." Keski-Alasen mielestä pandemian todellisista talousvaikutuksista ei voi vielä olla todennettua tietoa tarpeeksi, jotta näin radikaaleihin toimenpiteisiin voitaisiin perustellusti ryhtyä. "Aivan luokatonta toimintaa", toteaa Keski-Alanen.

Ja taas saadaan yksityisautoilua vähennettyä! Ja mieluusti myös lihansyöntiä!

"Tässä on selkeästi vihervasemmistolainen agenda taustalla", toteaa lehden politiikan erikoistutkija Pavel Möntönen. "Nyt on oiva tilaisuus muokata rakenteita heidän ihanteiden mukaiseen malliin, ja valtamedia toistelee auliaasti totuuksina kaiken. Pandemian vika, ei mahda mitään! Kolmas aalto on jo nurkan takana! Ja muita koottuja valheita. Tässä on kaikki klassisen salaliiton ainekset kasassa!", julistaa Möntönen.

Samainen Organisaatio on ollut tänään muutoinkin otsikoissa liittyen epäiltyyn tietovuotoon, jossa satojen henkilöiden tietoja olisi vuotanut verkkoon.

Tietovuodosta kertoi ensimmäiseksi teknologialehti ViTi.

3.2 Quacker: @make

”Noniin, tätä osattiin odottaa #Organisaatio. Tältä organisaatiolta saa varmasti kenkää.”

3.3 Quacker: @jaska

”TÄH-lehti kertoo taas totuuden! Se on saletti että Organisaatiolta voi odottaa vain kengänkuvaa.”

3.4 Quacker: @masa

”#Organisaatio #fudut #rkeleenkorona”

3.5 Tehtävät

Eri medioissa leviää epäilyttäviä uutisia organisaatiostanne.

1. Miltä uutinen ja somekeskustelu vaikuttavat? Ovatko uutinen ja somekeskustelu uskottavia?
2. Miten tunnistatte valeuutisen? Miten varmistatte uutisen aitouden?
3. Miten organisaationne reagoi tilanteeseen, jossa organisaatiosta leviää verkkomediassa vauhdilla tällaista tietoa? Miten reagoitte sosiaalisessa mediassa? Entä organisaation sisällä?
4. Onko organisaationne viestintäohjeistuksessa tai -politiikoissa määritelty, kuinka tällaisessa tilanteessa tulee reagoida? Kenellä on tiedotusvastuu?
5. Onko organisaatiossanne määritelty sosiaalisen median seurantaa? Miettikää, miten vastaava uutinen ja somekeskustelu havaittaisiin organisaatiossanne?
6. Onko roolit määritelty tällaisten tilanteiden varalle?
7. Oletteko jo tehneet viranomaisilmoitukset?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 10:30.

4 Tapahtuma inhimillinen virhe

4.1 Sähköposti: Organisaation työntekijältä ICT-tuelle

FROM: ville.tyontekija@organisaatio.fi
TO: Organisaation ICT-tuki
SUBJECT: Ongelma pilvipalvelun kanssa

Morjens!

Olisi vähän ongelmia pilvipalvelun kanssa, ja tarvitsisin pikaisesti apuja.

Minun työpuhelimeni vaihtui uuteen leasing-kauden päättyessä. Kun luuri vaihtui, minulla meni näemmä pääsy puhelimen omaan pilvipalveluun, joka oli siis ilmeisesti linkitetty

vanhan puhelimen tiliin. Minulla ei ainakaan ole sinne mitään tunnuksia, ja uusi puhelin on eri valmistajalta, joten en saanut tuota pilvipalvelu-äppiä ei tähän puhelimeen.

Olen ladannut erään hankkeen tietoja tuonne kyseiseen pilveen, koska en saanut niitä muuten lähetettyä sidosryhmäkumppanille. Kansio oli sen verran iso, että sitä ei onnistunut laittaa työsähköpostin liitetiedostoinakaan, ja oli kiire. Ongelma on se, että ainoat kopiot materiaalista ovat siellä pilvessä, ja tarvitsisin pääsyn niihin pikaisesti, jotta hommat jatkuu.

Mietin myös näin jälkikäteen, että eihän tiedot ole voineet päätyä vääriin käsiin?

Mitenköhän tässä pitäisi toimia ja miten saan noi tiedot tuolta pilvestä takaisin?

Terv. Ville
Asiantuntija
Organisaatio

4.2 Tehtävät

Organisaation työntekijä on ladannut tiedostoja henkilökohtaiseen/määrittelemättömään pilvipalveluun.

1. Onko organisaation tietoturvapolitiikka kattava ja ajantasainen?
2. Onko henkilöstölle järjestetty tietoturvakoulutusta ja tietoturvapolitiikka jalkautettu organisaatiossa?
3. Onko organisaatio varautunut vastaavaan tilanteeseen?
4. Miten lähdette ratkaisemaan tilannetta?
5. Kuinka tiedot saadaan pois pilvipalvelusta?
6. Miten voidaan varmistua, että tieto ei ole levinnyt?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 10:45.

5 Tapahtuma louhintahaittaohjelma

5.1 Sisäinen tiedote: IT-tuelta koko Organisaatiolle, Sisäverkossa hitautta

FROM: it_support@organisaatio.fi
TO: Organisaation jakelulista: kaikki työntekijät
SUBJECT: Sisäverkossa hitautta

Organisaation it-yksikkö tiedottaa
Häiriöitä sisäverkossa

Organisaation sisäverkossa on havaittu merkittävää hitautta.

IT-tuki on saanut lukuisia yhteydenottoja organisaation sisäverkon hitaudesta. Selvitämme häiriötä ja sen laajuutta. Tiedotamme asiasta uudelleen pian.

Lisätiedot IT-tuki

5.2 Quacker: @Maija Metsäläinen

”Jes, ei taas pääse kirjautumaan #Organisaation palveluun #Organisaatio #palvelut_alhaalla #pitihansearvata”

5.3 Quacker: @Petteri Kuusela

”ReQuack: @Maija_Metsäläinen Jep, kuulostaa aika normipäivältä. #Organisaatio #verkkoongelmat #ei_yllätä”

5.4 Sähköposti: Asiakaspalveluvastaavalta koko organisaatiolle

FROM: asiakaspalvelu@organisaatio.fi
TO: Organisaatio
SUBJECT: Asiakaspalvelu ruuhkautunut

Tiedoksi koko organisaatiolle,

asiakaspalvelumme on pahoin ruuhkautunut. Meille on tulvinut yhteydenottoja siitä, ettei verkkopalvelumme vastaa tai on äärimmäisen hidas.

Terv. Anja
Asiakaspalveluvastaava
Organisaatio

5.5 Quacker: @Jonna Böcker

”Luulin, että kaikkien uudistusten tarkoitus oli parantaa palvelun toimivuutta, mutta tuntuu siltä, että mentiin ojasta allikkoon” Erroria vaan pukkaa kun yritän kirjautua sisään. #Organisaatio #error”

5.6 Tehtävät

Organisaation sisäverkon toiminta on hidastunut. Lisäksi organisaation sähköisissä palveluissa on havaittu hitautta eivätkä ne vastaa pyyntöihin.

1. Miten reagoitte tietoihin sisäverkon ongelmista ja siihen liittyvään somekeskusteluun?
2. Miten toteutatte ja priorisoitte häiriötilanteessa sosiaalisen median seuraamisen?
3. Onko organisaatiollanne olemassa häiriönhallintasuunnitelmaa? Onko suunnitelma ajan tasalla? Onko vastaavan tilanteen varalle suunniteltu toimenpiteitä?
4. Mieti, mitä tapahtuu, jos organisaation palvelut eivät toimi sisäverkon hitauden vuoksi? Kuinka ongelma tunnistetaan organisaatiossa – onko ilmoitusketjut mietitty ennakolta?
5. Kuinka asiasta viestitään sisäisesti? Kenellä on sisäisen tiedottamisen vastuu?
6. Toimikaa organisaation ohjeiden mukaisesti. Ovatko ohjeistukset ja suunnitelmat ajan tasalla?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 11:04.

5.7 Talouslehti: ”Organisaation verkkopalveluissa vakavia ongelmia”

”Ongelmat organisaation sähköisissä palveluissa jatkuvat. Häiriö vaikeuttaa merkittävästi Organisaation sähköisten palveluiden käyttöä. Palvelun ongelmat ovat laajavaikutteisia, sillä Organisaation palvelut ovat erittäin suosittuja.

Toimitus tavoitti Organisaation ICT-asiantuntijan kommentoimaan tilannetta ja hänen mukaansa vielä ei osata arvioida, milloin ongelma saadaan kuntoon eikä ongelman syytä vielä tiedetä.

Organisaatio pitää tilannetta vakavana. Organisaatio on päättänyt sulkea palvelut häiriön selvityksen ajaksi.”

5.8 Tehtävät

Mediassa on uutisoitu Organisaation verkkopalveluiden ongelmista.

1. Miten reagoitte mediauutiseen?
2. Kenellä on tiedotusvastuu asiassa?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 11:14.

5.9 Sähköposti: Tietoliikennepalveluntarjoajalta ICT-vastaavalle

FROM: Tietoliikennepalveluntarjoaja
TO: Organisaation ICT-vastaava
SUBJECT: Komentopalvelinliikennettä havaittu

Hei,

Olemme havainneet tunnettua komentopalvelinliikennettä verkossanne. Havainto on tehty normaalissa verkkovalvonnassa.

Useat organisaatiot ovat ilmoittaneet louhintahaittaohjelmahavainnoista. Organisaatioiden tietoturva-asiantuntijoiden mukaan louhintahaittaohjelma on aiheuttanut hitautta organisaation palveluiden käytössä laajemminkin.

Terveisin:
Verkkovalvonta
Tietoliikennepalveluntarjoaja

5.10 Tehtävät

Organisaation verkoissa on havaittu komentopalvelinliikennettä, joka on aiheuttanut hitautta verkoissa.

1. Mikä on palvelun toimittajan rooli tässä tilanteessa?
2. Mitä pitää tehdä, jotta organisaatio voi varmistua siitä, että häiriön vuoksi toimimaton palvelu saadaan palautettua takaisin toimintaan?
3. Miten varmistatte, että palveluiden tietoturvallisuus ei ole vaarantunut häiriön vuoksi?
4. Miten ja kenelle tilanteen selviämisestä pitää viestiä?
5. Jos olette tehneet viranomaisilmoituksia, miten päivitätte niitä?
6. Millaisia ovat:
    1. häiriön aiheuttama ja potentiaalinen vaikutus tietojärjestelmiin?
    2. häiriön mahdolliset seurannaisvaikutukset organisaation toimintaan?
    3. häiriön ja siihen reagoimisen taloudelliset seuraukset?
    4. häiriön vaikutus organisaation julkisuuskuvaan ja sidosryhmiin
7. Oletteko huomioineet, tunnistaneet ja viestittäneet häiriöstä erityisesti niille tahoille, jotka ovat riippuvaisia teidän tuottamastanne palvelusta?
8. Kuka johtaa tilannetta?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 11:30.

6 Harjoituksen iltapäivän osuus

6.1 IL-TV: Työntekijöiden heikot digitaidot yleistyvien tietovuotojen takana?

”Tietoturvataitojen puutteiden lisäksi huolta on aiheuttanut yhä merkittävämpi vaatimus hyvästä medialukutaidosta. Lisääntynyt tietojen kalastelu, valeuutisointi ja erilaiset disinformaatiokampanjat huolettavat monia organisaatioita. Yhä useammalla henkilöllä on vaikeuksia tunnistaa virheellinen tai jopa haitallinen tieto oikeasta tiedosta.

Yhtenä syynä kasvaneisiin tietovuotojen määrään epäillääkin olevan digitaitojen puute. Katso alta verkkotoimituksemme haastattelu aiheesta.

Videoon pääset täältä https://www.youtube.com/watch?v=alBwhExb0DQ&feature=youtu.be”

7 Tapahtuma henkilö ei ole käytettävissä

7.1 Organisaation henkilö X joutuu poistumaan harjoituksesta

Valitkaa organisaatiolle yksi kriittinen henkilö, joka siirtyy sivuun harjoituksesta. Iltapäivän harjoitusosuuden teemat keskittyvät haavoittuvuuksien ja maksuliikenteen hyväksikäyttämiseen. Suosittelemme valitsemaan henkilön näistä rooleista. Vaihtoehdot harjoituksesta aktiivisesta osuudesta poistuvalle henkilölle ovat:

1. Henkilö siirtyy tarkkailemaan harjoitusryhmän toimintaa siitä näkökulmasta, miten toiminnot organisoidaan ja tehtävät saadaan suoritettua, kun kyseinen rooli on pois käytöstä tehtävien hoidosta. Kyseinen henkilö ei saa osallistua keskusteluun tai antaa neuvoja muille harjoitukseen osallistuville. Tarkkailijaksi siirtyvä henkilö voi havainnoida esimerkiksi seuraavia asioita:
   - Onko roolintehtävät ohjeistettu ja koulutettu riittävän hyvin, jotta tehtävät pystytään hoitamaan harjoituksessa?
   - Henkilö seuraa harjoitusryhmän toimintaa ja tekee havaintoja, jotka koskevat hänen vastuualueellaan olevia tehtäviä ja muodostaa niiden pohjalta kehittämistoimenpiteitä.

2. Henkilö vapautetaan kokonaan harjoituksesta.

Suosittelemme vaihtoehtoa yksi, jolloin organisaatio saa enemmän hyötyä harjoituksesta.

HUOM! TAISTO20 Tarkkailijan havainnot -lomake on liitteenä.

Seuraava syöte julkaistaan klo 12:40.

7.2 Tehtävät

Organisaation yhden kriittisen henkilön tehtävät ovat siirtyneet varahenkilön hoidettavaksi.

Pohtikaa oman organisaationne kannalta seuraavia teemoja:

1. Onko jokin osa-alue henkilöytynyt liikaa yhden asiantuntijan harteille?
2. Pohtikaa harjoituksen teemoja varahenkilöjärjestelyiden kautta.
3. Onko ohjeet, prosessit ja sijaisuusjärjestelyt organisaatiossanne ajantasaisia ja riittäviä?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 12:49.

7.3 Yleismedia: ”Somebotit haittaavat tiedonkulkua myös suomeksi yhä enemmän”

”Botiksi kutsutaan automatisoitua tiliä, joka pyrkii esiintymään oikeana ihmisenä. Toiset botit onnistuvat tässä paremmin kuin toiset. Bottitilejä löytyy kaikista sosiaalisen median palveluista, mutta viime aikoina botteja on tunnistettu myös yhä enemmän suomenkielisistä somesisällöistä. Aiemmin suomalainen oli paremmin turvassa harvinaisen kielensä takia, jonka tökeröt automaattikäännökset tunnistivat melko helposti. "Kielellisesti bottitilien tuottama teksti on parantunut merkittävästi, tosin tekstisisältö on edelleen usein melko päätöntä jargonia, vaikka kieliopillisesti olisikin lähes virheetöntä", toteaa tietoturva-asiantuntija Ari Arviainen I-secure Oy:stä.

Tukkii viestikanavat

Bottiverkostoja voidaan käyttää myös silloin, kun halutaan jokin asia puhutuimpien aiheiden listalle, eli niin sanotusti trendaamaan. Voi sanoa, ettei trending-listoilla ole enää mitään

merkitystä, koska niiden manipulointi on niin helppoa. Omaa, faktoihin perustuvaa tietoa voi olla vaikeaa saada esille, jos samalla aihetunnisteella asiasta tulvii bottiverkkojen tuottamaa sisältöä. Kiusantekijälle tämä ei välttämättä edes käy kalliiksi: jo muutamilla satasilla voi netistä tilata vastaavia palveluita omien tarkoitusperien toteuttamiseen. "Se on sitä nykyajan kiusantekoa, suhteellisen halpaa ja onnistuu kotisohvalta käsin", Arviainen kuittaa."

8 Tapahtuma tietovuoto

8.1 Sähköposti: Valkohattuhakkerilta organisaatiolle

FROM: whitehat@hackers.org
TO: Organisaatio
SUBJECT: Vinkki

Moikka moi!

Jälleen tiedoksi teille, että Darknetin rottatori-palstalla on myynnissä teidän organisaatioonne liittyviä asiakirjoja ja yksityiskohtaisia tietoja teidän järjestelmien haavoittuvuuksista.

Laadin tästä jo anonyymin nettivinkin poliisille. Alla kuvakaappaus.

Terkuin,

Verkkoritari86

PS. Koettakaa nyt saada näitä kuntoon. Kaikki eivät ole näin ystävällisiä kuin minä.

8.2 Quacker: @hackfin

”LOL Organisaation tietoturva FTW!

Darknetissä kiertää pitkä lista organisaation tietoturvan aukoista
#Organisaatio #haava”

8.3 Tehtävät

Organisaation tietoja kaupitellaan pimeässä verkossa.

1. Toimikaa organisaationne ohjeiden ja prosessien mukaisesti.

2. Onko olemassa ohjeistusta, kuinka viestiin reagoidaan?
3. Onko ohjeistettu, kenelle ilmoitus organisaatiossa tehdään?
4. Onko organisaatiolla käytettävissä asiantuntijaresurssia, joka on perehtynyt vastaavanlaiseen tilanteeseen?
5. Miten vastaatte viestiin?
6. Oletteko tehneet tarvittavat viranomaisilmoitukset, kenelle ja miksi?
7. Jos tietoja on vuotanut verkkoon, miten tiedot saadaan poistettua?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 13:14.

9 Tapahtuma tietojen muuttaminen

9.1 Sähköposti: Organisaation taloushallinnolta koko organisaatiolle

FROM: taloushallinto@organisaatio.fi
TO: Organisaatio
SUBJECT: Tiedoksi – asiakkailta tullut paljon yhteydenottopyyntöjä maksumuistutuksiin liittyen
---

Tiedoksi koko organisaatiolle,

taloushallintoon on tullut useita yhteydenottoja koskien lähetettyjä maksumuistutuksia. Tiedon mukaan, asiakkaat ovat maksaneet laskut ajallaan. Taloushallinto on aloittanut selvitystyön.

Terv. Mikko
Taloushallinto
Organisaatio

9.2 Quacker: @jannevirta

”Hei @Organisaatio, mikä homma? Miksi sain karhukirjeen, vaikka laskut on maksettu ajallaan?!? Tämän tarkistin verkkopankista ja raha on kyllä lähtenyt jo ennen eräpäivää! #organisaatio #perätönperintä”

9.3 Sanomat Uudeltamaalta: ”Onko organisaatiolla vakavia maksuliikenteen häiriöitä?”

”Toimituksemme on saanut yhteydenottoja useilta kansalaisilta sekä yrittäjiltä, joilla on ollut ongelmia Organisaation laskujen kanssa.

Toimittajamme haastatteli yrittäjä Pekka Mäkimaata, katso video alta!”

Linkki: https://www.youtube.com/watch?v=RMW1LCVVnDM&feature=youtu.be

9.4 Quacker: @jande

”Miksi @Organisaatio lähettää maksuhuomautuksen maksetusta laskusta???”

9.5 Quacker: @pekka_pienyrittajat

”Ahneudella ei mitään rajaa. @Organsaatio perii jo kertaalleen maksettuja laskuja korkojen kera!”

9.6 Quacker: @m01verkkosatabot

”On hyvin vaikea johdatella asioita siten, että @Organisaation perätön maksumuistutus järkeistää käsitystämme kyseisestä asiakokonaisuudesta, mihin tavallaan liittyy myös meihin kohdistuvaa tietotarvetta.”

9.7 Quacker: @m01verkkosatabot

”Tosiasia on, että @Organisaation perätön maksumuistutus mallintaa kokonaiskuvaa käyttäen hyödykseen esimerkiksi liian vähäisiä tuotannollisia resursseja.”

9.8 Quacker: @jaakkovirtamaki

”Koitin olla @Organisaatioon yhteydessä näistä laskuepäselvyyksistä. Siellä on linjat varattuina. Aika outoa viestiä liikkuu täällä somessakin.

Ollaankohan siellä nyt ihan tilanteen tasalla?”

9.9 Quacker: @m01verkkosatabot

”On hyvin vaikea johdatella asioita siten, että @Organisaation perätön maksumuistutus todistaa oikeaksi ilmiöiden liiallista nonfiguratiivisuutta.”

9.10 Quacker: @arviainen

”Nyt tarkkuutta, arvon somekupla. Ei kannata luottaa kaikkeen mitä somessa kirjoitetaan. Helpoimmin tunnistettavat botit ovat niitä, joiden käyttäjätunnus on sarja kirjaimia ja numeroita ja joilla ei ole profiilikuvaa. Tällaisten tilien verkostoja voi ostaa internetistä hyvinkin halvalla. #digitaidot #botit”

9.11 Talouslehti: ”Organisaatiolla vakavia ongelmia myös laskutuksessa”

Useat tahot ovat olleet yhteydessä toimitukseemme, kertoen mm. perättömistä maksumuistutus- ja perintäkirjeistä, joita Organisaatio on heille lähettänyt.

Osa toimitukseemme yhteydessä olleista henkilöistä kertoo tarkistaneen pankistaan, että maksut on maksettu ajallaan. "Olin yhteydessä Organisaation laskutukseen, ja he kuitenkin kivenkovaan väittivät, ettei maksua ole heille ikinä rekisteröitynyt", tuskailee espoolainen Tuire.

Tarkkuutta vaaditaan laskun vastaanottajalta yllättävän paljon

Markan Pankin asiantuntija kertoo, jos maksaa laskun väärälle tilinumerolle, kannattaa asiasta ottaa yhteyttä omaan pankkiin. Sieltä autetaan selvittämään, kenen tilille rahat menivät. Sen jälkeen voi sopia ylimääräistä rahaa saaneen henkilön kanssa rahojen palauttamisesta - mikäli vastaanottaja on ylipäätään selvitettävissä, ja on yhteistyöhaluinen.

9.12 Tehtävät

Organisaatio saa yhteydenottoja aiheettomiin maksumuistutuksiin liittyen. Lisäksi aihetta on käsitelty eri medioissa. Taloushallinto on käynnistänyt selvitystyön aiheesta.

HUOM! Tähän tapahtumaan liittyvät syötteet eivät edellytä taloushallinnon tai myynti/ostoreskontran järjestelmien tuntemusta, vaan pääpaino tehtävässä on poikkeavan tilanteen johtamisessa ja siitä tiedottamisessa.

1. Miten tilanteesta tiedotetaan sisäisesti etenkin asiakasrajapinnassa työskenteleviä työntekijöitä?
2. Miten reagoitte sosiaalisessa mediassa käytävään keskusteluun?
3. Miten reagoitte erilaisten automaattisten bottien tuottamiin viesteihin?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 13:35.

9.13 Sähköposti: Organisaation myyntireskontrasta koko organisaatiolle

Huom: Toimi tämän syötteen mukaisesti, jos organisaatiollasi on asiakaslaskutukseen liittyvää toimintaa.

Jos organisaatiolla ei ole asiakaslaskutusta/myyntireskontraa, siirry oheisen linkin kautta vaihtoehtoiseen syötteeseen TÄÄLTÄ (seuraava syöte yllä).

FROM: myyntireskontra@organisaatio.fi
TO: Organisaatio
SUBJECT: maksuissa häikkää

Hei,

Asiakkailta on tullut turhautuneita viestejä heille saapuneista maksukehotuksista, koska he ovat maksaneet laskut ajallaan. Olemme selvittäneet ristiin vertaamalla muutamia tapauksia, ja on ilmennyt, että lähetetyissä laskuissa on ollut vääriä tilitietoja. Näissä tapauksissa asiakkaat lähettivät maksutositteen ajallaan tehdyistä suorituksesta. Nämä neljä tapausta (kuva liitteenä) odottavat reskontramme mukaan kuitenkin edelleen suorituksia.

Selvitystyössä havaittiin, että laskutusjärjestelmässä on virheellisiä tili- ja viitetietoja. Tiedot eivät ole organisaation omia maksutietoja. Nämä tiedot ovat päätyneet laskutusohjelman kautta asiakkaille muodostettuihin laskuihin. Asiakkaat ovat maksaneet laskulla olleelle tilinumerolle. Tämä tilinumero on meille tuntematon.

	29461	Vänttinen	Erkki Eerikki	-154,54	14d overdue	sent	FI3636085451245654
	68451	Saarinen	Jaakko Mikael	-76,09	21d overdue	sent	FI3636085451245654
	74107	Hämäläinen	Visa Markku	-849,9	16d overdue	sent	FI3636085451245654
	88097	Jaakkola	Päivi Marketta	-15,95	35d overdue	sent	FI3636085451245654

Terv. Minna
Myyntireskontra
Organisaatio

9.14 Sähköposti: Organisaation ostoreskontrasta

Huom: Toimi tämän syötteen mukaisesti vain siinä tapauksessa, jos organisaatiollasi ei ole asiakaslaskutukseen/myyntireskontraan liittyvää toimintaa.

FROM: laskutus@organisaatio.fi
TO: Organisaatio
SUBJECT: maksuissa häikkää

Hei,

Muutamilta toimittajilta on tullut turhautuneita viestejä, joiden mukaan meiltä olisi jäänyt lasku tai joistain tapauksissa useampi lasku maksamatta.
Olemme selvittäneet ristiin vertaamalla muutamia tapauksia, ja on ilmennyt, että meillä suoritetuissa maksuissa on ollut vääriä tilitietoja. Muutamien toimittajien laskut, esimerkiksi Suomen Yritys Oy:ltä ovat isohkoja, muutamien tuhansien eurojen suuruisia laskuja. Alustavat selvityksen mukaan näyttäisi, että vastaavia tapauksia on jopa kymmeniä. Asian selvittely on melko hidasta käsityötä.

Selvitystyössä havaittiin, että laskutusjärjestelmässä on virheellisiä tili- ja viitetietoja. Tiedot eivät vastaa oikeita maksutietoja, se on nyt muutamalta toimittajalta tarkistettu. Tämä meidän järjestelmiimme kirjattu tilinumero on meille tuntematon.

Terveisin,
Mika
Taloushallinto
Organisaatio

9.15 Quacker: @Maija_Metsäläinen

”Kuulin tutultani, joka on töissä Organisaatiossa, että heillä on täysi paniikki päällä. Ilmeisesti siellä on kyberhyökkäys käynnissä ja toiminta polvillaan. #Organisaatio #kyberhyokkays #cyber”

9.16 Sähköposti: Organisaation ICT-osastolta johdolle

FROM: ICT@organisaatio.fi
TO: Organisaation johdolle
SUBJECT: Myynti/ostoreskontran tiedot korruptoituneet

Hei,

Selvitysten perusteella meillä on syytä olettaa, että myynti/ostoreskontran tiedot ovat korruptoituneet. Tietojen korruptoituminen vaikuttaa siten, että järjestelmän tuottamaan tietoon ei voi luottaa. Selvityksessä on ilmennyt, että tietojen korruptoitumisen taustalla on tahallinen toiminta. Lokitiedoista on pääteltävissä, että tietoja on muutettu Organisaation pääkäyttäjätunnuksia käyttäen, mutta tekijän henkilöllisyyttä ei vielä tiedetä.

Jatkamme selvitystyötä.

Terv. Minna
ICT-asiantuntija
Organisaatio

9.17 Iltanen: ”JUURI NYT - Organisaatio kyberhyökkäyksen kohteena -vakavat seuraukset?”

Iltasen saamien tietojen mukaan Organisaatio on laajan ja toimintaa halvaannuttavan kyberhyökkäyksen kohteena. Iltasen haastatteleman Naxu Oyj:n tietoturva-asiantuntijan mukaan kohdistettu tietoturvahyökkäys voi olla erittäin hankala ja sen seuraukset voivat olla merkittäviä, mikäli tilanteeseen ei ole varauduttu etukäteen ja varmennukset eivät ole kunnossa.

Organisaatio ei halunnut kommentoida tilannetta.

Iltanen seuraa tilannetta.

9.18 Lookbook: ORGANISAATIO -LookBook-seinä

Ville Virtanen: Hei, mikä mättää?! Onko teillä taas ongelmia järjestelmissä? Ei tunnu taas toimivan yhtään mikään... 👎
Tykkää Kommentoi

Vastaukset (2)

Santtu-Petteri
Joopajoo, pitihän se arvata. 😕 Nyt meni luottamus Organisaation toimintaan.
Tykkää Kommentoi

Minna Nieminen
Aaaapuuwa! Miksi ei toimi? Milloin saatte palvelut taas pystyyn?? 😖
Tykkää Kommentoi

Kalle Arviainen
Nostakaa käsi ylös, joka on yllättynyt? Ihmeellistä säätämistä koko homma. Hermot tässä vaan menee. Onneksi ei ole omat rahat kiinni. 😈
Tykkää Kommentoi

9.19 Tehtävät

Organisaation taloushallinnon selvitystyössä havaittiin, että taloushallinnon järjestelmässä on virheellisiä tili- ja viitetietoja. Selvityksessä ilmeni, että nämä tiedot ovat Organisaation taloushallinnon järjestelmässä virheellisiä.

1. Onko organisaatiolla suunnitelmia vastaavan tilanteen varalle?
2. Onko tilanteen johtovastuut ennalta suunniteltu ja selkeät?
3. Kenet tarvitsette mukaan selvitysprosessiin, jotta voidaan selvittää, miten tietoja on voitu muuttaa?
4. Oletteko jo tehneet viranomaisilmoitukset?
5. Onko organisaatiolla sovitut käytännöt lokitietojen keräämiseen ja käsittelyyn?
6. Onko organisaationne dokumentoinut käytännöt varmuuskopioinnista ja tietojen palauttamisesta?
7. Onko mahdollista tehdä palautuksia varmuuskopioilta? Kuka tekee päätöksen tietojen palauttamisesta?
8. Onko tietojen palauttamista varmuuskopioista testattu käytännössä? Kuinka usein palauttamista harjoitellaan / testataan?
9. Miten varmuuskopioitu tieto on varmennettu?
10. Onko varmuuskopioita kahdennettu useampaan fyysiseen paikkaan?
11. Onko menetettyä dataa / tietoa mahdollista saada takaisin tai korvata? Miten ja millä resursseilla?
12. Kuinka pitkän ajan varmuuskopiot kattavat ja mikä on varmuuskopiointisykli?
13. Kuinka paljon / pitkältä ajalta dataa menetetään, jos tiedot palautetaan varmuuskopiolta?
14. Miten uudelleenasennetun palvelimen tiedon validointi tapahtuu? Kauanko kestää, kuka tekee?
15. Miten toimintaa tulisi kehittää, jotta tietoturva ja reagointikyky olisi parempaa jatkossa?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Seuraava syöte julkaistaan klo 14:03.

10 Tapahtuma kiristys

10.1 Sähköposti: Organisaation johdolle

FROM: oraakkeli@anonymous.org
TO: Organisaation johtoryhmän jäsenille
SUBJECT: Kirje Organisaation johdolle

Arvoisa Organisaation johto,

Työntekijöiden oikeuksien polkeminen saa loppua! Olemme saaneet haltuumme merkittävän määrän Organisaatiollenne kuuluvaa dataa. Tämän lisäksi (kuten olette varmasti jo huomanneet) olemme muuttaneet kriittisen järjestelmänne tietoja. Tietojen palauttamista ei kannata yrittää. Se olisi vain turhaa ajan haaskausta.
Mikäli haluatte ratkaisun ongelmiinne, toimikaa seuraavien ohjeiden mukaisesti:

1. Älkää olko yhteydessä viranomaisiin.
2. Kilpailukyvyn nojalla tehdyt työntekijöiden oikeuksien heikennykset tulee lopettaa välittömästi.
3. Palkankorotukset tulee palauttaa normaaliin tasoon välittömästi.
4. Lomautukset ja irtisanomiset tulee peruuttaa välittömästi.
5. Julkaiskaa tiedote työntekijöiden sortamisen päättymisestä ja korvaavista toimenpiteistä.

Mikäli kaikkiin vaatimuksiimme ei suostuta 48 tunnin sisällä, alamme julkaisemaan haltuumme saamiamme tietoja 60min välein sosiaalisessa mediassa. Suostumalla vaatimuksiin palautamme ainoat kopiomme datasta takaisin.

Ystävällisin terveisin,
Oraakkeli

10.2 Quacker: @oraakkeli

”Anna sinäkin protestiäänesi ja lakkaa käyttämästä @Organisaatio:n palveluita tai tuotteita. #organisaatio-gate #somemyrsky #boikotti #väärinkäyttäjät”

10.3 Quacker: @oraakkeli

”Julkaisemme tällä tilillä pikapuoliin tietoja @Organisaatiosta jotka varmasti kiinnostavat mm. poliisin rahanpesuyksikköä.

Aivan sikamaisia väärinkäytöksiä! Meitä on turha koittaa vaientaa, vaikka ovatkin uhkailleet! #boikotti #Organisaatio”

10.4 Iltanen: JUURI NYT - Kansalaisten henkilötietoja vuotanut nettiin

Iltasen toimitus on saanut lukuisia vinkkejä lukijoilta somessa trendaavasta linkistä, jonka takaa löytyy suomalaisten henkilötietoja.

Linkkiä alun perin linkistä ilmoittaneen ja sitä jakaneen some-tilin päivitysten mukaan kyse olisi suomalaisten tiedoista. Sitä tukee myös vuodettu kuvakaappaus tietokannasta: joukossa on nimiä, osoitteita, tilinumeroita, henkilöiden rooleja yrityksissä ja paljon muita arkaluontoisia tietoja. Tietojen todenperäisyys tai lähde on toistaiseksi vahvistamatta.

Lisää aiheesta hetken kuluttua.

10.5 Quacker: @Oraakkeli

”Luotettavan tietolähteemme mukaan @Organisaatiolta peräisin olevat dokumentit paljastavat todelliset tapahtumat kulisseissa.

Tässä on pandemiatilanteesta otettu törkeästi kaikki hyöty irti ja väärinkäytökset on koitettu piilottaa kohinan alle.

Saimme onneksi käsiimme tätä Organisaation huolimattomuuttaan verkkoon vuotamaa tietoa, ja tulemme tekemään kaikki paljastukset kansan tietoon! #Organisaatio #rikollisuus #databreach #tietovuoto”

10.6 Iltanen: JUURI NYT - Organisaation ongelmat jatkuvat - tietovuoto?

Toimituksemme on saanut lukuisia vihjeitä liittyen epäiltyyn suomalaisen Organisaation tietovuotoon. Etenkin somessa on käyty tämän päivän aikana kiihtynyttä keskustelua liittyen Organisaation tietojärjestelmäongelmiin - nyt ilmi tulleet epäilyt tietojen vuotamisesta syventävät Organisaation ahdinkoa entisestään.

Iltanen ei ole tavoittanut Organisaation edustajia kommentoimaan asiaa.

Lisää aiheesta hetken kuluttua.

10.7 Sanomat Uudeltamaalta: Asiantuntija: Tarkista tietosi

Löytyvätkö tietosi netin pimeiltä markkinapaikoilta?

Jos henkilötietosi tai esimerkiksi käyttäjä-tunnuksesi ovat olleet osana tieto-vuotoa, joku voi käyttää tietojasi väärin. Tämä voi johtaa ongelmiin, pahimmillaan maksuhäiriöön tai puhelinliittymän tai vakuutuksen saamisen vaikeutumiseen - tällöin puhutaan identiteetti-varkaudesta. Eri palveluntarjoajilla on palveluita, joiden kautta voit ryhtyä selvittämään onko henkilö-tietojasi vuotanut tieto-vuotojen yhteydessä.

Omien tietojen säännöllinen tarkistaminen kannattaa, korostaa tietoturva-asiantuntija Ari Arviainen I-securelta. "Se on pieni vaiva verrattuna siihen myllyyn joutumisesta, joka voi aiheutua, jos joku avaa tiedoillasi maksullisia palveluita tai nostaa esimerkiksi pikavippejä."

10.8 Turun päivälehti: Identiteettiä vaihtanut Kirsi: Eikö tämä piina lopu koskaan?

Turvakiellon piirissä elävä Kirsi (nimi muutettu) on huolissaan omasta ja lähiomaistensa turvallisuudesta ja jaksamisesta.

Kolmekymppinen Kirsi on elänyt uuden nimen ja kotipaikkakunnan turvin erossa väkivaltaisesta ex-miehestään jo vuosia, mutta ei silti lakkaa pelkäämästä; "Edelleen tulee vilkuiltua olan yli, varsinkin jos on reissussa isommassa kaupungissa". Mahdollisuuden uuteen elämään uudella paikkakunnalla toi nimenmuutos ja maistraatilta haettu turvakielto.

Kun entinen elämänkumppani yrittää vahingoittaa perhettänsä, on pakko turvautua uuteen identiteettiin.

Epäilyt Organisaation tietovuodosta ovat nostaneet vanhat pelot Kirsin mieleen, "En voi uskoa tätä! En tiedä miten perheeni selviäisi uudestaan muuttoprosessista, kun olemme jo tänne asettautuneet". Vuodetut tiedot sisältävät väitetysti Organisaation asiakastietoja, joten Kirsin tiedot voisivat teoriassa olla kaikkien saatavilla. "Uudesta nimestä ei juuri ole hyötyä, kun vuodetuissa tiedoissa on kuulemma näkyvillä henkilötunnukset. Ja kotiosoitteet! Tämä on aivan kamala tilanne", Organisaation palveluita käyttänyt Kirsi tuskailee.

10.9 Tehtävät

Organisaatiolle on lähetetty kiristyssähköposti, jossa uhataan julkaista organisaatiolle kuuluvaa dataa. Lisäksi aiheesta on noussut keskustelua sosiaalisen median kanavilla ja tämän perusteella media on tarttunut aiheeseen.

1. Miten organisaatio on varautunut tilanteeseen, jossa tietoverkkorikolliset julkaisevat haltuunsa saamia salassa pidettäviä tai arkaluonteisia henkilötietoja?
2. Onko organisaatiolla toimintaohjeet tilanteeseen?
3. Onko tilanteen johtovastuut suunniteltu ja selkeät?
4. Miten toimitte tilanteessa?
5. Keneen olette yhteydessä?
6. Oletteko jo tehneet viranomaisilmoitukset?

Lisätehtävät:

1. Miten tutkinta käynnistetään?
2. Miten huomioitte todisteiden turvaamisen?
3. Miten varmistatte, että todisteet ovat turvassa muutoksilta eikä niitä päästä jälkikäteen muuttamaan?
4. Tiedättekö mitä tietoja tulee ottaa talteen?
5. Kenellä organisaatiossa on pääsy asiaan liittyvään informaatioon?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

10.10 Sähköposti: Organisaation ICT-osastolta Riskienhallintaan / turvallisuusyksikköön

FROM: ICT@organisaatio.fi
TO: Organisaation riskienhallinta/turvallisuus
SUBJECT: Hyökkäyksen toteuttanut henkilö selvillä

Hei

Olemme saaneet selville henkilön, jonka käyttäjätunnuksilla myynti/ostoreskontraan kohdennettu hyökkäys on toteutettu. Henkilö on Organisaatiomme asiantuntija, jolla on työtehtäviensä takia laajat käyttöoikeudet kriittiseen järjestelmäämme.

Miten haluatte, että toimimme tilanteessa?

Terv. Virpi
ICT-päällikkö
Organisaatio

10.11 Tehtävät

Selvitystyön perusteella organisaatio on saanut selville laskutustietoja muuttaneen henkilön, joka on organisaation oma työntekijä. Sama työntekijä on toiminut muidenkin tapahtumien takana.

1. Miten toimitte tilanteessa?
2. Miten pystytte varmistamaan mitä henkilö on tehnyt organisaation järjestelmissä (lokienhallinta ja seuranta)?
3. Miten riskienarvioinnissa on otettu huomioon sisäinen uhka?
4. Miten pysytte varmistamaan, että vastaavaa tilannetta ei pääse tapahtumaan?
5. Oletteko jo tehneet viranomaisilmoitukset?

HUOM! Jos päädytte tekemään tässä tilanteessa viranomaisilmoituksia, ohjeet TAISTO20-harjoituksessa tehtäviin viranomaisilmoituksiin löytyy tätä LINKKIÄ klikkaamalla.

Viimeinen syöte julkaistaan klo 15:00. Jos teille jää aikaa, käykää läpi aiempia tehtäviä ja täydentäkää vastauksia tarvittaessa.

11 Harjoitusinfo - Kokopäivän harjoitus on päättynyt

TAISTO20-harjoitus on päättynyt!

Käykää läpi kesken jääneet tehtävät ja täydentäkää vastauksia tarvittaessa, jos teille jää aikaa. Harjoitusalustalle ei julkaista enää lisää sisältöä.

Liite 1 Harjoituspäivän aikataulu

Julkaisu-aika	Syötteen otsikko
8:45:00	Ohje TAISTO20-harjoituksen näyttövastaaville
8:45:00	Harjoitusinfo
8:45:00	Harjoitusinfo - Tervetuloa TAISTO20-harjoitukseen
9:00:00	TAISTO20-harjoituksen avaus
9:02:00	Alivaltiosihteeri Päivi Nergin tervehdys TAISTO20-harjoitukseen osallistujille
9:04:00	Tietoisku KRP
9:06:00	Tietoisku TSV
9:08:00	Tietoisku Traficom
9:11:00	Yleismedian uutiset
9:15:00	@NCSC-FI (Kyberturvallisuuskeskus)
9:17:00	Iltasen gallup: Turhautuminen ja levottomuus ovat lisääntyneet pandemian aikana
9:18:00	#TAISTO20-kuvakisa
9:18:00	Suomalaiset pelkäävät pandemian aiheuttamaa tulevaisuuden epävarmuutta ja kansallista talous-kriisiä
9:19:00	Sähköposti - Onkohan nämä teidän tietoja?
9:20:00	Tehtävät
9:34:00	Suomalaisten henkilötietoja jälleen verkossa
9:35:00	Tehtävät
9:43:00	Sähköposti - Organisaation työntekijältä Riskienhallintajohtajalle/Turvallisuusjohtajalle
9:44:00	Sähköposti - Havainto admin-tunnuksista
9:45:00	Tehtävät
10:10:00	Shokkiuutinen: massiivisia irtisanomisia tiedossa Organisaatiossa
10:11:00	@make
10:12:00	@jaska
10:13:00	@masa
10:14:00	Tehtävät
10:30:00	Sähköposti - Organisaation työntekijältä ICT-tuelle
10:31:00	Tehtävät
10:45:00	Sähköposti - IT-tuelta koko Organisaatiolle, Sisäverkossa hitautta
10:46:00	@Maija_Metsäläinen
10:47:00	@Petteri_Kuusela
10:47:00	Sähköposti - asiakaspalveluvastaavalta koko organisaatiolle
10:48:00	@Jonna_Bocker
10:49:00	Tehtävät
11:04:00	Organisaation verkkopalveluissa vakavia ongelmia
11:05:00	Tehtävät
11:14:00	Sähköposti - tietoliikennepalveluntarjojalta ICT-vastaavalle
11:15:00	Tehtävät
11:30:00	Harjoitusinfo - Puolenpäivän harjoitus on päättynyt
12:30:00	Tervetuloa harjoituksen iltapäiväosuuteen!
12:30:20	IL-TV: Työntekijöiden heikot digitaidot yleistyvien tietovuotojen takana?
12:31:00	Tehtävät
12:40:00	Tehtävät

12:41:00	#TAISTO20-kuvakisa
12:49:00	Somebotit haittaavat tiedonkulkua myös suomeksi yhä enemmän
12:50:00	Sähköposti - valkohattuhakkerilta organisaatiolle
12:51:00	@hackfin
12:52:00	Tehtävät
13:14:00	Sähköposti - Organisaation taloushallinnolta koko organisaatiolle
13:15:00	@jannevirta
13:16:00	Organisaatiolla vakavia maksuliikenteen häiriöitä?
13:17:00	@jande
13:18:00	@pekka_pienyrittaja
13:19:00	@m01verkkosatabot
13:19:03	@m01verkkosatabot
13:19:10	@jaakkovirtamaki
13:19:30	@m01verkkosatabot
13:20:00	@arviainen
13:21:00	Organisaatiolla vakavia ongelmia myös laskutuksessa
13:22:00	Tehtävät
13:35:00	Sähköposti - Organisaation myyntireskontrasta koko organisaatiolle
13:35:01	Sähköposti - Organisaation ostoreskontrasta
13:37:00	@Maija_Metsäläinen
13:38:00	Sähköposti - Organisaation ICT-osastolta johdolle
13:39:00	JUURI NYT: Organisaatio kyberhyökkäyksen kohteena -vakavat seuraukset?
13:40:00	ORGANISAATIO -LookBook-seinä
13:41:00	Tehtävät
14:03:00	Sähköposti Organisaation johdolle
14:04:00	@oraakkeli
14:05:00	@oraakkeli
14:06:00	JUURI NYT: Kansalaisten henkilötietoja vuotanut nettiin
14:07:00	@oraakkeli
14:08:30	JUURI NYT: Organisaation ongelmat jatkuvat - tietovuoto?
14:09:00	Asiantuntija: Tarkista tietosi
14:10:00	Identiteettiä vaihtanut Kirsi: Eikö tämä piina lopu koskaan?
14:10:01	Tehtävät
14:30:00	Sähköposti - Organisaation ICT-osastolta Riskienhallintaan / turvallisuusyksikköön
14:31:00	Tehtävät
15:00:00	Harjoitusinfo - Kokopäivän harjoitus on päättynyt