KRIISIVIESTINTÄ KYBERKRIISISSÄ

Kyberkriiseihin valmistautuminen ja kriisiviestinnän harjoittelu pk-yrityksissä

Vesa Tuomala, Jouni Vaahtera & Miikka Mäkinen

XAMK
Kaakkois-Suomen ammattikorkeakoulu

Vesa Tuomala, Jouni Vaahtera & Miikka Mäkinen

KRIISIVIESTINTÄ KYBERKRIISISSÄ

Kyberkriiseihin valmistautuminen ja kriisiviestinnän harjoittelu pk-yrityksissä

XAMK KEHITTÄÄ 146

KAAKKOIS-SUOMEN AMMATTIKORKEAKOULU
KOTKA 2021

Kannen kuva: Pixabay
Taitto ja paino: Grano Oy
ISBN: 978-952-344-329-7 (PDF)
ISSN: 2489-3102 (verkkojulkaisu)
julkaisut@xamk.fi

TIIVISTELMÄ

Tämä julkaisu on perustutkimus kyberturvallisuuden kriisiviestinnän tehtävistä. Se on tarkoitettu pk-yrityksille, joiden kohderyhminä kriisiviestinnässä ovat heidän asiakkaansa ja yhteistyökumppaninsa sekä tietoturvaloukkausten uhrit.

Suomessa alle 50 hengen yrityksiä on kaikkiaan 288 481. Ne edustavat lähes 99:ää prosenttia koko kotimaisesta yrityskannasta. Näistä yrityksistä 70 prosenttia työllistää 1–3 henkilöä, joista harvalla on IT- ja tietoturvaosaamista.

Kriisiviestinnän avulla yritys suojaa mainettaan poikkeustilojen aikana. Hyvä maine ei tule itsestään, vaan se vaatii yritykseltä hyvää johtamis- ja hallintatapaa sekä eettisiä periaatteita. Maineenhallinta on jatkuvaa toimintaa ja ehkäisevää kriisiviestintää, myös sosiaalisessa mediassa. Julkaisussa pohditaan maineriskien vaikutusta yrityksen toimintaan.

Tutkimuksen tulokset on jaettu kolmeen osaan: kyberkriisin viestinnän suunnitteluun ja valmistautumiseen, kriisiviestintäsuunnitelman tekoon sekä kriisitilanteiden harjoitteluun. Pohdintaosuudessa tarkastelemme ja vertailemme tutkimustuloksia. Lisäksi olemme koonneet kyberturvallisuuden kriisiviestinnän parhaiden käytäntöjen listan.

Asiasanat: harjoittelu, kriisiviestintä, kyberturvallisuus, pk-yritykset, varautuminen

KIRJOITTAJAT

VESA TUOMALA, merikapteeni (AMK), Henley MBA, projektipäällikkö

JOUNI VAAHTERA, diplomi-insinööri, yksikönpäällikkö

MIIKKA MÄKINEN, insinööri, ylläpitopäällikkö

SISÄLLYS

TIIVISTELMÄ ... 3

KIRJOITTAJAT ... 4

1 JOHDANTO ... 6
1.1 Tutkimuksen tausta ... 6
1.2 Pienet ja keskisuuret yritykset Suomessa ... 7
1.3 Yrityksen maine ja maineenhallinta ... 7
1.4 Kriisiviestintä pk-yrityksissä ... 8
1.5 Tutkimuksen sisältö ... 8

2 MENETELMÄT ... 9

3 TULOKSET ... 10
3.1 Kyberkriisin viestinnän suunnittelu ja valmistautuminen ... 10
3.1 Vaatimukset viestinnälle ... 11
3.1.2 Kriisiviestinnän suunnittelu ... 13
3.1.3 Organisaation valmistautuminen ... 15
3.2 Kriisiviestintäsuunnitelma ... 16
3.2.1 Kriisiviestinnän sisältö ... 18
3.2.2 Kriisiviestinnän toteutus ... 18
3.3 Kriisitilanteiden harjoittelu ... 20
3.3.1 Kriisiviestinnän harjoittelu ... 20
3.3.2 Kyberkriisien viestinnän harjoittelu ... 23

4 POHDINTA ... 26
4.1 Parhaat käytännöt kyberturvallisuuden kriisiviestintään ... 27
4.2 Johtopäätökset ... 29
4.3 Ehdotukset jatkosuunnitelmia varten ... 29

LÄHDELUETTELO ... 30

LIITTEET ... 33

1 JOHDANTO

Tämä julkaisu on perustutkimus kyberturvallisuuden kriisiviestintään valmistautumisesta ja sen harjoittelusta.

Tutkimuksen kohderyhmänä ovat pienet ja keskisuuret yritykset (pk-yritykset) sekä muut pienet organisaatiot, joiden kriisiviestinnän kohteina ovat heidän asiakkaansa ja yhteistyökumppaninsa sekä tietoturvaloukkausten uhrit. Tämä julkaisu on kirjoittajien näkemys kriisiviestinnän tehtävistä, joita pk-yritysten tulee valmistella ja harjoitella ennen kyberhyökkäyksiä tai poikkeustapahtumaa.

Julkaisu on kirjoitettu pk-yritysten lisäksi opetus- ja kulttuuriministeriön rahoittaman korkeakouluyhteistyöhankkeen, autonomisen merenkulun koulutusverkoston (AutoMare EduNet), tarpeisiin.

Autonomisen merenkulun koulutusverkoston tavoitteena on meriklusterin kilpailukyvyn edistäminen sekä korkeakoulujen monitieteellinen yhteistyö, tiedonvaihto ja verkostoituminen. Kohderyhmänä ovat koko Suomen meriklusteri ja alan opiskelijat. Hanke keskittyy kyberturvallisuuden lisäksi teknologian kehityksen, IT-taitojen ja automaation haasteisiin. Tulevaisuuden toimintaympäristöt, käytännöt, lainsäädäntö ja muuttuvien liiketoimintamallien ymmärtäminen luovat haasteita turvallisuuden ja ilmastokysymysten hallintaan.

AutoMare EduNet -hankkeen yhteistyökumppaneina toimivat Xamkin lisäksi Aalto-yliopisto, Satakunnan ammattikorkeakoulu, Turun ammattikorkeakoulu, Turun yliopisto, Yrkeshögskolan Novia (Aboa Mare) sekä Åbo Akademi.

1.1 TUTKIMUKSEN TAUSTA

Julkaisun kirjoittajilla on laaja asiantuntemus eri tehtävistä teollisuuden, liiketoiminnan ja julkishallinnon aloilta. Kirjoittajia yhdistää tuote- ja palvelukehityksen lisäksi kiinnostus informaatio- ja viestintätekniikan kyberturvallisuuden kehittämiseen.

Kirjoittajien välisissä keskusteluissa oli aiemmin noussut aiheeksi tämänhetkinen tarve yhdistää kyberturvallisuuden ja kriisiviestinnän asiat. Alustavassa selvityksessä suomenkielisiä julkaisuja todettiin olevan yllättävän vähän, joten yhteinen toteama oli tutkia tätä tärkeää asiaa. Tutkimuksen aiheeksi valittiin pk-yritysten kriisiviestintäkyky kyberkriisitilanteissa. Keskustelujen jälkeen kirjoittajat totesivat, että kyberkriisin kriisiviestintään kuuluu suunnittelun ja valmistautumisen lisäksi tärkeänä osana viestinnän harjoittelu. Pohdinnan aiheena oli myös pk-yritysten osaamisen yleinen taso sekä kriisiviestinnän että kyberturvallisuuden osalta.

Suomen tunnetuin kohdistettu kyberhyökkäys ja tietovuoto lienee tällä hetkellä Psykoterapiakeskus Vastaamon tapaus. Sinne hyökättiin vuosina 2018 ja 2019, mutta tieto tapahtuneesta tuli julkisuuteen vasta lokakuussa 2020. Tämä herätti myös julkaisun kirjoittajat yhdistämään osaamisensa pk-yrittäjien tietoturvallisuuden lisäämiseksi ja parhaiden käytäntöjen (engl. Best Practices) kehittämiseksi kyberturvallisuuden kriisiviestintään.

Tässä johdanto-osassa avaamme myös tutkimuksessamme esiintyviä termejä.

1.2 PIENET JA KESKISUURET YRITYKSET SUOMESSA

Suomessa on yrityksiä kaikkiaan 292 377. Niistä alle 10 hengen mikroyrityksiä on 271 851 kappaletta (93 prosenttia, 2019) ja alle 50 hengen pienyrityksiä 16 630 kappaletta (5,7 prosenttia, 2019). Yrittäjistä 68 prosenttia on yksinyrittäjiä. Kotimaisista yrityksistä 70 prosenttia työllistää 1–3 henkilöä, joista harvalla on IT- ja tietoturvaosaamista (Kyberturvallisuuskeskus 2019; Suomen Yrittäjät 2021).

Tilastokeskus määrittelee pk-yrityksiksi alle 250 työntekijän yritykset, joiden liikevaihto ei ylitä 50:tä miljoonaa euroa tai joiden taseen loppusumma on alle 43 miljoonaa euroa. Riippumattomuuden perusteella pk-yrityksen pääomasta tai äänivaltaisista osakkeista ei tule olla yli 25:tä prosenttia yhden tai useamman sellaisen yrityksen (yhteis)omistuksessa, jota ei pidetä pienenä tai keskisuurena yrityksenä. (Tilastokeskus 2021.)

1.3 YRITYKSEN MAINE JA MAINEENHALLINTA

”Mainetta voi hallita, ihmistä ei” -sanonta tarkoittaa, että hyvin hallittu maine voi pelastaa tilanteen ennakoimattoman asian tapahduttua. Yrityksen mainetta voidaan pitää suojakilpenä huonoja uutisia vastaan. Hyvämaineisen yrityksen sidosryhmistä vain 25 prosenttia uskoo negatiivisen uutisen kuultuaan sen ensimmäisen kerran. Vastaavasti huonomaineiseen yritykseen liittyvän negatiivisen uutisen uskoo 57 prosenttia sidosryhmistä. Hyvän maineen perustekijät ovat yrityksen johtamistapa, eettiset periaatteet ja hyvä hallintotapa sekä yrityksen tuottamat palvelut ja tuotteet. Yrityksen kyky muuttaa ja kehittää vastuullisesti visiotaan, strategiaansa ja julkista kuvaansa on entistä tärkeämpää – riskienhallinnan lisäksi. Maineenhallinta on jatkuvaa toimintaa ja ehkäisevää kriisiviestintää, jota tehdään, jotta yritys vaikuttaisi uskottavalta ja luotettavalta myös kriisin aikana. Digitaalisuus kasvattaa maineenhallinnan merkitystä sosiaalisen median kanavissa. Sosiaalisen median merkitys yrityksen olemassaolon ja menestyksen elinehtona on lisääntynyt. Katastrofin sattuessa hyvin hallittu maine auttaa yritystä selviytymään kriisistä; yritystä pidetään luotettavana ja vahinko annetaan anteeksi. (Eisto 2020; Kinturi 2018; Piha & Vesanen 2014.)

1.4 KRIISIVIESTINTÄ PK-YRITYKSISSÄ

Maineriskejä tulee analysoida, kartoittaa ja mitata. Maineen saadessa kolhuja tilanne tulee hoitaa mahdollisimman nopeasti ja tehokkaasti kriisiviestinnän avulla. Yrityksellä tulee olla kriisiviestintävalmiudet maineriskien estämiseksi sekä suunnitelma, kuinka viestinnässä reagoidaan ja kommunikoidaan kriisin ratkaisemiseksi nopeasti. Kriisiviestinnän lisäksi yrityksen tulee muuttaa omia prosessejaan ja parantaa toimintaansa tapahtuman jälkeen. Lisäksi tulee selvittää, kuinka paljon vahinkoa kriisistä aiheutui. Kriisiviestinnän ja maineenhallinnan avulla suojellaan yrityksen aineetonta pääomaa eli goodwill-arvoa. (Kinturi 2018.) Tarve huolehtia kriisiviestinnästä korostuu pk-yrityksillä, koska ne ovat erityisen herkkiä poikkeustilanteiden aiheuttamille taloudellisille ja maineeseen vaikuttaville kolhuille.

1.5 TUTKIMUKSEN SISÄLTÖ

Tutkimuksen tulokset on jaettu kolmeen osaan: kyberkriisin viestinnän suunnitteluun ja valmistautumiseen, kriisiviestintäsuunnitelman tekoon sekä kriisitilanteiden harjoitteluun.

Sisällön jakamisella pyrimme esittämään lukijalle selkeän polun siitä, mitä kaikkea tulee huomioida varauduttaessa ja valmistauduttaessa maineenhallinnan kriisiviestintään ennen kyberhyökkäystä. Pohdintaosuudessa tarkastelemme tutkimustuloksia ja vertailemme niiden merkitystä toisiinsa. Artikkelin kirjoittajien parhaat käytännöt edustavat kriisiviestinnän tehtäviä ennen kyberkriisiä ja sen aikana sekä hyökkäyksen jälkeen tapahtuvia toimintoja.

Johtopäätöksessä esitämme näkemyksen seuraavista askeleista turvallisempaan kybertulevaisuuteen.

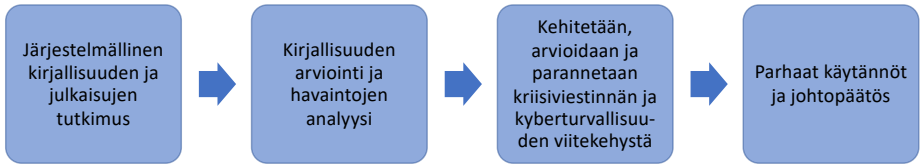
2 MENETELMÄT

Tutkimus toteutettiin kirjallisuustutkimuksena, ja tutkimusmenetelmänä oli julkisten lähteiden käyttö. Tietoa löydettiin viranomaisten, yliopistojen ja korkeakoulujen, tutkijoiden, toimittajien sekä konsultointiyrityksien lähteistä. Kirjoittajat kuitenkin totesivat, että kyberturvallisuuden kriisiviestinnästä löytyi vain hyvin vähän pk-yrityksien käyttöön tarkoitettuja ohjeita tai parhaita käytäntöjä (engl. Best Practices).

Tämä tutkimus keskittyy kriisiviestinnän valmisteluun ja harjoitteluun ennen kyberhyökkäystä.

- **Tutkimuskysymys: Voiko kriisiviestintää harjoitella menestyksekkäästi etukäteen?**

Tutkimuskysymyksen asettelu on päätetty FINER-menetelmällä (Feasible, Interesting, Novel, Ethical, Relevant). Se tarkoittaa, että tutkimuksen tulee olla laadullista sekä mahdollista, mielenkiintoista, uudenlaista, eettisesti toteutettua ja asiaankuuluvaa. Tekstin tulee pohjautua tietoon ja tulevaisuuden tutkimukseen. Viitekehyksen mallina käytetään seuraavaa kaaviota:



- **Tutkimuksen hypoteesi on, että pienillä organisaatioilla ei ole keinoja eikä välineitä kriisiviestintään valmistautumista varten.**

Hypoteesina on oletus, että pk-yrityksillä ei ole kriisiviestintään riittävästi osaamista eikä keinoja. Pk-yrityksien työntekijöiden tietoa ja valistusta viestinnästä ennen kyberhyökkäyksiä ja niiden aikana sekä siitä, mitä tulee tehdä hyökkäyksen jälkeen, on lisättävä.

3 TULOKSET

3.1 KYBERKRIISIN VIESTINNÄN SUUNNITTELU JA VALMISTAUTUMINEN

Yhdysvaltain keskusrikospoliisin FBI:n johtajan James Comeyn sanoin: ”Yhdysvalloissa on kahdenlaisia suuryrityksiä: ne, joihin on murtauduttu… ja ne, jotka eivät tiedä, että niihin on murtauduttu.” (DiStaso 2018.)

Kyberturvallisuus ei ole nykyisin pelkästään IT-osaston huolenaihe. Brändin maine on tärkeä osa menestystä, ja sitä on vaikea korjata, jos yrityksen maine vahingoittuu. Kyberhyökkäyksen uhreina ovat yrityksen lisäksi asiakkaat, sillä varastetut tiedot altistavat heidät henkilöllisyysvarkauksille ja taloudellisille vahingoille. Kyberturvallisuus suhdetoiminnassa on viime kädessä riskien hallintaa. (DiStaso 2018.)

Kriisi aiheuttaa merkittävän uhan toiminnalle tai maineelle. Mikäli kriisiä ei käsitellä oikein, sillä on negatiivisia seurauksia. Organisaation kohtaamat kriisit jaetaan kahteen kategoriaan: operatiivisiin ja maineenhallinnan kriiseihin. Operatiiviset kriisit häiritsevät toimintaa tai uhkaavat turvallisuutta. Sellaisia ovat muun muassa luonnonkatastrofit, teollisuus- ja kuljetusonnettomuudet, kemikaalipäästöt, tulipalot, räjähdykset ja tuotevahingot. Myös rikokset tai vaikkapa henkilökunnan väärinkäytökset voivat aiheuttaa operatiivisen kriisin. Maineenhallintakriisit puolestaan aiheuttavat vahinkoa organisaation maineelle. Niitä voivat aiheuttaa muun muassa johdon vastuuton käytös ja sidosryhmiä loukkaava viestittely. (Coombs 2014.) Kyberkriisi voi olla luonteeltaan sekä operatiivinen että maineenhallinnan kriisi.

Organisaation tulee valmistautua sitä uhkaavien kriisien hallintaan. Kriisiviestintä on keskeinen osa kriisinhallintaa. Kriisiviestinnällä on kolme tärkeää tehtävää: oikea-aikainen viestinvälitys, väärän ja virheellisen tiedon torjuminen sekä uhrien tukeminen. Organisaation vahingot ovat vähäisemmät sen viestiessä nopeasti ja aktiivisesti. Tässä tehtävässä sosiaalinen media on tehokas, ajasta riippumaton julkaisukanava. Kriisiviestinnässä tulee painottaa uhrien tietotarpeita ja organisaation keinoja auttaa heitä. Jos kriisi johtuu virheellisistä tiedoista (huhuista), organisaation tulee reagoida aggressiivisesti valheellisen tiedon korjaamiseksi ja kieltää se. Sosiaalisen median kriisit joudutaan käsittelemään julkisesti, mikä vaatii usein kykyä vuorovaikutukseen sosiaalisissa kanavissa. (Coombs 2014.)

3.1 VAATIMUKSET VIESTINNÄLLE

Teknologian kehittyessä useat organisaatiot digitalisoivat toimintojaan. Yhteiskunnan jatkuvasti lisääntyvä riippuvuus tieto- ja viestintäverkoista mahdollistaa laajamittaisia häiriöitä jopa yli kansallisten rajojen. Kyberhyökkäysten todennäköisyys on lisääntynyt, joten organisaation tulee tietää, kuinka tehdään parhaiten kriisiviestintää ja suhdetoimintaa hyökkäyksen jälkeen ottamalla huomioon asiakkaat, kumppanit ja sidosryhmät. Häiriötilanteesta tiedottaminen on laaja-alaista työtä, johon saattaa osallistua eri tiedotusvälineitä, yksityisiä kyberturvallisuusyrityksiä, muiden maiden tiedustelupalveluita ja erilaisia organisaatioita. Kyberhyökkäyksen jälkeen tärkeää on julkinen viestintä tapahtuman käsittelemiseksi ja mahdollisen yrityskriisin hallitsemiseksi. Organisaation kyberturvallisuuskriisi voi saada aikaan huomattavan mainevahingon, ja tällä on suora yhteys organisaation osakkeiden arvonmääritykseen. Julkinen spekulaatio ja väärinkäsitykset voivat lisääntyä myös yleisen tiedon puutteesta. (Agrafiotis ym. 2018; Knight & Nurse 2020; Turell ym. 2020; Wang & Johnson 2018.)

Viestinnän tehtävä on ohjeistaa organisaatiota poikkeustilanteessa, varmistaa oman viestin perillemeno, lisätä ymmärrystä ja antaa myötätuntoa asianomaisille. Viestin sisältö tulee miettiä huolellisesti ennen julkaisua. Tutkimuksen mukaan viestinnän pelisäännöt ovat selkeät: myönnä vastuu ottamalla tietovuoto vakavasti ja ole empaattinen ja selkeä viestinnässä. Palveluntarjoajien tai hyökkäävän ryhmittymän syyttäminen ei tuota viestinnällisesti onnistunutta tulosta. Oppien jakaminen tietovuodosta saattaa estää muita organisaatioita joutumasta kyberhyökkäyksen kohteeksi. (Knight & Nurse 2020; Valtioneuvoston kanslia 2019.)

Timothy Coombsin maineenhallintateoria (The Situational Crisis Communication Theory, SCCT) on usein käytetty menetelmä maineen suojaamiseksi kriisin aikana. SCCT on ohjeellinen järjestelmä kriisinhallintastrategioiden sovittamiseksi kriisitilanteeseen. Siinä on kolme ensisijaista reagointistrategiaa kriisin aikana ja sen jälkeen käytettäviksi: kieltäminen, vähättely ja jälleenrakentaminen. Kieltämisstrategiassa kielletään kriisin olemassaolo tai etsitään syntipukki, jos kriisistä ei ole näyttöä. Vähättelystrategiassa kriisin laajuutta vähätellään ja organisaation vastuu kriisistä kierretään. Jälleenrakennusstrategiassa tarjotaan korvauksia tai anteeksipyyntöjä kriisistä. Jos kriisissä on useita osapuolia, vähemmän tärkeä organisaatio voidaan uhrata arvokkaampien tai kannattavampien organisaatioiden suojelemiseksi. Syntipukkiteorian käytössä on havaittu suuttumuksen lisääntyvän, mikäli organisaatio kieltää vastuunsa mutta sen kuitenkin todetaan jälkikäteen olleen vastuussa tapahtumasta. Tärkeää on tiedostaa tiedotusvälineiden rooli julkisen käsityksen muodostumisessa: käyttäjät pitävät organisaatiota yleensä syyllisenä saadessaan tiedon tietoturvaloukkauksesta median välityksellä. Muita kriisiviestintästrategioissa käytettyjä työkaluja ovat Kim Witten kehittämä Extended Parallel Processing Model (EPPM) sekä David Bussin ja Martie Haseltonin Error management theory (EMT) -teoriamallit. (Knight & Nurse 2020; Wang & Johnson 2018.)

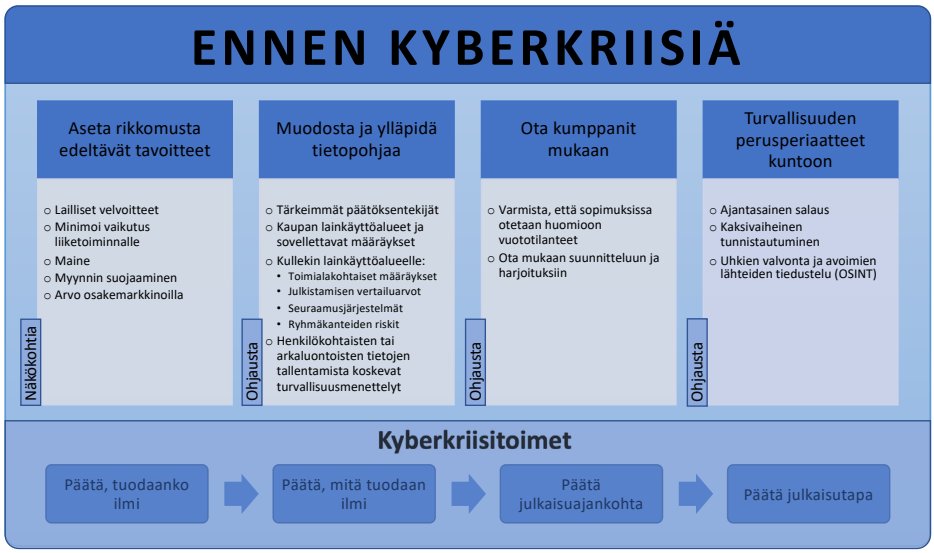
Viestinnän näkökulmasta erilaisista tietoturvapoikkeamista tulee ilmoittaa viranomaisille tietyn ajan kuluessa: 24 tai 72 tunnin kuluttua tapahtumasta tai viipymättä. Tiedottamiseen ja tiedonvaihtoon liittyy erityyppisiä vaatimuksia, kuten kuvasta 1 voi todeta. (Valtiovarainministeriö 2017.)

Tieto	Kenelle ilmoitetaan	Aika	Peruste
Kansainväliseen turvaluokiteltuun tietoon kohdistunut väärinkäytös	Kansallinen turvallisuus-viranomainen (UM/NSA) NSA@formin.fi http://formin.finland.fi/Public/default.aspx?nodeid=41940	24 h sisällä	Neuvoston turvallisuusmääräys
Henkilötietoihin kohdistunut väärinkäytös	Kansallinen valvontaviranomainen (tietosuojavaltuutettu)	72 h sisällä	EU:n tietosuoja-asetus, velvoittava 25.5.2018 jälkeen
Varoihin tai omaisuuteen kohdistunut väärinkäytös	Valtiontalouden tarkastusvirasto http://www.vtv.fi/toiminta/kantelut_ja_vaarinkaytokset/vaarinkaytoksesta_ilmoittaminen	Viipymättä	Laki (676/2000) 16 § VTV:n ohje 15.10.2003
Vakoilun tai törkeän vakoilun ilmoittaminen	Poliisi tai uhan kohde https://asiointi.poliisi.fi/	Viipymättä	Rikoslaki 15 luku, 10 §
Organisaatioon kohdistunut tietoturvaloukkaus	Viestintäviraston Kyberturvallisuuskeskus cert(at)ficora.fi https://www.viestintavirasto.fi/asioikanssamme/ilmoituksetjamuutlomakkeet/tietoturvailmoituksetja-hakemukset/ilmoitustietoturvaloukkauksesta.html		
Kriittiset, yli organisaatiorajojen vaikuttavat tietoturvatapahtumat	VIRT (Virtual Incident Response Team)		
Kriittiset, yli organisaatiorajojen vaikuttavat tietoturvatapahtumat	Valtorin SSOC-toiminto (Security and Service Operations Center)		

Kuva 1. Tietoturvapoikkeamista ilmoittaminen viranomaisille (Valtiovarainministeriö 2017).

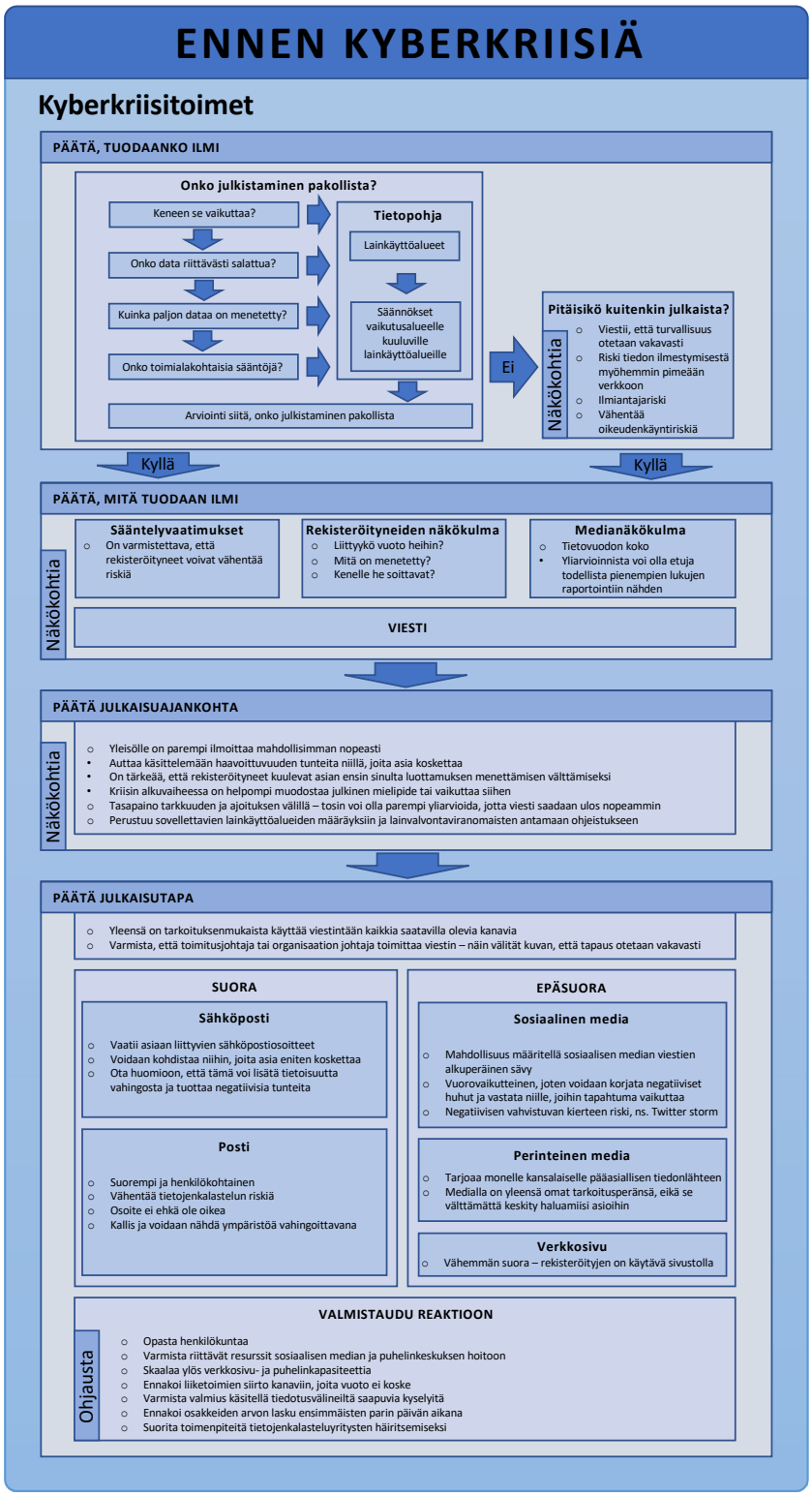
3.1.2 KRIISIVIESTINNÄN SUUNNITTELU

Kriisiviestinnän tutkimuksessaan Knight ja Nurse (2020) esittelevät viestinnän varautumismallin, joka määrittelee tarvittavat toimet, kun valmistaudutaan reagoimaan kyberhyökkäykseen (ks. kuva 2). Organisaation varautuessa viestintään kyberhyökkäystilanteessa sen tulee ottaa huomioon omien viestinnällisten tavoitteidensa lisäksi lainsäädännön vaatimukset, sidosryhmien tarpeet sekä tietoturva ja tietosuoja.



Kuva 2. Viitekehys tehtävistä ennen kyberkriisiä (Knight & Nurse 2020).

Tietovuodon tapahduttua viestinnän ohjeistuksen tulee olla selvää ja ennalta harkittua. Kriisiviestinnän mallissa tutkijat esittävät päätöksentekohetket askel askeleelta helpottaakseen organisaatiota päättämään, informoiko se ylipäätään vuodosta ja jos informoi, mitä se kertoo julkisuuteen, milloin ja miten (ks. kuva 3). Tehokkaat viestintästrategiat auttavat palauttamaan toivotun yrityskuvan, rakentamaan asiakkaiden luottamuksen yritykseen uudelleen ja minimoimaan sekä välittömät että välilliset tappiot. (Knight & Nurse 2020; Wang & Johnson 2018.)



Kuva 3. Viitekehys tehtävistä ennen poikkeustilannetta ja tietovuodon tapahtumista (Knight & Nurse 2020).

3.1.3 ORGANISAATION VALMISTAUTUMINEN

Kyberhäiriöiden lisääntyessä tiedonvaihdon ja koordinoinnin eri yrityksien välillä tulee olla tehokasta. Tämä myös kehittää sisäistä yhteenkuuluvuutta ja helpottaa ulkoisen tiedon jakamista. Erityisen tärkeää tämä on sidosryhmien kesken. Luottamusta tulee rakentaa ja ylläpitää organisaatioiden välisellä viestinnällä, koordinoinnilla ja raportoinnilla. Yhteistoimintaa voi kehittää myös harjoituksilla ja yhteisellä koulutuksella. Toiminnan tulee mahdollistaa yksityisen ja julkisen sektorin sekä viranomaisten yhteistyö. Viestintästrategioita ennakoimalla ja tosiasioihin pohjautuvaa tietoa tarjoamalla voidaan sopia viestinnän roolijako. Tilannetietoisuus sekä tapahtumien analysointi ja arviointi mahdollistavat ennakoidut toimintavaihtoehdot yhteistyössä viranomaisten, armeijan, tiedustelupalvelun ja eri lainvalvontaorganisaatioiden kanssa. (Turell ym. 2020.)

Kyberturvallisuusalalla on tällä hetkellä kasvavaa kysyntää pätevälle työvoimalle, jolla on hallussaan myös viestinnän osaaminen. Näitä taitoja tulisi sisällyttää opetussuunnitelmiin ja alan kursseihin oppilaitoksissa. Julkisen viestinnän osaamista tulisi myös arvioida kyberhäiriöiden torjunnassa ja käsittelyssä. (Wang & Johnson 2018.)

Riippumatta kyberhyökkäyksen laadusta yrityksen on otettava yhteyttä sidosryhmiinsä eli työntekijöihinsä, osakkeenomistajiinsa ja asiakkaisiinsa. Maineriski on otettava oma-aloitteisesti, sillä sosiaalisessa mediassa tieto leviää nopeasti ja helposti. Luottamuksen menetystä ja vaikutusta sidosryhmäsuhteisiin voi olla vaikea korjata. Yrityksille suurin vahinko kyberhyökkäyksistä voikin olla juuri maineen menetys. Viestinnän haasteet ovat seuraavat (DiStaso 2018):

- **Kyberturvallisuus vaatii riskinhallintakulttuuria**

Yritystoiminnassa on mahdollista menettää maine. Ennalta tehtävä organisaation riskinarviointi selvittää tason, jonka yritys on valmis sietämään sidosryhmien luottamuksen ja uskollisuuden menetyksenä tietoturvaloukkauksissa. Kriisisuunnitelmat on päivitettävä säännöllisesti. Viestinnän roolin tulee olla kaikissa suunnitelmissa selkeä jo ennen kyberhyökkäystä.

- **Kyberturvallisuutta ei voi omistaa mikään organisaation yksikkö**

Johtajien lisäksi eri yksiköiden, kuten IT-, laki-, tuotanto-, viestintä- ja muiden osastojen, tulee tunnistaa yhdessä hyökkäyksen mahdolliset varoitussignaalit.

- **Yhteisö vastaa kyberturvallisuudesta**

Kyberturvallisuuden heikoin lenkki on ihminen; osa tietoturvavuodoista on seurausta inhimillisistä virheistä. Kyberhyökkäykset voivat olla helpommin estettävissä, jos ihmiset

ymmärtävät vaarantavansa organisaation toiminnan sosiaalisessa mediassa ja verkossa. Kyberturvallisuuteen kohdistuu organisaatioissa selvää koulutusvajetta.

- **Verkkohyökkäykset muuttuvat alituisesti**

Teknologian kehittyessä myös kyberhyökkäykset kehittyvät. Yritykset saavat harvoin hengähdystaukoja hyökkäysten määrän jatkuvasti kasvaessa.

- **Tilannekuva on olennaisesti tärkein**

Organisaatio ei välttämättä tiedä olleensa tietoturvahyökkäyksen kohteena päivien, viikkojen tai jopa kuukausien ajan. Hyökkäyksen jälkeen maineen kannalta tärkeää on, että johtoryhmä käsittelee asian ja tietoturva korjataan. Uutiset leviävät nopeasti, joten myös vastaamisen tulee olla nopeaa. Varhainen viestintä vaikuttaa voimakkaasti tiedotusvälineiden ja sidosryhmien reaktioihin. Viestinnän tulee keskittyä sidosryhmään, jonka tulee saada tiedot suoraan ja avoimina faktoina.

3.2 KRIISIVIESTINTÄSUUNNITELMA

Johtaminen, viestintä ja toimintatavat korostuvat poikkeustilanteessa. Häiriötilanteessa tarvitaan normaalia enemmän viestintää, joka on avointa, ymmärrettävää, luotettavaa, selkeää ja yhdenmukaista. Poikkeamatilanteiden varalta organisaatiossa tulee olla erillinen viestintäsuunnitelma, joka kertoo, mitä ja miten sisäistä ja ulkoista viestintää toteutetaan. Suunnitelmassa ennakoidaan, kenen vastuulla viestintä on ja kuka tulee viestimään sekä miksi, kenelle ja milloin tapahtuneessa poikkeamatilanteessa viestitään. Käytettävät mediat valitaan poikkeaman kohderyhmien, vaikutusten ja laajuuden sekä käytettävissä olevien viestintätapojen perusteella. Kriisiviestintäsuunnitelmaan voidaan liittää ohjeita käytännön toimista, erilaisia toiminta- ja tarkistuslistoja, valmiita mallipohjia sekä yhteystietoja sidosryhmille, yhteistyökumppaneille ja median edustajille. Vastuiden jakaminen organisaation, sidosryhmien ja yhteistyökumppaneitten välillä on tärkeä osa varautumista. Viestinnän vastuun tulee kuitenkin olla vain yhdellä henkilöllä. Kriisiviestintäsuunnitelmaa voidaan testata toiminnallisessa kyberturvallisuusharjoituksessa. (Management Institute of Finland 2019; Valtiovarainministeriö 2017; Vertainen ym. 2020.)

Viestintästrategian noudattamiseksi tulee olla viestintäsuunnitelma. Sen on oltava kaikkien tarvitsevien tiedossa ja saatavilla, myös paperisena versiona. Kuvassa 4 on esimerkki VAHTI-ohjeistuksen viestintäsuunnitelman rungosta. (Valtiovarainministeriö 2017.)

Aihe ja tavoitteet

Kuvaus viestinnän aiheesta ja tavoitteista: viestintäsuunnitelman tarkoituksena on varmistaa, että organisaation viestimät tiedot ovat tarkkoja, oikea-aikaisia ja johdonmukaisia.

Kohderyhmät

Määrittely viestinnän kohteista (oma organisaatio, yhteistyökumppanit, viranomaiset, kansalaiset, media). Poikkeamista tiedotetaan pääsääntöisesti vain niitä, joiden toimintaan, oikeuksiin tai tietosuojaan poikkeama vaikuttaa.

Määritelmä siitä, minkälaista tietoa eri kohderyhmälle voidaan toimittaa. Tiedottamisessa on huomioitava tietojen salassapitovaatimukset.

Viestintäsuunnitelmassa on huomioitava eri kohderyhmien tiedottamisessa
- yhteystiedot ja toimintavalmius virka-aikana ja sen ulkopuolella
- mahdollisten salausavainten luominen ja toimittaminen suojattua yhteydenpitoa varten
- päätöksenteko- ja viestintämalli tilanteissa, joissa tietoturvapoikkeama koskee useampaa tahoa.

Viestintävälineet

Kuvaus siitä, minkälaisia kanavia viestinnässä käytetään. Viestintäkanavia voivat tilanteen mukaan olla mm.
- puhelin
- kirjalliset tiedotteet
- ilmoitustaulut
- suullinen informaatio
- tiedotusvälineet (TV, radio, sanomalehdet)
- sähköposti / sähköpostilistat
- tekstiviestit
- sähköiset ilmoitustaulut (esim. intranetissä)
- käyttöjärjestelmän sisäiset tiedotteet (esim. käyttäjän tietokoneen työpöydälle ilmestyvä tiedote)
- verkkosivut
- pikaviestimet
- sosiaalinen media (Facebook, Twitter tms.)

Myös viestintävälineiden toimimattomuuteen on varauduttava ja määriteltävä viestintäkanaville varajärjestelyt.

Organisaatio, roolit ja vastuut

Kuvaus viestintäorganisaation rakenteesta varahenkilöineen sekä siitä, mitä rooleja kullakin organisaation jäsenellä on. Määrittely siitä, kuka päättää viestinnän sisällöstä ja ajankohdasta.

Erityisvaatimukset

Poikkeamaviestinnän erityisvaatimukset esimerkiksi luottamuksellisen tiedon tai sopimusvelvoitteiden suhteen.

Viestintäsuunnitelmaan on syytä kuvata lähetettävistä tiedotteista ja muista viesteistä luonnokset, joita voidaan poikkeamatilanteessa helposti täydentää.

Kuva 4. Esimerkki tietoturvapoikkeamien viestintäsuunnitelman rungosta (Valtiovarainministeriö 2017).

3.2.1 KRIISIVIESTINNÄN SISÄLTÖ

Hyvä johtaminen, tilannekuva, kriisiviestintä, tiedon jakaminen, toiminnan jatkuvuus ja yhteistoiminta ovat varautumisen ja valmiuden kiinteitä osia (Lehto ym. 2018).

Kriisiviestinnässä nopean reaktion lisäksi on tärkeää ymmärtää tilannekuva: miten kriisi on syntynyt, mitä on tapahtunut, mitä tehdään ensimmäisinä toimenpiteinä ja mitä tehdään seuraavaksi. Sisäisen tiedottamisen ei tule hidastaa tietoturvapoikkeaman selvittämistä. Ulkoisille sidosryhmille tiedotetaan asiantuntevasti ja viestintäsuunnitelman mukaisesti: mitä kerrotaan julkisuuteen, kuka edustaa televisiossa ja eri medioissa sekä kuka kertoo asiasta sosiaalisessa mediassa. Kyberhäiriötilanteessa erityisesti sosiaalisen median merkitys on keskeinen. (Management Institute of Finland 2019; Traficom 2019; Valtiovarainministeriö 2017.)

Kuvassa 5 havainnollistetaan prosessi turvallisuuspoikkeaman toteutuessa. Se sisältää kriisivalmiuden, tapahtuman, tilannekuvan sekä poikkeamasta aiheutuvat tapahtumat, sen ratkaisemisen ja jälkihoidon (Management Institute of Finland 2019).

Kuva 5. Kriisiviestinnän tehtävät kyberturvallisuuspoikkeaman aikana ja sen jälkeen (Management Institute of Finland 2019).

3.2.2 KRIISIVIESTINNÄN TOTEUTUS

Viestintä on aina osa häiriötilanteen johtamista, ja siihen tulee varautua etukäteen. Maineenhallintaa varten tulee ensin määritellä organisaation arvot ja pääviesti, tavat toimia ja se, kuka antaa haastattelut. Määrittely voidaan toteuttaa organisaation järjestämässä kahden päivän suunnittelutyöpajassa, jossa on paikalla 2–6 henkilöä johtoryhmästä ja ydinhenkilöistä. Työpajojen kesto voi olla noin 2–3 tuntia kerrallaan. Suunnitelmassa tulee käsitellä kyberhyökkäyksen aikana maineenhallinnalle saavutettavaa aikaa ja jatkuvuutta sekä sisällöntuotannon samankaltaisuutta poikkeaman hallitsemiseen. Kriisivalmiutta voidaan pitää

yllä vuorokauden ympäri päivystysvuoroittain, myös viestinnän osalta. Kriisitapahtuman ensi minuuteille voidaan laatia tarkistuslista nopeaa käynnistämistä varten. Listan runko voi olla esimerkiksi seuraavanlainen (Eisto 2020; Management Institute of Finland 2019; Vertainen ym. 2020):

- lyhyt kuvaus tapahtuneesta johdolta tai vastaavalta
- avainhenkilöiden hälytyskanavana ennalta sovittu pikaviestipalvelu tai tekstiviestiryhmä
- eri skenaarioille tarkoitettujen tiedotepohjien oltava valmiina
- otettava huomioon sekä sisäinen että ulkoinen viestintä
- viestinnän päälinjojen valitseminen eri skenaarioista: kuka, mitä, keille, miten ja milloin tiedotetaan
-
- kanavien käyttötaidot ja -oikeudet oltava oikeilla henkilöillä
- kutsutaan eri alueiden viestintävastaavat koolle tai puhelinpalaveriin
- perustetaan viestintäkeskus
- pidetään sisäinen tiedotustilaisuus ja käynnistetään työyhteisöviestintä
- aktivoidaan kriisiviestintäsivut internetiin ja hyödynnetään digitaalista viestintää
-
- informoidaan puhelinvaihteet
- informoidaan sidosryhmiä ja yhteistyökumppaneita
- kanavoidaan median kyselyt ja haastattelupyynnöt oikeille henkilöille
- valmistellaan mediatilaisuus
- laaditaan ja tarkastetaan tiedote sekä päätetään sen jakelu
-
- järjestetään uutisoinnin seuranta ja analyysi
- monitoroidaan sosiaalisen median keskusteluita
- eri skenaariot päättyvät eri tavalla viestinnän näkökulmasta
- lopetetaan aktiivivaiheen toiminnot
- dokumentoidaan kriisitapahtuman viestintä ja toimenpiteet.

3.3 KRIISITILANTEIDEN HARJOITTELU

Kyberharjoitus on harjoitustapahtuma, jossa organisaatio mallintaa ja testaa varautumistaan erilaisiin kyberhäiriöihin. Kriisiviestintäsuunnitelman toimivuutta voidaan testata käytännössä osana muuta toiminnallista kyberturvallisuusharjoitusta. Harjoituksella tarkoitetaan organisaatiota potentiaalisesti kohtaavan kriisitilanteen fiktiivistä mallintamista tarkoitukseen parhaiten soveltuvalla tavalla. Harjoituksessa organisaation toimintoja sovitetaan yhteen kuten tosielämässä, jolloin kokonaisuus vahvistuu eri osien yhteistoiminnassa. Yleisimmät tavat harjoitella ovat seuraavat (Traficom 2019; Vertainen ym. 2020):

- työpöytäharjoitus kyberhäiriöiden hallintaan, johtamiseen, prosessien läpikäyntiin ja arviointiin
- juurisyyharjoitus (pre-mortem) ongelmien ennakointiin ja riskienhallinnan suuntaamiseen
- toiminnallinen harjoitus kriisijohtamisen harjoittelua, kriisiviestinnän harjoittelua ja yhteistoimintaharjoittelua varten
- tekninen harjoitus teknisten valmiuksien korottamiseen, järjestelmiin perehtymiseen ja palautumistesteihin
- Capture The Flag (CTF) -harjoitus teknisen osaamisen kehittämiseen ja järjestelmiin tutustumiseen
- suuret yhteisharjoitukset verkostojen luomiseen, yhteistoiminnan vahvistamiseen ja tilannekuvan muodostamiseen
- häiriönkäsittelyharjoitus, joka mittaa organisaation teknistä ja/tai hallinnollista kykyä selvittää organisaatioon kohdistuneen kyberhyökkäyksen vaikutukset sekä varmistaa mahdollisimman tehokas palautuminen ja oppi tapahtuneesta.

Kyberturvallisuusharjoitukset ovat erittäin tehokas tapa oppia tietoturvan käytäntöjä eri vaiheissa. Vaiheita ovat tavoitteiden määrittely, lähestymistavan valinta, verkkotopologian suunnittelu, skenaarion luominen, sääntöjen laatiminen ja sopivien mittareiden valitseminen sekä oppitunnit aiheista. Tavoitteiden perusteella päätetään harjoituksessa käytettävät laitteet, ohjelmistot ja verkkojen topologiat. Harjoituksen jälkeen tulee kerätä osallistujilta ja järjestäjiltä oppimiskokemuksia asetetuista tavoitteista. (Patriciu & Furtuna 2009.)

3.3.1 KRIISIVIESTINNÄN HARJOITTELU

Valtionhallinnon tehostetun viestinnän ohjeen mukaisesti varautuminen on osa kaikkien viranomaisten päivittäistä toimintaa ja lakisääteinen tehtävä. Sen mukaan viestintä sisällytetään kaikkiin valmiussuunnitelmiin ja toimintaan varataan riittävä henkilöstö. Organisaatiot harjoittelevat keskeisiä toimintoja ja viestinnän yhteensovittamista häiriötilanteissa. Viestintään varaudutaan suunnittelemalla, kouluttamalla henkilökuntaa ja harjoittelemalla. Varautumiseen kuuluvat myös viestintäympäristön ja sidosryhmien tapojen ja tarpeiden sel-

vittäminen ja ymmärtäminen. Viestinnällinen varautuminen on osa jokaisen organisaation päivittäistä riskinhallintaa. (Valtioneuvoston kanslia 2019.)

Viestintää on harjoiteltava muidenkin kuin vain viestinnän ammattilaisten. Viestinnän sekä muiden toimijoiden, kuten päättäjien ja asiantuntijoiden, on osallistuttava viestintäharjoituksiin yhdessä. Näin saavutetaan parempi käsitys kaikkien osapuolien rooleista kriisiviestinnässä sekä yhteisymmärrys siitä, miten yhtenäiset työtavat ja työkalut tukevat onnistunutta kriisiviestintää. Jos harjoitus analysoidaan lopuksi huolellisesti, siitä saadaan parhaat hyödyt irti. Osallistujien, järjestäjien ja tarkkailijoiden huomiot yhdistämällä harjoituksesta saadaan monipuolinen kuva, jota voidaan käyttää jatkossa kehitystyön pohjana. Analyysivaihe on usein harjoituksen tärkein vaihe. (Myndigheten för samhällsskydd och beredskap 2019; Traficom 2019.)

Kuvassa 6 on tietoturvapoikkeamasta aiheutuneen kyberkriisin viestintään sopiva rakenteellinen pohja viestin muodostamiseksi.

Kuva 6. Viesteillä on iso merkitys, ja ne tulee pohtia valmiiksi jo ennen tietoturvapoikkeamaa (Knight & Nurse 2020).

Harjoituksien avulla saadaan selville sekä hyvin toimivat että vielä kehittämistä vaativat viestinnän osa-alueet. Harjoituksien tavoitteena on omaksua eri toimijoiden kesken yhdenmukainen viestintätapa kriisitilanteita hoidettaessa. Harjoittelulla myös testataan, miten yhdenmukainen viestintä eri skenaarioissa onnistuu. Kokemukset ja havainnot harjoituksista – kuten myös todellisista tilanteista – on tärkeää dokumentoida ja hyödyntää systemaattisella tavalla, jotta kokemusta voidaan käyttää hyväksi osaamisen kehittämiseksi. Liikenne- ja viestintävirasto Traficomin (2019) mukaan on tärkeää, ettei harjoituksessa koeta vahvoja henkilökohtaisia epäonnistumisia. Harjoittelun avulla etsitään heikkouksia prosesseista ja toimintatavoista, ei ihmisistä. Harjoittelijoita pitää kannustaa toimimaan rohkeasti. Myönteiset kokemukset ovat tärkeitä, jotta kiinnostus ja motivaatio harjoituksiin säilyvät. Erityisen hyvin suoriutuneiden harjoittelijoiden onnistumisia kannattaa nostaa esiin reflektion yhteydessä. (Myndigheten för samhällsskydd och beredskap 2019; Traficom 2019.)

Kulloinkin sopiva harjoittelutapa riippuu kehittämistarpeista ja harjoittelun tavoitteista. Myös osallistujien ja organisaation kyvyillä on vaikutusta valittavaan harjoittelutapaan. Osallistujille vieraammassa asiayhteydessä helposti toteutettava lähestymistapa voi olla seminaarityyppinen harjoitus, jossa viestintäasiantuntijat etenevät muiden asiantuntijoiden kanssa kuvitteellisen tilanneskenaarion parissa vaiheittain keskustellen. (Myndigheten för samhällsskydd och beredskap 2019.)

Kriisitilanteiden hallintaa voidaan tehostaa valmistelemalla erilaisiin skenaarioihin liittyviä viestinnällisiä etukäteismalleja. Niiden avulla voidaan tunnistaa, mihin kohderyhmiin tietyn tyyppinen tilanne voi vaikuttaa ja mitkä saattaisivat olla heidän viestinnälliset tarpeensa. Vastuutahot voivat sitten valmistella koordinoituja ja yhtenäisiä viestejä näihin arviointeihin perustuen. Mallinnettavat skenaariot voidaan valita todennäköisten tapahtumien joukosta tai erityisen vaativien mutta epätodennäköisempien joukosta. Koska monet skenaariot vaikuttavat useiden toimijoiden viestintään organisaatiossa, etukäteisvalmistelujen tekeminen käy hyvästä yhteistoimintaharjoituksesta. (Myndigheten för samhällsskydd och beredskap 2019.)

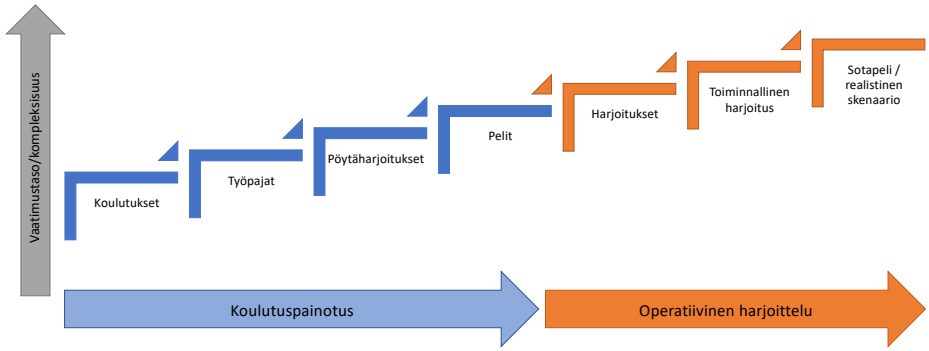
Etukäteisvalmistelulla ei kuitenkaan voida välttämättä ennakoida kaikkia tositilanteen kyberkriisin vaikutuksia ja kommunikaatiotarpeita. Valmistelun tuloksena tulee pyrkiä luomaan monipuolinen työkalulaatikko, jota toimijat voivat helposti soveltaa käyttöönsä kriisitilanteen ollessa päällä. Valmiit, harjoittelun kautta tutut työkalut voivat auttaa säästämään aikaa vaikeassa tilanteessa paineen alla. Etukäteisvalmistelun toinen hyöty on se, että harjoittelun myötä viestinnän ja asiantuntijoiden yhteistyö on alkanut jo ennen kriisiä. (Myndigheten för samhällsskydd och beredskap 2019.)

Etukäteisvalmistelun yhteydessä suoritetaan useita tehtäviä. Ensiksi tunnistetaan viestinnän kohderyhmät. Sitten arvioidaan valitun skenaarion mukaisten tapahtumien etenemistä sekä kommunikaatiotarpeita ja -prioriteetteja kussakin vaiheessa. Tämän jälkeen kriisiviestin-

nälle asetetaan yhteiset tavoitteet, kuten mitä viestinnällä tavoitellaan suhteessa ihmisten huoleen ja reagointiin tapahtumien keskellä. Lopuksi valmistellaan yhteisen viestinnän sisällöllinen runko ja suunnitellaan kriisiviestinnässä käytettävät keinot. (Myndigheten för samhällsskydd och beredskap 2019.)

3.3.2 KYBERKRIISIEN VIESTINNÄN HARJOITTELU

Kyberkriisien viestintää harjoitellaan yleensä osana muuta kriisitilanteiden harjoittelua. Harjoituksia voidaan toteuttaa useilla eri tavoilla, jolloin harjoituksen tavoitteet, intensiteetti ja vaativuus vaihtelevat. Harjoitukset voidaan jakaa päätasolla operatiivisiin ja koulutuksellisiin (ks. kuva 7). Koulutuksellisten harjoitusten tehtävä on kouluttaa osallistujia kybertilanteiden hoitoon sekä antaa valmiuksia toimia ja ymmärtää tilannetta. Operatiiviset harjoitukset taas pyrkivät arvioimaan tai testaamaan organisaation kykyä vastata kyberkriisiin. Harjoituksien suunnitteluun, valmisteluun ja räätälöintiin käytettävät resurssit kasvavat sen mukaan, mitä kompleksisempi ja vaativampi harjoitusjärjestely on päätetty toteuttaa. (Homeland Security 2011.)



Kuva 7. Kyberkriisiharjoitusten luokittelu, luonne ja toteutuksen monimutkaisuus (Homeland Security 2011).

Koulutukselliset harjoitukset pyrkivät ensisijaisesti kehittämään organisaation ja yksilöiden osaamista ja valmiuksia. Perustasolla järjestetään koulutuksia ja työpajoja vaikkapa organisaation turvallisuuskäytännöistä tai annetaan valmiuksia ymmärtää organisaatioon kohdistuvia kyberuhkia. Pöytäharjoitukset tai pelit ovat seuraava taso koulutuksellisten harjoitusten ryhmässä. Niissä tutustutaan usein ryhmätyönä johonkin uhkaskenaarioon ja pyritään yhteistyössä laatimaan ratkaisu, joka neutraloi uhan. Skenaariot voivat olla nimenomaan omalle yritykselle laadittuja tai yleisiä kyberuhkaskenaarioita. Pöytäharjoituksiin ja peleihin liittyy jonkin verran ratkaisujen etsimistä sekä päätöksien tekoa ja niiden vaikutusten arviointia. (Homeland Security 2011; Wong 2019.)

Operatiivisissa harjoituksissa pyritään arvioimaan organisaation toimintakykyä torjua ja hallita kyberuhkaa. Niissä myös pyritään testauksen keinoin löytämään heikkouksia ja kehittämiskohteita kyberpuolustuksesta ja reagointikyvystä. Operatiiviset harjoitukset voidaan jakaa kolmeen ryhmään: kyberharjoituksiin, toiminnallisiin harjoituksiin ja täysimittaisiin, sotapelityyppisiin harjoituksiin. Kyberharjoitus (engl. drill) on toiminnallisen harjoituksen muoto, jossa osallistujat opastetaan läpikäymään ja harjoittelemaan organisaation ennalta käsikirjoittama toimintasuunnitelma. Toiminnallisessa harjoituksessa taas harjoitellaan organisaation toimintaa ja valmiutta simuloidussa kybertilanteessa, joka usein on monimutkainen ja ajan myötä kehittyvä. Sotapelityyppinen harjoitus puolestaan on toiminnallisesta harjoituksesta edelleen jalostettu, harjoituksen vaativa muoto. Siinä mukana on muun muassa myös tunkeutujaa esittävä punainen tiimi, joka toimii aktiivisesti harjoituksen aikana harjoittelijoita vastaan. Sotapelissä pyritään mahdollisimman realistiseen skenaariotilanteeseen sisällön, tapahtumien ja aikajanan osalta. (Homeland Security 2011; Wong 2019.)

Toiminnallinen harjoittelu sopii hyvin kriisiviestinnän harjoitteluun. Harjoituksen pelinjohto tuottaa syötteitä osallistujille. Syötteet voivat liittyä kriisiviestintään, ja ne voivat olla sisällöltään mielikuvituksellisia. Kriisijohtamisen harjoituksessa voidaan harjoitella esimerkiksi yhteydenpitoa toimittajien kanssa. Harjoittelijoiden luokse voidaan lähettää jopa toimittaja ja kameramies tekemään reaaliaikainen haastattelu pelitilanteen tapahtumista. (Traficom 2019.)

Harjoitusympäristön simuloinnilla tai mallintamisella pyritään tosielämän toimintojen ja resurssien esittämiseen mahdollisimman uskottavalla tavalla harjoituksen aikana. Sosiaalista mediaa voidaan mallintaa erilaisilla ohjelmistoilla tai laatimalla niistä näköisversioita. Julkisen viestimisen mallintaminen tapahtuu melko suoraviivaisesti, sillä viestintä on pääsääntöisesti yksisuuntaista, kuten lehdistötiedotteiden laadintaa. Toiminnallisessa harjoituksessa pelikeskus reagoi pelaajien laatimiin viesteihin ja voi muuttaa harjoituksen kulkua niiden mukaisesti. Median, erityisesti sosiaalisen median, mallintaminen vaatii kuitenkin simulaattoriympäristöä. Harjoitussimulaattorissa on mahdollista viestiä sosiaalisessa mediassa reaalimaailman ulkopuolella ja mallintaa myös muuta viestintää. Myös erilaiset pikaviestin- ja julkaisuohjelmistot ovat mahdollisia, jos niitä osataan käyttää luovasti ja soveltaen. Samanaikaisesti, kun harjoitukseen osallistuvat ovat kiireisiä punaisen tiimin hyökkäykseen reagoidessaan, he joutuvat ottamaan huomioon viestintänäkökulman ja toimimaan sen mukaisesti. Näin harjoitukseen saadaan paljon todellisuuden tuntua. (Seker 2019; Traficom 2019.)

Viestintää harjoiteltaessa on syytä huolehtia harjoitushygieniasta siten, ettei harjoitusviestintä sekoitu aitoon viestintään. Sekoittuminen voi aiheuttaa sekaannusta tai pahimmassa tapauksessa vääriä reaalimaailman kriisihälytyksiä. Viestintä on syytä merkitä selkeästi, niin että vastaanottaja tunnistaa sen harjoituksen viestinnäksi. Selkeimmin tämä tehdään

merkitsemällä jokaiseen viestiin näkyvästi teksti, joka kertoo, että kyse on harjoituksesta. (Traficom 2019.)

Harjoitustoimintaan on syytä sisällyttää myös eri viestintästrategioiden käyttöä. Kriisitilanneviestinnässä on valittava tilanteen mukaan, mitä viestinnän päästrategiaa noudatetaan. Vaihtoehdot ja valintapäätös on huomioitava myös viestinnän etukäteisarvioinneissa sekä harjoituksissa. Valittavana on päätasolla kolme vaihtoehtoa, joista jokaiselle on olemassa tilannekohtaiset valintakriteerit ja perustelut: kriisin olemassaolo voidaan kiistää, kriisi voidaan pyrkiä häivyttämään taka-alalle tai viestintä voi keskittyä jälleenrakennukseen kriisin aikana ja sen jälkeen. (Coombs 2007.)

4 POHDINTA

Kyberhyökkäysten lisääntyminen on ollut nähtävissä viime vuosikymmenen nousevana trendinä. Viimeaikaiset tapahtumat Suomessa ovat avanneet silmiä todellisuuteen: digitalisaatio auttaa yhteiskuntaa toimimaan tehokkaammin, mutta toisaalta taas kyberhyökkäykset ja palvelimien tietovuodot saavat aikaan epäluottamusta ja sekasortoa yhteiskunnassa.

Maineenhallinta on yrityksille tärkeä tehtävä poikkeustilanteissa, sillä mainevahingoilla on suora yhteys yrityksen osakkeiden arvonmääritykseen. Organisaatiolla tulee olla valmiina hyvät yhteydet tiedotusvälineisiin, ja sosiaalisen median kanavien tulee olla tuttuja. Yleisen tiedon puuttuessa väärät julkiset arvailut ja väärinkäsitykset varsinkin sosiaalisessa mediassa tuottavat harmia organisaatiolle.

Kyberkriisien viestintään valmistaudutaan, jotta organisaatio kykenee viestinnän keinoin selviytymään kriisitilanteesta. Selkeä, organisaation strategiaa tukeva kriisiviestinnän valmiussuunnitelma sekä ohjeet käytännön toimiin, kuten vastuiden jakaminen, toiminta- ja tarkistuslistat, valmiit mallipohjat ja ennalta tehdyt yhteystietolomakkeet, nopeuttavat kriisiviestintää huomattavasti. Viestinnän vastuu on ainoastaan yhdellä henkilöllä.

Valmistautuminen ja harjoittelu tarkoittavat viestinnän toimenpiteiden ja sisältöjen suunnittelua ja henkilökunnan osaamisen kehittämistä. Viestintä on tärkeä osa kriisitilanteiden hallintaa. Sitä tulee suunnitella etukäteen, ja siihen tulee valmistautua muun muassa koulutuksella ja harjoittelulla.

Viestintään liittyvä säännöspohja tietoturva- ja tietosuojaloukkauksissa löytyy rikoslaista ja EU:n tietosuoja-asetuksesta. Säännöt koskevat niin pieniä kuin suuriakin organisaatioita. Viranomaisiin kohdistuu lisäksi erityisiä kyberkriisitilanteisiin liittyviä vaatimuksia. Varautuminen kriisitilanteisiin on kaikkien viranomaisten lakisääteinen tehtävä.

Jotta yritys menestyisi, sen palveluiden ja tuotteiden on oltava kyberturvallisia. Liiketoiminnan näkökulmasta kriisiviestinnän tärkeä tehtävä liittyy maineenhallintaan asiakkaiden ja sidosryhmien suuntaan. Kyberkriisi on hyvin potentiaalinen uhka organisaation maineelle ja luottamukselle. Kriisillä on suora vaikutus organisaation liiketoiminnan tulevaisuuteen. Luottamuksen ja maineen menettäminen voi supistaa liikevaihtoa, ja niiden palauttamiseen käytetyt resurssit voivat vaikuttaa kannattavuuteen merkittävästi. Kriisin seurauksena voidaan joutua maksamaan vahingonkorvauksia. Pienen yrityksen kohdalla kriisin kumuloituvat vaikutukset voivat olla kohtalokkaita, mikä voi johtaa toiminnan loppumiseen tai liiketoiminnan myyntiin pilkkahintaan. Kriisin jälkeen yrityksen tulee muuttaa omia prosessejaan ja parantaa toimintaansa sekä mitata, kuinka paljon vahinkoa kriisistä aiheutui. Opit kannattaa jakaa, jotta muut organisaatiot voisivat päästä helpommalla.

Kriisitilanteiden viestintään on kehitetty joitakin valmiita malleja, joista Timothy Coombsin maineenhallintateoria on tunnetuimpia. Sen mukaan on olemassa kolme ensisijaista viestinnän reagointistrategiaa kriisin aikana ja sen jälkeen käytettäviksi: kieltäminen, vähättely ja jälleenrakentaminen. Nimenomaisesti kyberkriisin viestintään on Knightin ja Nursen (2020) tutkimuksessa kehitetty varautumisen ja reagoinnin malli, joka panostaa avoimuuteen viestinnässä. Sen mukaan on kuitenkin huolellisesti mietittävä, julkaistaanko tietoja ja milloin. Huolellisuus valmistautumisessa ja avoimuus vaikuttavat paremmilta ohjeilta kuin kieltäminen ja vähättely. Coombsin maineenhallintateoria on hieman iäkäs eikä huomioi sosiaalisen median luomaa uutta tilannetta, jossa viestijä ei voi enää yksin hallita viestin sisältöä. Uusimmissa tutkimuksissaan Coombs suosittelee kriisiviestinnän aktiivista toimintaa siten, että organisaatio ilmoittaa tapahtumista ennen digitaalista tai perinteistä mediaa. Sosiaalisen median kriisiviestintäkeskustelut tulee käydä sosiaalisessa mediassa. Uhreille tulee kertoa, kuinka he voivat suojella itseään. Heille tulee antaa tietoa ja kertoa toimenpiteistä, joilla heitä autetaan selviytymään fyysisistä ja psyykkisistä henkilökohtaisista kriiseistä. Myötätunnon osoittaminen on tärkeää. Maineen palauttaminen nopeutuu aktiivisella kommunikoinnilla. Väärän huhun tai tiedon kohteeksi joutuessaan organisaation tulee kieltää asia heti.

Harjoittelu on tärkeä osa kyberkriisiin valmistautumista. Harjoittelun avulla voidaan varmistaa suunnitelmien käytännön toiminta ja laatu sekä kouluttaa henkilöstöä reagoimaan tehokkaasti kyberkriisitilanteisiin. Viestintä on aina moniammatillista yhteistyötä organisaation eri tasoilla. Sitä voidaan kehittää harjoittelulla.

Viestintä on syytä liittää aina osaksi harjoittelua sen kaikilla tasoilla työpöytäharjoituksista toiminnallisiin harjoituksiin. Se tulee nivoa yhteen offensiivisten toimenpiteiden sekä päätöksenteon harjoittelun kanssa, jotta tositilannetta varten voidaan muodostaa kriisistä selviämisen kannalta toimiva kokonaisuus. Näin organisaatio omaksuu myös viestinnälliset keinot osaksi kriisinhallintaa jo harjoitteluvaiheessa.

Kyberturvallisuusalalla on tällä hetkellä kasvavaa kysyntää pätevälle työvoimalle, jolla on hallussaan myös viestinnän osaaminen. Näitä taitoja tulisi sisällyttää opetussuunnitelmiin ja alan kursseihin oppilaitoksissa.

4.1 PARHAAT KÄYTÄNNÖT KYBERTURVALLISUUDEN KRIISIVIESTINTÄÄN

Suomessa suurin osa yrityksistä, yli 98 prosenttia, on kooltaan alle 50 hengen pienyrityksiä. Harvoilla yrityksillä on osaamista varautua kyberhyökkäyksiin sekä vastata niiden uhkiin ja itse tapahtumiin. Hyökkäykset ja tietomurrot organisaatioiden palvelimiin lisääntyvät, joten pienyrityksien tulee varautua ja valmistautua pitämään yllä brändikuvaansa ja mainettaan myös viestinnän keinoin.

Kirjoittajien parhaat käytännöt kyberturvallisuuden kriisiviestintään:

1. Pohdi oman organisaatiosi maineenhallintaa – mitä tapahtuu, jos yrityksesi tai organisaatiosi maine kokee kolhuja.
2. Analysoi, kartoita ja mittaa maineriskejä sekä tee suunnitelma niiden estämiseksi.
3. Järjestä maineenhallinnan suunnittelutyöpaja johtoryhmälle ja ydinhenkilöille.
4. Tee viestintäsuunnitelma ja sen tavoitteet – miten organisaatio reagoi, vastaa ja kommunikoi eri medioissa, kun kyberhyökkäys toteutuu.
5. Huomioi suunnitelmassasi oman organisaatiosi lisäksi asiakkaat, sidosryhmät ja yhteistyökumppanit sekä viranomaisvaatimukset – myös lainsäädännön noudattaminen on tärkeää.
6. Tee selvät toimintaohjeet ja sisältö kyberturvallisuuden kriisiviestinnälle sekä valmiit pohjat eri kriisitilanteisiin.
7. Jaa vastuuta mutta muista, että viestinnästä vastaa vain yksi henkilö.
8. Kouluta henkilökuntaa kriisiviestinnän tehtävistä, sillä kyberturvallisuudesta vastaa koko organisaatio.
9. Päivitä ohjeita ja seuraa verkkohyökkäysten kehittymistä.
10. Harjoittele kriisiviestintää toiminnallisessa kyberturvallisuusharjoituksessa.
11. Varautumisen jälkeen poikkeustilanteessa tilannekuvan saaminen sekä tapahtumien analysointi ja arviointi ovat tärkeitä tehtäviä.
12. Ole nopea viestinnässäsi – oikea-aikainen viestintä vaikuttaa tiedotusvälineiden ja sidosryhmien reaktioihin.
13. Huomioi myös sosiaalisen median merkitys – myös sitä tulee monitoroida.
14. Poikkeustilanteessa tarvitaan normaalia enemmän viestintää, joka on avointa, ymmärrettävää, luotettavaa, selkeää ja yhdenmukaista.
15. Varmista tiedon perillemeno – se lisää ymmärrystä sekä myötätunnon osoittamista asianomaisille – sekä rakenna luottamusta – sen takaisin saaminen on vaikeaa.
16. Muuta tapahtuman jälkeen organisaatiosi toimintatapoja, paranna toimintaa ja mittaa, kuinka paljon vahinkoa kyberkriisistä aiheutui.
17. Jaa kyberkriisin opit – se voi estää muita organisaatioita joutumasta kyberhyökkäyksen kohteeksi.
18. Pyri huomioimaan asiakkaiden varastettujen henkilötietojen johdosta seuraavat taloudelliset vahingot.
19. Dokumentoi aina kaikki kyberkriisin tapahtumat.
20. Pidä itsesi ajan tasalla kyberturvallisuuden haasteista sekä kouluta henkilökuntaa edelleen toimimaan turvallisesti ja ilmoittamaan tietoturvapoikkeuksista.

Lista käytännöistä on löydettävissä myös huoneentauluna liitteestä 1.

Liitteessä 2 on kuvaus tehokkaasta kriisiviestinnästä poikkeustilanteen tapahduttua ja tietovuodon jälkeen. Se on muokattu Knightin ja Nursen (2020) tutkimuksesta.

4.2 JOHTOPÄÄTÖKSET

Tutkimuskysymykseen ”Voiko kriisiviestintää harjoitella menestyksekkäästi etukäteen?” toteamme, että internetin julkisilta viranomaissivustoilta, viestintäalan yrityksiltä ja kriisiviestinnän ammattilaisilta löytyy paljon sekä kriisiviestinnän sisältöön että sen harjoitteluun liittyvää tietoa ja materiaalia. Etukäteisharjoituksilla organisaatio voi testata kykyään suoriutua viestinnästä kyberhäiriötilanteissa parhaiten sopivalla mallilla. Kuvitteellinen tilanne toteutetaan harjoituksessa kuten tosielämässä tapahtuisi, jolloin voidaan todeta koko organisaation toimintakyky poikkeustilanteessa. Harjoituksen jälkeen tulee kerätä osallistujien oppimiskokemukset ja palautteet asetetuista tavoitteista sekä kehittää harjoittelua paremmaksi kokonaisuudeksi.

Tutkimuksen hypoteesina oli, että pienillä organisaatioilla ei ole keinoja eikä välineitä kyberkriisiviestintään valmistautumista varten. Mielestämme tämä ei pidä paikkaansa. Keinoja ja välineitä kyllä on. Tässä tutkimuksessa selvitetyt keinot kriisiviestinnän suunnitteluun, valmistautumiseen ja harjoitteluun skaalautuvat hyvin sekä pienten että suurten organisaatioiden tarpeisiin. On kuitenkin totta, että pienillä organisaatioilla ei ole käytettävissään samanlaisia resursseja kuin suurilla, joten valmiuskaan ei välttämättä ole suurten organisaatioiden tasolla. Oletettavasti tässä on kuitenkin enemmän vaihtelua organisaatiokohtaisesti kuin eri suuruusluokkien välillä.

4.3 EHDOTUKSET JATKOSUUNNITELMIA VARTEN

Kirjoittajien mielestä seuraavaksi kannattaisi tutkia tapaustutkimuksena, miten pk-yrityksissä voidaan toteuttaa kriisiviestinnän harjoituksia ja millaisella harjoittelumallilla. Lisäksi voisi tutkia, miten harjoituksista saatuja kokemuksia ja arviointeja voidaan hyödyntää valmiuden kehittämisessä. Kolmantena aiheena voisi tutkia, miten pk-yritykset voisivat hyödyntää yritysverkostojaan kriisivalmiuden kohottamiseksi.

LÄHDELUETTELO

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. & Upton, D. 2018. A taxonomy of cyber-harms. Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4 (1). Verkkolehti. Saatavissa: https://doi.org/10.1093/cybsec/tyy006 [viitattu 17.2.2021].

Coombs, W. T. 2007. Protecting organization reputations during a crisis. The development and application of situational crisis communication theory. Corporate Reputation Review 10 (3), 163–176. Verkkolehti. Saatavissa: https://link.springer.com/article/10.1057/palgrave.crr.1550049 [viitattu 15.2.2021].

Coombs, W. T. 2014. State of crisis communication. Evidence and the bleeding edge. Research Journal of the Institute for Public Relations 1 (1). PDF-dokumentti. Saatavissa: https://instituteforpr.org/wp-content/uploads/CoombsFinalWES.pdf [viitattu 6.4.2021].

DiStaso, M. W. 2018. Communication challenges in cybersecurity. Journal of Communication Technology. PDF-dokumentti. Saatavissa: https://joctec.org/articles/1-1/114.pdf [viitattu 19.2.2021].

Eisto, S. 2020. 5 vinkkiä yrityksen maineenhallintaan. WWW-dokumentti. Päivitetty 1.9.2020. Saatavissa: https://y-studio.fi/yrityksen-kasvu/riskienhallinta/yrityksen-maineenhallinta-ota-5-vinkkia-haltuun [viitattu 11.3.2021].

Homeland Security. 2011. Introduction to cyber exercises. National Cyber Security Division Cyber Exercise Program. U.S. Department of Homeland Security. PDF-dokumentti. Saatavissa: https://www.hsdl.org/?view&did=770844 [viitattu 15.2.2021].

Kinturi, M.-L. 2018. Maine ei synny ilman mainetekoja. WWW-dokumentti. Päivitetty 26.6.2018. Saatavissa: https://www.asiakastieto.fi/web/fi/asiakastieto-media/uutiset/maine-ei-synny-ilman-mainetekoja.html [viitattu 11.3.2021].

Knight, R. & Nurse, J. R. C. 2020. A framework for effective corporate communication after cyber security incidents. Computers & Security 99. Verkkolehti. Saatavissa: https://doi.org/10.1016/j.cose.2020.102036 [viitattu 17.2.2021].

Kyberturvallisuuskeskus. 2019. Luottamuksen lähteillä. Näkökulmia tietoturvan standardointiin ja sertifiointiin. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf [viitattu 11.3.2021].

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. 2018. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. PDF-dokumentti. Saatavissa: https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen.pdf [viitattu 15.3.2021].

Management Institute of Finland. 2019. Kriisiviestintäsuunnitelma. Miten se tehdään? WWW-dokumentti. Päivitetty 14.1.2019. Saatavissa: https://mif.fi/kriisiviestintasuunnitelma-miten-se-tehdaan/ [viitattu 15.3.2021].

Myndigheten för samhällsskydd och beredskap. 2019. Kriskommunikation för ökad effekt vid hantering av samhällsstörningar. En vägledning om att integrera kommunikation i samverkan och ledning. PDF-dokumentti. Saatavissa: https://rib.msb.se/filer/pdf/28912.pdf [viitattu 15.2.2021].

Patriciu, V.-V. & Furtuna, A. 2009. Guide for designing cyber security exercises. PDF-dokumentti. Saatavissa: http://www.wseas.us/e-library/conferences/2009/tenerife/EACT-ISP/EACT-ISP-28.pdf [viitattu 18.2.2021].

Piha, K. & Vesanen, M. 2014. Voiko hyvän maineen tilata? WWW-dokumentti. Päivitetty 22.5.2014. Saatavissa: https://ellunkanat.fi/nakemys/artikkelit/voiko-hyvan-maineen-tilata [viitattu 11.3.2021].

Seker, E. 2019. The concept of cyber defence exercises (CDX). Planning, execution, evaluation. WWW-dokumentti. Saatavissa: https://arxiv.org/abs/1906.03184 [viitattu 17.3.2021].

Suomen Yrittäjät. 2021. Yrittäjyys Suomessa. WWW-dokumentti. Päivitetty 26.1.2021. Saatavissa: https://www.yrittajat.fi/suomen-yrittajat/yrittajyys-suomessa-316363 [viitattu 11.3.2021].

Tilastokeskus. 2021. PK-yritys. WWW-dokumentti. Saatavissa: https://www.stat.fi/meta/kas/pk_yritys.html [viitattu 11.3.2021].

Traficom. 2019. Kyberharjoitusohje. Käsikirja harjoituksen järjestäjälle. Traficomin julkaisuja 26/2019. PDF-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf [viitattu 15.2.2021].

Turell, J., Su, F. & Boulanin, V. 2020. Cyber-incident management. Identifying and dealing with the risk of escalation. SIPRI Policy Paper 55. WWW-dokumentti. Saatavissa: https://www.jstor.org/stable/resrep26199 [viitattu 18.2.2021].

Valtioneuvoston kanslia. 2019. Valtionhallinnon tehostetun viestinnän ohje. Viestintä normaalioloissa ja häiriötilanteissa. Valtioneuvoston kanslian julkaisuja 2019:23. Saatavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/161972 [viitattu 15.2.2021].

Valtiovarainministeriö. 2017. Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriön julkaisuja 8/2017. PDF-dokumentti. Saatavissa: https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf [viitattu 15.3.2021].

Wang, P. & Johnson, C. 2018. Cybersecurity incident handling. A case study of the Equifax data breach. Issues in Information Systems 19 (3), 150–159. PDF-dokumentti. Saatavissa: https://iacis.org/iis/2018/3_iis_2018_150-159.pdf [viitattu 17.2.2021].

Vertainen, V., Suni, E., Vatanen, M., Hautamäki, J., Laava, T. & Piispanen, J. 2020. Kyberhäiriöiden hallinta. Käsikirja terveydenhuollon toimijoille. Jyväskylän ammattikorkeakoulu, IT-instituutti / JYVSECTEC, Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä / Business Finland. PDF-dokumentti. Saatavissa: https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf [viitattu 15.3.2021].

Wong, E. 2019. Cyber crisis management exercise. Deloitte, Bursa Malaysia. PDF-dokumentti. Saatavissa: https://www2.deloitte.com/content/dam/Deloitte/my/Documents/tax/my-tax-bursa-2019-cyber-security-workshop-cyber-crisis-management.pdf [viitattu 15.2.2021].

PARHAAT KÄYTÄNNÖT KYBER-TURVALLISUUDEN KRIISIVIESTINTÄÄN

1. Pohdi oman organisaatiosi maineenhallintaa – mitä tapahtuu, jos yrityksesi tai organisaatiosi maine kokee kolhuja
2. Analysoi, kartoita ja mittaa maineriskejä sekä tee suunnitelma niiden estämiseksi
3. Järjestä maineenhallinnan suunnittelutyöpaja johtoryhmälle ja ydinhenkilöille
4. Tee viestintäsuunnitelma ja sen tavoitteet – miten organisaatio reagoi, vastaa ja kommunikoi eri medioissa, kun kyberhyökkäys toteutuu
5. Huomioi suunnitelmassasi oman organisaatiosi lisäksi asiakkaat, sidosryhmät ja yhteistyökumppanit sekä viranomaisvaatimukset – myös lainsäädännön noudattaminen on tärkeää
6. Tee selvät toimintaohjeet ja sisältö kyberturvallisuuden kriisiviestinnälle sekä valmiit pohjat eri kriisitilanteisiin
7. Jaa vastuuta mutta muista, että viestinnästä vastaa vain yksi henkilö
8. Kouluta henkilökuntaa kriisiviestinnän tehtävistä, sillä kyberturvallisuudesta vastaa koko organisaatio
9. Päivitä ohjeita ja seuraa verkkohyökkäysten kehittymistä
10. Harjoittele kriisiviestintää toiminnallisessa kyberturvallisuusharjoituksessa
11. Varautumisen jälkeen poikkeustilanteessa tilannekuvan saaminen sekä tapahtumien analysointi ja arviointi ovat tärkeitä tehtäviä
12. Ole nopea viestinnässäsi – oikea-aikainen viestintä vaikuttaa tiedotusvälineiden ja sidosryhmien reaktioihin
13. Huomioi myös sosiaalisen median merkitys – myös sitä tulee monitoroida
14. Poikkeustilanteessa tarvitaan normaalia enemmän viestintää, joka on avointa, ymmärrettävää, luotettavaa, selkeää ja yhdenmukaista
15. Varmista tiedon perillemeno – se lisää ymmärrystä ja myötätunnon osoittamista asianomaisille – sekä rakenna luottamusta – sen takaisin saaminen on vaikeaa
16. Muuta tapahtuman jälkeen organisaatiosi toimintatapoja, paranna toimintaa ja mittaa, kuinka paljon vahinkoa kyberkriisistä aiheutui
17. Jaa kyberkriisin opit – se voi estää muita organisaatioita joutumasta kyberhyökkäyksen kohteeksi
18. Pyri huomioimaan asiakkaiden varastettujen henkilötietojen johdosta seuraavat taloudelliset vahingot
19. Dokumentoi aina kaikki kyberkriisin tapahtumat
20. Pidä itsesi ajan tasalla kyberturvallisuuden haasteista sekä kouluta henkilökuntaa edelleen toimimaan turvallisesti ja ilmoittamaan tietoturvapoikkeuksista

ENNEN TAPAHTUMAA

ASETA TAI PRIORISOI RIKKOMUSTA EDELTÄVÄT TAVOITTEET

Näkökohtia
- Rekisteröityjen suojeleminen
- Keskeisten sidosryhmien hallinta
- Mainehaitan minimointi
- Myynnin suojaaminen / kyky käydä kauppaa
- Oikeudelliset velvoitteet
- Arvo osakemarkkinoilla
- Yritykselle aiheutuvien kustannusten minimointi

MÄÄRITÄ TIETOTURVA-AUKOT VIESTINNÄN VASTAUSTEN TUEKSI

Näkökohtia
- Tietoturvatarkastukset ja riskit
- Arvioi tärkeimmät hygieniatekijät
- Ajantasainen/vahva salaus
- Monitekijäinen todennus (MFA)
- Ota käyttöön uhkien valvonta ja avoimien lähteiden tiedustelu (OSINT)

MUODOSTA KRIISIVIESTINTÄKYKY JA YLLÄPIDÄ SITÄ

Ohjausta
- Sopivat päätöksentekijät ja toimiva kriisitiimi
- Kouluta, konsultoi ja tue päätöksentekijöitä tai hallitusta
- Perusta kriisitietokanta
  - Lainkäyttöalueet ja sovellettavat määräykset
  - Kullekin lainkäyttöalueelle:
    - Toimialakohtaiset määräykset
    - Julkistamisen vertailuarvot
    - Seuraamusjärjestelmät
    - Ryhmäkanteiden riskit
  - Kuinka henkilökohtainen tai arkaluontoinen tieto on salattu
  - Havaitut tietoturva-aukot, jotka voivat pitää sisällään mainehaitan
  - Varmista tietojen olevan suojattuja mutta käytettävissä IT-häiriötilanteen sattuessa
- Tarkista talon sisäinen kyvykkyys ja palkkaa tarvittaessa asiantuntijoita
- Laadi sidosryhmille tarvittaessa lähetettävät vastausluonnokset todennäköisille skenaarioille
- Harkitse kriisin aikana aktivoitavaa verkkosivua (usein kysytyille kysymyksille, vihjelinjalle jne.)
- Käsittele joukkoviestintään liittyviä haasteita, esimerkiksi joukkoviestien tulkintaa roskapostiksi

OTA MUKAAN KUMPPANIT JA TOIMITUSKETJU

Ohjausta
- Varmista yhteyshenkilöt vuotoitilanteita varten
- Määritä lähestymistapa toimittajaan kohdistuvaan tietomurtoon
- Ota keskeiset kumppanit mukaan suunnitteluun ja harjoituksiin

SUORITA SÄÄNNÖLLISIÄ HARJOITUKSIA JA TESTEJÄ

Näkökohtia
- Sisällytä viestinnän vastaukset liiketoiminnan jatkuvuussuunnitelmaan (BCP) ja suurten tapahtumien harjoituksiin
- Tärkeimmät päätöksentekijät mukaan
- Käykää läpi realistisia skenaarioita
- Ottakaa mukaan toimitusketjun sisäpuolelle kohdistuvia skenaarioita

VERKKOKRIISITOIMET

Merkittävä arkaluontoisen tai henkilökohtaisen tiedon vuoto

PÄÄTÄ, TUODAANKO ILMI

Onko julkistaminen pakollista?

- Keneen se vaikuttaa?
- Onko data riittävästi salattua?
- Kuinka paljon dataa on menetetty?
- Onko toimialakohtaisia sääntöjä?

→ **Tietopohja**
- Lainkäyttöalueet
- Säännökset vaikutusalueelle kuuluville lainkäyttöalueille

→ Kyllä

Arviointi siitä, onko julkistaminen pakollista → Ei

Pitäisikö kuitenkin julkaista?

Näkökohtia
- Viestii, että turvallisuus otetaan vakavasti
- Riski tiedon ilmestymisestä myöhemmin pimeään verkkoon
- Ilmiantajariski
- Vähentää oikeudenkäyntiriskiä

→ Kyllä

PÄÄTÄ, MITÄ TUODAAN ILMI

Sääntelyvaatimukset
- On varmistettava, että rekisteröityneet voivat vähentää riskiä

Rekisteröityneiden näkökulma
- Liittyykö vuoto heihin?
- Mitä on menetetty?
- Kenelle he soittavat?

Medianäkökulma
- Tietovuodon koko
- Vältä aliarviointia

Näkökohtia

MUODOSTA VIESTI

Ohjausta
- Hyväksy vastuu
- Olet heidän tietojensa säilyttäjä – pyydä anteeksi
- Siinäkin tapauksessa, että sidosryhmä (asiakas mukaanluettuna) on syypää (esimerkiksi salasanojen uudelleenkäyttö), sinun odotetaan lieventävän riskejä seurannalla tai muulla ohjauksella (esimerkiksi monivaiheisella tunnistautumisella)
- Vältä vähättelyä – se voidaan nähdä tai tulkita niin, ettei tietovuotoa oteta vakavasti
- Puutu haavoittuvuuden tunteisiin
- Tunnista tapoja, joilla rekisteröidyt voivat suojata itseään
- Tarjoa luotonvalvontaa – toteutettava ilmaiseksi tai voidaan tulkita voiton tavoitteluksi
- Älä syyttele muita, kuten
- hakkeriryhmiä – se tuo heidät parrasvaloihin
- palvelukumppaneita – se voi johtaa julkisiin erimielisyyksiin ja vahingoittaa mainettasi

Näkökohtia
- Tarkista raskauttavat tekijät välttääksesi viestin aiheuttamat vahingot uskottavuudelle
- Aikaisemmat tietovuodot – "Otatteko tietoturvan oikeasti tosissanne?"
- Organisaatiollisten rajoitusten paljastuminen – "Onko kattava turvallisuussuunnitelmanne niin hyvä?"
- Kolmannen osapuolen havaitsema tietovuoto – "Onko asiakastiedon turvallisuus todella sen ytimessä, mitä teette?"
- Ota huomioon ikä- ja sukupuolierot sekä muut asiakkaan ominaisuudet
- Eettinen asenne – sukupuoli- ja ikäerot
- Nuorempi sukupolvi voi olla vähemmän vaikuttunut luotonvalvonnasta lieventävänä asianhaarana
- Muuta huomioitavaa
- Mitä ollaan tekemässä syyllisten saamiseksi oikeuden eteen?
- Voitko aikanaan jakaa oppimaanne auttaaksesi muita välttämään tekemiänne virheitä?

PÄÄTÄ JULKAISUAJANKOHTA

Näkökohtia
- Parempi ilmoittaa mahdollisimman nopeasti
- Auttaa käsittelemään haavoittuvuuden tunteita niillä, joita asia koskettaa
- On tärkeää, että rekisteröityneet kuulevat asian ensin sinulta luottamuksen menettämisen välttämiseksi
- Julkisen mielipiteen luominen on helpompaa kriisin alkuvaiheessa
- Tasapaino tarkkuuden ja ajoituksen välillä
- Vuodon todellisen laajuuden vahvistaminen voi joskus olla vaikeaa
- Vältä aliarviointia
- Perustuu sovellettavien lainkäyttöalueiden määräyksiin ja lainvalvontaviranomaisten antamaan ohjeistukseen

PÄÄTÄ JULKAISUTAPA

- Jos mahdollista, olisi tärkeää, että rekisteröityneet kuulevat asian ensin teiltä; muuten seurauksena voi olla luottamuksen menettäminen
- Kaikkien saatavilla olevien viestintäkanavien käyttö voi olla perusteltua ulottuvuuden lisääntyessä

SUORA

Sähköposti
- Vaatii sähköpostiosoitteen
- Voi lisätä tietoisuutta vahingosta ja tuottaa negatiivisia tunteita
- Voidaan räätälöidä koskemaan niitä, joita asia koskee eniten
- Haasteina palvelimen suorituskyky ja roskapostisuodattimet

Posti
- Suorempi ja henkilökohtaisempi
- Vähentää tietojenkalastelun riskiä
- Osoite ei ehkä ole oikea (ajantasainen)
- Kallis ja voidaan nähdä ympäristöä vahingoittavana

Verkkosivu
- Vähemmän suora – rekisteröityjen on käytävä sivustolla
- Voi sisältää FAQ:n ja vihjelinjanumerot

Puhelin
- Henkilökohtaisempi, välittävä
- Resursseja vaativa
- Ajantasainen numero voi puuttua

EPÄSUORA

Sosiaalinen media
- Mahdollisuus määritellä sosiaalisen median viestien alkuperäinen sävy
- Vuorovaikutteinen, joten negatiiviset huhut voidaan korjata
- Negatiivisen vahvistuvan kierteen riski, ns. Twitter storm

Perinteinen media
- Usein pääasiallinen tiedonlähde
- Omat tarkoituksenperät, eikä välttämättä keskity haluamiisi asioihin
- Harkitse luotettavien toimittajien listaa tiedonlevityksen helpottamiseksi

VALMISTAUDU REAKTIOON

Ohjausta
- Opasta henkilökuntaa
- Varmista riittävät resurssit sosiaalisen median ja puhelinkeskuksen hoitoon
- Skaalaa ylös verkkosivu- ja puhelinkapasiteettia
- Ennakoi liiketoimien siirto kanaviin, joita vuoto ei koske
- Varmista valmius käsitellä tiedotusvälineiltä saapuvia kyselyitä
- Ennakoi osakkeiden arvon lasku ensimmäisten parin päivän aikana
- Suorita toimenpiteitä tietojenkalasteluyritysten häiritsemiseksi

TOIMITA VIESTI

Ohjausta
- Pidä viesti selkeänä ja helppona ymmärtää
- Vältä ammattikieltä
- Pidä se yksinkertaisena
- Varmista, että toimitusjohtaja tai organisaation johtaja toimittaa viestin – näin voit välittää kuvan siitä, että organisaatio ottaa asiat vakavasti
- Vahvista, että vuoto merkitsee kriisiä – näin voit estää tarpeettoman kärjistymisen
- Tiedottajaa valitessasi ota huomioon hänen kykynsä toimia median edessä

XAMK
KEHITTÄÄ