TRAFICOM
Liikenne- ja viestintävirasto

Miten viestiä kyberhyökkäyksistä?

Kriisiviestintäohje organisaatioille

Traficomin julkaisuja
11/2025

Miten viestiä kyberhyökkäyksistä?

Traficomin Kyberturvallisuuskeskuksen laatima ohje on tehty yhteistyössä Finanssivalvonnan, Keskusrikospoliisin, Kuntaliiton, Poliisihallituksen, Suojelupoliisin ja tietosuojavaltuutetun toimiston kanssa.

Ohjeen luonnosversioita ovat kommentoineet SOK:n mediajohtaja Päivi Anttikoski, CISO Ilja Ikonen Verkkokauppa.com Oyj:stä, viestintäjohtaja Katja Kannonlahti Tampereen kaupungilta, viestintäjohtaja Eriikka Koistinen sisäministeriöstä, viestintäjohtaja Marjo Loisa Terveyden ja hyvinvoinnin laitokselta, viestinnän johtamisen professori Vilma Luoma-aho Jyväskylän yliopiston Kauppakorkeakoulusta, viestintäjohtaja Pipsa Lotta Marjamäki Kelasta, viestintäjohtaja Marika Nöjd Tallink Silja Oy:stä valtioneuvoston apulaisviestintäjohtaja Jyri Rantala valtioneuvoston kansliasta, johtava erityisasiantuntija Kimmo Rousku Digi- ja väestötietovirastosta, viestintäjohtaja Päivyt Tallqvist Finnair Oyj:stä sekä yksikönpäällikkö Päivi Tampere Naton strategisen viestinnän osaamiskeskuksesta Riikasta (Nato StratCom COE).

Organisaatioista ohjeen luonnoksia ovat kommentoineet: Fiskars Oyj, Lähitapiola Oy, Rikosuhripäivystys, Telia Finland Oyj ja valtioneuvoston kanslia

Haluamme kiittää lämpimästi kaikkia asiantuntijoita ja organisaatioita kommenteista ja tuesta ohjeen tuottamiseen.

Lisätietoja: viestintäpäällikkö Jussi Toivanen, etunimi.sukunimi@traficom.fi, Liikenne- ja viestintävirasto Traficom

Johdanto

Yhteiskunnan digitalisoituessa olemme entistä riippuvaisempia toimintavarmoista ja tietoturvallisista palveluista arjessamme. Viime vuosien aikana valitettavasti entistä useampi organisaatio ja yksilö ovat joutuneet kyberhyökkäyksen ja sitä kautta tietovuodon tai -murron kohteeksi.

Liikenne- ja viestintävirasto Traficom ja Suojelupoliisi ovat todenneet yhdessä kyberturvallisuuden uhkatason nousseen Suomessa[1]. Syy tähän muutokseen on se, että suomalaisiin organisaatioihin kohdistuvat kyberhyökkäykset ovat aiempaa tarkemmin kohdennettuja ja räätälöityjä. Hyökkääjät valitsevat tietoisesti kohteensa ja suunnittelevat hyökkäysstrategiansa organisaatiokohtaisesti. Lisäksi he ovat valmiita jatkuvasti kokeilemaan uusia keinoja tunkeutumisyrityksissä, jos yksi lähestymistapa ei tuota tulosta.

Käytännön kokemus kyberhyökkäyksistä on osoittanut, että organisaatioiden on panostettava viestintään, eikä sen merkitystä ja roolia johtamisessa saa unohtaa. Viestinnän on oltava avointa, säännöllistä, kohdeyleisöjä huomioivaa ja proaktiivista.

Kyberhyökkäysten kohteena ja uhrina on ihminen, työntekijä, asiakas tai kumppani. Kyberhyökkäys aiheuttaa huolta, epätietoisuutta ja pelkoa. Rahansa tai arkaluontoiset tietonsa menettänyt ihminen voi kokea vakaviakin taloudellisia, sosiaalisia, psyykkisiä ja terveydellisiä seurauksia. Sen vuoksi kybertilanteiden johtamisessa ja viestinnässä on tärkeä pitää ihminen keskiössä. Ihmistä ei saa unohtaa teknisten asioiden, kuten palvelimien, VPN-yhteyksien ja reitittimien sekä bittien ja bottien taakse.

Kyberhyökkäyksien viestintään liittyy erityispiirteitä, jotka on hyvä tuntea. Erityisen viestinnällisen haasteen asettaa se, että tilannekuva ja -ymmärrys usein muuttuvat selvitystyön edetessä. Yritys tai organisaatio joutuu siis usein viestimään vajavaisilla tai muuttuvilla tiedoilla, joskus hyvin pitkäkestoisesti. Kaikissa tilanteissa tärkeimmät yleisöt ovat ne ihmiset, joiden henkilötiedot ovat saattaneet vaarantua ja oma henkilöstö. Henkilötietoihin kohdistuneista tietoturvaloukkauksista täytyy myös muistaa viestiä loukkauksen kohteeksi joutuneille henkilöille tietosuojalainsäädännön edellyttämällä tavalla.

[1] Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut | Traficom

Tässä ohjeessa kerromme erilaisista kyberhyökkäyksistä sekä rikollisten käyttämistä menetelmistä ja keinoista. Lisäksi annamme vinkkejä viestinnällisen varautumiseen sekä viestintään kyberhyökkäyksen aikana ja sen jälkeen.

Ohje on suunnattu organisaatioiden johdolle, turvallisuuden ja viestinnän asiantuntijoille sekä tilannekuvasta ja varautumisesta vastaaville asiantuntijoille. Kybertilanteiden johtamisessa, hallinnassa ja viestinnässä on tärkeää, että tieto tapahtuneesta ja suunnitelluista ja toteutetuista toimenpiteistä kulkee saumattomasti johtamisen, viestinnän ja tilannekuvatoiminnon välillä.

2 Kyberrikollisuus ja -vaikuttamisen keinot

Kyberrikollisuus on rikollista toimintaa, joka tapahtuu digitaalisten järjestelmien ja verkkojen kautta. Se voi sisältää monenlaisia rikoksia, kuten identiteettivarkauksia, tietomurtoja, tietosuojarikoksia, tietojenkalastelua (phishing), haittaohjelmien levittämistä, kiristysohjelmia Kyberrikollisuus on kansainvälistä ja kaupallista toimintaa. Siihen kannustaa mahdollisuus merkittävään taloudelliseen hyötyyn ja toisaalta pieni kiinnijäämisen riski. Rikollisuuden mittaluokkaa kuvastaa hyvin se, että jos vertailtaisiin maailmanlaajuisesti rikollisten saamaa rahahyötyä vuosittain valtioiden kansantalouksiin, kyseessä olisi maailman kolmanneksi suurin kansantalous Yhdysvaltain ja Kiinan jälkeen. Kyberhyökkäysten tekemiseksi ei tarvitse hallita tekniikkaa tai teknologioita, vaan hyökkäyksen voi tilata rikollisilta kaupallisesti avaimet käteen -palveluna netistä (Crime-as-a-Service).

Kyberhyökkäysten seuraukset voivat olla vakavia yksilöille, organisaatioille ja valtioille. Ne voivat aiheuttaa taloudellisia menetyksiä, mainehaittoja ja jopa uhkia kansalliselle turvallisuudelle. Ne voivat myös rapauttaa luottamusta instituutioihin ja yhteiskunnan toimivuuteen.

Kyberhyökkäyksissä ja -vaikuttamisessa huomio kiinnittyy helposti toiminnan teknisiin puoliin. On kuitenkin hyvä huomata, että kyse on ennen kaikkea sosiaalisesta ja psykologisesta vaikuttamisesta ja toiminnasta. Keinoista, jotka yhdistävät kybervaikuttamisen myös informaatiovaikuttamiseen.

Kyberrikolliset ja muut pahantahtoiset toimijat kohdistavat vaikuttamispyrkimyksensä meihin yksilöihin. Rikolliset hyödyntävät toiminnassa meidän inhimillisiä heikkouksiamme, kuten tarvetta tulla pidetyksi tai toimia nopeasti kiireessä ja välttää virheitä. Käytännössä tällainen toiminta näkyy esimerkiksi siinä, että verkkorikolliset yrittävät saada meidät antamaan tietomme tai avaamaan haittaohjelman sisältävän liitetiedoston sähköpostissamme vetoamalla kiireeseen. "Et ole maksanut laskuamme, joten sinun pitää toimia nyt, ettet joudu ulosottoon. Klikkaa oheista linkkiä ja suorita maksu heti". Kiirehtivän, tai jopa painostavan sävyn ohella viesti voi olla houkutteleva, ”Olet maksanut laskun kahteen kertaan, palautamme sinulle rahaa” -tyylisesti.

Keinoina rikollisilla ja pahantahtoisilla toimijoilla ovat myös kiristys ja uhkailu. "Jos et toimi tietyllä tavalla, julkaisemme sinusta tai yrityksestäsi meillä hallussa olevia arkaluonteisia tietoja". Toiminnan ja vaikuttamisen

tarkoituksena on se, että kohteena oleva henkilö toimii omaa tai edustamansa organisaation etua vastaan.

Kyberhyökkäyksiä voidaan käyttää informaatiovaikuttamisen keinoina. Toiminnalla voidaan pyrkiä aiheuttamaan epävarmuutta yhteiskunnassa tai rapauttamaan suuren yleisön luottamusta organisaatioihin ja laajemminkin digitaaliseen yhteiskuntaan. Keinoina kyberhyökkäykset ovat näyttäviä ja niillä voi saada helposti julkisuutta. Toiminnan taustalla oleva motiivi ratkaisee sen, onko kyse kiusan- ja vahingonteosta, taloudellisen hyödyn tavoittelusta vai informaatiovaikuttamisena pidettävästä toiminnasta. Tätä toiminnan taustalla olevaa motiivia tai tavoitetta voi olla vaikea päätellä ja arvioida. Informaatiovaikuttamisen näkökulmasta on kuitenkin tärkeä huomata, että joka tapauksessa kyberhyökkäyksen tultua julkiseksi, sillä on vaikutuksia informaatioympäristöön.

Informaatiovaikuttamisen keinoja voidaan käyttää kyberhyökkäysten tukena esimerkiksi huomion kiinnittämiseksi toisaalle, toimijan piilottamiseksi tai lavastamiseksi. Nykyisessä digitaalisessa yhteiskunnassa kyber- ja informaatiovaikuttaminen ovat tiiviisti yhteydessä toisiinsa ja tukevat toisiaan. Jos kyberhyökkäyksissä on onnistuneesti vaikutettu esimerkiksi ihmisten tuntemaan luottamukseen organisaatiota tai laajemmin yhteiskuntaa kohtaan, palautuminen entiseen voi olla vaikeampaa.

Tietoturvassa on tärkeää huomioida kyberkeinojen käyttäminen informaatio-operaatioiden osana. Teknologinen kehitys, kuten deepfake-teknologiat (syväväärennös), tarjoavat entistä vaikuttavampia, tehokkaampia ja räätälöitävämpiä keinoja sosiaaliselle manipuloinnille. Valheet voidaan naamioida entistä uskottavimmiksi ja vaikeammin tunnistettavaksi. Rikolliset ja muut pahantahtoiset toimijat voivat esimerkiksi hyödyntää tekoälysovelluksia luodakseen virtuaalisia kopioita henkilöistä, jotka työskentelevät organisaatioiden johtotehtävissä. Tällöin videolla esiintyvät kopiot näyttävät ja kuulostavat oikeilta henkilöiltä, mutta tekevät ja sanovat asioita, joita nämä henkilöt eivät ole koskaan tehneet tai eivät tekisi.

Videon tai äänitallenteen nähnyt tai kuullut henkilö ei välttämättä tunnista, että kyseessä on väärennös, joka on luotu deepfake-teknologialla, vaan uskoo sen olevan totta. Maailmalla on jo raportoitu tapauksista, joissa reaaliaikaisia videopuheluja on onnistuttu väärennöksillä huijaamaan. Tämä ei ole science fictionia, vaan arkipäivää ja todellisuutta, johon organisaatioissa on varauduttava. Teknologisen suorituskyvyn vuosittainen merkittävä parantuminen mahdollistaa näiden väärennösten laadun merkittävän parantumisen ja tarvittavan tekniikan osalta hintatason laskun.

Kyberhyökkäykset ovat myös yksi hybridivaikuttamisen ja vakoilun keinoista. Hybridivaikuttamisella tarkoitetaan vieraan valtion vihamielistä, suunnitelmallista ja jatkuvaa toiseen valtioon kohdistuvaa toimintaa, jossa käytetään hyväksi kohteena olevan maan heikkouksia. Hybridivaikuttamisen tavoitteena on muun muassa yhteiskunnan toiminta- ja päätöksentekokyvyn heikentäminen. Tällaisessa toiminnassa käytetään poliittisia, diplomaattisia, taloudellisia ja sotilaallisia keinoja, mutta myös kyber- ja informaatiovaikuttamista ja vakoilua.

Arjessa vaikuttamistoiminta näkyy esimeriksi erilaisina häiriöinä yhteiskunnan toiminnassa, kyberhyökkäyksinä tai disinformaation levittämisenä. Vaikuttamistoiminnan onnistuminen näkyy yhteiskunnallisen vastakkainasettelun ja pelkojen lisääntymisenä sekä luottamuksen murentumisena yhteiskuntaan. Tässä yhteydessä on hyvä muistuttaa, että suurin osa kyberhyökkäyksistä on edelleen rikollisten taloudellisen hyödyn tavoittelua, eli toimintaa, jolla ei ole mitään yhteyttä valtiolliseen hybridivaikuttamiseen tai vakoiluun.

1 Kybermaailman ilmiöt

Digitaalinen yhteiskuntamme on riippuvainen erilaisista sähköisistä palveluista ja tietojärjestelmistä. Tämän vuoksi niihin kohdistuvat häiriöt vaikuttavat merkittävästi meidän jokaisen arkeen, organisaatioiden ja laajemminkin yhteiskunnan toimintaan. Digitaalisessa yhteiskunnassa myös salassa pidettävää tietoa säilytetään laajasti digitaalisissa tietojärjestelmissä, jotka ovat sen vuoksi kiinnostavia kohteita kybervakoilulle.

Kyberhäiriöt ovat tilanteita, joissa organisaatioiden digitaaliset palvelut tai järjestelmät eivät toimi normaalisti esimerkiksi teknisen vian takia.

Kyberhyökkäys on vahingonteko tai häirintää, joka voi kohdistua esimerkiksi tietoverkkoihin, järjestelmiin, laitteisiin tai digitaalisesti tallennettuihin tietoihin eli dataan. Myös tietojen kalasteleminen suoraan ihmisiltä on kyberhyökkäys. Tässä osiossa esittelemme tarkemmin erilaisia kybermaailman ilmiöitä ja rikollisten keinoja, joiden avulla he pyrkivät toteuttamaan hyökkäyksiään organisaatioita vastaan. Ilmiöiden ja toimintamallien tuntemus on tärkeää vastatoimien ja myös viestinnän suunnittelussa ja toteuttamisessa.

Rikollisilla, vakoilijoilla ja muilla pahantahtoisilla toimijoilla on käytettävissään erilaisia kyberhyökkäystaktiikoita. Hyökkäykset voivat vaihdella yksinkertaisista palvelunestohyökkäyksistä, jotka häiritsevät organisaation verkkosivujen tai palvelujen toimintaa, aina vakavampiin muotoihin, kuten tietomurtoihin, joissa varastetaan, mahdollisesti myös vuodetaan julkisuuteen tai vahingoitetaan arkaluonteista tietoa.

Myös **kiristyshaittaohjelmat** ovat yleisiä. Ne voivat lukita organisaation tietojärjestelmät tai estää pääsyn kriittisiin tietoihin vaatimalla lunnaita. Tällaiset hyökkäykset voivat aiheuttaa merkittäviä taloudellisia ja mainehaittoja organisaatioille ja yksilöille.

Kyberhyökkäyksillä on **taloudellisten vaikutusten** lisäksi myös aina **inhimillisiä ja psykososiaalisia vaikutuksia**. Esimerkiksi tietomurron kohteeksi joutuneen organisaation työntekijä saattaa kokea pelkoa ja ahdistusta, koska hän ei välttämättä tiedä, mitä tietoja on varastettu ja miten niitä voidaan käyttää häntä vastaan. Tietomurroissa on aina kysymys myös tunkeutumisesta organisaation työntekijöiden ja asiakkaiden yksityisyyteen. Tiedontarve eri kohderyhmissä kyberhyökkäysten jälkeen on suurta.

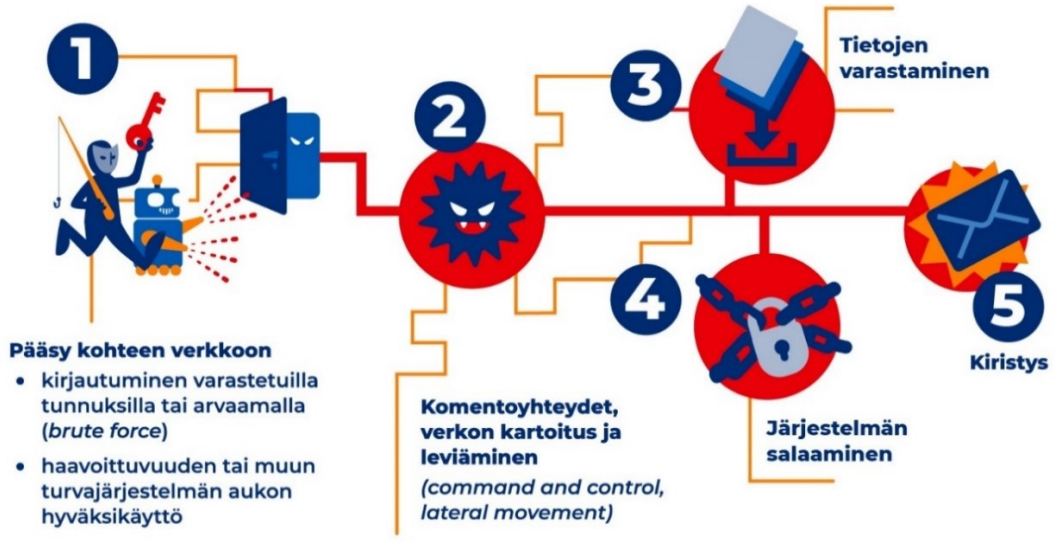
1.1 Kiristyshaittaohjelmat

1.1.1 Mistä kysymys?

Kiristyshaittaohjelma on ohjelma, joka estää laitteen tai palvelun normaalin käytön ja esittää vaatimuksen lunnaiden maksamisesta rikollisille. Haittaohjelmatyypistä käytetään myös nimitystä lunnastroijalainen. Kiristyshaittaohjelma (engl. ransomware) tyypillisesti salaa laitteella olevat tiedostot salausalgoritmilla ja avaimella, joka on vain hyökkääjän tiedossa. Usein hyökkääjä pyrkii myös varastamaan uhrin tietoja.

Tiedostojen salauksen tai näytön lukitsemisen jälkeen rikollisen käyttämä haittaohjelma jättää uhrille yleensä viestin, jossa se kertoo palauttavansa laitteen omistajansa käyttöön lunnasmaksua vastaan. Lunnaita vaaditaan maksettavaksi usein kryptovaluutassa, mikä tekee maksun jäljittämisestä vaikeampaa kuin perinteisillä valuutoilla tehtyjen maksujen. Kiristyshaittaohjelma yhä useammin on vain toinen puoli hyökkäyksestä. Toinen puoli taas on tietojen varastaminen ja niiden vuotamisella uhkailu lunnaiden toivossa.

Rikolliset levittävät kiristyshaittaohjelmia sekä satunnaisiin kohteisiin – esimerkiksi sähköpostin välityksellä – että kohdennettujen tietomurtojen avulla. Tyypillisimpiä levityskeinoja ovat sähköpostissa olevat linkit ja liitetiedostot, väärennetyt ladattavat tiedostot kuten maksullisten ohjelmistojen piraattikopiot, sekä tunnettujen ohjelmistohaavoittuvuuksien hyväksikäyttö.



Kuva 1. Kiristyshaittaohjelmasta (eng. ransomware) käytetään myös nimitystä lunnastroijalainen.

1.1.2 Millaiset vaikutukset organisaatioille?

Kiristyshaittaohjelmahyökkäyksen voi havaita esimerkiksi kiristysviestin, tietoturvatuotteen hälytyksen tai sen myötä, että pääsy tiedostoihin estyy. Tärkeimmät onnistuneen hyökkäyksen seuraukset liittyvät siihen, että käyttäjät eivät pääse enää käsiksi tartunnan saaneessa laitteessa oleviin tietoihin. Jos tiedoista ei ole varmuuskopiota, saattavat tiedot olla lopullisesti mennyttä.

Yrityksille kiristyshaittaohjelmahyökkäyksen taloudelliset vaikutukset voivat olla merkittävät. Yritys voi menettää suuria summia rahaa liiketoiminnan keskeytyessä ja korjaustoimenpiteissä. Jo pelkästään satunnaisesti levitettävän haittaohjelman tarttuminen voi aiheuttaa merkittävän katkoksen yrityksen toimintaan, sillä tilanteen alkuvaiheessa on harvoin selvää, miten laajasta ongelmasta on kyse, kun yhdessä laitteessa havaitaan kiristyshaittaohjelma.

Kiristyshaittaohjelmatoimijoiden vaatimia lunnaita ei tule maksaa. Lunnaiden maksaminen edistää rikollisen toiminnan jatkumista, eikä tietojen palautumisesta tai kiristyksen päättymisestä ole mitään takeita.

1.1.3 Viestinnässä huomioitavaa

Kiristyshaittaohjelmalla toteutetulla kyberhyökkäyksellä on vakavia vaikutuksia organisaation johtamiseen, päivittäiseen toimintaan ja viestintään. Tilanteessa on mahdollista, että tiedonkulkuun ja viestintään sekä toiminnanohjaamiseen ja johtamiseen liittyvien kanavien käyttöä joudutaan rajoittamaan merkittävästi tai kieltämään niiden käyttö kokonaan. Luotettava tiedonkulku ja organisaation sisäinen ja mahdollisesti myös ulkoinen viestintä joudutaan siten siirtämään vaihtoehtoisiin kanaviin.

Kiristyshaittaohjelmalla toteutetun hyökkäyksen vaikutusten todellisen laajuuden selvittämisessä voi kestää. On mahdollista, että hyökkääjä on saanut haltuunsa myös organisaation toiminnan kannalta arkaluonteisia tietoja, kuten työntekijöiden henkilötietoja ja liiketoiminnan kannalta salassa pidettäviä asiakastietoja.

Tilanteen alkuvaiheen viestinnässä kannattaa varautua heti jo pahimpaan vaihtoehtoon, eli tilanteeseen, jossa organisaation hallussa olevia arkaluonteisia tietoja (asiakastiedot, yrityssalaisuudet, sopimukset ja tiedot työntekijöistä) on vuotanut rikollisille. Jos ihmisten henkilötietoja on vuotanut, organisaation tulee muistaa myös yleisen tietosuoja-asetuksen velvoitteet, joista on kerrottu tiiviisti tämän oppaan luvun 2.2.6. kohdassa Tietosuojavelvoitteet.

Vaikka tilanne on epäselvä, todennäköisesti pitkäänkin, organisaatio ei voi olla viestimättä tapahtuneesta. Viestinnän tulee olla oikea-aikaista ja lainsäädännönmukaista ja avointa sekä eri kohdeyleisöjen oikeudet ja tarpeet täyttävää. Listayhtiön eli yhtiön, jonka arvopaperi on kaupankäynnin kohteena, on otettava viestinnän aikataulutuksessa huomioon esimerkiksi mahdollinen markkinoihin vaikuttava sisäpiiritiedon syntyminen ja julkistettava se sääntelyn edellyttämällä tavalla. Kyse on organisaation toiminnan ja tulevaisuuden kannalta ratkaisevan luottamuksen lunastamisesta ja/tai palauttamisesta.

Organisaation on varauduttava myös siihen, että rikolliset voivat aktivoitua milloin tahansa omassa viestinnässään, esimerkiksi julkaisemalla tietoa hyökkäyksestä tai varastamiaan tietoja omissa kanavissaan. He voivat myös ottaa yhteyttä suoraan organisaation asiakkaisiin tai työntekijöihin ja yrittää kiristää heitä hyödyntäen saatuja tietoja. On aina parempi, jos hyökkäyksen kohteena oleva organisaatio saa itse ensin viestittyä asiasta keskeisimmille kohderyhmille. Avoin ja läpinäkyvä viestintä sekä selkeiden toimintaohjeiden antaminen henkilökunnalle, asiakkaille ja muille sidosryhmille tilanteen kehittymisestä on ratkaisevan tärkeää.

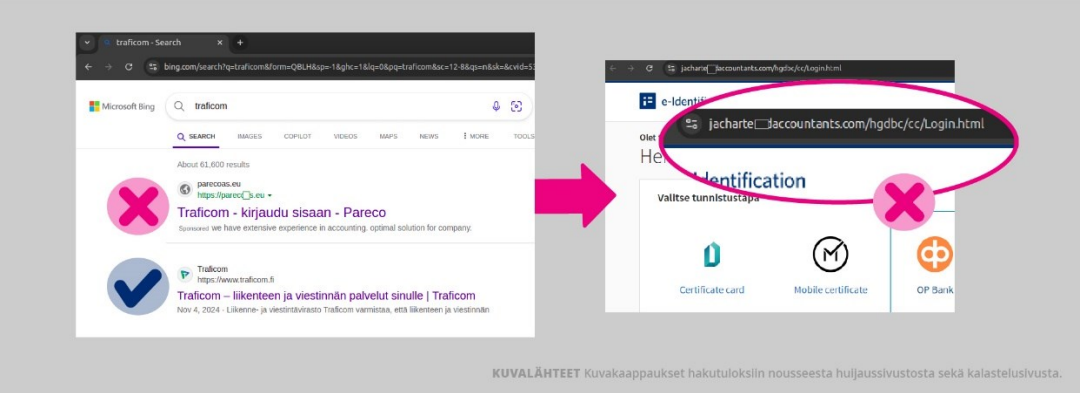
Mikäli organisaatiolla on toimipisteitä ja toimintaa Suomen ulkopuolella, viestinnän ja ohjeistuksen on tavoitettava myös kansainväliset asiakkaat ja työntekijät. Ohjeistuksissa on huomioitavat kunkin maan paikalliset säännökset ja viranomaisten ohjeet.

1.2 Tietojenkalastelu

1.2.1 Mistä kysymys?

Tietojenkalastelulla rikolliset yrittävät saada haltuunsa esimerkiksi ihmisten henkilötietoja, pankkitunnuksia tai maksukorttien tietoja. Myös erilaisissa sähköisissä palveluissa käytettävät käyttäjätunnukset ja salasanat kiinnostavat rikollisia ja vakoojia. Rikollisia kiinnostaa kaikki se tieto, josta on mahdollista saada taloudellista hyötyä ja vakoojia tieto, jota toinen valtio voi hyödyntää omaksi edukseen.

Tietojenkalastelukampanjoissa on hyödynnetty tunnettujen brändien ja organisaatioiden logoja sekä valheellisesti esiinnytty organisaation työntekijänä tai johtavana henkilönä osana huijausta. Rikolliset pyrkivät usein kiirehtimään asiaa, vetoamaan tunteisiin ja saamaan huijauksen kohteen ohittamaan tavalliset prosessit. Lisäksi rikolliset käyttävät myös hakukoneiden maksullisia ja optimoituja hakutuloksia hyväkseen levittääkseen linkkejään.



Kuva 2. Tietojenkalastelussa rikolliset kaappaavat tunnettujen ja luotettujen organisaatioiden logot tai brändit huijaustensa välikappaleiksi. Rikolliset hyödyntävät myös maksettuja hakutuloksia linkkien levittämisessä.

1.2.2 Millaiset vaikutukset organisaatioille?

Tietojenkalastelussa rikolliset kaappaavat tunnettujen ja luotettujen organisaatioiden logot tai brändit huijaustensa välikappaleiksi. Keinoina ovat esimerkiksi sähköpostitse tai tekstiviesteillä suurelle yleisölle lähetetyt huijausviestit, joissa hyödynnetään organisaation omassa viestinnässä käytettäviä viestipohjia, tuotemerkkejä ja logoja. Organisaation kannalta tällainen toiminta muodostaa maineriskin, vaikka organisaatio ei ole millään tavalla mukana rikollisessa toiminnassa. Rikollisten toiminta voi vaikuttaa suuren yleisön organisaatiota kohtaan tuntemaan luottamukseen ja oman viestinnän uskottavuuteen.

On hyvä nostaa esiin, että tässä ohjeessa tietojenkalastelua tarkastellaan brändin väärinkäytön näkökulmasta. Tärkeä on kuitenkin muistaa, että organisaation omat työntekijät voivat olla mahdollisia kohteita tällaiselle toiminnalle. Tietojenkalastelu voi olla kiristyshaittaohjelmahyökkäyksen ensimmäinen askel.

Kuva 3. Tietojenkalastelulla varastetut tunnukset ovat yksi yleisimmistä tavoista tunkeutua organisaation järjestelmiin. Monivaiheinen tunnistautuminen hankaloittaa tunkeutujan sisäänpääsyä.

1.2.3 Viestinnässä huomioitavaa

Tietojenkalastelu organisaation nimissä on ilmiö, josta voi ja kannattaa viestiä ennakoiden. Kalastelun mahdollisuudesta kannattaa kertoa verkossa asioiville asiakkaille esimerkiksi bannerilla yrityksen nettisivuilla tai viestimällä huijausviesteistä yrityksen omilla sosiaalisen median kanavilla. Jos organisaatio on usein huijausviestien kohteena, viestiä kannattaa toistaa säännöllisesti. Samoin organisaatio voi ylläpitää sivustoa yleisimmistä sen nimissä toteutetuista huijauksista esimerkkeinä. Huijauksia tehtaillaan koko ajan uusilla osoitteilla ja profiileilla, joten siksi yleisen tietoisuuden nostaminen on tärkeä torjuntakeino.

Lisäksi organisaation on valmistauduttava reagoimaan nopeasti huijausviesteihin, joita levitetään sen tai sen johtohenkilöiden/työntekijöiden nimissä.

Nopea reagointi ja tietoisuuden lisääminen auttavat estämään mahdollisimman monen ihmisen joutumisen huijatuksi ja rikoksen uhriksi. Organisaation kannalta kyse on myös luotettavuudesta ja maineesta. Vaikka organisaatio ei itse olisi syyllistynyt rikokseen, sen logon esiintyminen rikollisessa toiminnan yhteydessä voi heikentää ihmisten luottamusta siihen. Organisaation nimissä levitetyt huijausviestit ovat rikoksia, joiden kohteena organisaatio on.

1.3 Palvelunestohyökkäykset

1.3.1 Mistä kysymys?

Palvelunestohyökkäyksissä verkkosivuille tai -palveluihin ohjataan suuria määriä liikennettä.

Tämä näkyy käyttäjälle siten, että verkkosivuille ei pääse tai niiden käyttäminen on erittäin hidasta. Palvelunestohyökkäykset ovat helposti toteutettava ja näyttävä hyökkäystekniikka. Ne saavatkin usein huomiota myös mediassa. Yleensä palvelunestohyökkäyksistä ei aiheudu käyttäjille näkyviä vaikutuksia ja pahimmillaankin ne johtavat lähinnä julkisten verkkopalveluiden lyhyisiin käyttökatkoksiin.

Nykyisin palvelunestohyökkäykset ovat erityisen yleisiä haktivismin muotona. Haktivismi on kyberrikollisuutta, jossa taloudellisen hyödyn sijaan motiivit ovat poliittisia. Palvelunestohyökkäyksillä osoitetaan tyytymättömyyttä kohteen poliittiseen päätökseen tai muuhun toimintaan, ja pyritään vaikuttamaan informaatioympäristöön tapauksen ympärillä. Lisäksi lyhyetkin käyttökatkokset voivat kasvattaa epäluottamusta kohteena olevan tahon asiakkaissa ja sidosryhmissä sekä herättää huolta siitä, ovatko heidän henkilökohtaiset tietonsa turvassa.

1.3.2 Millaiset vaikutukset organisaatioille?

Palvelunestohyökkäys on keinona näyttävä, sillä saavuttamattomissa oleva sivusto on käyttäjälle hyvin konkreettinen asia ja saattaa aiheuttaa harmia, jos palvelu ei ole käytettävissä. Lisäksi sähköiseen palveluun tai esimerkiksi verkkokaupan nettisivuille kohdistuvat hyökkäykset saattavat herättää ihmisissä huolta siitä, ovatko heidän tietonsa turvassa. On hyvä kuitenkin muistuttaa, että häiriöt palveluissa jäävät usein lyhytaikaisiksi. Todellisia ja pitkäkestoisia vahinkoja niillä onnistutaan käytännössä aiheuttamaan hyvin harvoin. Myös ihmisten tiedot vaarantuvat näissä hyökkäyksissä äärimmäisen harvoin. Kyse on enemmän ns. näyteikkunan töhrimisestä (digitaalinen graffiti), eli verkkosivuston tai palvelun kaatamisesta.

1.3.3 Viestinnässä huomioitavaa

Saavuttamattomaksi jäävä palvelu tai sivusto hankaloittaa asiakkaiden arkea ja aiheuttaa turhautumista, epävarmuutta ja huolta. Viestinnässä on tärkeää olla aktiivinen ja nopea. Viestinnässä kerrotaan, mistä palvelunestohyökkäyksissä on kysymys, mitä niiden taustalla on ja kuinka ne ovat vaikuttaneet organisaation toimintaan. Lisäksi on tärkeä kertoa, mitä toimenpiteitä on toteutettu tilanteen palauttamiseksi normaaliksi ja miten kauan palvelut ovat mahdollisesti poissa käytöstä ja onko

vaihtoehtoisia asiointitapoja. On myös tärkeää kertoa, kun palvelunestohyökkäys on ohi ja palvelut jälleen toiminnassa.

Mikäli organisaation verkkosivut ja palvelut ovat kaatuneet palvelunestohyökkäyksen takia, kannattaa seurata tarkasti, ryhtyykö joku taho levittämään organisaation nimissä ja tunnuksilla erilaisia huijaus- ja kalasteluviestejä. Mikäli organisaation kanavat ja keinot viestiä suurelle yleisölle ovat palvelunestohyökkäyksen vuoksi rajoittuneet, opportunistinen rikollinen voi yrittää hyödyntää tätä "informaatiotyhjiötä" edukseen kaappaamalla organisaation viestinnän osittain tai kokonaan.

Tilannetta voidaan myös hyödyntää informaatiovaikuttamisen keinona, eli pyrittäessä rapauttamaan ihmisten luottamusta organisaatioon tai laajemmin digitaaliseen yhteiskuntaan.

Listayhtiön eli yhtiön, jonka arvopaperi on kaupankäynnin kohteena, on otettava viestinnän aikataulutuksessa huomioon esimerkiksi mahdollinen markkinoihin vaikuttava sisäpiiritiedon syntyminen ja julkistettava se sääntelyn edellyttämällä tavalla.

1.4 Kybervakoilu

1.4.1 Mistä kysymys?

Kohdistetut kyberhyökkäykset voivat olla myös valtiollisten toimijoiden tai niiden lukuun toimivien tahojen suorittamia kybervakoiluoperaatioita. Niiden tavoitteena on tyypillisesti hankkia tietoa esimerkiksi toisen valtion päätöksenteosta tai yrityksen tuotekehityksestä. Tiedonhankinnan lisäksi kybervakoilu voi sisältää vaikuttamista ja jopa tietojärjestelmien tuhoamista tai muuta vahingontekoa.

Vakoilua harjoittavalle valtiolle kybervakoilu on tehokas ja suhteellisen vähäriskinen keino hankkia merkittäviä määriä luottamukselliseksi tarkoitettua tietoa. Kybervakoilun kohde ei välttämättä itse huomaa joutuneensa vakoilun kohteeksi.

Vakoilua harjoittava valtio voi toteuttaa kybervakoiluoperaation esimerkiksi tunkeutumalla tietojärjestelmiin teknisen haavoittuvuuden kautta. Se voi myös velvoittaa omassa vaikutuspiirissään olevia laite- tai ohjelmistotoimittajia hankkimaan niiden ulkomaisten asiakkaiden dataa. Myös kybervakoilussa pääsy voidaan hankkia taitavasti kohdennetun kalasteluviestin tai muun yksittäiseen henkilöön kohdistetun toimenpiteen avulla. Lopullisena tavoitteena on päästä käsiksi luottamukselliseksi tarkoitettuun tietoon.

Jokainen merkittävässä tehtävässä työskentelevä tai merkittävää tietoa käsittelevä työntekijä voi olla vieraan valtion tiedustelun kohde.

1.4.2 Millaiset vaikutukset organisaatioille?

Kybervakoilun vaikutukset ulottuvat pahimmillaan yhtä organisaatiota laajemmalle, jos Suomen kansallisen turvallisuuden kannalta merkittävää tietoa vuotaa vihamieliselle valtiolle. Usein tilanteen alkaessa ei ole selvää, miten laajalle kybervakoiluoperaatio on onnistunut tunkeutumaan ja mitä tietoa on mahdollisesti menetetty. Kun epäillään valtiollista kybervakoilua, viranomaiset auttavat selvittämään ja rajaamaan vahinkoja. On tärkeää olla välittömästi yhteydessä viranomaisiin (Suojelupoliisiin, poliisiin tai Traficomin Kyberturvallisuuskeskukseen), jos organisaatiosi käsittelee Suomea vastaan toimivia vieraita valtioita kiinnostavaa tietoa ja syntyy epäilys kyberhyökkäyksestä.

1.4.3 Viestinnässä huomioitavaa

Kybervakoilu on sekä rikos, josta poliisi voi käynnistää esitutkinnan, että Suomen kansainvälisiin suhteisiin vaikuttava tapahtuma. Niinpä viestinnässä joudutaan usein ottamaan huomioon myös tapahtuman ulkopoliittiset vaikutukset. Rikostutkinnassa syyllisyyden ratkaisee tuomioistuin, kybervakoilun attribuutiosta eli tekijän mahdollisesta virallisesta nimeämisestä päättää viime kädessä viranomaisten selvitysten perusteella ulko- ja turvallisuuspoliittinen johto.

Organisaation on kuitenkin viestittävä omalle henkilöstölleen sekä tapauksesta riippuen myös ulkoisille sidosryhmilleen tapahtuneesta, mutta tässä viestinnässä kannattaa keskittyä tapauksen konkreettisiin vaikutuksiin ja toimenpiteisiin vahinkojen rajaamiseksi. Tarvittaessa organisaation johto tai viestintä voi keskustella asiaa selvittävien viranomaisten kanssa ja sopia yhteisistä viestinnän toimintatavoista.

1.5 Tietomurto ja tietovuoto

1.5.1 Mistä kysymys?

Tietomurto tarkoittaa luvatonta tietojärjestelmään, palveluun tai laitteeseen tunkeutumista tai sovelluksen, kuten esimerkiksi sähköpostitilin luvatonta käyttöä haltuun saatujen tunnusten avulla. Tietomurtoja tehdään myös tunkeutumalla eri tavoilla turvajärjestelmien ohi, esimerkiksi haavoittuvuuksia hyväksikäyttämällä. Tietomurto on rikoslaissa määritelty rangaistava teko ja myös tietomurron yritys on rangaistava.

1.5.2 Millaiset vaikutukset organisaatioille?

Tietomurrosta voi seurata organisaatiolle esimerkiksi taloudellisia vahinkoja, katkoksia toiminnassa sekä mainehaittaa. Anastettuja tietoja voidaan esimerkiksi julkaista luvattomasti tai niiden haltija voi kiristää uhria vaatimalla lunnaita. Mikäli tietomurrossa on onnistuttu varastamaan organisaation työntekijöiden tai asiakkaiden henkilötietoja, niitä voidaan käyttää esimerkiksi identiteettivarkauksissa, kiristämisessä tai häirinnän keinona.

Tietomurto voi johtaa tietovuotoon, jos murtautuja pääsee käsiksi tietojärjestelmässä olevaan arkaluonteiseen tietoon. Tietovuodossa hyökkääjä voi saada käsiinsä henkilötietoja, laskutustietoja, tilitietoja, maksukortteja, yrityssalaisuuksia, erityisiin henkilötietoryhmiin kuuluvia arkaluonteisia tietoja asiakkaista tai yksittäisistä työntekijöistä tai muuta salassa pidettävää tai rahan arvoista tietoa. Henkilötietoihin kohdistuneesta tietovuodosta on tehtävä ilmoitus tietosuojavaltuutetun toimistolle, kun yleisessä tietosuoja-asetuksessa määritelty ilmoituskynnys ylittyy.

Tekijän motiivina voi olla esimerkiksi haitanteko, kiristäminen tai jopa valtiollisen toimijan vakoilu. Tietomurtoja tekevät rikolliset, valtiolliset toimijat tai jopa yksittäiset ihmiset.

1.5.3 Viestinnässä huomioitavaa

Tietomurrolla on vakavia vaikutuksia organisaation johtamiseen, päivittäiseen toimintaa, tiedonkulkuun ja viestintään. Tilanteessa on mahdollista, että osa tiedonkulkuun ja viestintään sekä toiminnanohjaamiseen ja johtamiseen liittyvien kanavien käyttöä joudutaan rajoittamaan merkittävästi tai kieltämään niiden käyttö kokonaan. Luotettava tiedonkulku ja organisaation sisäinen ja mahdollisesti myös ulkoinen viestintä joudutaan siten siirtämään vaihtoehtoisiin kanaviin.

Tietomurtotapauksessa tapahtuman todellisen laajuuden ja vaikutusten selvittämisessä voi kestää. Organisaation on kuitenkin viestittävä nopeasti,

oikea-aikaisesti, avoimesti ja mahdollisille uhreille tapahtuneesta. Listayhtiön eli yhtiön, jonka arvopaperi on kaupankäynnin kohteena, on otettava viestinnän aikataulutuksessa huomioon esimerkiksi mahdollinen markkinoihin vaikuttava sisäpiiritiedon syntyminen ja julkistettava se sääntelyn edellyttämällä tavalla. Kyse on organisaation toiminnan ja tulevaisuuden kannalta ratkaisevan luottamuksen lunastamisesta tai palauttamisesta.

Viestinnässä kannattaa varautua pahimpaan vaihtoehtoon, eli tilanteeseen, että kaikki tai osa organisaation hallussa olevista tiedoista (asiakas- ja henkilötiedot ja tiedot työntekijöistä) ovat vuotaneet rikollisille.

Mikäli ihmisten henkilötietoja on kyberhyökkäyksen vuoksi päätynyt hyökkääjälle, on tärkeä muistaa, että uhrien näkökulmasta tietovuodosta aiheutuva riski ei koskaan ole ohi. Riski on erityisen suuri, jos hyökkääjälle on päätynyt arkaluonteisia henkilötietoja, kuten terveystietoja. Rikollinen/rikolliset toimijat voivat koska tahansa myöhemmin tulevaisuudessa julkistaa tietoja uudelleen esimerkiksi kiristystarkoituksessa tai pyrkiessään lokaamaan uhrin mainetta. Tämän vuoksi organisaation on hyvä muistaa, että tietovuoto on kriisi, joka ei uhrien näkökulmasta koskaan pääty. Siksi jälkiviestintään ja tiedonkulkuun kaikille, joita tilanne on koskettanut, on kiinnitettävä erityistä huomiota organisaatioissa.

Ensi tilassa tietoturvaloukkauksen uhrille on olennaista saada nopeasti helppotajuista tietoa tapahtuneesta ja häneen kohdistuvasta riskistä sekä mahdollisimman selkeät toimintaohjeet, jotta hän pystyy varautumaan riskeihin ja ryhtymään nopeasti varotoimiin. Organisaation velvollisuuksista tietoturvaloukkaustapauksissa on kerrottu tarkemmin tämän oppaan luvun 3.1 kohdassa Tietosuojavelvoitteet.

Kuva 4. Tietomurto voi johtaa tietovuotoon, jos murtautuja pääsee käsiksi tietojärjestelmässä olevaan arkaluonteiseen tietoon.

1.6 Teknologinen kehitys muuttaa uhkakenttää

Teknologinen kehitys muuttaa nopealla vauhdilla uhkakenttää. Taloudellisen hyödyn mahdollisuus ja teknologisen kehityksen myötä laskeva kynnys lähteä mukaan rikolliseen toimintaan houkuttelevat uusia toimijoita mukaan.

Erilaiset organisaatioiden nimissä käynnistettävät ja levitettävät huijauskampanjat ovat lähitulevaisuudessa entistä taitavammin tehtyjä, räätälöidympiä ja kohdennetumpia. Niiden tunnistaminen huijauksiksi on entistä vaikeampaa. Todellisuuden ja fiktion välinen raja hämärtyy entisestään.

Erilaiset tekoälyteknologiat, -sovellukset ja -palvelut kehittyvät todella nopeaa vauhtia ja niiden käyttö yleistyy arjessamme. Esimerkiksi generatiivinen tekoäly auttaa etsimään suuresta massasta tietoa ja tuottamaan erilaisia sisältöjä. Tekoälyn avulla voidaan luoda virtuaalisia kopioita ihmisistä yhdistämällä ääntä, videota, tekstiä ja kuvia. Tällaista teknologiaa on käytetty elokuvissa ja sosiaalisessa mediassa, kuten Metaversumissa, luomalla virtuaalisia kopioita todellisista ihmisistä, eli AI-avatar-hahmoja.

Deepfake-teknologiat puolestaan yhdistävät eri tekniikoita luodakseen esimerkiksi väärennettyjä videoita, joissa henkilö tekee tai sanoo asioita, joita ei ole oikeasti tehnyt. Tätä käytetään jo huijauksissa, maineen mustamaalauksessa ja disinformaation levittämisessä. Tekoäly voi luoda uskottavia virtuaalisia kopioita pelkän ääni- tai videonäytteen perusteella ja jopa väärentää reaaliaikaisia videopuheluja.

Termillä "deepfake" (syväväärennös) viitataan useisiin tekniikoihin

- Näitä ovat esimerkiksi videolla olevan henkilön kasvojen korvaaminen toisella. Tällöin videolla "esiintyvä" tekee asioita, joita hän ei ole todellisuudessa tehnyt.
- Lisäksi voidaan synkronoida huulten liikkeet, jolloin videolla näkyvä hahmo puhuu asioita, joita hän ei ole koskaan sanonut.
- Kuvankäsittelyn avulla voidaan luoda aidon oloisia valokuvia jostain henkilöstä. Tätä voidaan hyödyntää esimerkiksi valeprofiilien luomisessa sosiaalisen median palveluihin.
- Ääni-deepfakeissa tehdään henkilön äänellä tuotettuja sisältöjä, joissa esimerkiksi sosiaalisessa mediassa leviävällä ”tallenteella” henkilön kuullaan sanovan asioita, joita hän ei ole koskaan sanonut.
- Jo nykyisellään tekniikat mahdollistavat kohdehenkilöiden eleiden ja ilmeiden jäljittelyn. Tämä parantaa entisestään näiden valevideoiden uskottavuutta.
- Rikolliset voivat hyödyntää tekoälyä myös tietomurrossa haltuunsa saamien henkilötietojen yhdistelyssä hyödyntäen henkilöstä julkisesti saatavia tietoja.

Uhkat ja riskit saavat usein paljon huomiota julkisuudessa. On kuitenkin tärkeää muistaa, että vaikka teknologinen kehitys tuo mukanaan uusia uhkia ja muuttaa olemassa olevia, se tarjoaa myös välineitä niiden torjumiseksi. Uudet teknologiat voivat siis paitsi luoda riskejä ja uhkia, myös auttaa suojautumaan ja torjumaan niitä.

2 Viestintä kybertilanteissa

Oma organisaatio voi olla suora kyberhyökkäyksen kohde, mutta se voi myös joutua osaksi niin sanottua toimitusketjuhyökkäystä. Toimitusketjuhyökkäyksessä hyökkäys ei kohdistu suoraan omaan organisaatioon, vaan toiseen toimijaan, mutta vaikutukset voivat silti ulottua omaan organisaatioon, jos sillä on yhteyksiä hyökkäyksen kohteena olevaan toimijaan esimerkiksi verkon tai järjestelmien kautta. Organisaation arkaluonteisia tietoja voi myös päätyä rikollisten käsiin toiseen organisaatioon kohdistuneen onnistuneen tietomurron kautta.

Tällaisissa tilanteissa tarvitaan sujuvaa ja luottamuksellista tiedonvaihtoa organisaatioiden välillä, jotta yhdenmukainen ja oikea-aikainen viestintä voi onnistua.

Tavallisesti organisaation on viestittävä kyberhyökkäyksistä tai sen vaikutuksista hyvin nopeasti. Oma henkilöstö, asiakkaat ja erilaiset kumppanit odottavat tietoja tapahtuneesta ja selkeitä toimintaohjeita.

Viestinnän suunnittelussa ja toteutuksessa huomioidaan eri kohdeyleisöt, kuten: oma henkilöstö, asiakkaat, hyökkäyksen kohteena olevat mahdolliset erityisryhmät, kumppanit, sopimuskumppanit/alihankkijat, toimialan muut toimijat, media, sidosryhmät ja päättäjät.

Viestinnän suunnittelussa ja toteutuksessa huomioidaan eri kohdeyleisöt, kuten

- oma henkilöstö,
- asiakkaat,
- hyökkäyksen kohteena olevat mahdolliset erityisryhmät,
- kumppanit,
- sopimuskumppanit/alihankkijat,
- toimialan muut toimijat,
- media,
- sidosryhmät ja
- päättäjät.

2.1 Kybertilanteiden johtaminen ja viestintä

Viestinnän kuusi pointtia

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

Kyberhyökkäyksissä viestintää hoidetaan samoin periaattein kuin päivittäisessä viestinnässä, mutta viestinnän määrä ja nopeus kasvavat. On tärkeää, että viestintä on oikea-aikaista ja selkeää. Viestinnässä on otettava huomioon erilaiset kohdeyleisöt ja heidän erilaiset tiedontarpeensa sekä mahdollinen sääntely, esimerkiksi sisäpiiritiedon julkistamiseen liittyvä sääntely.

Tilanteen johtaminen, hallinta ja viestintä joudutaan erityisesti alkuvaiheessa tekemään tilanteessa, jossa on enemmän avoimia kysymyksiä kuin vastauksia. Kaikkia kysymyksiä ei ole mahdollista edes tunnistaa. Lisäksi on mahdollista, että arjessa normaalisti käytössä olevat työvälineet sekä luotettavat johtamisen, tiedonkulun ja viestinnän kanavat eivät välttämättä ole käytössä esimerkiksi kiristyshaittaohjelmatilanteessa. Jos organisaatiolla ei ole käsitystä siitä, mihin kaikkialle hyökkääjä on päässyt organisaation tietoverkossa, on tällaisessa tilanteessa organisaation toimintaa, työvälineiden käyttöä ja tiedonkulkua rajoitettava mahdollisten lisävahinkojen estämiseksi.

Organisaatioiden on tärkeä ymmärtää, että henkilöstö tai julkisuudessa esiintyvät asiantuntijat tai heidän perheenjäsenensä voivat joutua häirinnän tai maalittamisen kohteeksi tapahtuneen vuoksi. Tämän vuoksi organisaation on tärkeää luoda selkeät ohjeet ja käytännöt ja tukimuodot, jotka sisältävät psykososiaalisen tuen, fyysisen turvallisuuden varmistamisen sekä oikeussuojakeinot. Selkeät toimintatavat häirintä- ja vainoamistilanteiden hoitamiseen sekä johdon vahva tuki viestivät sekä henkilöstölle että ulkopuolisille organisaation arvoista ja toimintaperiaatteista.

2.1.1 Tilannetta johdetaan ja siitä viestitään, vaikka kaikkea ei tiedetä

Kriisijohtamisella on keskeinen rooli tilanteen hallinnassa ja toiminnan jatkuvuuden turvaamisessa. Jokaisella organisaatiolla tulisi olla kriisiryhmä, joka on koottu vastaamaan organisaation tarpeita. Ryhmässä tulisi olla edustus viestinnästä, lakiosastosta, henkilöstöhallinnosta, IT-osastosta sekä liiketoiminta- ja operatiivisista toiminnoista. Ryhmän kokoonpano riippuu organisaation koosta ja rakenteesta. On tärkeää, että kriisiryhmällä on suora ja välitön yhteys ylimpään johtoon, mikä takaa nopean päätöksenteon ja tehokkaan yhteistyön kriisin keskellä.

On erittäin todennäköistä, että alkuperäinen tilannekuva tapahtuneesta, sen seurauksista ja vaikutuksista eri kohderyhmille tulee muuttumaan selvitystyön edetessä. Viestinnässä ei kuitenkaan voi jäädä odottamaan selvitystyön lopullisia tuloksia, vaan on tärkeää kertoa edes yleisellä tasolla tilanteesta. Näin vältetään informaatiotyhjiön syntyminen.

Viestinnässä voi esimerkiksi kertoa, että tilannetta ja sen laajuutta selvitetään. Ensisijaisesti kerrotaan asioista, joista on täysi varmuus. Samoin voidaan kertoa, että tieto ja ymmärrys tapahtuneesta täydentyy koko ajan.

Viestinnässä on hyvä välttää toteamasta asioita, joista ei ole täyttä varmuutta. Jos organisaatio on antanut väärää tietoa, se pitää korjata välittömästi. Johdon on otettava näkyvä rooli myös julkisuudessa.

Johtamisessa ja viestinnässä on tärkeää pohtia heti alusta alkaen myös sitä, mihin tilanne voi kehittyä ja mitä yllättäviäkin asioita voi selvitä ja miten tilanteen alussa viestitty vaikuttaa kohderyhmien tulkintaan tilanteen hoidon tehokkuudesta ja uskottavuudesta. Kysymys on tulevan toiminnan, johtamisen sekä viestintätarpeiden ennakoinnista ja varautumisesta.

2.1.2 Luotettava organisaatio kertoo itse aina kun voi

Kybertilanteiden viestinnässä haasteena on myös se, että hyökkäyksen tehneellä rikollisella tai muulla toimijalla on mahdollisuus ottaa tilanteessa viestinnällinen aloite haltuunsa. Esimerkiksi ennen kuin organisaatio on saanut kokonaiskuvaa siitä, mitä on ylipäätään tapahtunut, rikollinen voi julkistaa tekonsa esimerkiksi lähettämällä lunnasvaatimuksen tai julkistamalla organisaation sisäisiä sähköposteja tai asiakirjoja tai asiakkaiden arkaluonteisia henkilötietoja netissä. Tämän vuoksi on tärkeää, että organisaatiolla on kyky ja valmius reagoida nopeastikin muuttuviin tilanteisiin mahdollisimman nopeasti myös viestinnällisesti.

Varautuminen ja harjoittelu ovat tässä avainsanoja. Nopea reagointikyky edellyttää sitä, että roolit, vastuut ja viestinnälliset materiaalit ja sisällöt eri kybertilanteisiin on mietitty ja tuotettu ennakkoon. Näin ei hukata aikaa nopeaa reagointia edellyttävässä tilanteessa ja estetään mahdollisten lisävahinkojen syntyminen sekä suojellaan ja tuetaan uhreja.

2.1.3 Viestinnässä korostuu tapahtuman kuvaus ja selkeät ohjeet

Viestinnän kohdeyleisöt ovat pääsääntöisesti tavallisia ihmisiä, jotka eivät tunne kyberturvallisuuden yksityiskohtia tai teknisiä termejä. Tämän vuoksi on tärkeää, että viestinnässä käytetään ymmärrettävää kieltä ja vältetään teknistä sanastoa. Viestinnän painopisteen tulee olla tapahtuman ja vaikutusten selkeässä kuvaamisessa ja toimintaohjeiden antamisessa. Tietoa on varauduttava antamaan eri kielillä.

Viestintää on suunniteltava, jotta voidaan varmistua siitä, että henkilöstö ja kaikki tahot, joita tilanne koskettaa, pystyvät muodostamaan kokonaiskuvan tapahtuneesta, tietävät miten tulee toimia sekä pystyvät valvomaan oikeuksiaan. Selkeällä ja säännöllisellä viestinnällä estetään lisäksi mahdollisten lisävahinkojen syntyminen.

Tilanne voi herättää kiinnostusta mediassa ja tämän vuoksi on tärkeä kertoa henkilöstölle organisaation viestintävastuista tilanteessa. Eli siitä, kuka organisaatiossa vastaa viestinnästä ja kuka tai ketkä antavat haastattelut tai kommentoivat medialle. Selkeiden viestintäroolien ja vastuiden määrittely ja niiden kertominen henkilöstölle auttaa ehkäisemään ristiriitaisten tietojen ja viestien välittymisen.

2.1.4 Tukea hyökkäyksen uhreille on varauduttava antamaan pitkään

Mikäli ihmisten arkaluonteisia tietoja on kyberhyökkäyksen vuoksi päätynyt hyökkääjälle, on tärkeä muistaa, että uhrien näkökulmasta tietovuoto on kriisi, joka ei koskaan pääty. Rikollinen/rikolliset toimijat voivat koska tahansa myöhemmin tulevaisuudessa julkistaa tietoja uudelleen esimerkiksi kiristystarkoituksessa, häirinnässä tai pyrkiessä lokaamaan uhrin mainetta. Siksi jälkiviestintään ja tiedonkulkuun kaikille, joita tilanne on koskettanut, on kiinnitettävä erityistä huomiota organisaatioissa myös teknisen selvitystyön ja toiminnan operatiivisen palautumisen jälkeenkin. Monissa kyberrikostilanteissa uhreja voi kehottaa kääntymään tukipalveluiden, kuten Rikosuhripäivystyksen puoleen, joka tarjoaa tukea ja käytännön neuvoja rikosasiassa.

2.1.5 Kansainvälisen viestinnän tarvetta ei saa unohtaa

Mikäli organisaatiolla on toimintaa (esim. tytäryhtiö) Suomen ulkopuolella, tulee viestinnässä ottaa huomioon asemamaan säännökset, velvoitteet ja ohjeet viestinnälle. Tämä koskee viestintää niin organisaation työntekijöille, sopimuskumppaneille kuin asiakkaillekin. On tärkeää, että kaikki työntekijät riippumatta asemamaastaan saavat oikea-aikaisesti, selkeät ja riittävät ohjeet siitä, mitä on tapahtunut, mitä heille tapahtuneesta voi aiheutua ja miten heidän tulee tilanteessa toimia. Tämä koskee myös asiakkaita, alihankkijoita ja muita sopimuskumppaneita.

Koska informaatioympäristö on nykyisin aidosti kansainvälinen eikä tunne valtioiden rajoja, on organisaation hyvä muistaa, että kybertilanne voi herättää kiinnostusta kansainvälisessä mediassa tai levitä laajalle sosiaalisessa mediassa. Viestintään on varauduttava myös muilla kielillä kuin suomeksi. Ulkomaisille sidosryhmille viestittäessä on myös usein hyödyllistä avata suomalaista toimintaympäristöä ja toimijoita, jos ne eivät ole ennalta tuttuja.

2.1.6 Säännöllinen viestintä rakentaa luottamusta

Kyberhyökkäyksen ja siihen liittyvän selvitystyön aikana on hyvä tarjota näkymää siihen, milloin tietoa on saatavilla seuraavan kerran. Mikäli uutta kerrottavaa ei ole, on sekin parempi tieto uhrien kannalta, kuin hiljaisuus. Säännöllisyydellä varmistetaan se, että eri kohdeyleisöt tietävät, että heidän asiaansa hoidetaan, eikä heitä ole unohdettu. He voivat myös luottaa siihen, että saavat ajankohtaista tietoa heihin vaikuttavista asioista heti kun sitä on vain saatavilla.

Ihmisten kysymykset ovat hyvin konkreettisia ja henkilökohtaisia, ja tietoa halutaan saada nopeasti

- Mitä on tapahtunut ja miksi?
- Kuka on tällaisen tapahtuman takana?
- Mitä tietoja minusta on vuotanut?
- Mistä ja keneltä saan lisätietoja ja miten minun tulee nyt toimia?
- Millaisia vaikutuksia tällä on minuun?
- Mitä pahaa minulle voi tästä aiheutua?
- Kuka korvaa mahdolliset vahingot? Olisinko voinut tehdä joitain asian estämiseksi?
- Mihin toimiin olette ryhtyneet tämän johdosta? Miten varmistatte, ettei näin tapahdu uudestaan?

Alihankkijat, asiakkaat ja muut sopimuskumppanit tarvitsevat tietoa

- Mitä on tapahtunut ja miksi?
- Kuka on tällaisen tapahtuman takana?
- Mitä tietoja on vuotanut?
- Mistä ja keneltä saan lisätietoja?
- Onko oman organisaationi tietoturvallisuus ja toiminta myös vaarantunut?
- Onko hyökkääjä päässyt myös meidän järjestelmiin?
- Miten oman organisaationi tulee nyt toimia?
- Millaisia vaikutuksia tapahtuneella on oman organisaationi operatiiviseen toimintaan ja omiin asiakkaisiimme?
- Kuka korvaa mahdolliset omalle organisaatiolleni aiheutuvat vahingot?

2.1.7 Turha spekulointi lisää epävarmuutta, pelkoja ja misinformaation leviämistä

Kyberhyökkäyksen taustalla olevan toimijan nimeäminen ja osoittaminen ei ole helppoa. Digitaalisessa maailmassa toimija pystyy helposti peittämään jälkensä tai lavastamaan toimijaksi jonkun muun. Myös toiminnan taustalla olevan toimijan motiivin arvioiminen voi olla joissain tapauksissa vaikeaa. Nämä seikat on hyvä ottaa huomioon tapahtunutta koskevassa viestinnässä ja kommentoinnissa. Erityisen tärkeää tämä on silloin, jos tilanteessa on valtiollisen kybervakoilun mahdollisuus.

Kyberhyökkäyksiin liittyvässä viestinnässä on suositeltavaa välttää spekulointia. Spekulointi perustuu usein ennakkotietoihin tai oletuksiin, jotka eivät välttämättä pidä paikkaansa ko. tilanteessa. Erityisesti kyberhyökkäysten alkuvaiheiden kaltaisissa epäselvissä tilanteissa uhkilla ja riskeillä spekulointi vain lisää epävarmuutta, pelkoja sekä mahdollisen virheellisen tiedon (misinformaation) leviämistä. Viestinnässä on kiinnitettävä huomio oikean ja ajantasaisen tiedon välittämiseen epäkohtia ja virheitä peittelemättä. Merkitykselliset virheelliset tiedot on korjattava viipymättä, ja eri kohdeyleisöjen tiedontarpeita on seurattava jatkuvasti.

2.2 Viestinnässä huomioitava erilaiset ohjeet, rajoitukset ja säännöt

2.2.1 Valtionhallinnon viestintä kyberhäiriötilanteissa

Erilaisten kyberhäiriötilanteiden viestinnässä noudatetaan Valtionhallinnon tehostetun viestinnän ohjeessa[2] (VNK 2019:23) määriteltyjä periaatteita.

Häiriötilanteissa toimivaltainen viranomainen johtaa operatiivista toimintaa ja vastaa myös siihen liittyvästä viestinnästä. Jokainen ministeriö vastaa toimintaansa koskevasta viestinnästä ja oman hallinnonalansa viestinnän yhteensovittamisesta.

Moniviranomaistilanteessa toimintaa johtavan viranomaisen on huolehdittava siitä, että muut tapahtumaan kytkeytyvät viranomaiset saavat riittävästi tietoa tapahtumista. Tällaisessa tilanteessa vastuuviranomaiset vastaavat edelleenkin operatiivisesta tai esimerkiksi esitutkinnasta tiedottamisesta. Toimintaa johtava viranomainen vastaa myös siitä, että valtioneuvoston tilannekeskus saa ajantasaiset tiedot tapahtumista.

Kyberhäiriötilanteissa viestinnän johtovastuu voi siirtyä valtioneuvoston päätöksellä valtioneuvoston kanslialle. Tällainen tilanne voisi olla esimerkiksi laajasti kriittistä infrastruktuuria ja yhteiskuntaa lamauttava kyberhyökkäys. Siinäkin tilanteessa vastuuviranomaiset vastaavat operatiivisesta tai esimerkiksi esitutkinnasta tiedottamisesta. Samalla kuitenkin korostuu tarve koordinoida viranomaisviestintää myös valtiojohdon viestinnän kanssa. Häiriötilanteissa on keskeistä, että valtioneuvosto ja viranomaiset kykenevät tarjoamaan ajantasaista ja luotettavaa tietoa, joka vähentää mahdollisten yhteiskuntaan kohdistuvien vaikuttamisyritysten haitallisia vaikutuksia

Viranomaisten on sovittava keskinäisestä vastuunjaosta ja tiedotettava siinä tapahtuvista muutoksista sekä varmistettava viestinnän yhdenmukaisuus. Yhteistyötä jatketaan tärkeimpien sidosryhmien kanssa myös häiriötilanteissa. Yhteistyömuodoista sovitaan jo normaalioloissa.

2.2.2 Kuntien viestintä kyberhäiriötilanteissa

Tämän ohjeen sisältö on hyödynnettävissä suoraan kuntien kyberhäiriöiden viestinnän kehittämiseksi. Ohjeen luvussa 2 mainitut kybermaailman uhkat ovat tyypillisiä riskejä myös kunnan digitaalisessa toimintaympäristössä. Tietojenkalastelukampanjoista varoittamisen sekä mahdollisten palvelunestohyökkäysten ja kiristyshaittaohjelmien aiheuttamiin

[2] Valtionhallinnon tehostetun viestinnän ohje: Viestintä normaalioloissa ja häiriötilanteissa - Valto

palvelukatkoksiin liittyvän viestinnän pitäisi olla kunnalle jo melko tavanomaista ”perushäiriötilanne viestintää”.

Tietomurtotapaus on kunnalle mahdollisista kyberhäiriöviestintätilanteista mittavin ja haastavin. Siinä voi olla kriisiviestinnän kohteena jopa koko kunnan tai laajemmankin alueen väestö. Tietomurrosta viestiminen vaatii tavanomaista suurempia viestintäresursseja ja tavanomaista huomattavasti merkittävämpää pitkäjänteisyyttä. Kuntien tulee kyetä tunnistamaan myös hybridivaikuttamistilanteet ja osata reagoida niihin.

Kunnat noudattavat myös kyberhäiriötilanteissa omia viestintäperiaatteitaan ja toimintatapojaan. Tavallisesta poikkeavassa tilanteessa tiedon tarve kasvaa nopeasti. Viestinnän tulisi olla nopeaa ja selkeää sekä pitkäjänteistä. Johtamisen ja viestinnän tehokkuudelle asetetaankin suuria odotuksia, joita ei voi täyttää varautumatta ja harjoittelematta.

Ensimmäinen edellytys toimivalle kriisiviestinnälle on, että kunnan tavanomainen viestintä toimii ja on tiiviissä yhteydessä johtamiseen. Erityistilanteessa viestintää hoidetaan tehostamalla hyvin toimivia ja luotettavia viestintäprosesseja.

Kuntien poikkeustilanneviestinnässä erityinen piirre on varsin laaja toimijakenttä. Häiriötilanteessa kunnalla on todennäköisesti tarve muodostaa tilannekuvaa ja tehdä yhteistyötä niin valtion toimijoiden, hyvinvointialueen ja muiden kuntien kanssa kuin oman konsernin sisälläkin. Nämä yhteydet tulisi luoda ja yhteistyön toimintatavat harjoitella ennakkoon.

Kyberhäiriöihin varautumisen osana kunnan tulisi harjoittaa myös ennakkoviestintää: kertoa, että kunta varautuu kyberhäiriöihin ja että kunta pyrkii suojaamaan omat digitaaliset palvelunsa huolellisesti kyberuhkien varalta. Lisäksi kunta voi välittää viranomaisten ohjeita ja suosituksia kuntalaisille siitä, miten he voivat suojata omaa digitaalista toimintaansa kyberrikoksilta.

Usein mikä tahansa yhteiskunnan häiriötilanne heijastuu myös paikalliselle tasolle. Kunta on kaikista julkisen sektorin toimijoista lähimpänä asukkaita, joten kuntalaiset ovat tottuneet kääntymään kunnan puoleen ja saamaan tietoa kunnalta myös tilanteissa, joissa häiriö tai kriisi ei liity suoraan kuntaorganisaatioon. Kunnalla voi siis olla tarve viestiä myös häiriöistä, jotka eivät liity suoraan kunnan omaan toimintaan. Sidosryhmien tulisikin tunnistaa kunnan laaja merkitys ja huomioida se jo ennalta varautumisen ja häiriötilanteiden hallinnan suunnitelmissaan.

Kuntaliitolta löytyy vuonna 2020 julkaistu Opas kuntien viestinnästä kriisi- ja erityistilanteissa (https://www.kuntaliitto.fi/julkaisut/2020/2048-opas-kunnan-viestintaan-kriisi-ja-erityistilanteissa), josta on apua kunnan viestinnän suunnittelussa.

2.2.3 Pörssitiedottaminen

Mikäli yritys on listattu pörssissä, sitä koskevat pörssitiedottamisen säännöt.

Listayhtiön eli yhtiön, jonka arvopaperi on kaupankäynnin kohteena, on otettava tiedottamisessa huomioon, että erilaisissa kyberhäiriötilanteissa voi syntyä sisäpiiritietoa, jonka julkistamista sääntelee markkinoiden väärinkäyttöasetuksen säännökset. Nämä säännökset koskevat sekä Helsingin pörssissä säännellyllä markkinalla että First North Finland -kauppapaikalla kaupankäynnin kohteena olevia liikkeeseenlaskijoita.

Sisäpiiritiedolla tarkoitetaan täsmällistä ja julkistamatonta tietoa, joka liittyy suoraan tai välillisesti liikkeeseenlaskijaan ja jolla, jos se julkistettaisiin, todennäköisesti olisi huomattava vaikutus arvopaperin hintaan. Liikkeeseenlaskijan tulee tehdä arvio siitä, onko kysymys sisäpiiritiedosta.

Sisäpiiritieto on julkistettava mahdollisimman pian. Tietyissä sääntelyssä kuvatuissa tilanteissa liikkeeseenlaskija voi kuitenkin omalla vastuullaan lykätä sisäpiiritiedon julkistamista esimerkiksi silloin, kun tiedon välitön julkistaminen todennäköisesti vaarantaisi liikkeeseenlaskijan oikeutetut edut. Sisäpiiritiedon julkistamisesta löytyy tarkemmin Finanssivalvonnan verkkopalvelusta *Sisäpiiritiedon julkistaminen ja julkistamisen lykkääminen - Sisäpiiriasiat - www.finanssivalvonta.fi*

Arvopaperin liikkeeseenlaskijan tulee sisäpiiritiedon julkistamiseen liittyvän sääntelyn noudattamisen lisäksi huomioida arvopaperimarkkinalain säännökset totuudenvastaisten ja harhaanjohtavien tietojen antamisen kiellosta sekä pörssin säännöt, jotka myös sisältävät tiedottamiseen liittyvää ohjeistusta.

2.2.4 Tutkinnan rajoitukset

Kun poliisi aloittaa esitutkinnan epäillystä rikoksesta, voi esitutkinta asettaa rajoituksia organisaation omalle viestinnälle. Viestintä on suunniteltava ja toteutettava siten, ettei viestintä ja tietojen julkistaminen haittaa tai vaaranna tutkintaa. Tutkinnanjohtajan kanssa neuvotellen viestintä onnistuu parhaiten siten, ettei se vaaranna esitutkinnan suorittamista.

Poliisi suosittaa tekemään mahdollisimman aikaisessa vaiheessa rikosilmoituksen organisaatioon kohdistuneista teosta, jossa on syytä epäillä rikosta.

Kybervakoilutapauksessa viestinnässä on huomioitava esitutkinnan lisäksi vaikutukset Suomen ulko- ja turvallisuuspolitiikkaan. Esimerkiksi päätöksen toisen valtion nimeämisestä kybervakoilun tekijäksi tekee valtiojohto viranomaisten selvitysten pohjalta.

2.2.5 NIS2-direktiivi ja velvoitteet viestinnälle

Euroopan unionin NIS2-direktiivi asettaa sääntöjä tietoturvavelvollisuuksista ja häiriöraportoinnista eri sektoreilla. Se velvoittaa erityisesti kriittisiä sektoreita parantamaan kyberturvallisuutta riskien hallinnan ja raportointivelvollisuuksien avulla. Direktiivissä määritellään vähimmäistoimenpiteet, joita kaikkien organisaatioiden on noudatettava kyberturvallisuusriskien hallitsemiseksi.

NIS2-direktiivin soveltamisalaan kuuluvat organisaatiot[3] ovat velvollisia ilmoittamaan valvovalle viranomaiselle merkittävistä poikkeamista, jotka voivat aiheuttaa vakavan toimintahäiriön tai taloudellisia tappioita. Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä poikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. NIS2-direktiivi edellyttää organisaatioilta selkeää, nopeaa ja läpinäkyvää viestintää niin viranomaisten kuin asiakkaiden kanssa, erityisesti tietoturvapoikkeamien aikana ja niiden jälkeen.

Toimijan on ilmoitettava viipymättä myös merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.

[3] Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2) | Kyberturvallisuuskeskus

NIS2-direktiivi vaikuttaa organisaatioiden viestintään erityisesti sen raportointivelvollisuuksien ja tiedon jakamisen osalta

- **Raportointivelvollisuus viranomaisille:** NIS2 velvoittaa organisaatioita ilmoittamaan merkittävistä tietoturvapoikkeamista viipymättä valvoville viranomaisille. Ensimmäinen ilmoitus on tehtävä 24 tunnin kuluessa ja jatkoilmoitus 72 tunnin sisällä merkittävän poikkeaman havaitsemisesta. Tämä tarkoittaa, että organisaatioiden on oltava valmiita nopeasti keräämään tietoa poikkeamasta ja välittämään se viranomaisille.
- **Viestintä asiakkaiden kanssa**: Jos poikkeama todennäköisesti vaikuttaa palvelujen saatavuuteen, organisaation on ilmoitettava asiakkailleen tapahtuneesta mahdollisimman pian.
- **Sisäinen viestintä:** Organisaatioiden on varmistettava, että henkilöstö saa ajantasaisen tiedon tapahtuneesta ja selkeät toimintaohjeet.
- **Loppuraportti:** Organisaation tulee toimittaa loppuraportti tapahtuneesta viranomaisille kuukauden kuluessa jatkoilmoituksen toimittamisesta tai, jos kyseessä on pitkäkestoinen poikkeama, kuukauden kuluessa sen käsittelyn päättymisestä. Raportin tulee kattaa
    - yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;
    - selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;
    - selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja
    - selvitys mahdollisista rajat ylittävistä vaikutuksista.

Kuva 5. NIS2 velvoittaa organisaatioita ilmoittamaan merkittävistä tietoturvapoikkeamista viipymättä valvoville viranomaisille.

2.2.6 Tietosuojaloukkauksista ilmoittaminen ja viestintä

Jos kyberhyökkäys kohdistuu henkilötietoihin, eli tietoihin, joista henkilö voidaan tunnistaa suoraan tai epäsuorasti, on kyseessä henkilötietojen tietoturvaloukkaus. Silloin organisaation täytyy noudattaa yleisestä tietosuoja-asetuksesta (GDPR) tulevia velvoitteita.

Yleisessä tietosuoja-asetuksessa säädetään muun muassa, millaisissa tilanteissa organisaation on ilmoitettava tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle ja kohteeksi joutuneille henkilöille. Vastuu tietoturvaloukkauksesta viestimisestä on lainsäädännön nojalla rekisterinpitäjällä, eli sillä organisaatiolla, joka on vastuussa henkilötietojen käsittelystä.

Organisaation lakisääteiset ilmoitusvelvollisuudet määräytyvät sen perusteella, kuinka korkea riski tietoturvaloukkauksesta aiheutuu sen kohteena oleville henkilöille (henkilön oikeuksiin ja vapauksiin kohdistuva riski).

Riskin tason arvioinnissa on huomioitava muun muassa

- tietoturvaloukkauksen tyyppi,
- henkilötietojen luonne, arkaluonteisuus ja määrä,
- kuinka helposti henkilöt ovat tunnistettavissa aineistosta,
- kohdistuuko tietoturvaloukkaus esimerkiksi lapsiin tai muihin haavoittuvammassa asemassa oleviin,
- organisaation toimiala ja rooli sekä
- tietovuodon seurauksien vakavuus ja todennäköisyys.

Jos henkilötietoihin kohdistuneesta tietoturvaloukkauksesta voi aiheutua henkilöille riski, siitä on ilmoitettava tietosuojavaltuutetun toimistolle. Ilmoitus on tehtävä ilman aiheetonta viivytystä viimeistään 72 tunnin kuluessa loukkauksen havaitsemisesta, vaikka kaikki tapahtumaa koskevat tiedot eivät olisikaan vielä täysin selvillä. Kynnys tietosuojavaltuutetulle ilmoittamiselle ei edellytä korkeaa riskiä tai riskin suurta todennäköisyyttä.

Jos loukkaus todennäköisesti aiheuttaa ihmisille korkean riskin, tapahtuneesta täytyy ilmoittaa myös niille henkilöille, joiden tiedot ovat vaarantuneet. Ilmoitus on tehtävä ilman aiheetonta viivytystä, jotta ihmisillä on mahdollisuus varautua riskeihin ja ryhtyä varotoimiin esimerkiksi sulkemalla luottokorttinsa. Kiireellisiä toimia vaativissa tilanteissa ihmisille on kerrottava tilanteesta mahdollisimman pikaisesti.

Ilmoituksessa on kerrottava ainakin

- selkeä kuvaus, mitä on tapahtunut,
- todennäköiset seuraukset henkilölle,
- organisaation toteuttamat tai suunnittelemat toimenpiteet mahdollisten haittavaikutusten lieventämiseksi sekä
- organisaation tietosuojavastaavan tai muun lisätietojen antajan yhteystiedot.

Pääsääntö on, että informointi on tehtävä ihmisille henkilökohtaisesti. Kaikissa tilanteissa tämä ei kuitenkaan välttämättä ole mahdollista, esimerkiksi jos kohteeksi joutuneita henkilöitä on mahdoton yksilöidä. Tällöin ilmoitus voi olla mahdollista tehdä myös muulla keinolla, kuten julkisella tiedoksiannolla. Organisaation pitää kuitenkin pystyä osoittamaan, ettei kohteeksi joutuneita henkilöitä pystytä yksilöimään niin, että heille voitaisiin ilmoittaa suoraan. Tiedottamisen on joka tapauksessa oltava yhtä tehokasta. Tilanteista, joissa henkilökohtaista ilmoitusta kohteeksi joutuneille henkilöille ei lain mukaan vaadita, säädetään tarkemmin tietosuoja-asetuksen 34 artiklassa.

Kaikki henkilötietojen tietoturvaloukkauksiin liittyvät toimenpiteet on dokumentoitava. Tarkemmat tiedot organisaation velvollisuuksista tietoturvaloukkaustapauksissa tietosuojavaltuutetun toimiston verkkosivuilla: https://tietosuoja.fi/tietoturvaloukkaukset.

2.3 Varautuminen

Hyvällä varautumisella varmistetaan, että organisaatio on valmis ja kykenevä viestimään nopeasti hyökkäyksestä, minimoidaan virheellisen tiedon leviäminen sekä varmistetaan, että kaikki osapuolet saavat oikeat tiedot oikeaan aikaan. Kriisiviestintäsuunnitelmien laatiminen on esimerkiksi finanssialalla pakollista[4].

Pohdittavaa varautumistyön yhteydessä:

- Mitkä ovat työmme kannalta keskeiset työvälineet ja kanavat? Miten voimme työskennellä ja viestiä ilman niitä?
- Millaisia kyberuhkia organisaatioomme voi kohdistua? Miten vastaamme niihin viestinnällisesti eri kohdeyleisöt ja kanavat huomioiden?
- Mitkä ovat organisaatiomme toiminnan kannalta keskeiset tiedot tai rekisterit, joiden päätyminen rikollisten käsiin voi vaarantaa organisaatiomme toiminnan tai organisaatiotamme kohtaan tunnetun luottamuksen? Keiden tietoja näissä rekistereissä on?
- Mitkä ovat viestinnälliset toimenpiteet (esimerkiksi viestit ja sisällöt eri tilanteisiin ja kohdeyleisöille), jotka voimme tehdä jo ennakkoon?
- Organisaatiollamme on toimintaa useissa maissa, mitkä ovat ohjeet eri maissa organisaatioille ja yksittäisille ihmisille esimerkiksi tietovuoto- tai kiristyshaittaohjelmatapauksessa?
- Miten organisoimme toimintamme erilaisissa kybertilanteissa? Ovatko roolit ja vastuut selvät?
- Millaisia ohjeita ja suosituksia organisaatiomme voisi antaa uhreille henkilötietojen tietoturvaloukkauksen haittavaikutusten lieventämiseksi?
- Olemmeko kartoittaneet keskeisten sidosryhmiemme ja kohdeyleisöjemme yhteyshenkilöt ja sopineet tiedonvaihdon kanavista kybertilanteissa?
- Miten varmistamme organisaatiossamme luotettava tiedon ja viestien vaihdon kanavat?
- Miten saamme tiedon tapahtuneesta ja toimintaohjeet henkilöstöllemme myös tilanteessa, jossa esimerkiksi intranet ja sähköpostijärjestelmä ei ole käytössä?

[4] Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 finanssialan digitaalisesta häiriönsietokyvystä (DORA), artikla 14.

- Miten saamme tiedon tapahtuneesta ja toimintaohjeet asiakkaillemme, ulkoisille kumppaneillemme ja sidosryhmillemme tilanteessa, jossa normaalisti käytössä olevat ulkoisen viestinnän kanavat eivät ole käytettävissä, joko kokonaan tai osittain?
- Miten varmistamme viestinnän resurssit ja henkilöstön jaksamisen pitkäkestoisessa tilanteessa?
- Miten varaudumme siihen, että henkilökuntamme voi joutua häirinnän tai suoranaisen maalittamisen kohteeksi tapahtuneen johdosta?
- Miten olemme varautuneet siihen, että hyökkääjän tavoitteena on julkisesti haastaa organisaatio tai että kaikki tilanteen osapuolet eivät pelaa reiluilla korteilla?

2.4 Viestintä kyberkriisitilanteiden aikana

- Miten organisoimme tapahtuneessa luotettavan tiedonkulun tilanteen hallintaan osallistuvien asiantuntijoiden ja mahdollisten ulkopuolisten kumppaneiden välillä?
- Miten saamme ajantasaisen tilannekuvan ja -tiedon viestinnän suunnittelua ja toteuttamista varten?
- Onko viestinnän edustus läsnä kaikissa kokoonpanoissa, joissa tilannetta käsitellään ja hallitaan?
- Ketkä kaikki toimijat ja organisaatiot olisi hyvä saada viestinnän koordinaation piiriin? Ketä kaikkia myös organisaatiomme ulkopuolella tämä kyseinen tapaus saattaa koskettaa?
- Miten viestimme teknisistä asioista ymmärrettävästi, oikea-aikaisesti ja selkeästi eri kohderyhmille?
- Miten yhteensovitamme avoimuuden ja läpinäkyvyyden esimerkiksi rikostutkinnan rajoituksiin?
- Miten vastaamme eri kohdeyleisöjen tiedontarpeeseen?
- Miten selvitämme, ketkä kaikki ovat henkilötietoihin kohdistuneen tietoturvaloukkauksen uhreja ja miten viestimme heille? Onko uhrien joukossa henkilöitä, joiden äidinkieli ei ole suomi tai ruotsi?
- Miten viestimme asiasta ja ohjeistamme eri puolilla maailmaa työskenteleville työntekijöillemme ja asiakkaillemme huomioiden kansalliset ohjeistukset ja määräykset?

- Miten tavoitamme ja viestimme asiasta ja ohjeistamme uhreja (esimerkiksi asiakkaat), jotka eivät asu Suomessa ja joiden äidinkielet eivät ole suomi tai ruotsi?
- Mikä on pahin lopputulos, joka on mahdollisesti voinut tapahtua ja johon meidän pitäisi viestinnässämme varautua?
- Mikäli asiakkaidemme tai työntekijöidemme arkaluonteisia tietoja on varastettu, miten suurta joukkoa ihmisiä vuoto mahdollisesti koskettaa? Miten pitkältä ajalta tietoja on mahdollisesti vuotanut?
- Miten varaudumme siihen, että rikollinen aktivoituu?
- Missä kanavissa viestimme eri kohdeyleisöille?
- Millaisia vaikutuksia tapahtuneella on organisaatiomme henkilöstölle, asiakkaille tai kumppaneille?
- Miten heidän tulee toimia tässä tilanteessa?

2.5 Jälkiviestintä

- Miten huolehdimme tiedonkulusta ja viestinnästä tapahtuman jälkeen? Koskee myös resursointia?
- Missä kanavissa viestimme jatkossa tapahtuneesta ja annamme tilannetietoa sekä mahdollisia uusia toimintaohjeita?
- Miten huolehdimme ja varmistamme mahdollisten uhrien tiedonsaannin myös jatkossa?
- Miten viestimme ja toimimme, jos rikollinen alkaa uudelleen esimerkiksi levittää ihmisistä saamiaan arkaluonteisia tietoja tai kiristämään uhreja?
- Miten kerromme toimista, joilla varmistamme, että tapahtunut ei toistu?

2.6 Arviointi

- Miten keskeiset kumppanimme arvioivat viestintämme onnistumisen?
- Miten sisäiset tiedonkulun, johtamisen ja viestinnän prosessit toimivat?
- Saimmeko riittävästi tietoa viestinnän suunnittelua ja toteuttamista varten?
- Oliko varautumisemme riittävää ja onnistunutta?

2.7 Harjoitustoiminta osaksi arkea

Vastuullinen organisaatio ottaa harjoittelun osaksi varautumis- ja jatkuvuussuunnitteluaan. Harjoitusta suunnitellessa on tärkeintä kirkastaa se ongelma tai epäkohta, jota harjoittelemalla pyritään ratkaisemaan. Viestinnän näkökulmasta kyseessä voi olla esimerkiksi viestinnän roolien selkeyttäminen yhteistyökumppanien kanssa, lainsäädännön mukaisen toiminnan varmistaminen kriisissä tai esimerkiksi viestinnän asianmukaisuuden varmistaminen kyberhyökkäystilanteessa. Harjoituksista tulisi aina kerätä opit ja kehittämiskohteet sekä varmistaa kehittämiskohteiden toteuttaminen seurannalla.

Riskiarvion perusteella voi määritellä omalle organisaatiolle sopivan harjoittelun määrän ja sisällön. Oletuksena viestintäasiantuntijoiden ja tiimin kannattaisi harjoitella vähintään kerran vuodessa. Joka vuonna ei tarvitse pitää mittavaa harjoitusta, vaan erilaiset harjoittelun tavat voivat vuorotella: organisaation ja palveluntuottajien omia prosesseja läpikäyvät työpöytäharjoitukset, organisaation sisäiset ja sidosryhmät laajemmin osallistavat simuloidut johtamisharjoitukset sekä laajat, useiden sidosryhmien valmiusharjoitukset tarjoavat erilaisia vaihtoehtoja kehittää organisaation kriisiviestintää.

Harjoitustoiminnassa voi hyödyntää valmiita aineistoja ja julkisen hallinnon tarjoamia harjoituksia. Digi- ja väestötietoviraston vuosittain järjestettävä, julkisen sektorin organisaatioille ensisijaisesti suunnattu Taisto-harjoitus tarjoaa matalan kynnyksen ohjatun kyberharjoituksen organisaatioille. Aikaisempien vuosien harjoitusten materiaalit ovat vapaasti käytettävissä Taiston sivuilla, jolloin niitä voi hyödyntää myös omissa harjoituksissa: https://dvv.fi/taisto .

Huoltovarmuusorganisaation Digipoolin joka toinen vuosi järjestettävä TIETO-harjoitus kutsuu yhteen huoltovarmuuskriittisiä organisaatioita harjoittelemaan laajoja yhteiskunnan kyberturvallisuuteen kohdistuvia häiriöitä. Lisää TIETO-harjoituksesta voit lukea harjoituksen kotisivuilta: https://teknologiateollisuus.fi/digipooli/tieto/

Traficomin Kyberturvallisuuskeskuksen harjoituspalvelut tarjoavat matalan kynnyksen suunnitteluapua harjoitusten järjestämiseen ja skenaarioiden luomiseen. Traficom ylläpitää myös sivuillaan listaa kaupallisia kyberturvallisuusharjoituksia järjestävistä yrityksistä. Harjoituspalvelun tavoitat osoitteesta https://www.kyberharjoitukset.fi .

3 Kriisiviestinnän huoneentaulu

3.1 Varautuminen

- **Arvioikaa riskit:** Tunnistakaa mahdolliset kyberhäiriötilanteet ja luokaa hyvin konkreettiset toiminta- ja viestintäsuunnitelmat eri tilanteiden varalle. Huomioikaa resursointi ja viestinnän varakanavat.
- **Vastuuhenkilöt:** Määritelkää kriisiviestinnästä vastaavat henkilöt, heidän roolinsa ja vastuunsa eri tilanteisiin. Myös varahenkilöiden määrittely on keskeinen osa varautumista.
- **Tiedonkulku:** Varmistakaa, että organisaation valmius- ja varautumissuunnitelmissa on huomioitu, että viestinnän asiantuntijat ovat mukana kaikissa ryhmissä, joissa tilanteita johdetaan ja käsitellään.
- **Yhteystiedot:** Pitäkää ajan tasalla lista tärkeistä sisäisistä ja ulkoisista yhteystiedoista, kuten organisaation keskeisistä johtajista ja asiantuntijoista, sopimuskumppaneista, sidosryhmistä, mediasta ja asiakkaista. Varmistakaa, että tiedot ovat saatavilla, vaikka perinteiset käyttämänne palvelut eivät ole käytettävissä.
- **Harjoitukset:** Järjestäkää säännöllisesti kriisiharjoituksia, jotta olette valmiina toimimaan.

3.2 Kriisin alkaessa

- **Tilannekuvan arviointi:** Selvittäkää, mitä on tapahtunut ja mikä on organisaation vastuu ja rooli tilanteessa. Varmistakaa, että saatte ajantasaisen tiedon tilanteesta ja sen selvittämisestä.
- **Toimijoiden tunnistaminen:** Mitkä organisaatiot ja asiantuntijat ovat mukana tilanteen hallinnassa ja johtamisessa?
- **Viestinnän käytössä olevat kanavat ja työvälineet:** Selvittäkää, mitkä työvälineet ja kanavat ovat käytössänne. Hyödyntäkää tarvittaessa varakanavia. Muistakaa viestinnällisen yhteistyön merkitys ja mahdollisuudet.
- **Kohdeyleisöjen tunnistaminen:** Selvittäkää, mitkä ovat tapaukseen liittyvät kohdeyleisöt, joille on viestittävä ja annettava toimintaohjeita.
- **Viestintäkanavat:** Valitkaa kanavat, joilla tavoitatte kohderyhmänne tehokkaimmin, esimerkiksi sosiaalinen media, verkkosivut tai lehdistötiedotteet.

- **Viestinnän rajoitukset:** Selvittäkää, miten ja mitä voitte tilanteessa viestiä. Varmistakaa, ettei viestinnällä vaaranneta poliisin tutkintaa ja aiheuteta lisävahinkoja.

3.3 Viestinnän periaatteet

- **Avoimuus:** Olkaa rehellisiä ja läpinäkyviä. Välttäkää tietojen pimittämistä, sillä se voi vahingoittaa luottamusta ja vaarantaa organisaation toiminnan tulevaisuudessa. Älkää spekuloiko tai vähätelkö tapahtunutta.

- **Tärkeimmät kohdeyleisöt:** Tunnistakaa tärkeimmät kohdeyleisönne eli oman henkilöstönne lisäksi kaikki, joiden henkilötiedot ovat saattaneet vaarantua.

- **Johdonmukaisuus:** Varmistakaa, että kaikilla viestinnästä vastaavilla on yhtenäinen viesti. Näin vältytään ristiriitaisilta viesteiltä ja virheellisiltä ohjeistuksilta. Panostakaa viestinnän selkeyteen ja ymmärrettävyyteen. Muistakaa viestinnän säännöllisyys sekä jälkiviestinnän ja mahdollisen kansainvälisen viestinnän tarve.

- **Kuunnelkaa ja tukekaa:** Tunnistakaa kriisin vaikutus ihmisiin ja osoittakaa myötätuntoa viestinnässä.

3.4 Toiminta kriisin aikana

- **Säännöllinen viestintä:** Pitäkää kaikki, joita tilanne koskettaa, kuten mahdolliset uhrit ja muut sidosryhmät, ajan tasalla tilanteen kehittymisestä. Tuottakaa selkeitä toimintaohjeita päivittyvän tilannekuvan perusteella.

- **Vastatkaa kysymyksiin:** Valmistautukaa vastaamaan median, asiakkaiden ja yleisön kysymyksiin selkeästi, ymmärrettävästi ja rauhallisesti. Kannattaa myöntää, mikäli jokin asia ei ole vielä tiedossa, ja esittää arvio, milloin lisätietoa on mahdollisesti saatavilla. Palatkaa asiaan sovitusti myöhemmin.

- **Jakakaa oikeita tietoja:** Varmistakaa, että jaatte vain vahvistettuja ja tarkkoja tietoja. Älkää vähättelkö tapahtunutta älkääkä spekuloiko.

- **Välttäkää informaatiotyhjiön syntymistä:** Huolehtikaa siitä, että tietoa on jatkuvasti ja oikea-aikaisesti saatavilla eri kohdeyleisöille.

3.5 Kriisin jälkeen

- **Arvioikaa tilanne:** Käykää kriisi läpi organisaationne johdon ja asiantuntijoiden kanssa. Kerätkää palautetta organisaatioilta, kumppaneilta ja sidosryhmiltä, jotka ovat olleet mukana tilanteen hallinnassa. Tunnistakaa osa-alueet, joita tulisi kehittää ja toimintatavat, joita tulisi 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.

Kriisiviestintä kyberhyökkäyksessä

1 Varautuminen

Arvioikaa riskit
Tunnistakaa mahdolliset kyberhäiriötilanteet ja luokaa hyvin konkreettiset toiminta- ja viestintäsuunnitelmat eri tilanteiden varalle. Huomioikaa resursointi ja viestinnän varakanavat.

Vastuuhenkilöt
Määritelkää kriisiviestinnästä vastaavat henkilöt, heidän roolinsa ja vastuunsa eri tilanteisiin. Myös varahenkilöiden määrittely on keskeinen osa varautumista.

Tiedonkulku
Varmistakaa, että organisaation valmius- ja varautumissuunnitelmissa on huomioitu, että viestinnän asiantuntijat ovat mukana kaikissa ryhmissä, joissa tilanteita johdetaan ja käsitellään.

Yhteystiedot
Pitäkää ajan tasalla lista tärkeistä sisäisistä ja ulkoisista yhteystiedoista, kuten organisaation keskeisistä johtajista ja asiantuntijoista, sopimuskumppaneista, sidosryhmistä, mediasta ja asiakkaista. Varmistakaa, että tiedot ovat saatavilla, vaikka perinteiset käyttämänne palvelut eivät ole käytettävissä.

Harjoitukset
Järjestäkää säännöllisesti kriisiharjoituksia, jotta olette valmiina toimimaan.

2 Kriisin alkaessa

Tilannekuvan arviointi
Selvittäkää, mitä on tapahtunut ja mikä on organisaation vastuu ja rooli tilanteessa. Varmistakaa, että saatte ajantasaisen tiedon tilanteesta ja sen selvittämisestä.

Toimijoiden tunnistaminen
Mitkä organisaatiot ja asiantuntijat ovat mukana tilanteen hallinnassa ja johtamisessa?

Viestinnän kanavat ja työvälineet
Selvittäkää viestinnän käytössä olevat työvälineet ja kanavat. Hyödyntäkää tarvittaessa varakanavia. Muistakaa viestinnällisen yhteistyön merkitys ja mahdollisuudet.

Kohdeyleisöjen tunnistaminen
Selvittäkää, mitkä ovat tapaukseen liittyvät kohdeyleisöt, joille on viestittävä ja annettava toimintaohjeita.

Viestintäkanavat
Valitkaa kanavat, joilla tavoitatte kohderyhmänne tehokkaimmin, esimerkiksi sosiaalinen media, verkkosivut tai lehdistötiedotteet.

Viestinnän rajoitukset
Selvittäkää, miten ja mitä voitte tilanteessa viestiä. Varmistakaa, ettei viestinnällä vaaranneta poliisin tutkintaa ja aiheuteta lisävahinkoja.

3 Viestinnän periaatteet

Avoimuus
Olkaa rehellisiä ja läpinäkyviä. Välttäkää tietojen pimittämistä, sillä se voi vahingoittaa luottamusta ja vaarantaa organisaation toiminnan tulevaisuudessa. Älkää spekuloiko tai vähätelkö tapahtunutta.

Tärkeimmät kohdeyleisöt
Tunnistakaa tärkeimmät kohdeyleisöt, eli oman henkilöstönne lisäksi kaikki, joiden henkilötiedot ovat saattaneet vaarantua.

Johdonmukaisuus
Varmistakaa, että kaikilla viestinnästä vastaavilla on yhtenäinen viesti. Näin vältytään ristiriitaisilta viesteiltä ja virheellisiltä ohjeistuksilta. Panostakaa viestinnän selkeyteen ja ymmärrettävyyteen. Muistakaa viestinnän säännöllisyys sekä jälkiviestinnän ja mahdollisen kansainvälisen viestinnän tarve.

Kuunnelkaa ja tukekaa
Tunnistakaa kriisin vaikutus ihmisiin ja osoittakaa myötätuntoa viestinnässä.

4 Kriisin hallinta

Säännöllinen viestintä
Pitäkää kaikki, joita tilanne koskettaa, kuten mahdolliset uhrit ja muut sidosryhmät, ajan tasalla tilanteen kehittymisestä. Tuottakaa selkeitä toimintaohjeita päivittyvän tilannekuvan perusteella.

Jakakaa oikeita tietoja
Varmistakaa, että jaatte vain vahvistettuja ja tarkkoja tietoja. Älkää spekuloiko.

Vastatkaa kysymyksiin
Valmistautukaa vastaamaan median, asiakkaiden ja yleisön kysymyksiin selkeästi ja rauhallisesti. Kannattaa myöntää, mikäli jokin asia ei ole vielä tiedossa, ja esittää arvio, milloin lisätietoa on mahdollisesti saatavilla. Palatkaa asiaan sovitusti myöhemmin.

Välttäkää informaatiotyhjiön syntymistä
Huolehtikaa siitä, että tietoa on jatkuvasti ja oikea-aikaisesti saatavilla eri kohdeyleisöille.

5 Kriisin jälkihoito

Arvioikaa tilanne
Käykää kriisi läpi organisaation johdon ja asiantuntijoiden kanssa. Kerätkää palautetta organisaatioilta, kumppaneilta ja sidosryhmiltä, jotka ovat olleet mukana tilanteen hallinnassa. Tunnistakaa osa-alueet, joita tulisi kehittää ja toimintatavat, joita tulisi 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.

4 Lisätietoa

Viranomaisten tuottama opas tietomurron ja tietovuodon uhreille: https://www.suomi.fi/oppaat/tietovuoto

Valtionhallinnon tehostetun viestinnän ohje: Viestintä normaalioloissa ja häiriötilanteissa. Valtioneuvoston kanslian julkaisuja 2019:23 https://julkaisut.valtioneuvosto.fi/handle/10024/161972

Informaatiovaikuttamiseen tunnistaminen, Traficomin Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkeja-informaatiovaikuttamisen-tunnistamiseksi-ole-tarkkana-ja-toimi

Informaatiovaikuttamiseen vastaaminen - opas viestijöille. Valtioneuvoston kanslian julkaisuja 2019:11
Informaatiovaikuttamiseen vastaaminen: Opas viestijöille - Valto

Tietosuojavaltuutetun toimiston ohjeet organisaatioille tietoturvaloukkaustilanteissa: https://tietosuoja.fi/tietoturvaloukkaukset

Traficomin Kyberturvallisuuskeskuksen tuottamat ohjeet ja oppaat organisaatioille ja yrityksille: Tietoturvaohjeita yrityksille | Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978-952-311-973-4
ISSN 2669-8757 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto