TRAFICOM
Liikenne- ja viestintävirasto

Myötäelä ja viesti selkeästi Kyberhyökkäyksessä

Maria Kellokumpu
Johtava viestintäasiantuntija

Agenda

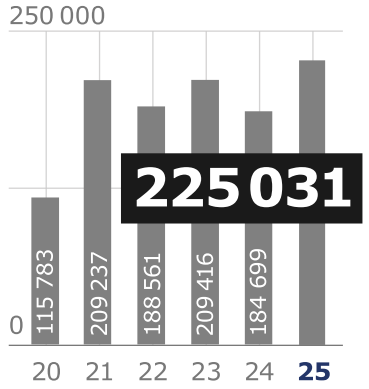
- Miksi juuri nyt tarvitaan erillinen ohje kyberhyökkäyksistä viestimiseen?
- Kyberhyökkäysten viestinnällisiä erityispiirteitä
- Tilanteen johtaminen
- Konkreettisia työkaluja kyberhyökkäysviestintään

Miksi juuri nyt tarvitaan erillinen ohje kyberhyökkäyksistä viestimiseen?

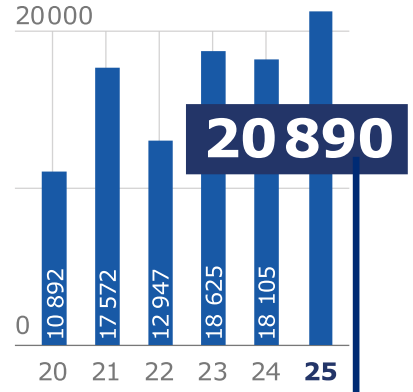
2025 lukuina

Viimeisen vuoden aikana vakavien tapausten määrä on kasvanut ja useat organisaatiot ovat joutuneet kiristyshaittaohjelmien kohteiksi. Uusia haavoittuvuuksia hyödynnetään hyökkäyksissä nopeasti

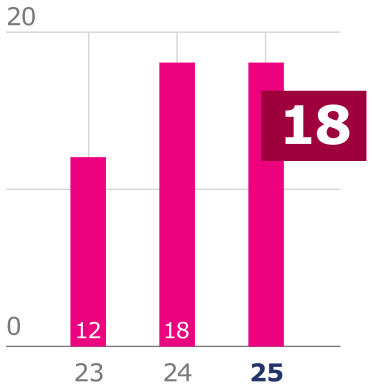
Automaattisesti käsitellyt havainnot



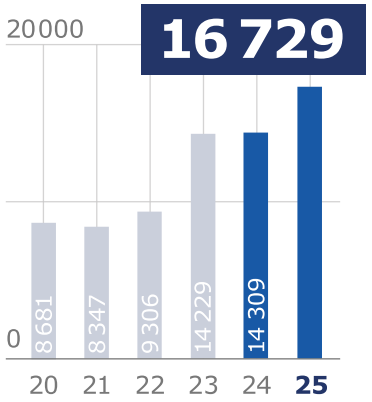
Kaikki kyberpoikkeama-ilmoitukset yhteensä



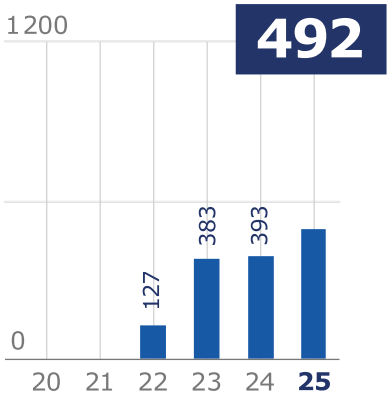
Merkittävät kyberpoikkeaman-hallintaoperaatiot



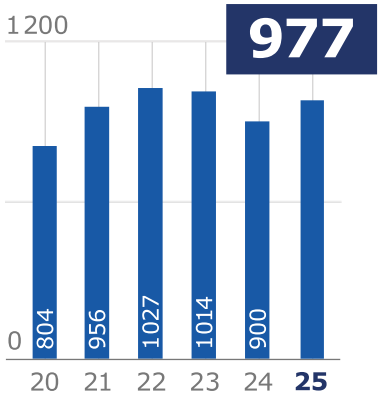
Huijaukset ja kalastelut[1]



Tietomurron yritykset[2]

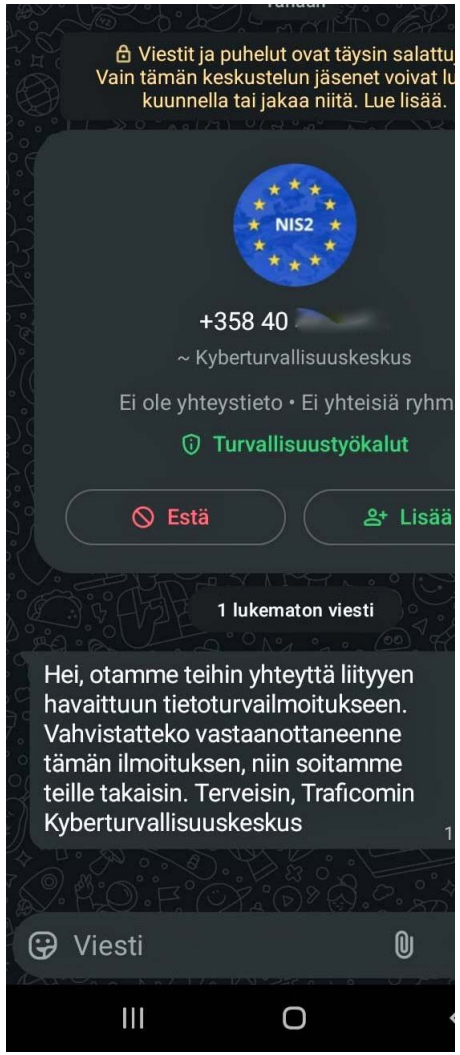


Tietomurrot



LÄHDE: Kyberturvallisuuskeskus | [1] Huijausten ja kalastelujen tilastointi on muuttunut vuonna 2024, joten luvut eivät ole täysin vertailukelpoisia. | [2] Tietomurtoyritysilmoituksia on raportoitu alkaen vuodesta 2022.

Kukaan ei ole immuuni



Tietoliikenne

Valtorin tietomurto uhkaa tuhansien virkahenkilöiden tietoturvaa

Yli 50 000 valtion mobiililaitteen käyttäjätiedon vuotamisen riskinä on se, että ne ovat päätyneet vääriin käsiin yhtenä valmi pakettina.

Kuva: Petteri Bülow / Yle

VILLE KOLARI

9.2. 16:30

Kuuntele juttu 2:41

Valtion tieto- ja viestintätekniikkakeskukseen on tehty viime viikolla s tietomurto, jota keskusrikospoliisi tutkii tässä vaiheessa törkeänä tietomurtona.

Tietomurto on paljastanut esimerkiksi syyttäjien ja ministeriöiden tietoja, mahdollisesti muitakin.

Tämä on merkittävä tietoturvariski, sanoo Valtorin ICT-toiminnan tukipalveluiden ylijohtaja **Hannu Naumanen**.

Naumasen mukaan riski syntyy siitä, että murtautujalla on nyt hallussaan virkahenkilöiden nimet ja yhteystiedot.

From: Domainhoteeli [redacted]
Subject: Älä ota riskejä: Uusi palvelusi jo tänään varmistaaksesi jatkuvuuden verkossa.
Date: 30 October AD 2024 at 14:38
To: [redacted]

domainhotelli

Hyvä asiakas,

Otamme yhteyttä ilmoittaaksemme kiireellisestä o

Palveluumme liittyvä tilauksesi on vanhentunut, ja muistutuksista, emme ole vieläkään vastaanottan vuoksi saatat menettää pian pääsyn palveluihimm

Tärkeää! Sinulla on 7 päivää tämän sähköpostivie aikaa uusia tilauksesi. Jos et päivitä tietojasi mää palvelusi kytkeytyvät automaattisesti pois käytöst merkittäviä keskeytyksiä ja lisäkustannuksia palve uudelleenaktivoinnista.

Pyydämme ystävällisesti, että klikkaat alla ole päivittääksesi tietosi ja jatkaaksesi nauttimist keskeytyksiä. Kiitos nopeasta huomiostasi täh jotta voimme varmistaa jatkuvan ongelmattom

Päivitä tietosi

Kiitos, että valitset palvelumme, ja että k tarvittavalla vakavuudella.

Microsoftin sähköpostiohjelmassa havaittu vakava haavoittuvuus

Kyberturvallisuuskeskuksen mukaan kyseistä haavoittuvuutta on jo hyödynnetty verkkohyökkäyksissä.

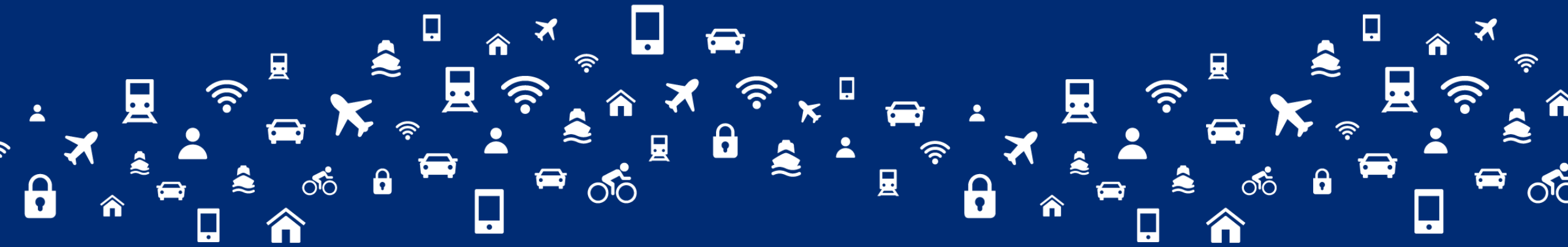
Haavoittuvuudelta

TRAFICOM

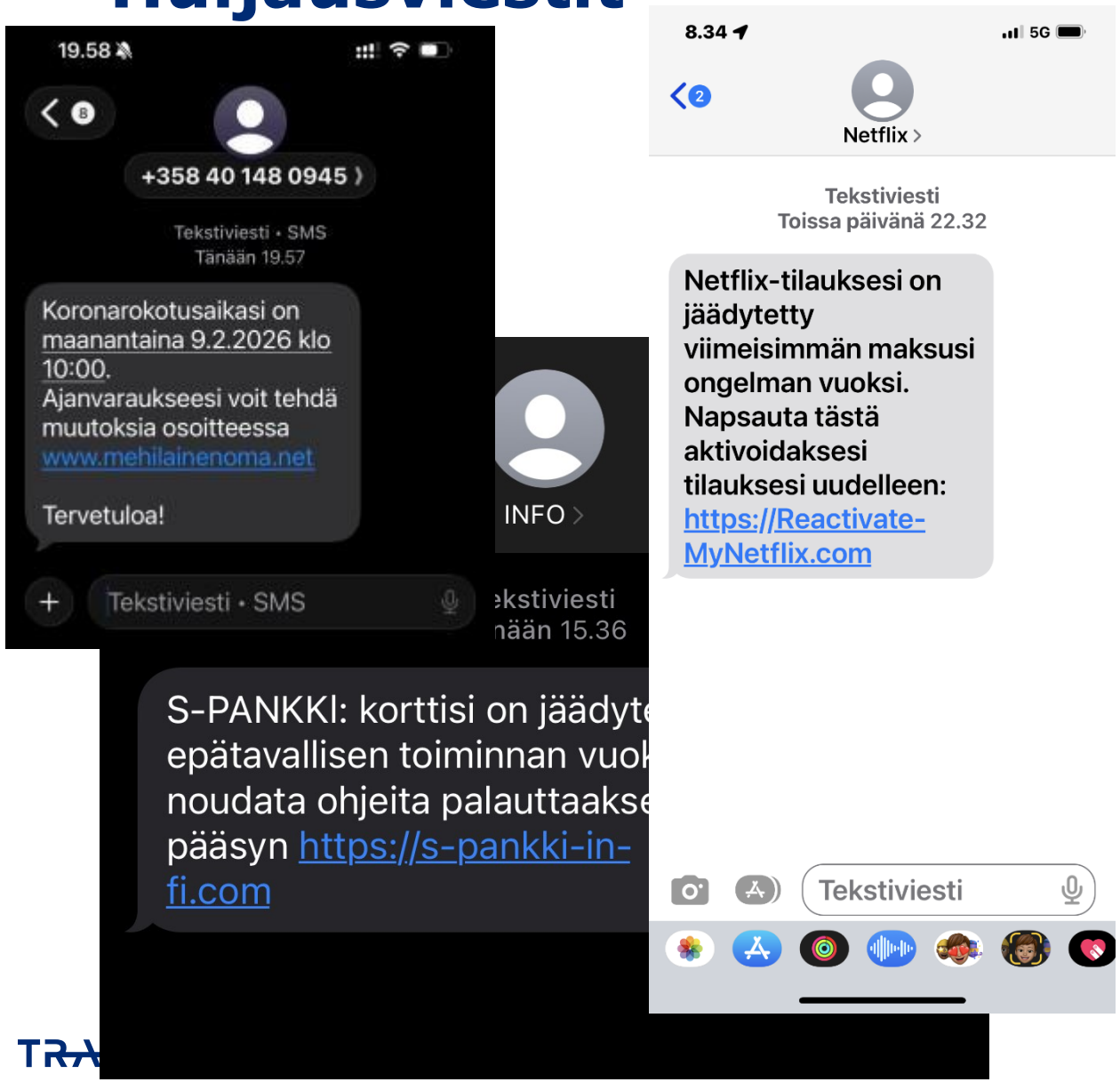
Miksi juuri nyt?

- Kyberturvallisuuden uhkataso on pysynyt kohonneena
- Suomalaisiin organisaatioihin kohdistuu kohdennettuja ja räätälöityjä kyberhyökkäyksiä
- Kyberuhat huolestuttavat suomalaisista
- Kyberrikollisuus kukoistaa
- Kyberhäiriön vaikutukset ja tarve viestinnälle pitkäaikaisia.
- NIS2:n ilmoitus/viestintävelvoite

Kyberhyökkäysviestinnän erityispiirteitä



Huijausviestit



Esimerkkiviesti

- Hei,
- ..organisaatiomme nimissä on lähetetty huijausviestejä. Valheellisesti Firma Oy:nä esiintyvissä viesteissä kerrotaan...
- Oikeasti Firmalta tulevissa viesteissä ei koskaan ole linkkejä...
- Emme koskaan kysy tunnuksiasi puhelimessa tai lähetä kirjautumislinkkejä tekstiviestillä!
- Olemme tehneet tapauksesta rikosilmoituksen ja ilmoittaneet Kyberturvallisuuskeskukselle kalasteluviesteistä haitallisten-

Huijaukset

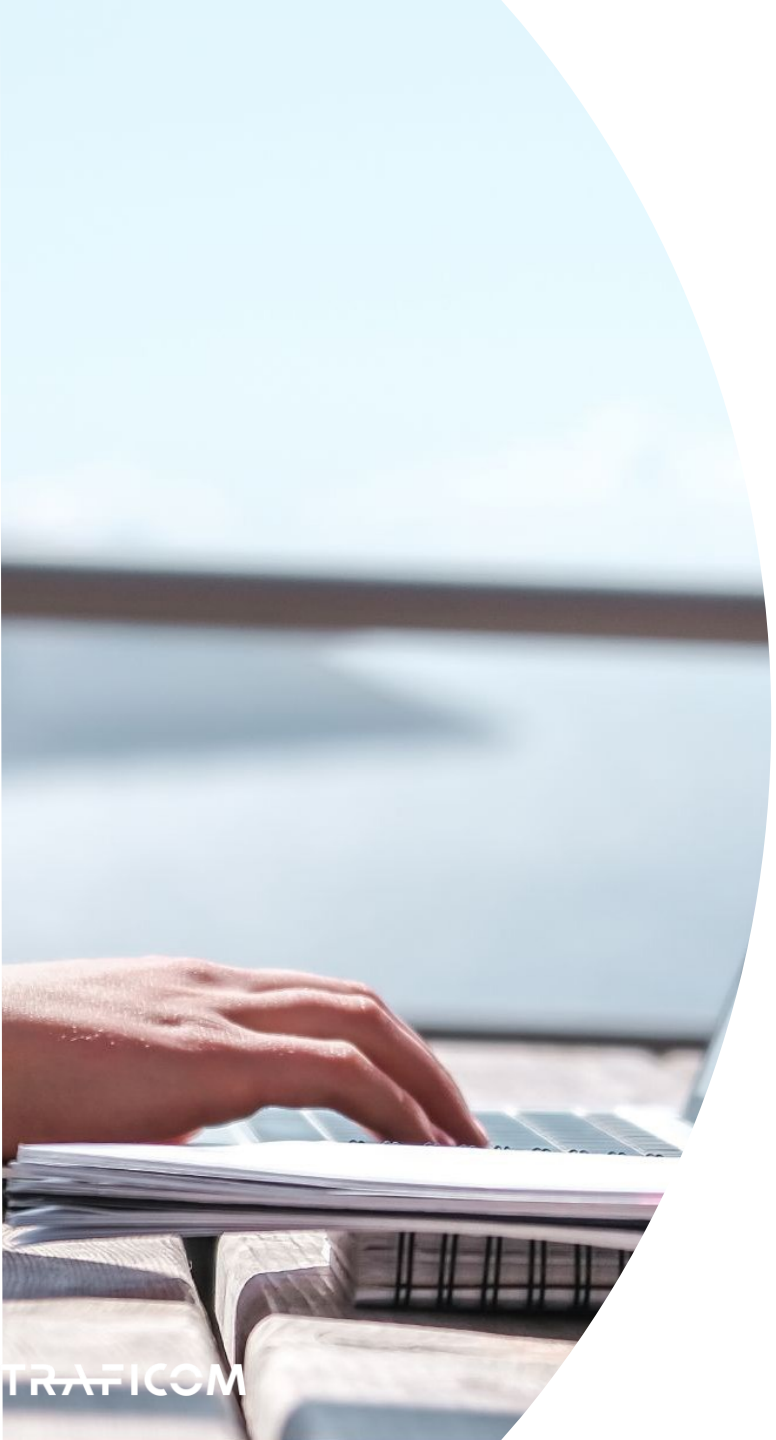
Viestin liitteenä on asetustiedosto, joka voi antaa rikolliselle pääsyn puhelimelle.

Älä siis avaa epäilyttäviä liitetiedostoja tai hyväksy käyttöön tuntemattomia asetuksia.

TRAFICOM

M365 sähköpostitilimurto

- Ilmiöstä varoitettiin jo 2018, 2023
- Sisäinen viestintä - mitä on käynyt, toimenpidesuositukset
- Ulkoinen viestintä: jos murretulta tililtä on lähetetty kalasteluviestejä, lähettäkää kaikille vastaanottaneille nopeasti varoitusviesti
- Rikosilmoitus poliisille ja noudattakaa poliisin antamia ohjeita myös tapahtuneesta viestimisessä.
- Verkkosivuille lisätietoa



Tietomurto

- Ilmoitus tietosuojavaltuutetulle ja asiakkaille, joita tietovuoto koskee.
- Tee poliisille rikosilmoitus.
- Mikäli asiakkaita on paljon, verkkotiedote on paras vaihtoehto, muttei korvaa uhrien henkilökohtaista kontaktointia
- Varautukaa mediayhteydenottoihin mahdollisen julkisuuden vuoksi. Tietosuojalaki velvoittaa kattavaan ilmoittamiseen tietovuototapauksissa, ja siten ne päätyvät lähes aina myös julkisuuteen.
- Poikkeaman juurisyy kiinnostaa ja sitä tullaan kysymään. On tärkeää myös viestiä, mihin toimenpiteisiin on tapauksen johdosta ryhdytty ja miten vastaavaa estetään tapahtumasta jatkossa.

Palvelunestohyökkäys

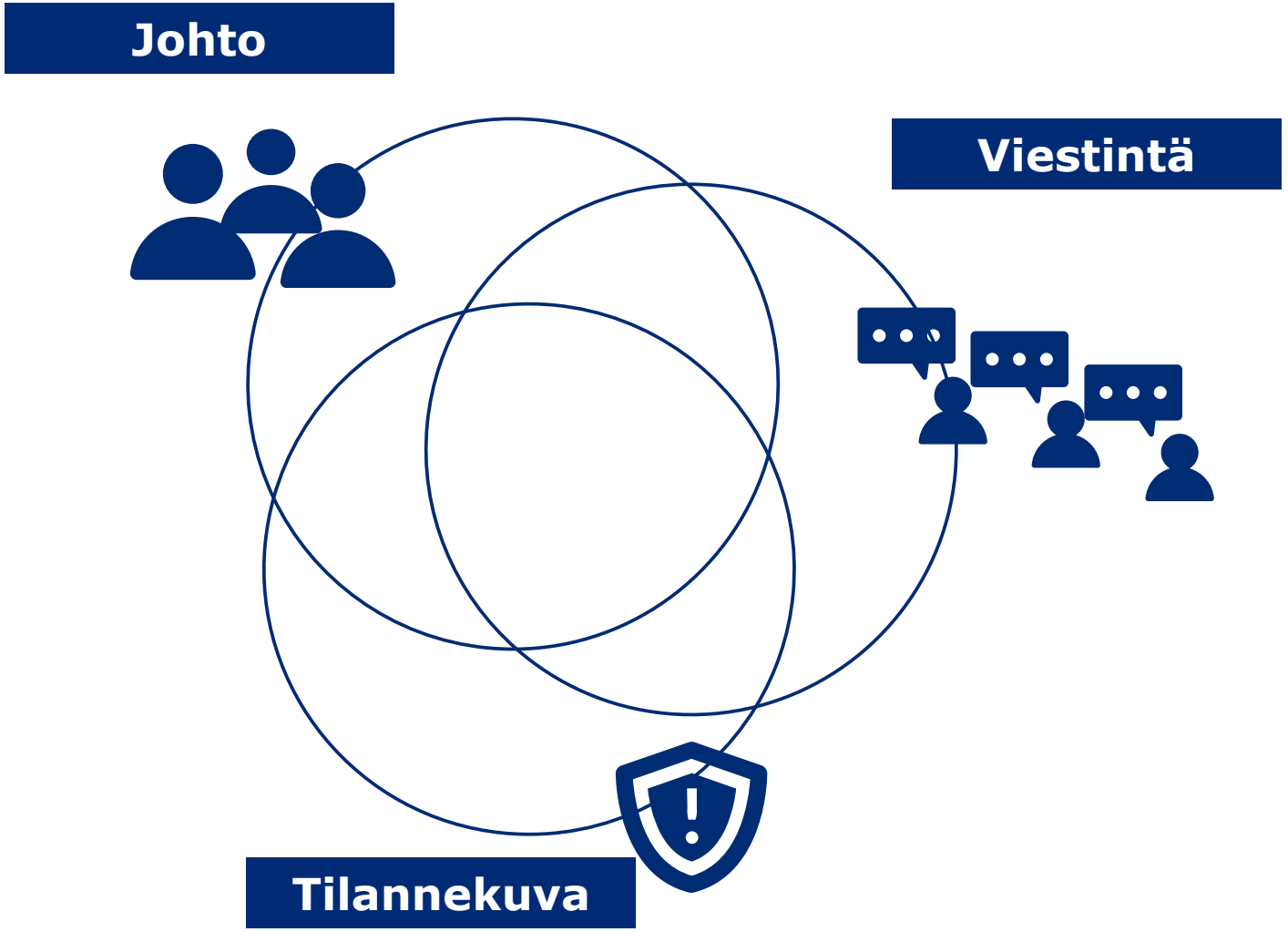
- Hei, sivustoomme/palveluumme organisaatio.fi kohdistuu palvelunestohyökkäys. Se tarkoittaa, että sivustoomme/palveluumme kohdistuu poikkeuksellisen paljon tietoliikennettä, jolla hyökkääjä pyrkii häiritsemään sivuston toimintaa.
- Rahasi/tietosi yms. eivät ole vaarassa, eikä kukaan ulkopuolinen ole päässyt käsiksi palvelun sisältämiin tietoihin. Asiantuntijamme selvittävät asiaa palveluntarjoajan kanssa.
- Sivuston toiminta pyritään palauttamaan mahdollisimman pian. Kiireellisissä asioissa voitte olla yhteydessä asiakaspalveluumme **asiakaspalvelu@organisaatio.fi** t ai 091231132.

[AKIRA]
Well, you are here. It means that you're suffering from cyber incident right now. Think of our
as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that data is a
price to make it all go away. Do not rush to assess what is happening - we did it to you. No one
you can do is to follow our instructions to get back to your daily routine, by contacting us we
will minimize the damage that might be done. Those who choose different path will be shamed on
The functionality of this blog is extremely simple - enter the desired command in the field and
enjoy the juiciest information that corporations around the world wanted to stay confidential.
You are unable to recover without our help. Your data is already gone and cannot be traced to
of final storage nor deleted by anyone besides us.
Guest@akira:~$ help
List of all commands:
leaks — hacked companies
news — news about upcoming data releases
contact — send us a message and we will contact you
help — available commands
clear — clear screen
akira:~$

Kiristyshaittaohjelma

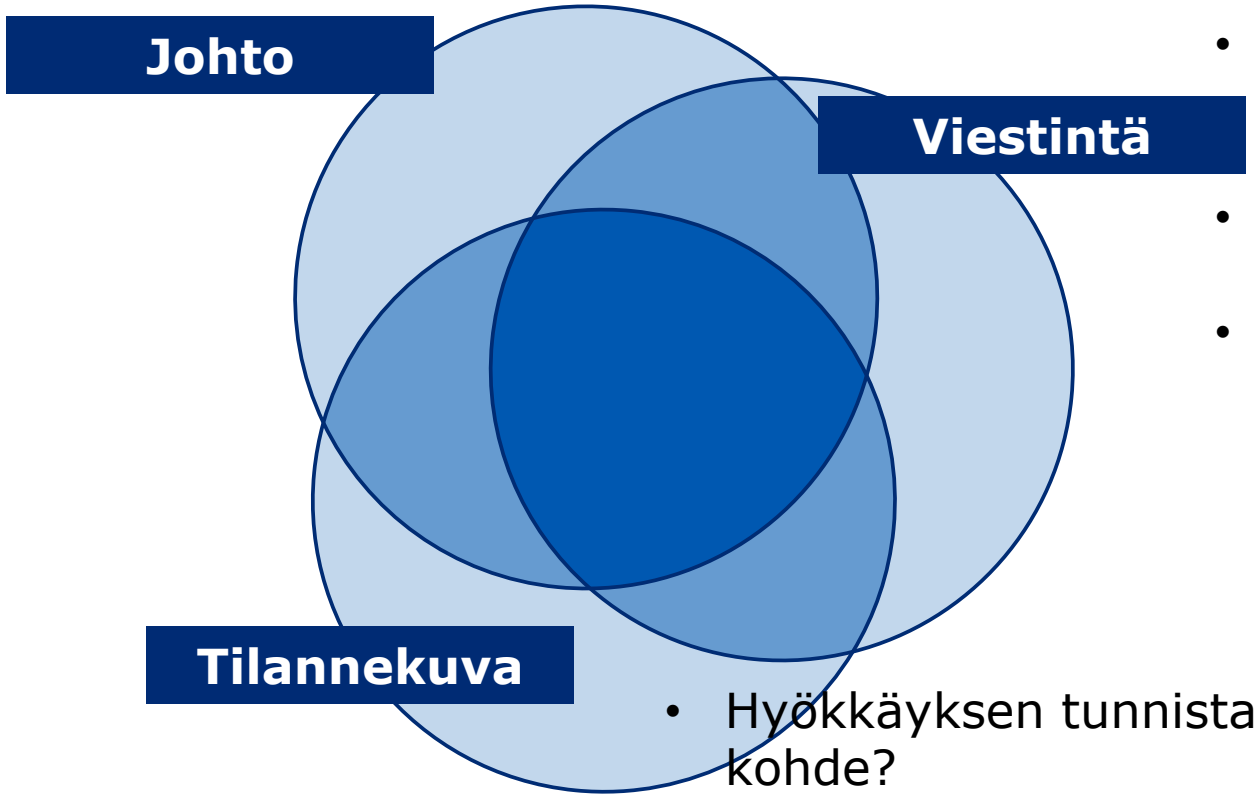
- Viesti poikkeamasta ja vaikutuksista sisäisesti, ohjeista henkilöstölle vaihtoehtoiset toimintatavat ja -palvelut.
- Varaudu henkilöstön reagointiin poikkeustilanteessa, mm tehostamlla viestintää
- Viesti poikkeamasta ja häiriöistä asiakkaille ja sidosryhmille.
- Muista tietosuojalain asettamat velvoitteet uhreille ja tietosuojavaltuutetulle ilmoittamisesta, jos hlötietoja on varastettu.
- Pohtikaa organisaatiossa tapaa ja termejä etukäteen: miten kuvailisitte kiristyshaittaohjelman tapaista vakavaa poikkeamaa eri sidosryhmille? Miten tapauksesta viestitään, jos normaalit järjestelmät eivät ole käytettävissä?
- Kiinnittäkää huomiota viestinnän ja ohjeiden selkeyteen, ymmärrettävyyteen ja kattavuuteen. Muistakaa viestinnän ja ohjeistamisen tarve uhreille myös tilanteen jälkeen.
- Rikosilmoitus poliisille ja noudattakaa poliisin antamia ohjeita myös tapahtuneesta viestimisessä.

Johtaminen, tilannekuva ja viestintä



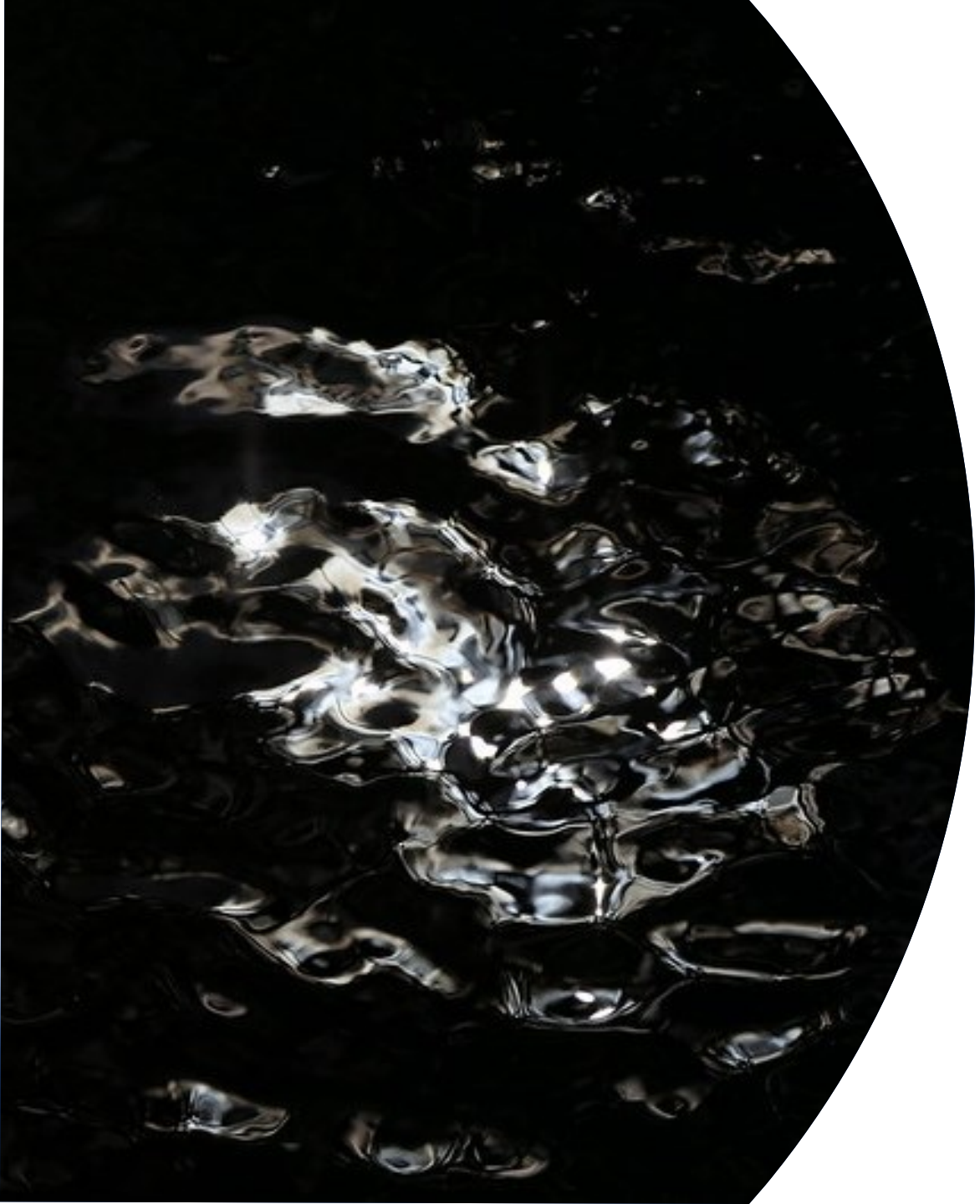
Johtamisen, tilannekuvan ja viestinnän yhteys

- Miten organisoidaan tilanteen hallinta ja johto?
- Miten organisaation toiminnan jatkuvuus turvataan?
- Miten turvataan toiminnan jatkuvuus?
- Kenelle tapahtuneesta tulee ilmoittaa? Lakien ja säädösten noudattaminen



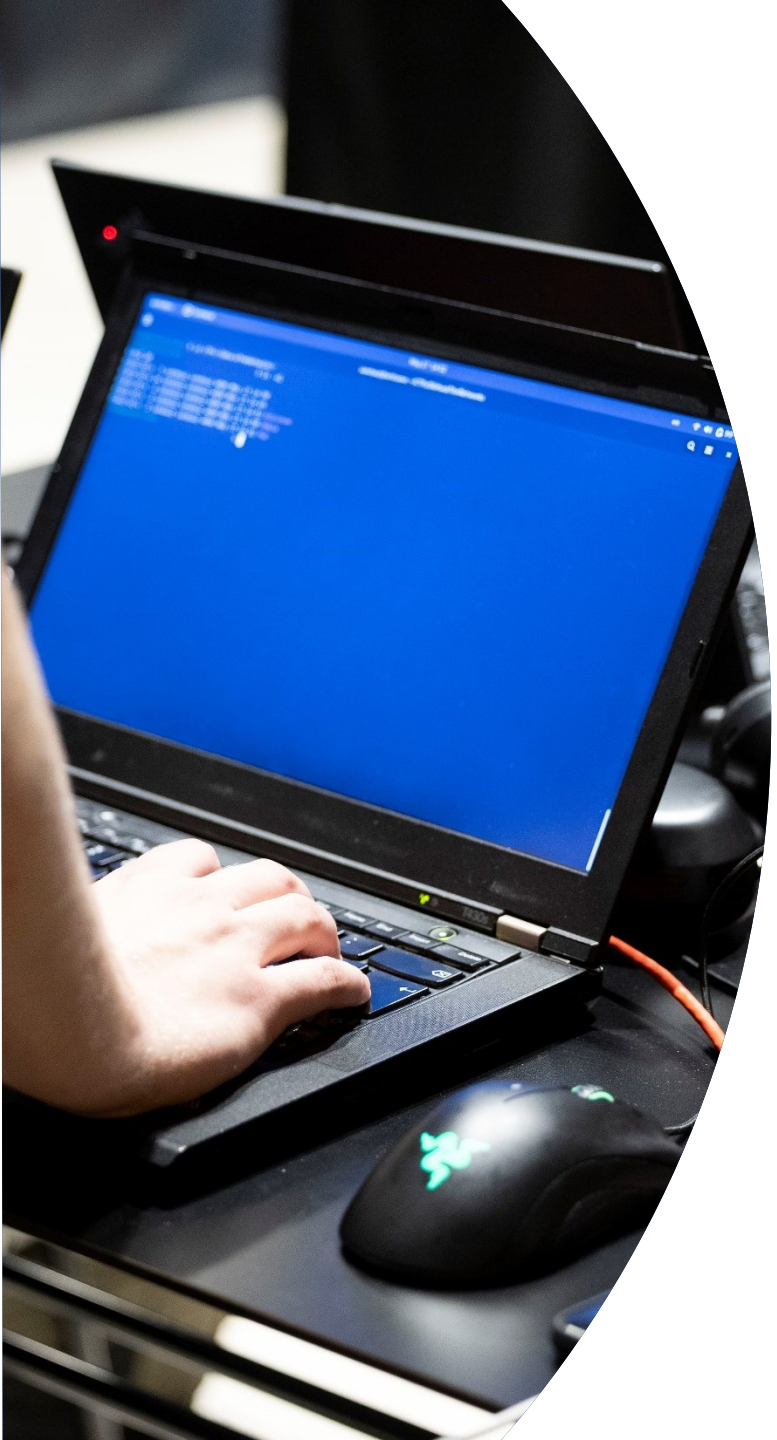
- Miten varmistetaan tiedonkulku ja viestinnän yhteensovittaminen?
- Onko viestintä edustettuna siellä missä tarvitaan?
- Viestinnän kanavat, keinot, kohderyhmät?
- Viestinnän roolit, resursointi

- Hyökkäyksen tunnistaminen, laajuus, kohde?
- Hyökkäyksen vaikutukset?
- Hyökkäykset tekniset piirteet?
- Tilannekuvan ajantasaisuus?



Kriisiviestinnän kuusi pointtia

- Tilannetta johdetaan ja siitä viestitään, vaikka kaikkea ei tiedetä.
- Luotettava organisaatio kertoo itse aina kun voi. Informaatiotila täyttyy aina
- Viestinnässä korostuvat tapahtuman kuvaus ja selkeät ohjeet.
- Tukea hyökkäyksen uhreille on varauduttava antamaan pitkään.
- Muista kansainvälisen viestinnän mahdollinen tarve.
- Säännöllinen viestintä rakentaa luottamusta.



Konkreettisia viestinnän haasteita

- Kyberhäiriöitä on ”harmittavista” ”toiminnan lamauttaviin”
- Viestintävastuut, johtaminen, tiedonkulku
- Miten vastaamme tiedontarpeeseen ja huoleen?
- Miten viestimme mahdollisista uhkista ja riskeistä?
- Miten huolehdimme omasta jaksamisestamme pitkäkestoisessa tilanteessa?

Viestinnässä muista myös

- Valtionhallinnon viestintä kyberhäiriötilanteissa
- Kuntien viestintä kyberhäiriötilanteissa
- Pörssitiedottaminen
- Tutkinnan rajoitukset
- NIS2-direktiivi ja velvoitteet viestinnälle

Varautumisesta jälkihoitoon

TRAFICOM

Varautuminen

1

- Arvioikaa riskit: **Tunnistakaa mahdolliset kyberhäiriötilanteet**
- Luokaa konkreettiset toiminta- ja viestintäsuunnitelmat eri tilanteiden varalle.
- Vastuuhenkilöt: Määritelkää kriisiviestinnästä vastaavat henkilöt ja varahenkilöt, heidän roolinsa ja vastuunsa eri tilanteisiin.
- Tiedonkulku: Varmistakaa, että organisaation **valmius- ja varautumissuunnitelmissa** on huomioitu, että viestintä on mukana kaikissa ryhmissä, joissa tilanteita johdetaan ja käsitellään.
- **Yhteystiedot** tärkeistä sisäisistä ja ulkoisista tahoista ja henkilöistä, saatavilla myös, kun palvelut ovat alhaalla.
- **Harjoitukset**: Harjoitelkaa säännöllisesti.

Kriisin alkaessa

2

- **Tilannekuvan** arviointi: Selvittäkää, mitä on tapahtunut ja mikä on organisaation vastuu ja rooli tilanteessa. Varmistakaa, että saatte ajantasaisen tiedon tilanteesta ja sen selvittämisestä.
- **Tiimi:** Toimijoiden tunnistaminen: Mitkä organisaatiot ja asiantuntijat ovat mukana tilanteen hallinnassa ja johtamisessa?
- **Työvälineet:** Selvittäkää, mitkä työvälineet ovat käytössänne. Hyödyntäkää tarvittaessa varakanavia. Muistakaa viestinnällisen yhteistyön merkitys ja mahdollisuudet.
- **Tunnista** kohdeyleisöt.
- Valitkaa viestintäkanavat, joilla tavoitatte kohderyhmänne tehokkaimmin, esimerkiksi sosiaalinen media, verkkosivut tai lehdistötiedotteet. Tai jotka ovat saatavilla.
- Viestinnän rajoitukset: Selvittäkää, miten ja mitä voitte tilanteessa viestiä. Varmistakaa, ettei viestinnällä vaaranneta poliisin tutkintaa ja aiheuteta lisävahinkoja.

Viestinnän periaatteet

3

- Avoimuus: Olkaa rehellisiä ja läpinäkyviä.
- Välttäkää tietojen pimittämistä.
- Älkää spekuloiko tai vähätelkö tapahtunutta.
- Tunnistakaa tärkeimmät kohdeyleisönne eli oman henkilöstönne lisäksi kaikki, joiden henkilötiedot ovat saattaneet vaarantua.
- Johdonmukaisuus: Varmistakaa, yhtenäinen viesti. Näin vältytään ristiriitaisilta viesteiltä ja virheellisiltä ohjeistuksilta. Panostakaa viestinnän selkeyteen ja ymmärrettävyyteen.
- Muistakaa viestinnän säännöllisyys, jälkiviestintä ja kansainvälisen viestinnän tarve.
- Kuunnelkaa ja tukekaa: Tunnistakaa kriisin vaikutus ihmisiin ja osoittakaa myötätuntoa viestinnässä.

Kriisin hallinta

4

- Säännöllinen viestintä: Pitäkää kaikki, joita tilanne koskettaa, ajan tasalla. – Viestinnän loki!
- Tuottakaa selkeitä toimintaohjeita päivittyvän tilannekuvan perusteella.
- Jakakaa oikeita tietoja: Varmistakaa, että jaatte vain vahvistettuja ja tarkkoja tietoja.
- Älkää vähätelkö tapahtunutta älkääkä spekuloiko.
- Vastatkaa median, asiakkaiden ja yleisön kysymyksiin selkeästi, ymmärrettävästi ja rauhallisesti.
- Jos jokin asia ei ole vielä tiedossa, kannattaa esittää arvio ja milloin lisätietoa on mahdollisesti saatavilla.
- Palatkaa asiaan sovitusti.
- Välttäkää informaatiotyhjiön syntymistä: Huolehtikaa siitä, että tietoa on jatkuvasti ja oikea-aikaisesti saatavilla eri kohdeyleisöille.

Kriisin jälkihoito

5

- Arvioikaa tilanne: Käykää kriisi läpi organisaationne johdon ja asiantuntijoiden kanssa. Kerätkää palautetta organisaatioilta, kumppaneilta ja sidosryhmiltä, jotka ovat olleet mukana tilanteen hallinnassa.
- Raportoi ja jaa opit
- Tunnistakaa osa-alueet ja toimintatavat, joita tulisi kehittää ja parantaa tulevaisuudessa.
- Viekää opit ohjeistuksiin ja käytäntöön.
- Jälkiviestintä: Muistakaa jälkiviestinnän tarve. Mahdolliset uhrit voivat tarvita tietoa, tukea ja selkeitä toimintaohjeita myös kriisin akuutin vaiheen jälkeen.
- Rakenna luottamus takaisin pitkäjänteisesti

Lopuksi

- Kyberhäiriöissä viestinnän keskiössä on ihminen.
- Viestintä on osa kriisijohtamista.
- Valmistautuminen ratkaisee onnistumisen.
- Hyvä viestintä rakentaa luottamusta – huono syventää kriisiä.

Muista:
Varaudu!
Viesti!
Välitä!

Älä koskaan:
Valehtele!
Vähättele!
Viivyttele!

Lisätietoa:

- Kriisiviestintäohje kyberhyökkäyksiin löytyy Traficomin verkkosivuilta
- Kriisiviestinnän toimintaohjeet kybertilanteisiin löytyvät Kyberturvallisuuskeskuksen sivuilta
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/miten-viestimme-0

Lähteet

- Kyberturvallisuuden vuosi
- https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2025
- Digiturvabarometri 2025 / Digi- ja väestötietovirasto
- https://dvv.fi/-/digiturvabarometri-2025-suomalaiset-luottavat-viranomaisiin-mutta-digihuijaukset-ja-kyberuhat-huolestuttavat

Kyberturvallista päivän jatkoa!

LinkedIn:
https://www.linkedin.com/in/mariakellokumpu/