DIGI- JA VÄESTÖTIETO-VIRASTO

TAISTO21-harjoitus

Käsikirjoitus

18.1.2022

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

Dokumentinhallinta

Omistaja	Hanna Heikkinen
Laatinut	Hanna Heikkinen, Laura Penttilä

Sisällysluettelo

1 Harjoituksen aloitus 5
1.1 Harjoitusinfo videot 5
1.2 Harjoituksen maailmankuva 5
2 Tapahtuma: Häiriö globaalissa pilvipalvelussa 5
2.1 Sanomat Uudeltamaalta: PilviPalvelun alasajon taustalla vakava tietomurtoepäily 5
2.2 Sähköposti: Organisaation johdosta jatkuvuudenhallinnasta vastaaville henkilöille 6
2.3 Quacker: @ATKjäbä 6
2.4 Quacker: @Raqqadi 6
2.5 Sähköposti: Organisaation työntekijältä Organisaation tietoturvavastaavalle 6
2.6 Quacker: @daniela 7
2.6.1 Quacker: @ATKjäbä 7
2.7 Sähköposti: Poissaoloviesti Organisaation tietoturvavastaavalta 7
2.8 Quacker: @uivelo 7
2.8.1 Quacker: @Raqqadi 7
2.9 Tehtävät 8
2.9.1 Lisätehtävät 8
2.9.2 Viestintätehtävät 8
3 Tapahtuma: Tilaturvallisuus, epäilty tietovuoto 8
3.1 Sähköposti: Organisaation turvallisuusvastaavalle 8
3.2 Sähköposti: Organisaation henkilöstöhallinnolle 9
3.3 Sähköposti: Organisaation riskienhallinnasta / jatkuvuudesta vastaavalle johtajalle 9
3.4 Quacker: @Suomi-vuotaa 9
3.5 Quacker: @FIN-Leaks 9
3.6 Quacker: @Suomi-vuotaa 9
3.7 Quacker: @Pekka Virtanen 10
3.8 Iltanen: Julkishallinnon tietovuoto – taustalla Organisaation heikko turvallisuuskulttuuri? 10
3.9 Tehtävät 10
3.9.1 Lisätehtävät 10
3.9.2 Viestintätehtävät 10
4 Tapahtuma: Kopioitu tapahtumahuijaussivu sosiaalisessa mediassa 11
4.1 Tehtävät 11
4.1.1 Viestintätehtävät 11
5 Tapahtuma: Tietovuotoepäily paisuu mediassa ja epäily kadonneista henkilöstöhallinnon tietokoneista 11
5.1 YME-uutislähetys 11

5.2 Quacker: @FIN-Leaks 11
5.3 Quacker: @Mirva Möttönen 11
5.4 Quacker: @Kari Arviainen 12
5.5 Sähköposti: Organisaation henkilöstöhallinnon työntekijältä turvallisuusvastaavalle 12
5.6 Tehtävät 12
5.6.1 Viestintätehtävät 12
5.6.2 Haastattelutehtävä 13
5.7 YME-uutisten puhelinhaastattelu 13
5.7.1 Tehtävät 13
6 Tapahtuma: Haavoittuvuus globaalissa online-käännöspalvelussa 14
6.1 Tietoturva NYT: ”Käytätkö Uugle-translatea? - Varo tietojen vuotamista” 14
6.2 Quacker: @Uugle 14
6.3 ViTi: Uugle-Translate mahdollisen tietomurron kohteena 14
6.4 Sanomat Uudeltamaalta: Asiantuntija: ”Netissä leviävät tiedot todennäköisesti peräisin Uugle-kääntäjän tietovuodosta” 15
6.5 Tehtävät 15
6.5.1 Viestintätehtävät 15
7 Harjoituksen iltapäiväosuus 15
8 Tapahtuma: PilviPalvelu palautetaan viikon takaiseen palautuspisteeseen 16
8.1 Sähköposti: PilviPalvelun palveluntuottaja tiedottaa 16
8.2 Tehtävät 16
8.2.1 Lisätehtävät 16
8.2.2 Viestintätehtävät 16
9 Tapahtuma: Poliisin tietopyyntö liittyen epäilyttävästä toiminnasta Organisaation IP-osoitteessa 17
9.1 Sähköposti: Poliisilta saapuva tiedonsaantipyyntö koskien organisaation epäilyttävää ip-osoitetta 17
9.2 Tehtävät 17
10 Tapahtuma: Toimittajariippuvuus - Kiina ostaa kriittisen palvelutuottajan liiketoiminnan 18
10.1 Iltanen: JUURI NYT: Alimama ostaa suomalaisen IT-yhtiön 18
10.2 Quacker: @Anni Nieminen 18
10.3 Quacker: @Santtu Matalamaki 18
10.4 Quacker: @Matti Möttönen 18
10.5 Sähköposti: Organisaatiolle kriittisen IT-palveluntoimittajan yhteyshenkilöltä 18
10.6 Tehtävät 19
10.6.1 Viestintätehtävät 19

11 Tapahtuma: Organisaation läppäri myynnissä netissä 19
11.1 Sähköposti: Organisaation työntekijältä Organisaation turvallisuusvastaavalle 19
11.2 Iltanen: JUURI NYT: Jussi hämmästyi - Osti nettikirpparilta käytetyn läppärin ja siellä oli Organisaation arkaluonteisia tiedostoja 20
11.3 Quacker: @jussiwiz 21
11.4 Sähköposti: Iltasen toimittajan artikkelin täydennyspyyntö Organisaation viestinnälle 21
11.5 Tehtävät 22
11.5.1 Viestintätehtävät 22
12 Tapahtuma: Salassa pidettävän tiedon vuotaminen 22
12.1 Quacker: @tarkkamarkka 22
12.2 Quacker: @yrittäjäyrmeli 22
12.3 Quacker: @Pera 23
12.4 Tehtävät 23
12.4.1 Viestintätehtävät 23
13 Harjoitusinfo – koko päivän harjoitus on päättynyt 23

TAISTO21-harjoitus

1 Harjoituksen aloitus

TAISTO21-harjoitus alkoi harjoitusalustalla julkaistuilla infosyötteillä, joissa ohjeistettiin harjoituspäivän kulkua. Harjoituspäivän aikataulu on käsikirjoituksen liitteenä.

1.1 Harjoitusinfo videot

- **TAISTO-harjoituksen avaustervehdys**

  Linkki videoon: https://youtu.be/IchTJxO8fk0

- **Kyberturvallisuusjohtaja Rauli Paanasen avaustervehdys**

  Linkki videoon: https://youtu.be/1I6NBL-sA20

1.2 Harjoituksen maailmankuva

- **Yleismedian uutiset**

  Linkki videoon: https://youtu.be/9XIpYAgHtfs

- **Quacker: @VilleVihreäniitty**

  Ihan kiva päästä taas pitkästä aikaa toimistolle. Ongelmana vain on, että meidän organisaatiossa ei ole varauduttu kasvaneeseen sähköautojen lataamistarpeeseen… #etätyö

- **Quacker: @Teslanainen**

  Ei näyttänyt olevan työpaikalla vapaata latausasemaa. Ilmeisesti sähköä ei saa kaupallisilta latauspisteiltäkään, saattaa jäädä Tesla kotimatkan varrelle… #lisäälatauspisteitä #Tesla #häiriölatauspisteillä

2 Tapahtuma: Häiriö globaalissa pilvipalvelussa

2.1 Sanomat Uudeltamaalta: PilviPalvelun alasajon taustalla vakava tietomurtoepäily

NY Times on saanut tietoonsa, että Pilvipalveluun kohdistettu kyberhyökkäys on voinut altistaa lukuisia yrityksiä ja organisaatioita tietomurrolle.

NY Times on julkaissut tietoja ja dokumentteja, jotka on toimitettu heille PilviPalvelun palveluntuottajan sisäpiiristä. Ne viittaavat siihen, että PilviPalvelu olisi ajettu alas tarkoituksella, koska on haluttu estää laajan kyberhyökkäyksen eteneminen yrityksen tietojärjestelmissä.

Taustalla on myös epäily laajasta tietomurrosta, jossa käyttäjien dataa olisi päätynyt vääriin käsiin. Sisäpiiritietojen mukaan nyt käynnissä on tietomurron peittelyoperaatio.

Tietojemme mukaan tällä hetkellä kukaan ei pääse käsiksi niihin tietojärjestelmiin, jotka ovat Pilvipalvelussa.

Pilvipalvelun ongelmat ovat globaaleja, ja palvelua käytetään laajasti myös Suomessa. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tietoturva-asiantuntija Mikko Manttisen mukaan viranomaisilla on tiedossa useita yrityksiä ja organisaatioita, joilla Pilvipalvelu on käytössään. Manttisen mukaan kyseessä on suuri määrä organisaatioita niin julkisen ja yksityisen sektorin puolelta.

Tietoturva-asiantuntija Teija Toiveikas ICT-kamu yrityksestä pitää tapahtumaa havahduttavana: ”Tällaiset tilanteet muistuttavat meitä siitä, että kun jotain tapahtuu, välttämättä emme voi tehdä asialle mitään.”

PilviPalvelun tuottaja ei ole toistaiseksi kommentoinut väitteitä.

2.2 Sähköposti: Organisaation johdosta jatkuvuudenhallinnasta vastaaville henkilöille

Lähettäjä: johtaja@organisaatio.fi
Vastaanottaja: jatkuvuudenhallista vastaava@organisaatio.fi
Aihe: Tärkeä: Toiminnan jatkuvuuden turvaaminen

Hei,

Olen huolestuneena seurannut uutisointia liittyen PilviPalvelun häiriötilanteeseen. Miten häiriötilanne vaikuttaa meidän organisaatiomme toimintaan? Olemmeko varautuneet siihen, että koko PilviPalvelu on pois käytöstä ja miten pystymme korvaamaan PilviPalvelun jatkossa, mikäli katkos kestää odotettua pidempään?

Terveisin,

Johtaja,
ORGANISAATIO

2.3 Quacker: @ATKjäbä

Tässä nähdään, miten riippuvaisia olemme suuresta it-yhtiöstä. Jos asiat eivät yhtäkkiä toimikaan, kätemme ovat sidotut.

2.4 Quacker: @Raqqadi

Tämä pistää miettimään, miten paljon tietoa ja liiketoimintaa on laitettu kyseiseen Pilvipalveluun.

2.5 Sähköposti: Organisaation työntekijältä Organisaation tietoturvavastaavalle

Lähettäjä: mikko.mallikas@organisaatio.fi
Vastaanottaja: tietoturvavastaava@organisatio.fi
Aihe: Ovatko Organisaation työntekijöiden tiedot turvassa?

Hei,

Ollaan kollegoiden kanssa keskusteltu kahvitunnilla liittyen PilviPalvelun globaalista häiriöstä ja sen vaikutuksista. Meillä heräsi huoli erityisesti siitä, että uutisoinnin mukaan häiriön taustalla saattaa olla laaja tietovuoto. Mitä tietoja tuohon järjestelmään on syötetty ja voivatko nämä tiedot nyt olla vaarassa? Erityisesti meitä huolettaa omat henkilökohtaiset tietomme. Voisiko näihin saada vastausta ja mielellään tieto koko henkilöstölle, kiitos!

Terveisin,

Mikko Mallikas,
Virkahenkilö,
Organisaatio

2.6 Quacker: @daniela

Kuka maksaa tästä aiheutuneet kustannukset???

2.6.1 Quacker: @ATKjäbä

Jos organisaation / yrityksen maine ja luottamus menee tämän johdosta, ei paljoa auta korvaukset siinä vaiheessa.

2.7 Sähköposti: Poissaoloviesti Organisaation tietoturvavastaavalta

Lähettäjä: tietoturvavastaava@oraganisaatio.fi
Vastaanottaja: mikko.mallikas@organisaatio.fi
Aihe: VS: Ovatko Organisaation työntekijöiden tiedot turvassa?

Tervehdys,

Olen bongaamassa valaita Lofooteilla ja minua ei tavoita seuraavan viikon aikana. Paikan päällä ei ole puhelinkenttää, joten en valitettavasti voi vastata lomani aikana puhelimeen enkä sähköpostiin.

Kiireisissä asioissa voit olla yhteydessä Organisaation nimettyyn varahenkilöön.

Terveisin,

Tietoturvavastaava,
ORGANISAATIO

2.8 Quacker: @uivelo

Onko suomalainen yhteiskunta ja yritykset riittävässä määrin valmistautuneet siihen, että järjestelmät voivat myös kaatua?

2.8.1 Quacker: @Raqqadi

Kuten tässäkin nähdään, yksi häiriö vaikuttaa moneen toimijaan. Miten varmistamme, että voimme jatkamme toimintaa tällaisissa tilanteissa?

2.9 Tehtävät

Organisaationne tietoja on mahdollisesti vuotanut.

- Valitkaa organisaationne käytössä oleva kriittinen pilvipalvelu ja peilatkaa kuvattua häiriötä valitsemanne palvelun toimintaan läpi koko harjoituksen.
- Millaisia vaikutuksia PilviPalvelun häiriöllä on organisaationne toiminnalle?
- Mitä toimia tilanne edellyttää organisaatiossanne?
- Miten tilanteen selvitystyö organisoidaan ja vastuutetaan?

2.9.1 Lisätehtävät

- Mihin tahoihin olette yhteydessä?
- Tekisittekö tässä vaiheessa viranomaisilmoituksia?
- Onko organisaatiossanne määritelty viestivälineitä ja varajärjestelyitä?
    - Mitä voidaan viestiä esim. pikaviestinpalveluilla (WhatsApp/Signal), jos ensisijaiset viestiyhteydet eivät toimi?

2.9.2 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Aiheuttaako tämä viestintätoimia organisaatiossanne? Jos, niin mitä?
    - Keille viestitte tilanteesta?
    - Mitä kanavia käyttäisitte?
    - Mitä viestitte asiasta eri kohderyhmille?
- Kirjoittakaa tarvittavat tiedotteet ja somejulkaisut ja julkaiskaa ne.

3 Tapahtuma: Tilaturvallisuus, epäilty tietovuoto

3.1 Sähköposti: Organisaation turvallisuusvastaavalle

Lähettäjä: anni.kojas@Organisaatio.fi
Vastaanottaja: turvallisuus@Organisaatio.fi
Aihe: Tuntematon henkilö havaittu toimitiloissa

Hei,

Tänään kahvihuoneessa keskusteltiin työkavereiden kanssa, että toimitiloissamme on liikkunut tuntematon henkilö. Tällä henkilöllä kerrottiin olevan mukanaan erikoisia laitteita. Emme ehtineet ottaa selvää, kuka henkilö oli ennen kuin hän poistui tiloista. Meille heräsi huoli, että millä asioilla henkilö täällä oli ja onko mahdollista, että henkilö on saanut haltuunsa jotain arkaluonteisia tietoja tai tehnyt toimitiloissa jotain haitallista?

Terveisin,

Anni Kojas,
Henkilöstöhallinnon asiantuntija,
ORGANISAATIO

3.2 Sähköposti: Organisaation henkilöstöhallinnolle

Lähettäjä: turvallisuus@Organisaatio.fi
Vastaanottaja: anni.kojas@Organisaatio.fi
Aihe: VS: Tuntematon henkilö havaittu toimitiloissa

Hei,

Kiitos ilmoituksesta. Otamme asian selvitykseen.

Turvallisuusyksikkö
ORGANISAATIO

3.3 Sähköposti: Organisaation riskienhallinnasta / jatkuvuudesta vastaavalle johtajalle

Lähettäjä: turvallisuus@Organisaatio.fi
Vastaanottaja: riskienhallinnasta ja jatkuvuudesta vastaava johtaja@Organisaatio.fi
Aihe: Tiedoksi: turvallisuuspoikkeama selvityksessä

Hei,

Olemme saaneet ilmoitukset toimitiloissamme havaitusta henkilöstä, jota ei ole tunnistettu. Asia on meillä tarkemmassa selvityksessä. Selvityksessä on havaittu, ettei kulunvalvonnan lokitietoja saada palveluntuottajalta. Tämä johtuu todennäköisesti parhaillaan käynnissä olevista PilviPalvelun ongelmista. Kameravalvonnasta on selvitetty, että kyseisenä aikana yksi organisaatioon kuulumaton henkilö on ollut organisaation toimiston tiloissa reilun 2 tunnin ajan aikavälillä 10:05-12:17.

Terveisin,

Turvallisuusyksikkö
ORGANISAATIO

3.4 Quacker: @Suomi-vuotaa

Ei kauaakaan niin tullaan julkaisemaan kuvia haltuun saamistamme Organisaation paperidokumenteista. Kriittistä tavaraa, muun muassa henkilöstön tietoja sekä tietoja Organisaation asiakasrekisteristä.

Pysykää kuulolla! ;)

3.5 Quacker: @FIN-Leaks

Suomalaisen julkishallinnon tietoja vuotanut laajasti. Lisätietoja sivuiltamme.

3.6 Quacker: @Suomi-vuotaa

Julkishallinnon tilaturvallisuus on vitsi. Tulen esittelemään erilaisia salaisia tietoja, joita olen hankkinut kävelemällä suoraan julkishallinnon hallinnoimiin tiloihin. #kunnat #virastot #ministeriot #julkishallinto

3.7 Quacker: @Pekka Virtanen

Ei yllättänyt @Suomi-vuotaa julkaisema päivitys. Olen itsekin joskus työskennellyt nimeltä mainitsemattoman julkishallinnon organisaation respassa ja meno oli kuin Stokkan hulluilla päivillä – porukkaa lappasi sisään ja ulos ihan hallitsemattomasti.

3.8 Iltanen: Julkishallinnon tietovuoto – taustalla Organisaation heikko turvallisuuskulttuuri?

FIN-Leaks –sivusto kertoi hiljattain tietovuodosta, joka koskettaa julkishallinnon Organisaatioita. Sosiaalisessa mediassa on kuohunut tietovuototeeman ympärillä muutenkin aamupäivän aikana, sillä Quacker-käyttäjä @Suomi-vuotaa on uhannut julkaista Organisaatiolta haltuunsa saamia tietoja. Tiedoissa on käyttäjätilin julkaisemien päivitysten mukaan ainakin henkilötietoja, sekä Organisaation asiakasrekisterin tietoja.

Somepäivitysten mukaan vuodettavat tiedot ovat alun perin paperisista dokumenteista, joiden pääsy vääriin käsiin onkin herättänyt runsaasti huolta. Somessa on ruoditty Organisaation tilaturvallisuusjärjestelyiden heikkoutta ja laajemmin myös kehnoa turvallisuuskulttuuria. Tietovuodon todenperäisyydestä ei ole toistaiseksi saatu vahvistusta.

Iltanen seuraa tilannetta.

3.9 Tehtävät

Tiloissanne on liikkunut organisaationne ulkopuolinen henkilö, jonka henkilöllisyyttä ei ole pystytty tunnistamaan. Sosiaalisessa mediassa liikkuu huhuja Organisaatioonne kohdistuvasta mahdollisesta tietovuodosta.

- Mitä tämä tarkoittaa organisaatiossanne?
- Miten lähdette selvittämään tilannetta?
- Mitä toimia tilanne edellyttää?
- Oletteko tehneet viranomaisilmoituksia?

3.9.1 Lisätehtävät

- Miten varmistatte, ettei tiloihin ole jätetty ylimääräisiä laitteita?
- Miten varmistatte, ettei tiloissa oleviin laitteisiin ole asennettu mitään ylimääräistä?

3.9.2 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Aiheuttaako tämä viestintätoimia organisaatiossanne? Jos, niin mitä?
    - Keille organisaationne sisällä ilmoitatte mediassa olevista uutisista?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa lausunnot medialle?
- Kirjoittakaa tarvittavat tiedotteet ja somejulkaisut ja julkaiskaa ne.

4 Tapahtuma: Kopioitu tapahtumahuijaussivu sosiaalisessa mediassa

Organisaation työntekijä on ostanut Organisaation maksukortilla liput teatteritapahtumaan henkilöstön virkistyspäivää varten. Työntekijä on ostanut liput Lookbookin teatteritapahtuman sivulta. Työntekijä on kirjautunut tapahtumasivulle organisaation sähköpostilla ja samalla salasanalla kuin hänellä on Organisaatiossa käytössä. Lisäksi työntekijä on antanut sivustolle henkilötietonsa ja Organisaation maksukortin tiedot. Lookbookin teatteritapahtuma on paljastunut väärennetyksi tapahtumaksi, joka on johtanut kalastelusivulle. Organisaation tietoja on päätynyt vääriin käsiin tietojenkalastelusivun kautta.

4.1 Tehtävät

Organisaationne tietoja on päätynyt vääriin käsiin tietojenkalastelusivun kautta.

- Miten toimitte tilanteessa?
- Onko organisaatiossanne ajantasaisia ohjeita vastaavanlaisia tilanteita varten?
- Minkälaisia riskejä tapahtumasta syntyy organisaatiollenne?
- Onko organisaatiollanne ajantasaiset ohjeet salasanojen hallintaan?
- Onko organisaatiossanne käytössä salasanamanageri ohjelma?
- Tuleeko asiasta ilmoittaa viranomaisille?
- Mihin muualle asiasta tulee ilmoittaa?

4.1.1 Viestintätehtävät

- Miten viestitte asiasta omalle henkilöstöllenne?
- Kirjoittakaa tarvittavat tiedotteet ja julkaiskaa ne.

5 Tapahtuma: Tietovuotoepäily paisuu mediassa ja epäily kadonneista henkilöstöhallinnon tietokoneista

5.1 YME-uutislähetys

Linkki videoon: https://youtu.be/sjv0licQP3M

5.2 Quacker: @FIN-Leaks

Julkishallinnon tietoja vuotanut laajasti. #Tarkistakaa onko teidän omat tiedot vuotaneet www.fin-leaksi.fi

(HUOM! linkki on kuvitteellinen)

5.3 Quacker: @Mirva Möttönen

Kauhea, miten laajasti on päässyt vuotamaan tietoa. Kävin äkkiä katsomassa, että omaa nimeä ei onneksi näkynyt listoilla. Paljon oli julkishallinnon organisaatioiden nimiä.

5.4 Quacker: @Kari Arviainen

Amatöörien puuhastelua. Nyt poliisi tiukka linja näihin tietovuotoihin. Syylliset linnaan! Eikös näistä pitäisi tulla sakkoja kovalla kädellä? #TSV #ORGANISAATIO #poliisi

5.5 Sähköposti: Organisaation henkilöstöhallinnon työntekijältä turvallisuusvastaavalle

Lähettäjä: tietohallinto@organisaatio.fi
Vastaanottaja: turvallisuus@organisaatio.fi
Aihe: Aiempi ilmoitus tuntemattomasta henkilöstä

Hei,

Toimitiloissa havaitun tuntemattoman henkilön tilanteen johdosta saamamme laiteinventaariopyynnön perusteella on havaittu, että meiltä on useita laitteita, mm. kannettavia tietokoneita kateissa. Selvitämme parhaillaan tilannetta, josko laitteet jostain löytyisi. Palaan asiaan mahdollisimman pian.

Terveisin,
Tietohallintoyksikkö

5.6 Tehtävät

Verkkoon vuodetuissa tiedoissa on organisaatiostanne tietoja. Lisäksi epäillään, että organisaationne laitteita on kateissa.

- Onko organisaationne prosessia rikosilmoituksen tekemiseksi ja siihen liittyvien tietojen keräämiseksi?
- Onko rikosilmoituksen tekeminen vastuutettu jollekin henkilölle?
- Onko vastuutetulla henkilöllä oikeus vaatia rangaistusta / korvausta organisaation puolesta taikka luopua näistä vaateista?
- Toimiiko vastuuhenkilö myös yhteyshenkilönä poliisin kanssa tietojen vaihdon osalta?
- Onko turvallisuuspoikkeaman yhteydessä huolehdittu siitä, että selvittelyn yhteydessä otetaan talteen todistusaineistoa esitutkintaa varten (esim. kulunvalvontajärjestelmä- taikka tallennusjärjestelmätiedot)?

5.6.1 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Keille organisaationne sisällä ilmoitatte havaitsemastanne uutisoinnista / some-keskustelusta?
- Mitä viestintätoimia tämä aiheuttaa organisaatiossanne?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa lausunnot medialle?

5.6.2 Haastattelutehtävä

Organisaationne on yhdistetty epäiltyyn tietovuotoon. Verkosta on löytynyt muun muassa henkilöiden ja organisaatioiden nimiä, jotka vaikuttavat olevan peräisin asiakaspalvelunne sähköposteista.

Seuraavassa klo 10.40 julkaistavassa syötteessä YME-uutisten toimittaja soittaa organisaationne ja pyytää puhelinhaastattelua suoraan televisiolähetykseen. Käynnistäkää haastatteluvideo, kun olette valmiita antamaan haastattelun.

- Valmistautukaa antamaan haastattelu.
- Kuka antaa haastattelun?
- Mitä asioita kerrotte julkisuudessa? Mitä ette?
- Nauhoittakaa haastattelu - esimerkiksi kännykällä - sisäistä läpikäyntiä varten, jos pysytte tekemään nauhoituksen. Tallennus jää organisaation omaan käyttöön eikä sitä lähetetä edelleen, esim. harjoitusalustalle. Kannustamme tekemään nauhoituksen, jotta tilanteesta tulee mahdollisimman todentuntuinen ja saatte kokemusta.

5.7 YME-uutisten puhelinhaastattelu

Nauhoittakaa haastattelu - esimerkiksi kännykällä - sisäistä läpikäyntiä varten, jos pysytte tekemään nauhoituksen. Tallennus jää organisaation omaan käyttöön eikä sitä lähetetä edelleen, esim. harjoitusalustalle. Kannustamme tekemään nauhoituksen, jotta tilanteesta tulee mahdollisimman todentuntuinen ja saatte kokemusta.
Painakaa videon vasemmasta alakulmasta play-kuvaketta aloittaaksenne haastattelutehtävän. Toimittaja kysyy viisi kysymystä. Jokaiseen kysymykseen on aikaa vastata 30 sekuntia. Sekuntikello käynnistyy jokaisen kysymyksen jälkeen ja on näkyvillä ruudulla. Jos ette ehdi vastata kysymykseen annetussa ajassa, voitte painaa videon vasemmasta alakulmasta pause-kuvaketta ja jatkaa vastauksenne loppuun. Painakaa play-kuvaketta, kun haluatte siirtyä vastaamaan seuraavaan kysymykseen.

Haastatteluvideo löytyy täältä: https://youtu.be/wfe1DoL7-dc

Videon käsikirjoitus

Suomessa epäillään tapahtuneen laaja tietovuoto. Verkosta on löytynyt muun muassa henkilöiden ja organisaatioiden nimiä, jotka vaikuttavat olevan peräisin asiakaspalvelun sähköposteista. Organisaationne on yhdistetty epäiltyyn tietovuotoon.

- Miten kommentoitte asiaa?
- Miten organisaatiossanne on tätä tilannetta selvitetty?
- Millaisista tiedoista on kyse?
- Miten näin on voinut käydä?
- Miten varmistatte, että tällaista ei pääse jatkossa tapahtumaan?

5.7.1 Tehtävät

- Mitä viestintätoimia haastattelu aiheuttaa?
- Viestittekö siitä organisaatiossanne sisäisesti? Entä sidosryhmille?

6 Tapahtuma: Haavoittuvuus globaalissa online-käännöspalvelussa

6.1 Tietoturva NYT: ”Käytätkö Uugle-translatea? - Varo tietojen vuotamista”

Tietoturva nyt! TAISTO21 harjoitus

Käytätkö Uugle-translatea? - Varo tietojen vuotamista

Kyberturvallisuuskeskus on saanut tietoonsa kriittisen haavoittuvuuden koskien globaalia online-käännöspalvelua Uugle-translatea. Kyseinen onlinekäännöspalvelu on käytössä merkittävissä määrin globaalisti.

Uugle-translate online-käännöspalvelun avulla voidaan kääntää käyttäjän syöttämiä tekstejä toiselle kielelle nopeasti ja helposti.

Valmistajan mukaan ainakin kahden kuukauden ajan on ollut hyväksikäytettävissä haavoittuvuus, joka on voinut mahdollistaa joidenkin palveluun syötettyjen tekstien päätymisen vääriin käsiin. Palveluun syötetyt tekstit ovat voineet vuotaa palvelun välimuistista, mutta vielä ei ole tunnistettu tarkkaa laajuutta haavoittuvuudelle.

Palveluun ladatut tekstisisällöt tulisi pyrkiä tunnistamaan, mikäli kyseistä onlinekäännöspalvelua on käyttänyt ainakin viimeisen kahden kuukauden aikana. Lisäksi olisi hyvä tunnistaa aiheuttavatko kyseiset tekstisisällöt vuotaessaan haittaa väärissä käsissä.

6.2 Quacker: @Uugle

Uuglen tiedote

Laajasti käytössä olevaan Translate-palveluun on mahdollisesti kohdistunut tietomurto ja epäilemme laajaa tietovuotoa. Tilanteen selvitystyö on käynnissä. Pahoittelemme tilannetta.

6.3 ViTi: Uugle-Translate mahdollisen tietomurron kohteena

Uugle tiedotti juuri Translate-palveluun kohdistetusta mahdollisesta tietomurrosta ja epäillystä laajasta tietovuodosta. VitTin saamien tietojen mukaan tietomurron mahdollistanut haavoittuvuus on ollut hyväksikäytettävissä ainakin kahden kuukauden ajan. Tässä vaiheessa tilanteen todellisesta laajuutta tai mahdollista murron tekijää ei tiedetä.

Traficomin Kyberturvallisuuskeskus on julkaissut aiheesta Tietoturva NYT artikkelin, jossa kehotetaan tunnistamaan tekstisisällöt, joita viimeisen kahden kuukauden aikana on ladattu Uugle-Translate –palveluun, sekä arvioimaan, millaisia vaikutuksia palveluun ladattujen tietojen joutumisella vääriin käsiin on.

ViTi seuraa tilanteen kehittymistä.

6.4 Sanomat Uudeltamaalta: Asiantuntija: ”Netissä leviävät tiedot todennäköisesti peräisin Uugle-kääntäjän tietovuodosta”

Toimituksemme oli yhteydessä kyberturvallisuusasiantuntija Tuomas Tarkkaan liittyen julkisuudessa laajasti esillä olevaan epäilyyn Uugle-Translate –palveluun kohdistetusta tietomurrosta ja sieltä vuodetuista tiedoista, josta myös Uugle itse on tiedottanut.

”Vaikuttaa siltä, että nämä tiedot mitä nyt on julkisuuteen jo ehtinyt päätyä, ovat suurella todennäköisyydellä peräisin Uugle-kääntäjä –palvelusta. Nyt tulisi käynnistää pikimmiten selvitystoimet mahdollisesti vuotaneiden tietojen määrästä ja laadusta, mikäli on vähänkään epäilystä, että oman organisaation käsittelemää tietoa voisi olla vuotanut Uugle-kääntäjän kautta. Myös yhteistyö viranomaisten kanssa tulisi käynnistää välittömästi.”

6.5 Tehtävät

Online-käännöspalvelussa on havaittu haavoittuvuus, jota on mahdollisesti käytetty hyväksi.

- Mitä translate-tietovuoto tarkoittaa organisaatiolle?
- Onko organisaatiossanne ohjeita vastaavanlaisia tilanteita varten?
- Miten selvitätte, onko vuotaneiden tietojen joukossa organisaationne tietoja?
- Millaisia ilmoituksia viranomaisille tulisi tehdä? Kenen vastuulla ilmoitusten teko on?

6.5.1 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Keille organisaationne sisällä ilmoitatte havaitsemastanne uutisoinnista / some-keskustelusta?
- Mitä viestintätoimia tämä aiheuttaa organisaatiossanne?
    - Keille viestitte asiasta?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa tarvittaessa lausunnot medialle?
- Miten viestintä hoidettaisiin, jos tällainen tilanne tulisi vastaan virka-ajan ulkopuolella?
    - Miten viestintä on resursoitu?
    - Ovatko tarvittavat viestintävälineet ja -kanavat käytettävissä myös virka-ajan ulkopuolella? Ovatko esim. viestintäkanavien käyttöoikeudet vain jollain yhdellä henkilöllä?

7 Harjoituksen iltapäiväosuus

TAISTO21-harjoituksen iltapäiväosuus alkoi harjoitusalustalla julkaistulla infosyötteellä, joissa ohjeistettiin iltapäivän kulkua.

8 Tapahtuma: PilviPalvelu palautetaan viikon takaiseen palautuspisteeseen

8.1 Sähköposti: PilviPalvelun palveluntuottaja tiedottaa

Lähettäjä: PilviPalvelu@palveluntuottaja.fi
Vastaanottaja: Palvelunomistaja@organisaatio.fi
Aihe: Tiedote Pilvipalvelun häiriöistä

Hyvä asiakkaamme,

PilviPalvelussamme on ollut häiriöitä. Pahoittelemme PilviPalvelussamme olleiden häiriöiden teille aiheuttamaa haittaa.

PilviPalvelu saadaan takaisin toimintaan tämän vuorokauden kuluessa. Häiriöstä johtuen PilviPalvelun tiedot palautetaan viikon takaiseen tietoon.

Ystävällisin terveisin,
Pilvipalvelun tuottaja

8.2 Tehtävät

Olette saaneet tiedon PilviPalvelun palveluntuottajalta, että tiedot palautetaan viikon takkaiseen tietoon varmuuskopioilta.

- Millaisia vaikutuksia on organisaationne toimintaan, kun tiedot palautetaan viikon takaiseen tilanteeseen?
- Mitä toimenpiteitä viikon takaiseen tietoon palautuminen aiheuttaa Organisaatiollenne?
- Millaisia ilmoituksia viranomaisille tulisi tehdä? Kenen vastuulla ilmoitusten teko on?
- Oletteko tehneet viranomaisilmoitukset?

8.2.1 Lisätehtävät

Keskeinen henkilö organisaatiostanne jää pois pidemmäksi aikaa.

- Miten toimitaan, jos henkilö ei ole tavoitettavissa / jää sivuun pidemmäksi aikaa?
- Onko organisaatiossanne jokin osa-alue esimerkiksi turvallisuudessa henkilöitynyt liiaksi tietylle henkilölle?
- Onko prosessit ja ohjeet kunnossa ja toiminta hyvin dokumentoitua?

8.2.2 Viestintätehtävät

Edellyttääkö tämä asia viestintätoimenpiteitä organisaatiossanne? Jos edellyttää, niin miten ja kenelle viestitte?

9 Tapahtuma: Poliisin tietopyyntö liittyen epäilyttävästä toiminnasta Organisaation IP-osoitteessa

9.1 Sähköposti: Poliisilta saapuva tiedonsaantipyyntö koskien organisaation epäilyttävää ip-osoitetta

Lähettäjä: poliisi@poliisi.fi
Vastaanottaja: Organisaatio@organisaatio.fi
Aihe: Poliisin tiedonsaantipyyntö (Poliisilaki 4:3§)

Hei,

Poliisilla on tutkinnassa rikos, jonka esitutkinnan nojalla pyydämme teiltä tietoja, jotka voivat auttaa epäillyn tekijän tunnistamisessa.

Pyydämme teiltä ip-osoitteeseen xxx.yyy.zzz.qqq liittyvät lokitiedot järjestelmästänne, sekä palomuuristanne.

Tiedot voi toimittaa sähköpostilla suoraan asian tutkijalle timo.terava@poliisi.fi

Formaattina mieluiten excel-taulukko, tai pdf-tuloste, mistä pystyy kopioimaan tekstiä.

Tämä pyyntö perustuu Poliisilain (22.7.2011/872) 4 luvun 3§:ssä säädettyyn tietojensaantioikeuteen yksityiseltä yhteisöltä tai henkilöltä.

Poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä. Poliisilla on sama oikeus saada 6 luvussa tarkoitetussa poliisitutkinnassa tarvittavia tietoja, jos tärkeä yleinen tai yksityinen etu sitä vaatii.

Pyydän huomioimaan, että todisteiden hävittämisvaaran vuoksi tiedustelusta ei saa ilmoittaa edellä mainituille henkilöille, yhteisöille tai heidän edustajilleen.

Terveisin,
Komisario Terävä

9.2 Tehtävät

Olette saaneet poliisilta tiedonsaantipyynnön.

- Miten käynnistätte prosessin poliisin tiedonsaantipyynnön mukaisesti?
- Miten lähdette selvittämään pyynnön mukaisesti annetulta aikaväliltä lokitietoja pyydetyistä kohteista?
- Onko organisaatiollanne toimintamallit ja ohjeet?
- Pystyttekö itse selvittämään miten ja mistä edellä mainitut tiedot ovat saatavissa ja kuinka organisaation on mahdollista saada ne itselleen?

10 Tapahtuma: Toimittajariippuvuus - Kiina ostaa kriittisen palvelutuottajan liiketoiminnan

10.1 Iltanen: JUURI NYT: Alimama ostaa suomalaisen IT-yhtiön

IT-yhtiö ilmoitti juuri tiedotteessaan, että se on myynyt koko osakekannan kiinalaiselle IT solutions and services nimiselle yhtiölle. Yhtiön taustalla on Kiinalainen IT-jätti Alimama, joka omistaa yhtiön sataprosenttisesti. IT-yhtiön mukaan omistajavaihdoksella ei ole vaikutusta henkilöstölle. Palvelut jatkuvat myös normaalisti yrityskaupasta huolimatta.

IT-yhtiön toimitusjohtaja kommentoi, että kaupan myötä IT-yhtiö saavuttaa paremman kilpailukyvyn Euroopan markkinoilla. ”Tähyämme jatkossa liiketoiminnan kasvattamiseen. Tällä kaupalla tulee olemaan ainoastaan positiivisia vaikutuksia yhtiömme toimintaan. Alimama on yksi Kiinan suurimmista IT-konserneista. Tämä avaa meille aivan uudenlaisia mahdollisuuksia. Tulemme esimerkiksi avaamaan Lianongin alueelle uuden ekologisen datakeskuksen, jossa voidaan hyödyntää luonnon omaa viilennystä, tämä tulee tarjoamaan asiakkaillemme mahdollisuuden pienentää hiilijalanjälkeä edullisesti ja luotettavasti.”

10.2 Quacker: @Anni Nieminen

Kaikki suomalaiset yhtiöt myydään lopulta maailmalle.

10.3 Quacker: @Santtu Matalamaki

Itseäni hirvittää nähdä, että suomalaista teknologiaa ja huippuosaamista valuu kiinalaisten käsiin.

10.4 Quacker: @Matti Möttönen

Minun tietojani ei kiinalaisiin konesaleihin laiteta! #ORGANISAATIO

10.5 Sähköposti: Organisaatiolle kriittisen IT-palveluntoimittajan yhteyshenkilöltä

Lähettäjä: toimitusjohtaja@it-yhtio.fi
Vastaanottaja: palvelunomistaja@organisaatio.fi
Aihe: Tiedote omistajajärjestelyistä

Arvoisa asiakkaamme,

Yhtiössämme on käynnissä omistusjärjestelty, joiden seurauksena Kiinalainen IT solutions and services yhtiö hankkii yhtiömme koko osakekannan. Jatkamme tulevaisuudessakin samalla nimellä ja henkilöstöllä. Omistajavaihdos astuu voimaan 1.1.2022. Omistajavaihdoksella ei ole vaikutusta teille tuottamaamme palveluun.

Vastaan mielelläni omistajavaihdokseen liittyviin kysymyksiin.

Terveisin IT-yhtiön toimitusjohtaja

10.6 Tehtävät

Organisaationne kriittinen palveluntoimittaja myy koko osakekantansa ulkomaille toimijalle.

- Valitkaa organisaatiollenne kriittinen tietojärjestelmä/palveluntuottaja ja peilatkaa tapahtuman vaikutuksia teidän organisaatioonne. Tehtävässä ei tarvita hankinta- ja lakiasioiden osaamista. Miettikää yleisesti, mitä tapahtuma merkitsee organisaatiossanne.
    - Mitä vaikutuksia yrityskaupalla voi olla organisaationne toimintaan sekä palveluiden luotettavuuteen ja tietosuojaan?
    - Aiheuttaako yritysjärjestely toimenpiteitä organisaatiossanne?
    - Onko palvelusopimuksissanne mainintaa yritysjärjestelyihin liittyen?
    - Miten varmistatte palvelun jatkuvuuden, mikäli yritysjärjestelyn johdosta joudutaan tilanteeseen, jossa joudutaan vaihtamaan palveluntuottajaa?

10.6.1 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Keille organisaationne sisällä ilmoitatte havaitsemastanne uutisoinnista / some-keskustelusta?
- Mitä viestintätoimia tämä aiheuttaa organisaatiossanne?
    - Keille viestitte asiasta?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa tarvittaessa lausunnot medialle?
- Kirjoittakaa tarvittavat tiedotteet ja somejulkaisut ja julkaiskaa ne.

11 Tapahtuma: Organisaation läppäri myynnissä netissä

11.1 Sähköposti: Organisaation työntekijältä Organisaation turvallisuusvastaavalle

Lähettäjä: olli.maki@organisaatio.fi
Vastaanottaja: turvallisuus@organisaatio.fi
Aihe: FW: Pikainen selvityspyyntö

Hei,

sain sähköpostiini yhteydenoton Jussi Virtasella, viesti alla.

Vaikuttaa aika huolestuttavalta. Normaalisti meiltä poistuvat työasemat menevät kyllä kierrätykseen ja tyhjätään sovitun prosessi mukaisesti. He kyllä myös poistavat mahdolliset tarrat yms tunnisteet koneista.

Kuulin että meidän tiloissa oli tavattu hiljattain tuntematon henkilö? Voisiko tämä liittyä jotenkin siihen?

Mitä tälle Jussille pitäisi vastata?

Terv.

Olli Mäki
Asiantuntija,
ORGANISAATIO

---------- välitetty viesti alkaa----------

From: jussi.wiz98@tech.fi
To: olli.maki@organisaatio.fi
Aihe: Pikainen selvityspyyntö

Hei,

pyytäisin selvitystä pikaisesti alla olevaan asiaan.

Ostin muutama päivä sitten tori.fi nettikirpputorilta käytetyn kannettavan tietokoneen.

(kuva läppäristä jossa Organisaation tarra)

Koneen piti olla tyhjä myyjän ilmoituksen mukaan, mutta sieltä löytyikin sekalaisia tiedostoja melko runsaasti. Näiden joukossa oli teidän Organisaation toimintaan liittyviä tiedostoja, mm. PDF, Excel ja Word-tiedostoja. Asiakirjoissa on mainintoja tilinumeroista ja rahasummista, sekä muutamien henkilöiden tietoja, joiden perusteella päätin ottaa teihin yhteyttä.

Olen huolissani että tällaista voi tapahtua, miten voi olla mahdollista? Olen itsekin ollut tekemisissä teidän Organisaationne kanssa. Hoidetaanko teillä näin leväperäisesti tietosuoja-asioita? Olen ollut asiasta myös yhteydessä Iltapäivälehden toimitukseen. Haluaisin saada pikaisen selvityksen, onko myös minun tietojani käsitelty näin huolimattomasti?

Terveisin,
Jussi Eemeli Virtanen
0501231234
Kauppatie 3, Porvoo

11.2 Iltanen: JUURI NYT: Jussi hämmästyi - Osti nettikirpparilta käytetyn läppärin ja siellä oli Organisaation arkaluonteisia tiedostoja

Tietoturva-alan yksityisyrittäjänä työskentelevä porvoolainen Jussi osti koneen tori.fi -nettikirpputorilta ja hämmästyi ”piti ostaa halpa ja hyvä läppäri pojalle koulua varten. Tarkastin koneen ennen pojalle antamista, ja sieltähän löytyikin sitten vaikka mitä. Koneessa oli suomalaisen Organisaation tarra kiinni, mutta ajattelin että se on vain siihen jäänyt kun ei ole irti saatu. Kuitenkin koneesta löytyi muutakin Organisaatiolta peräisin olevaa: runsaasti tiedostoja!” Jussi kummastelee. Kovalevyltä löytyi paljon tiedostoja, joista osa selkeästi jonkin aiemman käyttäjän omia henkilökohtaisia tiedostoja, mutta seassa vaikutti olevan myös Organisaation toimintaan liittyviä asioita. ”Erikoista oli myös se, että koneessa ei ollut minkään-laista salasanasuojausta käytössä, olin varautunut asentamaan oman puhtaan käyttöjärjestelmän mutta uteliaisuus vei voiton katsoa ensin mitä sieltä löytyy”, Jussi myöntää.

Jussille Organisaatio on tuttu, ”aloin huolestumaan, kun olen itsekin asioinut Organisaation kanssa. Siellä oli henkilötietojakin näkyvillä. Omiani en löytänyt, mutta omasta asioinnista Organisaation kanssa onkin tosin jo vuosia aikaa.”

Jussi kertoo olleensa yhteydessä myös Organisaatioon, ”jotta he saavat selvitettyä onko tässä tapahtunut laajemminkin laiminlyöntejä.” Lisäksi Jussi kertoo, että haluaa tuoda asian julki, ”jotta asia varmasti selvitetään pohjamutia myöten eikä lakaista maton alle”. ”Mielestäni on myös tärkeää, että kaikki Organisaation kanssa asioineet saavat tietää asiasta, ja pystyvät siten olemaan yhteydessä omien tietojensa tarkastamiseksi.

Toimituksemme ei ole toistaiseksi saanut kommenttia Organisaatiolta.

11.3 Quacker: @jussiwiz

Aika paha moka Organisaatiolta. Ostin läppärin joka osoittautui ilmeisesti Organisaation käytöstä poistetuksi – ainoa vaan että kovalevyä ei oltu putsattu. Siellä löytyi vaikka ja mitä.

Kaikille omista tiedoistaan huolestuneille: latasin läpinäkyvyyden nimissä dumpin löytyneestä datasta pastebiniin jakoon: paste.bin/3424232. Käy tarkastamassa löytyykö omia tietoja! Sitten vain rikosilmoitusta tekemään! #Organisaatio #tietovuoto #jussidataoy #whistleblow

11.4 Sähköposti: Iltasen toimittajan artikkelin täydennyspyyntö Organisaation viestinnälle

Lähettäjä: toimittaja@iltanen.fi
Vastaanottaja: organisaatio@organisaatio.fi
Aihe: Organisaation kommentit julkaistavaan artikkeliin

Hei,

Toimittaja Vieno Kainonen Iltasesta päivää! Olemme saaneet tiedon, että nettikirpparilta ostetusta käytetyn läppäristä on löytynyt organisaationne arkaluontoisia tiedostoja. Olemme tekemässä asiasta vielä jatkojuttua ja haluaisimme teidän kommenttinne asiaan.

- Oletteko tietoisia, että tällaista on tapahtunut?
- Miten olette selvittämässä asiaa?
- Miten tällaista on voinut tapahtua? Onko tietoturvanne ollenkaan ajan tasalla?
- Voiko tällaisia koneita löytyä lisää?
- Miten ohjeistatte toimimaan, jos joku löytää ostamastaan koneesta tällaisia tietoja?

Pyydän vastaustanne mahdollisimman pian. Olen julkaisemassa artikkelin tänään.

Terveisin,
Vieno Kainonen

11.5 Tehtävät

Mediassa on esitetty, että Organisaationne tietoja sisältäviä tietokone on mahdollisesti päätynyt organisaationne ulkopuoliselle taholle.

- Miten organisaatiossanne on järjestetty käytettyjen laitteiden poistoprosessi?
- Onko olemassa ajantasaista ohjeistusta tai politiikkaa käytettyjen laitteiden kierrättämiseen?
- Miten voidaan varmistua, että kyseessä on juuri teidän organisaatiostanne peräisin olevasta materiaalista?
- Miten yhteydenottajaan tulisi reagoida?
- Tulisiko tilanteesta tehdä viranomaisilmoituksia?

11.5.1 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon uutisista ja some-keskustelusta?
- Keille organisaationne sisällä ilmoitatte havaitsemastanne uutisoinnista / some-keskustelusta?
- Miten reagoitte somekeskusteluun ja uutisointiin ja millaisiin viestintätoimiin ryhdytte?
    - Keille viestitte asiasta?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa lausunnot medialle?

Toimittaja Vieno Kainonen on yhteydessä organisaatioonne jutun kirjoitusvaiheessa, ja pyytää teiltä kommenttia.

- Miten reagoitte toimittajan tietopyyntöön?
- Kenelle kerrotte toimittajan yhteydenotosta?
- Kuka vastaa toimittajan kysymyksiin?
- Miten lähdette selvittämään tapauksen taustoja, keneen olette yhteydessä organisaatiossanne?
- Mitä vastaatte toimittajan kysymyksiin (mitä kerrotaan ulos ja mitä ei)?
- Vastatkaa toimittajan esittämiin kysymyksiin ja kirjoittakaa tästä vastine.

12 Tapahtuma: Salassa pidettävän tiedon vuotaminen

12.1 Quacker: @tarkkamarkka

Kylläpä turhauttaa saada tarjouspyyntö sähköpostiin tällaisella kommentilla! Keltaisella palkilla peitetty palveluntuottaja joka varsin selvästi on jo etukäteen valittu.

12.2 Quacker: @yrittäjäyrmeli

Pitihän se arvata, itsekkin olen hävinnyt monet julkiset kilpailutukset. Mietityttää, että tuttuja suosittu? #syylliset vastuuseen

12.3 Quacker: @Pera

Näin niitä veronmaksajien rahoja taas haaskataan! # veronmaksajienrahat

12.4 Tehtävät

Organisaationne lähettämässä dokumentissa paljastuu erhe, johon oli jäänyt organisaationne sisäinen kommentti, joka selkeästi vääristää esimerkiksi kilpailutilannetta (ks. kuva). Kyseessä on Word-dokumenttina lähetetty tiedosto, joka sisältää kommentteja, joita ei virallisessa versiossa pitänyt olla.

- Minkälainen ohjeistus organisaatiossanne on tiedostojen siistimiseen ennen lähettämistä?
- Miten varmistatte, ettei asiaan kuulumattomia tietoja siirry dokumentista toiseen?
- Miten reagoitte yhteydenottoon?

12.4.1 Viestintätehtävät

- Miten saatte organisaatiossanne tiedon some-keskustelusta?
- Keille organisaationne sisällä ilmoitatte havaitsemastanne some-keskustelusta?
- Miten reagoitte somekeskusteluun ja uutisointiin ja millaisiin viestintätoimiin ryhdytte?
    - Keille viestitte asiasta?
    - Mitä viestitte eri kohderyhmille?
    - Mitä kanavia käytätte asian viestimiseen?
    - Kuka teillä antaa tarvittaessa lausunnot medialle?

13 Harjoitusinfo – koko päivän harjoitus on päättynyt

TAISTO21-harjoitus on päättynyt!

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

Yhteenveto harjoituspäivän tapahtumista

- Pilvipalvelun häiriössä oli kyse globaalista häiriöstä, jolla oli vaikutuksia useaan organisaatioon.
- Toimitiloissa tavattu tuntematon henkilö oli kiinteistöhuollosta, mutta tieto henkilön käynnistä ei ollut välittynyt eteenpäin organisaatiossa. Tapahtumalla ei ollut yhteyttä tietovuotoon.
- Organisaatiosta ei ollut kadonnut tietokoneita, tämä osoittautui virheelliseksi tiedoksi.
- Uugle translate -tapahtumassa oli kyse globaalissa käännöspalvelussa tapahtuneesta tietovuodosta. Organisaation henkilö oli käyttänyt maksuttomasti käytössä olevaa käännöspalvelua työtehtäviin liittyen.
- Tiedon saantipyyntö Poliisilta organisaatiolle koskien tutkinnassa olevaa rikosta. Rikos ei liity harjoituksen tapahtumiin.

- Kriittisen palvelutoimittajan liiketoiminta on myyty EU-alueen ulkopuolelle, tapahtumaan ei liity tietoturva- tai tietosuojaloukkausta.
- Organisaation ulkopuolelle päätynyt tietokone oli tyhjennetty prosessien mukaisesti ja tietokoneesta ei löytynyt organisaation asiakirjoja tai vastaavaa. Kyseessä oli klikkiotsikko.
- Organisaation hankinta-asiakirjoihin oli jäänyt näkyville metatietoja, jotka päätyivät julkaistuille kilpailutusasiakirjoille.

Digitalisaation tukipalvelut ja yhteentoimivuus / Penttilä Laura (DVV) 18.1.2022

Liite 1 Harjoituspäivän aikataulu

Julkaisu-aika	Syötteen otsikko (suluissa oleva numero kuvaa tapahtumakokonaisuutta)
8:00:00	Harjoitusinfo
8:00:00	Harjoitusinfo: Harjoituksen medialähteet
8:00:00	Harjoitusinfo: Tervetuloa TAISTO21-harjoitukseen
9:00:00	TAISTO21-harjoituksen avaustervehdys
9:01:00	Kyberturvallisuusjohtaja Rauli Paanasen tervehdys
9:02:00	(1) Uutislähetys YME Uutiset
9:07:00	(1) NY Times paljastaa: PilviPalvelun alasajon taustalla vakava tietomurtoepäily
9:08:00	(1) @ATKjäbä
9:08:00	(1) Sähköposti Organisaation johdosta jatkuvuudenhallinnasta vastaaville henkilöille
9:08:01	(1) @Raqqadi
9:09:00	(1) @ATKjäbä
9:09:00	(1) Sähköposti Organisaation työntekijältä Organisaation tietoturvavastaavalle
9:10:00	(1) @Raqqadi
9:10:00	(1) Sähköpostin poissaoloviesti Organisaation tietoturvavastaavalta
9:11:00	(1) Tehtävät
9:30:00	(2) Sähköposti Organisaation turvallisuusvastaavalle
9:31:00	(2) Sähköposti Organisaation henkilöstöhallinnolle
9:32:00	(2) Sähköposti Organisaation riskienhallinnasta / jatkuvuudesta vastaavalle johtajalle
9:33:00	(2) @Suomi-vuotaa
9:33:30	(2) @FIN-Leaks
9:34:00	(2) @Suomi-vuotaa
9:34:30	(2) @Pekka Virtanen
9:35:00	(2) Julkishallinnon tietovuoto – taustalla Organisaation heikko turvallisuuskulttuuri?
9:36:00	(2) Tehtävät
10:00:00	(3) Organisaation työntekijä on antanut Organisaation tietoja huijaussivustolle
10:01:00	(3) Tehtävät
10:30:00	(4) Uutislähetys
10:35:00	(4) @FIN-Leaks
10:35:30	(4) @MirvaMöttönen
10:35:40	(4) @KariArviainen
10:36:00	(4) Sähköposti Organisaation henkilöstöhallinnon työntekijältä turvallisuusvastaavalle
10:37:00	(4) Tehtävät
10:40:00	(4) YME-uutisten puhelinhaastattelu
10:50:00	(4) Tehtävät haastattelun jälkeen
11:00:30	(5) Tietoturva nyt! TAISTO21 harjoitus
11:01:30	(5) @Uugle
11:02:00	(5) Uugle-Translate mahdollisen tietomurron kohteena
11:03:00	(5) Asiantuntija: ”Netissä leviävät tiedot todennäköisesti peräisin Uugle-kääntäjän tietovuodost
11:04:00	(5) Tehtävät
11:30:00	Harjoitusinfo: Puolenpäivän harjoitus on päättynyt
12:30:00	Harjoitusinfo: Tervetuloa harjoituksen iltapäiväosuuteen!
12:31:00	(6) Sähköposti PilviPalvelun palveluntuottajalta Organisaation palvelunomistajalle

Digitalisaation tukipalvelut ja yhteentoimivuus / Penttilä Laura (DVV) 18.1.2022

12:32:00	(6) Tehtävät
13:00:15	(7) Sähköposti Poliisilta Organisaatiolle saapuva tiedonsaantipyyntö
13:01:00	(7) Tehtävät
13:30:00	(8) JUURI NYT: Alimama ostaa suomalaisen IT-yhtiön
13:31:30	(8) @AnniNieminen
13:32:00	(8) @SanttuMatalamaki
13:32:30	(8) @MattiMöttönen
13:33:00	(8) Sähköposti Organisaatiolle kriittisen IT-palveluntoimittajan yhteyshenkilöltä
13:34:00	(8) Tehtävät
14:00:00	(9) Sähköposti Organisaation työntekijältä Organisaation turvallisuusvastaavalle
14:01:00	(9) JUURI NYT: Ostin nettikirpparilta käytetyn läppärin ja siellä oli Organisaation arkaluonteisia
14:01:01	(9) @jussiwiz
14:02:00	(9) Sähköposti Iltasen toimittajan artikkelin täydennyspyyntö Organisaation viestinnälle
14:03:00	(9) Tehtävät
14:30:00	(10) @tarkkamarkka
14:31:00	(10) @yrittäjäyrmeli
14:31:30	(10) @Pera
14:32:00	(10) Tehtävät
15:00:00	Harjoitusinfo: Kokopäivän harjoitus on päättynyt