Samuel Kallio

Tietoturva ja kyberturvallisuus digitaalisessa viestinnässä

Digitaalisen muotoilijan näkökulma ja vastuu

Viestinnän tutkinto-ohjelma

Medianomi (AMK)

17.04.2024

Tiivistelmä

Tekijä(t):	Samuel Kallio
Otsikko:	Tietoturva ja kyberturvallisuus digitaalisessa viestinnässä: Digitaalisen muotoilijan näkökulma ja vastuu
Sivumäärä:	46 sivua + 3 liitettä
Aika:	17.4.2024
Tutkinto:	Medianomi (AMK)
Tutkinto-ohjelma:	Viestinnän tutkinto-ohjelma
Suuntautumisvaihtoehto:	Ammatillisena pääaineena digitaalinen viestintä
Ohjaaja(t):	Lehtori Markus Norrena

Opinnäytetyön tutkimuksen tavoitteena on ensisijaisesti selvittää tietoturvan ja kyberturvallisuuden merkitys digitaalisen viestinnän kontekstissa. Toinen keskeinen tavoite on hahmottaa digitaalisen muotoilijan roolin laajuutta ja sitä analysoimalla kartoittaa heidän tiedontarpeitaan tietoturvasta ja kyberturvallisuudesta. Tutkimuksessa tarkastellaan tyypillisimpiä kyberuhkia ja niiden vaikutuksia digitaalisen viestinnän turvallisuuteen.

Aihe on luonteensa puolesta ajankohtainen, intensiivinen sekä muutosaltis, joten on tärkeää oppia ymmärtämään viestinnän ja digitalisaation rajapinnassa tapahtuneiden muutosten mukanaan tuomia vaikutuksia. Samasta syystä on perusteltua painottaa myös jatkuvan oppimisen ja yksilön vastuun merkitystä aiheen kannalta. Lopulta mittasuhteet aiheen kannalta on jokainen itse velvollinen määrittämään itselleen, kunnes ne määritellään ulkopuolisen tahon toimesta joko turvallisuusohjeistuksen muodossa tai kyberuhkana.

Opinnäytetyössä käydään läpi tietoturvaan ja kyberturvallisuuteen liittyviä käsitteitä ja periaatteita. Näiden käsitteiden merkitystä tarkastellaan digitaalisen viestinnän näkökulmasta henkilötietojen suojaamisen, luottamuksellisuuden säilyttämisen sekä paremman yleiskuvan luomisen kannalta. Tämän kaltainen tulokulma aiheeseen edellyttää digitaalisen viestinnän viitekehyksen monitahoisen ja laaja-alaisen toimialan tuntemista. Lopputuloksena pyritään tuottamaan käytännöllinen tietopaketti, jonka avulla voi tehdä tietoisia päätöksiä verkkotoimintansa suhteen.

On tärkeää huomioida turvallisuusympäristön dynaaminen luonne, pysyä ajan tasalla viimeisimmistä kehityksistä kyberturva-alalla sekä suorittaa jatkuvaa tiedonkeruuta ja tiedon jakamista. Tietopaketti tarjoaa käytännön neuvoja ja ohjeita tietoturvaan liittyvissä kysymyksissä ja auttaa ymmärtämään digitaalisen viestinnän turvallisuusuhkia ja niiden hallintaa. Se sisältää parhaita käytäntöjä sekä laadukkaita linkkejä vastaamaan ajan haasteisiin.

Avainsanat: kyberturvallisuus, digitaalinen viestintä, digitaalisen viestinnän ammattilaiset, henkilötietojen suojaus, luottamuksellisuus, jatkuva oppiminen, yksilön vastuu, tietopaketti, verkkotoiminta, turvallisuusuhkat, parhaat käytännöt, laadukkaat linkit, omaehtoinen perehdyttäminen, itseopiskelu, dynaaminen turvallisuusympäristö, tiedonkeruu, tiedon jakaminen, digitaaliset muotoilijat

---

Abstract

Author(s):	Samuel Kallio
Title:	Information Security and Cybersecurity in Digital Media: The Perspective and Responsibility of a Digital Designer
Number of Pages:	46 pages + 3 appendices
Date:	17 April 2024
Degree:	Bachelor of Culture and Arts
Degree Programme:	Degree Programme in Media
Specialisation option:	Professional Major Digital Media
Instructor(s):	Markus Norrena, Head of Degree Programme in XR Design and Senior Lecturer in Digital Design

---

The main objective of this thesis was primarily to explore the significance of information security and cybersecurity in the context of digital communication. The secondary aim was to map out and analyze the extent of the role of digital communication professionals and their information needs regarding these security issues. Additionally, there was a significant focus on the typical cyber threats and their impacts on the security of digital communication.

Given the nature of the topic, albeit it being inherently timely, intense, and subject to change, made it even more crucial to understand the effects of the changes that have occurred at the interface of communication and digitalization. Based on the same line of reasoning, it was justified to emphasize the importance of continuous learning and individual responsibility concerning the topic. Ultimately, the scale of the topic is determined by each individual until the level of required security protocol has been established by an outside authority or an actual cyber threat emerges.

My thesis covers concepts and principles related to information security and cybersecurity. These concepts are approached from the perspective of digital communication, in terms of protecting personal data, maintaining confidentiality, and creating a better overview. Such an approach to the current topic requires a comprehensive understanding of the multifaceted and wide-ranging domain of digital communication. One of the primary objectives of this research was to generate a practical information package to help make more informed decisions online.

It is essential to consider the dynamic nature of the security environment, stay up-to-date with the latest developments in the cybersecurity field, and engage in continuous data collection and dissemination. The information package has been designed to help navigate the security threats of digital communication and their management. It includes best practices and high-quality links to address the challenges of self-directed learning.

Keywords: information security, cybersecurity, cyber threats, cyber hygiene, digital communication, digital communication professionals, online activities, personal data protection, confidentiality, continuous learning, individual responsibility, information package, dynamic security environment, data collection, dissemination, digital designers

Sisällys

1 Johdanto

Digitalisaatiosta on puhuttu paljon merkittävänä muutosvoimana, joka kiihdyttäisi yritysten tuottavuutta ja loisi arvoa koko taloudelle. Sen sijaan olemmekin kohdanneet ”tuottavuusparadoksin”, jossa nopeiksi arvioidut digitalisaatioaskeleet ovat osuneet yksiin kokonaistuottavuuskasvun pitkäaikaisen hidastumisen kanssa viimeisten vuosikymmenten aikana. Tämä todetaan Euroopan keskuspankin Working Paper Series -julkaisussa (2023). Siirtyminen digitaaliseen talouteen on vahvistunut ensisijaiseksi tavoitteeksi sekä päättäjien että kansainvälisten instituutioiden keskuudessa. Tämä on edellyttänyt monien erilaisten käytäntöjen käyttöönottoa, joilla pyritään kiihdyttämään digitaalisen teknologian käyttöönottoa ja siten lisäämään tuottavuutta. (Anderton, Botelho & Reimers 2023, 4.)

Generatiivisen tekoälyn nopean kehityksen on arvioitu muuttavan monia työtehtäviä radikaalisti. Sen laajempi soveltaminen voisi tuoda merkittäviä hyötyjä talouskasvulle ja tuottavuudelle. Vastaavasti tekoälyn vaikutusten on odotettu näkyvän monissa ammateissa eri toimialoilla. Aiempien Digibarometrien perusteella tiedämme, että Suomi on heräämisensä jälkeen sijoittunut hyvin, ja vuoden 2023 tulokset vahvistavat tämän trendin. (Ali-Yrkkö, Kässi, Pajarinen & Rouvinen 2023, 27.) Näiden tosiasioiden valossa, sekä tässä digitalisaation vallankumouksellisen muutosvoiman myllerryksessä, on johdonmukaista ja perusteltua nostaa esille kysymys Suomen sijoituksesta tietoturvan ja kyberturvallisuuden osalta.

Huomionarvoista aiheen kannalta on muutoksen vastaanottaminen hallitusti ja sen vaikutuksille alttiiden osapuolten osallistaminen. Siitä pääsemme tutkimukseni aiheeseen tietoturvan ja kyberturvallisuuden merkityksestä digitaalisessa viestinnässä sekä olennaisten avainhenkilöiden, kuten digitaalisten muotoilijoiden, roolista ja vastuusta. Digitaalisen viestinnän juuret ovat perinteisessä viestinnässä, jossa korostuvat vastuullisuus, avoimuus ja ammattitaito. Laadukkaan

viestinnän kolme peruspilaria auttavat kohdentamaan huomion tämän tutkimuksen keskeiseen pohdintaan digitaalisen viestinnän merkityksestä. Digitaalisen viestinnän ammattilaisen roolista ja eri vastuualueiden merkityksistä vastuullisuus ja strateginen merkitys korostuvat suomalaisessa viestintäkulttuurissa nykyään yhä enemmän. (Liana Technologies 2023.)

Nykyaikainen digitaalinen viestintä on tuonut mukanaan uusia ilmiöitä ja haasteita, kuten tietoturvaan liittyviä riskejä, joita ei aiemmin tarvinnut ottaa huomioon perinteisessä viestinnässä. Relevantin tiedon tarvetta osaltaan kasvattavat myös maailman tapahtumien nopeat muutokset, kriisit, sodat, katastrofit ja levottomuudet yleensä. (Liana Technologies 2023.) Strateginen viestintä on moniulotteista ja monitasoista suunnitelmallisesti toteutettua viestintää. Viestintä ei pelkästään määrää maailman suuntaa, vaan sen vuorovaikutteisen luonteen ansiosta sillä voidaan vaikuttaa ja määrittää suuntaviivoja myös yksilöille eri puolilla maailmaa. Viestinnän ammattilaisilla tai kenellä tahansa, joka osaa tulkita viestejä, hallita niitä ja luoda merkityksiä, on valta ja vastuu määritellä tulevaisuutta. (Kääntä & Salmela 2018, 2, 7, 40, 82.)

Digitaalisen viestinnän ammattilaisella on siis paitsi eettis-moraalinen vastuu suhteessa viestimänsä tiedon strategisiin vaikutuksiin myös ammatillinen rooli omalla esimerkillään edistää turvallisempaa verkkokäyttäytymistä. Kyseisen viitekehyksen ymmärtämistä auttaa oikeanlaisten kysymysten esittäminen. Tämä opinnäyte keskittyy kartoittamaan digitaalisten muotoilijoiden tiedontarpeita tietoturvasta ja kyberturvallisuudesta. Niiden kannalta olisi olennaista hahmottaa digitaalisen muotoilijan työtehtävien laajuus ja niiden suhde erilaisiin pilvipalveluihin, alustoihin ja verkostoihin. Lisäksi tutkimuksessa painotetaan jatkuvan oppimisen merkitystä, mikä on välttämätöntä nykyaikaiselle digitaalisen muotoilun ammattilaiselle. Samalla tarkastellaan yksilön vastuun merkitystä lähempää.

2 Tutkimuskysymys ja menetelmät

2.1 Tutkimuskysymyksen ja ongelman määrittely

Viestinnän kontekstissa digitaalinen kehitys on muuttanut perinteisen viestinnän ja markkinoinnin raja-aitoja (Kääntä & Salmela 2018, 13). Digitaalinen viestintä on numeerisesti koodattua kommunikaatiota elektronisilla välineillä. Se käsittää digitaalisesti siirrettävää ääntä, kuvaa ja tekstiä sekä mahdollistaa hypertekstin ja multimedian käyttämisen. Tämän tyyppistä mediaa voidaan luoda, katsella, muokata ja jakaa elektronisten laitteiden avulla. Digitaalisia medioita käytetään yleisesti ohjelmistoissa, videopeleissä, videoissa, verkkosivustoissa, sosiaalisessa mediassa ja verkkomainonnassa. Digitaalisen viestinnän monia hyötyjä ovat sen mahdollistamat nopean ja tehokkaan tiedonvälityksen työkalut eri sidosryhmien kesken organisaation sisällä ja sen ulkopuolella. Digitaalinen viestintä voi sisältää monenlaisia välineitä, kuten sähköpostit, pikaviestit erilaisissa sovelluksissa, videoneuvottelut ja sosiaalisen median alustat. Tässä opinnäytetyössäni keskityn tutkimaan, miten nämä viestintävälineet vaikuttavat tietoturvaan, samalla, kun pyrin kartoittamaan parhaita toimintamalleja niiden käyttämiseen turvallisesti ja vastuullisesti.

Yhtä lailla viestinnällisesti kriittinen osa-alue löytyy kriisiviestinnän viitekehyksestä, jossa digitaalinen viestintä on avainasemassa kriisitilanteissa, kuten tietomurroissa, tietovuodoissa sekä muissa turvallisuusuhaksi luokiteltavissa tilanteissa. Kriisiviestinnän kannalta huomionarvoisia ovat ennaltaehkäisevät ja valmistavat toimenpiteet sekä kyky reagoida nopeasti. Etukäteen suunnitellussa prosessissa valppaus, ennakoiva päätöksenteko ja hajautettu viestintäprosessi lunastavat paikkansa kriisitilanteissa. (Juholin 2013, 330, 377.) Digitaalinen viestintä on hyvä keino vaikuttaa myös organisaation sisäiseen ilmapiiriin ja kulttuuriin. Laadukkaasti suunniteltu ja hyvin toteutettu organisaation sisäinen markkinointi voi olla merkittävä voimavara yritykselle. Sillä on paitsi psykologista

merkitystä, sillä voidaan myös parhaimmillaan onnistua vaikuttamaan työntekijöiden sitoutumiseen ja tuottavuuteen.

2.2 Käytetyt tutkimusmenetelmät

Opinnäytetyöni tutkimuksen tavoitteena on ensisijaisesti selvittää tietoturvan ja kyberturvallisuuden merkitys digitaalisen viestinnän kontekstissa. Digitaalisen muotoilijan roolin ymmärtäminen digitaalisen viestinnän viitekehyksessä auttaa sen tehtävien kartoittamista ja niiden ulottuvuuden hahmottamista eri verkostoihin. Tämä opinnäytetyö on konstruktiivinen tutkimus, jonka yhtenä tavoitteena on luoda konkreettinen tuotos, kuten esimerkiksi uusi tuote, järjestelmä tai suunnitelma. Suunnitelma on sisältönsä puolesta parhaat käytännöt esittelevä ja niihin viittaavan lyhytlistauksen kattava tuotos, joka keskittyy tietoturvan ja kyberturvallisuuden kannalta olennaisten kysymysten käsittelyyn digitaalisen muotoilijan työssä. Suunnitelma voi myös aloittaa sarjan julkaisuja, joista ensimmäinen on tämän tutkimuksen yhteydessä laadittu. Se voi olla myös eräänlainen elävä dokumentti, kuten verkkosivusto, joka muuttuu ja jota päivitetään uusilla ja ajankohtaisilla linkeillä.

Konstruktiivisen tutkimuksen prosessi käsittää ongelman määrittämisen sekä teoreettisen ja käytännöllisen tiedon hankinnan. Niiden pohjalta prosessiin kuuluu myös ratkaisumallien toimivuuden testaaminen ja niiden oikeellisuuden osoittaminen, jotka tämän tutkimuksen osalta pohjaavat alan kyberturva-asiantuntijoiden suosituksiin. Kvalitatiivisessa analyysissa hyödynnetään sekä kyselytutkimuksella että haastatteluilla keräämääni aineistoa teema-analyysin avulla. Tavoitteena on tunnistaa toistuvia teemoja ja kuvioita vastauksissa. Dokumentaation osalta pyritään reflektoimaan kerätyn aineiston luonnetta ja sen yhteyksiä tutkimuskysymyksiin sekä selittämään, miten analyysimenetelmät tukevat tutkimuksen tavoitteiden saavuttamista.

Opinnäytetyöni lähdemateriaalina käytän tietoturvaa ja kyberturvallisuutta käsittelevää kirjallisuutta, digitaalisia julkaisuja ja artikkeleita sekä alan tunnettujen ja luotettavien toimijoiden julkaisemia blogikirjoituksia ja muita e-julkaisuja. Lähdemateriaalin valinnassa kiinnitin erityistä huomiota tietoturva- ja kyberturvallisuusalan johtaviin tutkimuslaitoksiin sekä alan asiantuntijoiden julkaisemiin teoksiin. Aiheeseen perehtyminen syvällisemmän tapahtuu erilaisilla kyberturvallisuuteen keskittyneillä koulutusalustoilla ja verkko-oppimisympäristöissä. Niiden kautta pyrin hankkimaan kokonaisvaltaisemman käsityksen aihepiirin laajuudesta ja tuottamaan laadullisesti relevantin tuotoksen parhaiden käytäntöjen osalta. Tutkimukseni luotettavuutta pyrin arvioimaan vertailemalla eri näkökulmia voidakseni tunnistaa ja ratkaista mahdollisia ristiriitoja.

2.3 Tietoturva ja kyberturvallisuus käsitteinä

Tietoturva ja kyberturvallisuus ovat käsitteitä, joita käytetään usein synonyymeinä, vaikka niillä selkeitä eroja niiden tarkkojen merkityksiensä suhteen. Molemmat ovat käsitteitä, jotka liittyvät tietojen ja tietojärjestelmien suojaamiseen erilaisilta uhilta ja vaaroilta. Tietoturva on näistä kahdesta se, kumpi viittaa laajempaan käsitteeseen, joka kattaa kaikki toimenpiteet ja käytännöt tietojen suojaamiseksi kaikenlaisilta uhilta. Tietoturva kattaa muuan muassa fyysiset turvatoimet, kuten lukot ja valvontakamerat, sekä digitaaliset turvatoimet, kuten salasanat ja kryptografian eli tietojen salauksen. Kyberturvallisuus puolestaan keskittyy nimenomaisesti digitaalisten järjestelmien ja verkkojen suojaamiseen tietoverkkohyökkäyksiltä ja tietoturvauhilta.

Kyberturvallisuus on ikään kuin tietoturvasektorin digitaalinen segmentti, mikä käsittelee erityisesti tietoverkkoihin, tietotekniikkaan ja tietokoneisiin liittyviä riskejä ja haavoittuvuuksia. Palomuurit, haittaohjelmien torjuntaohjelmistot, salaustekniikat ja tietoturva-alan parhaat käytännöt kuuluvat kybertuvallisuuden piiriin. Lyhyesti asia ilmaistuna, tietoturva on laajempi käsite, joka kattaa kaikki tietojen

suojaamisen näkökohdat, kun taas kyberturvallisuus keskittyy erityisesti digitaalisten järjestelmien ja verkkojen suojaamiseen. (Calder 2022.)

Yrityksille kyberturvallisuus merkitsee ennen kaikkea toimintavarmuutta. Sen avulla suojaudutaan uhkia vastaan, ennalta ehkäistään ja torjutaan niitä sekä lievennetään niiden seurauksia. Kyberturvallisuuden merkitys ei kuitenkaan ole pelkästään negatiivinen uhka, vaan sitä voidaan parhaimmillaan hyödyntää ja se voi luoda uutta kehitystä, tehostaa ja laajentaa yrityksen toimintaa sekä tarjota uusia mahdollisuuksia. Kyberturvallisuuden takaaminen on olennainen osa tulevaisuuden toiminnan turvaamista. (Laitinen 2023.)

3 Tietoperusta tai teoreettiset lähtökohdat

3.1 Digitaalisen viestinnän merkitys

Digitaalisen viestinnän juuret ovat perinteisessä viestinnässä, jossa korostetaan vastuullisuutta, avoimuutta ja ammattitaitoa (Liana Technologies 2023). Nämä kolme laadukkaan viestinnän peruspilaria auttavat kohdentamaan huomion tämän tutkimuksen keskeiseen pohdintaan digitaalisen viestinnän merkityksestä. Digitaalisen viestinnän ammattilaisen roolista ja eri vastuualueiden merkityksistä vastuullisuus ja strateginen merkitys korostuvat suomalaisessa viestintäkulttuurissa nykyään yhä enemmän. Nykyaikainen digitaalinen viestintä on tuonut mukanaan uusia ilmiöitä ja haasteita, kuten tietoturvaan liittyviä riskejä, joita ei aiemmin tarvinnut ottaa huomioon perinteisessä viestinnässä. Relevantin tiedon tarvetta osaltaan kasvattavat myös maailman tapahtumien nopeat muutokset, kriisit, sodat, katastrofit, ja levottomuudet yleensä. Kriisitilanteissa informaation kysyntä kasvaa, ja epävarmuuden vallitessa tarvitaan uskottavaa ja ajanmukaista tietoa (Liana Technologies 2023).

3.2 Tietoturvan ja kyberturvallisuuden kasvava rooli

Kyberturvallisuuden rooli on muodostunut merkittäväksi ilmiöksi yhteiskunnissamme viimeisen kymmenen vuoden aikana. Aiemminkin, mutta sen tiedostaminen on korostunut sitä mukaa, kun yhteiskunnan palvelut ja prosessit ovat sähköistyneet. Uudet palvelut suunnitellaan nykyään alusta asti pelkästään tietokoneiden välityksellä käytettäviksi. Samoin organisaatioissa käytettävien digitaalisten työkalujen hyödyntäminen on lisääntynyt myös huomattavasti. Elinkeinoelämän tutkimuslaitoksen mukaan se tarkoittaa kyberuhkien tilannekuvan radikaalia muutosta lyhyessä ajassa sekä kyberturvallisuuden merkityksen lisääntymistä. (Savolainen 2022, 5.)

Vain muutamia vuosia sitten kyberuhkiin varautuminen suomalaisissa yrityksissä oli jäämässä muiden Pohjoismaiden vauhdista. Suomen heräämisen myötä kyberturvallisuuspalveluiden ja -tuotteiden kysyntä on lisääntynyt ja lisääntyy edelleen. Kyberturvallisuuteen keskittyneen alan liikevaihdon ennustetaan kasvavan noin kymmenen prosentin vuositahtia. Kyberturvayritysten liikevaihdoksi arvioitiin globaalisti noin 125 miljardia euroa vuonna 2017. Suomen kyberturva-alan edunvalvontajärjestön FISC:n mukaan kyberturvallisuusalan kasvua ja mahdollisuuksia Suomessa jarruttaa akuutti osaajapula. Vastaavasti kyberuhkien nopea kasvu vaikuttaa digitaaliseen kulutuskysyntään. Esimerkiksi Etlan tutkija Juri Mattila kertoi jopa 58 prosentin kotimaisista kuluttajista jättäneen kokonaan käyttämättä joitakin digitaalisia tuotteita tai palveluita vuonna 2019 johtuen niihin liittyvistä turvallisuusepäilyistä. (Päivän Lehti 2020.)

Kyberturvallisuuden kasvava rooli näyttäytyy nykypäivänä monella sektorilla aiempaa selkeämmin. Kyberturvakeskukselta on saatavilla laadukasta informaatiota pidemmän aikavälin ilmiöistä samoin kuin viimeisimmän lyhyemmän ajanjakson kybersää tammikuulta 2024. Siitä ilmenee kyberturvallisuuden kasvavan roolin merkitys eri viitekehyksissä. Viimeaikaiset maailmantapahtumat ja niiden vaikutukset ovat nähtävillä kyberturvallisuuden yleiskuvassa, kun venäläismielisten haktivistiryhmien palvelunestohyökkäykset jatkuivat alkuvuodesta

2024. Suomeen kohdistuneiden kyberhyökkäysten määrä on noussut, joten kyberympäristön uhkataso on pysynyt kohonneena. Merkittävä uhka organisaatioille ovat vuoden 2023 aikana havaittujen palvelunestohyökkäysten lisäksi olleet yhä lisääntyneet kyberrikollisten kiristyshaittaohjelmat. (Kyberturvallisuuskeskus 2024.) Kyberuhkien konkretisoitumien muuttuneen maailmantilanteen myötä on nostanut suomalaisten tietoturvatietoisuutta, ja samalla tietoturvan näkyvyys erityisesti suuryritysten johdossa on parantunut. Palo Alton teknisenä johtajana Suomessa työskentelevä Antti Lehtonen toivoisi tietoturvariskien tiedostamisen näkyvän enemmän myös ennakoivina tekoina. Tietoturvan näkyvyys on parantunut erityisesti suuryritysten johdossa eikä sen merkitystä vähätellä enää pienemmissäkään yrityksissä. (Lehtinen 2022.) Kyberhyökkäysten kohteeksi joutumisen mahdollisuus on alettu tiedostamaan digitaalisen viestinnän viitekehyksessä konkreettisena mahdollisuutena niin pienissä kuin suuremmissakin organisaatioissa.

3.2.1 COVID-19-pandemian vaikutukset kyberturvallisuuteen

COVID-19-pandemian vaikutukset loivat monitahoisen asetelman suhteessa etätyöskentelyyn. Yritysten ja organisaatioiden vanhat työskentelymenetelmät ja tottumukset menivät kertaheitolla uusiksi, kun hallitustasolta annettujen COVID-19-pandemian määräysten ja suositusten noudattaminen edellytti talon sisäisten työntekijöiden siirtymistä etätöihin. Nopean aikataulun sisällä pakotettu siirtyminen verkon yli työskentelyyn johti kyberturvatilanteiden ja niihin liittyvien uhkatasojen nousuun. Siirtyminen joko kokonaan tai osittain etätyöskentelymallin mukaiseen toimintatapaan tapahtui monessa organisaatiossa ilman asianmukaista verkkotukipalveluita tai digitalisoitumisen mahdollisuuksia. Kuvaavaa pandemian aiheuttamien kulujen ja tuhojen korjaamisen kannalta on Euroopan unionin elvytystoimien yhtenä pääkohtana keskittyä yritysten digitalisaation ja etätyöskentelyn kehittämiseen ja turvaamiseen. (Rantala 2021, 6.)

3.2.2 Etätyön vaikutus tietoturvaan

Vaikka Suomessa ei ole virallisesti olekaan mitään etätyön määritelmää, niin Työturvallisuuskeskus määrittelee etätyön seuraavalla tavalla: ”Etätyöllä tarkoitetaan joustavaa, vapaaehtoisuuteen, sopimukseen ja sääntöihin perustuvaa työn tekemistä muualla kuin työnantajan tiloissa. Työskentely voi tapahtua yhdessä tai useammassa paikassa ja olla kestoltaan ja säännöllisyydeltään hyvin vaihtelevaa.” (Työturvallisuuskeskus 2023.) Puhuttaessa etätyöstä ja sen laadukkaan suorittamisen edellytyksistä on toimivan teknologian ja tietoturvan merkitys kiistaton. Lisäksi huomionarvoinen aspekti etätyön luonteen kannalta on henkilötietojen käsittely, kuten henkilötietojen kerääminen, säilyttäminen, siirtäminen ja luovuttaminen. Tietosuojalainsäädännössä on säädetty tietosuojaperiaatteet, joita on aina noudatettava henkilötietojen käsittelyssä. Etätyöasetelmasta huolimatta etätyöntekijän käsittelemien tietojen tulee tietosuojaustasoltaan vastata samaa kuin työnantajan tiloissa, mikä osaltaan korostaa henkilötietojen käsittelijän omaa vastuuta tietosuojan huomioimisessa. (Heikkinen 2022, 24.)

COVID-19-pandemian aikana koetut muutokset ovat vaikuttaneet merkittävästi tietoturvaan etätyön yleistymisen myötä. Organisaatioiden siirtyminen laajamittaiseen etätyöhön on korostanut tietoturvaan liittyviä muutoksia. Työnantajan rooli ja vastuu etätyön tietoturvan kannalta on keskeinen, ja riskeihin on varauduttava jo etukäteen. Vastuunjaon kannalta tietoturvan järjestäminen kuuluu työnantajan vastuulle, kun toimintatapojen ja tietojen käsittelyn osalta vastuu siirtyy työntekijälle. Lisäksi työnantaja valitsee keinot tietojen suojaamiseen riippuen työn luonteesta ja suojattavan tiedon tärkeydestä. Tähän suojaamisen kategoriaan kuuluvat myös käytettävät välineet ja tietoliikenneyhteydet sekä mahdolliset suorat yhteydet työpaikan sisäverkkoon. Huomionarvoista on työnantajan vastuu myös tilanteissa, joissa työn tekemiseen käytetään työntekijän omia henkilökohtaisia välineitä. (Heikkinen 2022, 25–28.)

Tietoturvauhilta suojautumisen yksi tärkeimmistä toimenpiteistä on johdon laatima tietoturva- ja tietosuojapolitiikka, josta selviää johdon näkemys tavoitteista aiheen kannalta. Olennaista ja suoranainen edellytys onnistuneen tietosuojan ja tietoturvan kannalta on johdon tuki ja osallistuminen (Heikkinen 2022, 27.) Edellä mainittujen lisäksi on hyvä laatia kyberturvallisuusstrategia, johon on määritelty liiketoiminnan turvaaminen normaali- ja häiriötilanteessa. Se mahdollistaa nopean reagoinnin proaktiivisesti sekä tuottaa edellytyksiä priorisoida toimenpiteitä turvallisuutta johdettaessa. Kyberturvallisuusstrategian tulisi kattaa seuraavat aiheet: kyky kestää häiriötilanteita sekä nykyhetkellä että tulevaisuudessa, tietoturvakustannukset, mainehaitan ja menetetyn liikevaihdon arviointi, todennäköisimmät uhat ja niiden jälkien selvittely, haluttu kyberturvan taso sekä sovellettavat lait ja asetukset. (Heikkinen 2022, 27.)

3.3 Digitaalisen median tulevaisuuden uhkakuvia

Vaikka tekoälyn tuomiin haasteisiin on liitetty paljon monenlaisia uhkakuvia ja skenaarioita, kuten esimerkiksi sen kyvystä koodata aiempaa parempia haittaohjelmia, niin ainakin toistaiseksi sen vaikutukset aidosti toimivien haittaohjelmien osalta ovat olleet rajalliset. Pidemmän aikavälin kyberturvaennusteen kannalta on järkevää pysyä relevantin tiedon parissa ja seurata, miten asiat kehittyvät tekoälyn ympärillä. Organisaatioissa olisi hyvä tunnistaa tekoälyn tuomia haasteita ja varautua niihin liittyvien uhkien torjumiseen esimerkiksi lisäämällä oman henkilökunnan koulutusta aiheesta. (Soini 2018.) Tekoälyn ohella digitaalinen media pitää sisällään laajan kirjon erilaisia ilmiöitä, joista suuren osan huomiosta on saanut tekoälyyn perustuva sisältögenerointi. Tämän aspektin tarkastelu, jaotteleminen erilaisiin kokonaisuuksiin ja niiden uhkatekijöihin syventyminen onkin jo itsessään merkittävä aihepiiri.

Tämän tutkimuksen kannalta olennaista on keskittyä enemmänkin erilaisten digitaalisen median alustojen hyödyntämiseen ja niiden käyttöön liittyviin

tulevaisuuden tietoturva- ja kyberturvallisuusuhkiin. Sosiaalinen media osana digitaalista viestintää pitää sisällään monia ajankohtaisia ilmiöitä ja ansaitsee kaiken mahdollisen eettis-moraalisesti perustellun huomion kyseenalaisen luonteensa takia. Tämä opinnäyte ei kuitenkaan keskity siihen. Olennaiseksi aiheen kannalta nousevat kysymykset digitaalisten työkalujen, datan siirron ja keräämisen sekä kyseisen toimintaympäristön suhteen relevantit uhkatekijät ja tulevaisuuden näkymät.

3.3.1 Datan keräämisen pimeä puoli – ”jumalsovellukset”

Tulevaisuuden uhkakuvista on esitetty monipuolisesti erilaisia teorioita. Niistä on kirjoitettu kirjoja, kuten esimerkiksi George Orwellin teokset. Hyvä esimerkki on hänen klassinen dystooppinen romaaninsa Vuonna 1984, jossa on kuvattu totalitaarista valvontayhteiskuntaa, jossa yksilönvapaudet on kavennettu ja “Isoveli valvoo”. Kyseinen teos on paitsi hyvin tunnettu myös erinomainen esimerkki teoksesta, joka on vaikuttanut syvästi tulevaisuuden uhkakuvia käsittelevään fiktioon. Se on inspiroinut useita elokuvia ja televisiosarjoja ja on edelleen ajankohtainen. Näillä tulevaisuuden uhkaskenaarioilla on usein yhteistä jonkinlainen kulissien takana toimiva taho, kollektiivi tai kontrolloiva entiteetti. Miten paljon kyseessä on validi argumentti Orwellin kirjassa kuvatun dystopian puolesta kuin esimerkiksi uudelleenlöytämisen trendistä, sitä pohtii myös Miikka Vuori artikkelissaan. Orwellilaisuudesta puhuttaessa tehdään paljon rinnastuksia, mutta teoksen dystopia ei ole seurausta kierosta teknologiasta vaan yhteiskunnasta. (Ks. Vuori 2023.)

Nyt tämä näkymätön voima kuitenkin on täällä. ja se on tullut jäädäkseen. Näin kertoo Heikki Soini artikkelissaan, jossa hän summaa YLE Puheen ohjelmantekijöiden Jani Halmeen ja Tomi Saarisen listaamaa seitsemää tärkeintä asiaa, joiden he uskovat tapahtuvan digitaalisessa mediassa lähitulevaisuudessa (Soini 2018). Näkymättömän bittikäden ulottuvuudesta on tullut osa arkitodellisuuttamme, ja olemme sen otteessa kiinni yhä tiukemmin jatkossakin.

Näkymättömällä bittikädellä tarkoitan algoritmien ohjaamaa verkkokäyttäytymistä. Nimittäin joukko sääntöjä tai paremmin julkaisualgoritmien käyttämät säännöt määrittävät sen, mitä meille yksilöinä digitaalisessa mediassa näytetään. Tulevaisuudessa olemme entistä tiiviimmin omassa massamediakuplassamme. (Soini 2018.) Tämä kehityksen suunta herättää monella tapaa ristiriitaisia ajatuksia, vaikka se ei yllätyksenä tulekaan. Pikaviestinten rooli tulee jatkossa kasvamaan entisestään, ja niiden kehityssuunta on ollut rakentaa chat-palveluista käyttöliittymiä, joiden avulla voidaan hallita monenlaisia toimintoja. WeChat on hyvä esimerkki palvelusta, josta on tullut todellinen jumalsovellus Kiinassa. Sitä käytetään laskujen maksamiseen, ruokatilausten tekemiseen ja ruuhkatilanteen tarkastamiseen. Datan keräämisen pelottavat puolet ovat myös hyvin havaittavissa Kiinassa, kun paikalliset IT-yhtiöt ovat valtion tukemina alkaneet pisteyttää asiakkaitaan heidän käyttäytymisensä perusteella. Sosiaalinen luottojärjestelmä on tehokas keino toisinajattelijoiden nujertamiseksi. (Soini 2018.)

3.3.2 Syväväärennökset ja informaatiovaikuttaminen

Viimeaikaisia trendejä kyberrikollisuuden ilmiöistä digitaalisessa viestinnässä ovat syväväärennökset (engl. deepfake). Syväväärennökset ovat aidolta vaikuttavaa kuva-, video tai äänimateriaalia. Lopputuote syväväärennöksestä saadaan joko yhdistelemällä tai muuntamalla olemassa olevaa materiaalia koneoppivan tekoälyn avulla. Deepfake-tekniikan käytöstä kyberhuijauksissa on kansainvälisessä uutisoinnissa puhuttu jo pidempään. Syväväärennösten käyttäminen informaatiovaikuttamisessa on yleistynyt. Deepfake-tuotokset ovat erinomaisia keinoja väärän tiedon levittämiseen, kun halutaan vaikuttaa esimerkiksi yhteiskunnalliseen keskusteluun, politiikkaan tai vaaleihin. (Kyberturvallisuuskeskus 2024.) Samoin kuin väärän tiedon – disinformaation, epätiedon-erottaminen totuudesta myös deepfake-tuotosten tunnistaminen edellyttää kykyä tehdä oikeita havaintoja ja riittävää kriittisyyttä informaatiota kohtaan. Yksi tapa

oppia erottamaan tosiasiat propagandasta on asioiden jatkuva seuraaminen ja sen myötä karttuva kokemus oppia tekemään havaintoja. Miten tunnistaa syväväärennös etenkin, kun syväväärennöksien tunnistaminen vaikeutuu sitä enemmän, mitä paremmaksi teknologia kehittyy? Ammattimaisia vinkkejä syväväärennösten tunnistamiseen löytyy esimerkiksi Kyberturvallisuuskeskuksen sivuilta, kuten Kyberturvallisuuskeskuksen viikkokatsaus - 03/2024. (Kyberturvallisuuskeskus 2024.)

Ohessa muutamia vinkkejä auttamaan syväväärennösten tunnistamisessa. Olemalla mediakriittinen suhtaudut näkemääsi materiaaliin analyyttisesti, katselet ja kuuntelet näkemääsi sekä tutkit videota ja tarvittaessa pysäytät sen. Kuvissa olevien henkilöiden fyysiset ominaisuudet, kuten ihmisten sormien määrä, silmien liikkeet ja mahdolliset sumentumat ovat keskeisessä roolissa, kun etsitään poikkeavuuksia. Syväväärennöksissä väärennetyt kasvot voivat joskus näyttää luonnottoman tasaisilta, kun ne on asetettu alla olevan alkuperäisen hahmon kasvojen päälle. Ääniväärennöksien osalta voidaan kysyä jotain, mihin vain kyseinen henkilö osaa vastata. Lisäksi ääniväärennöksissä saatetaan käyttää epätyypillisiä ilmauksia tai niissä pyydetään tekemään jotain poikkeavaa tai yllättävää, kuten suuria rahansiirtoja. Tulevaisuudessa palveluntarjoajat pyrkivät yhä enemmän torjumaan myös syväväärennöksien väärinkäyttöä. Vaikka syväväärennösten tekeminen ja niiden käyttäminen houkutteleekin rikollisia, niin Kyberturvallisuuskeskukselle tehtyjen yksittäisten ilmoitusten valossa suomenkielisten syväväärennöksien käyttö ei vaikuttaisi olevan vielä kovin yleistä. (Kyberturvallisuuskeskus 2024.)

3.4 Kyberuhat ja tietoturva digitaalisessa ympäristössä

Tietoturva ja kyberturvallisuus ovat käsitteinä olennaisia digitaalisessa toimintaympäristössä. Samoin niiden rooli nyky-yhteiskunnassa on merkittävä, jopa keskeinen. Tietoturva on näistä kahdesta se laajempi käsite ja viittaa

käytäntöihin, jotka sisältävät kattavasti toimenpiteitä, kuten tietojen salauksen, vahvistetun tunnistautumisen ja järjestelmänvalvonnan, joilla voidaan suojata tietoja ja järjestelmiä. Kyberturvallisuus puolestaan liittyy tietoturvaan, mutta se keskittyy kohdennetusti digitaaliseen ympäristöön ja verkossa tapahtuviin uhkiin. Kyberturvallisuuden huomio on pyrkiä suojelemaan erityisesti verkossa tapahtuvilta hyökkäyksiltä, kuten haittaohjelmilta, tietomurroilta ja tietovuodoilta. Lisäksi kyberturvallisuus sisältää ennaltaehkäiseviä toimenpiteitä sekä strategioita reagoida mahdollisimman tehokkaasti ja nopeasti uhkien havaitsemiseksi ja torjumiseksi.

Digitaalisen viestinnän kontekstissa tietoturva ja kyberturvallisuus ovat keskeisiä siksi, että lähes kaikki nykyaikainen viestintä tapahtuu digitaalisessa muodossa, mikä käsittää sähköpostit, pikaviestit, sosiaalinen media, verkkosivustot ja muut digitaaliset alustat. Tämän kaltaisten viestimien hyödyntäminen ilman asiaan kuuluvaa tietoturvaa ja kyberturvallisuuden palveluita asettaisi viestinnän osapuolet alttiiksi erilaisille uhille ja mahdollisille väärinkäytöksille. Niitä ovat esimerkiksi tietovuodot, identiteettivarkaudet sekä tietojärjestelmien vahingoittaminen. Kaiken digitaalisen viestinnän sekä verkossa tapahtuvan toiminnan kannalta olisikin ensisijaisen tärkeää ymmärtää tietojen ja järjestelmien turvallisuuden varmistamisen merkitys. Soveltamalla parhaita tietoturva- ja kyberturvallisuuskäytäntöjä tehokkaasti on mahdollista luoda hyviä käytäntöjä ja edistää kyberhygieniaa omassa organisaatiossaan itsensä ja muiden suojaamiseksi.

3.4.1 Kyberturvallisuus osana digitaalista transformaatiota

Kyberturvallisuus osana digitaalista transformaatiota käsittelee digitaalisen transformaation ja digitalisaation välistä suhdetta sekä niiden vaikutusta organisaatioihin ja yhteiskuntaan. Vaikka nämä käsitteet liittyvät toisiinsa ja niitä käytetään joskus synonyymeinä, digitaalinen transformaatio on laajempi käsite, joka kattaa digitalisaation ja ulottuu strategisempiin ja syvällisempiin muutoksiin organisaatiossa. Digitalisaatio viittaa prosessiin, jossa perinteisiä toimintoja,

kuten palveluita tai prosesseja muutetaan digitaaliseen muotoon. Yksinkertaistettuna digitalisaatio nojautuu teknologian kehitykseen, minkä takia sen yhteydessä puhutaan usein digitaalisesta vallankumouksesta (Pilli 2023, 5).

Digitaalinen transformaatio puolestaan viittaa laajempaan muutokseen, joka kattaa organisaation toimintatapojen, liiketoimintamallien ja strategioiden kokonaisvaltaisen uudelleenmäärittelyn digitaalista teknologiaa hyödyntäen (Pilli 2023, 7). Se on globaali ilmiö, jonka huomionarvoinen rooli kannustaa merkittäviin investointeihin toimialasta riippumatta. Kuitenkin digitaalinen transformaatio ei ole yksittäinen tarkoitusperä, vaan se on monitahoinen lähestymismalli riippuen aina kyseessä olevan teollisuuden tai toimialan tavoitteista ja digitaalisesta maturiteetista (Möller 2023, 1). Organisaatioiden siirtyminen kohti digitaalista transformaatiota hyödyntämällä digitalisaatiota käsittää uusien digitaalisten teknologioiden ja prosessien käyttöönoton, mikä vaikuttaa myös niiden kyberturvallisuuteen.

3.4.2 Digimaturiteetin merkitys kyberturvan parantamiseksi

Saksassa, Reutlingenin yliopistossa, tutkimuksen tehnyt Alexander Rossmann oli vuonna 2018 päätynyt johtopäätökseen, jossa hän totesi digitaalisten toimintojen vahvistamisen organisaatiossa olevan merkittävä kilpailukykyä parantava tekijä. (Salonen 2024, 28.) Rossmann toteaa tutkimustulostensa edistävän digitaalisen kypsyyden – tai digimaturiteetin-konseptien teoreettista käsitteellistämistä sekä erilaisten relevanttien tekijöiden ymmärtämistä, jotka ohjaavat digitaalisen transformaation aloitteita yrityksissä. Hänen mukaansa ilman asianmukaisia digitaalisia toimintoja ei yritys olisi enää kauaa mukana kilpailussa. (Salonen 2024, 28.) Käsiteltäessä aihetta kyberturvallisuuden näkökulmasta on hyvä tiedostaa, mitä kybertoimintaympäristö tarkoittaa. Se ei tarkoita vain elektronista irrallista entiteettiä, vaan se koostuu ihmisten, organisaatioiden ja fyysisten järjestelmien yhdessä muodostamasta vaikutusympäristöstä. Siinä kokonaisuudessa jokaisella on oma roolinsa kyseisen ympäristön kyberturvallisuuden

ylläpidossa (Korhonen 2024, 18). Kybertoimintaympäristön näkökulmasta kyberturvallisuus osana digitaalista transformaatiota korostaa digimaturiteetin kasvattamisen merkityksen.

Yhdistäen Rossmannin digimaturiteettimallin ja kyberturvallisuuden näkökulman voidaan tarkastella, miten organisaation digitaalinen kypsyys tai valmius vaikuttaa sen kykyyn suojautua kyberuhilta ja varmistaa tietoturvan toteutuminen. Rossmannin digimaturiteettimallin kategorioita ovat muun muassa digitalisaatiostrategia, johtaminen, liiketoimintamalli, toiminta, henkilöstö, organisaatiokulttuuri, hallinto ja teknologia (Salonen 2024, 18). Tämän kontekstin sisällä organisaatio voi paremmin ymmärtää nykyisen tilansa suhteessa digimaturiteettiin ja tunnistaa kehityskohteita Rossmannin digimaturiteettimallin kategorioiden avulla. Näitä kategorioita hyödyntämällä organisaatiot voivat arvioida ja kehittää digimaturiteettiastettaan, mikä puolestaan muodostaa osan siitä laajemmasta ymmärryksestä, mitä meillä on kybertoimintaympäristöstä. Digimaturiteettimalli ja sen mittaaminen auttavat organisaatiota ymmärtämään nykytilanteensa sekä tunnistamaan heikkoudet ja vahvuudet digitalisaatiostrategian suunnittelussa. Lisäksi digimaturiteettimallia hyödyntämällä organisaation oman digitaalisen polun selkeyttäminen edistää oikeanlaisten teknologioiden hankintaa, mikä voi johtaa kustannussäästöihin ja vahvistaa kilpailuasemaa omalla toimialalla. Lopulta digimaturiteettimalli ohjaa organisaatiota etenemään oman digitaalisen muutoksensa kanssa ja pitämään asiakkaan tarpeet ensisijaisina kaikessa kehityksessä. (Salonen 2024, 41.)

Kyberturvallisuusstrategian tulisi sisältää seuraavat näkökohdat: kyky kestää häiriötilanteita nykyhetkellä ja tulevaisuudessa, tietoturvakustannukset, mainehaitan ja menetetyn liikevaihdon arviointi, todennäköisimmät uhat ja niistä toipuminen, kyberturvan toivottu taso sekä ne lait ja asetukset, jotka on otettava huomioon. Viisi tärkeintä oppia: 1) Digitaalinen maturiteetti mahdollistaa yrityksille kyberhyökkäysten tehokkaan hallinnan, jopa pienille ja keskisuurille yrityksille. 2) Secure DevOps- tai DevSecOps-menetelmä integroi tietoturvan kehitysprosessiin, mikä edistää yhteistyötä ja varmistaa tietoturvan koko

ohjelmistokehityksen elinkaaren ajan. 3) Aktiivinen sääntöjenmukaisuuden varmistaminen on tärkeää, ja digitaalinen kypsyys auttaa yrityksiä saavuttamaan ja ylläpitämään vaaditun sääntöjenmukaisuuden tason. 4) Turvallisuuskulttuurin juurruttaminen organisaatioon auttaa vähentämään inhimillisten tekijöiden vaikutusta kyberuhkiin ja parantaa yleistä tietoturvatietoisuutta. 5) Kybermaturiteettimallit tarjoavat puitteet yrityksen kybermaturiteetin arvioimiseen ja parantamiseen, ja ne ovat olennainen osa kokonaisvaltaista kyberturvallisuusstrategiaa. (IT Knowledge Zone 2023.)

3.4.3 Pilvipalveluiden vakiintuminen ja riskit

Pitkäaikaisesta kehityksen kaaresta huolimatta pilvipalvelut ovat yksi aikamme teknologiatrendejä. Pilvipalveluiden vallankumouksellista yleistymistä vuodesta 2010 lähtien siivitti internet ja nopeat verkkoyhteydet sekä tekniikan kehitys ja IT:n teollistuminen. (Tulisalmi-Eskola 2020, 14.) Kuten pilvipalveluiden luonteeseen kuuluu, ne tarjoavat asiakkailleen maailmanlaajuisessa mittakaavassa vaivattoman käyttöympäristön. Vaikka palveluntarjoajilla on usein vahvemmat tietoturvaresurssit kuin heidän asiakkaillaan, siitä huolimatta pilvipalveluihin liittyy erilaisia riskejä, jotka organisaatioiden on syytä huomioida. Puhuttaessa pilvipalveluiden kokonaisturvallisuudesta on hyvä ymmärtää niiden muodostuvan kokonaisuudesta, johon vaikuttavat sekä palveluntarjoajan että asiakkaan tietoturvakäytännöt ja lopulta myös pilvipalvelusovelluksen tietoturva. Pilvipalveluihin liittyvät ei-tekniset riskit käsittävät esimerkiksi palveluntarjoajan poistumisen markkinoilta. Lisäksi maantieteellinen sijainti puolestaan vaikuttaa sovellettavaan lainsäädäntöön. Vastuu talletetusta datasta säilyy yrityksellä, vaikka pilvipalveluiden tarjoaja vastaa yrityksen puolesta turvallisuudesta. Lisäksi on olennaista varmistaa, että datan säilytyspaikka täyttää asianmukaiset säädökset, kuten esimerkiksi EU:n tietosuoja-asetuksen (GDPR) vaatimukset. (Tulisalmi-Eskola 2020, 19.)

Kyberturvallisuuden osalta suuret globaalit pilvipalveluiden tuottajat tarjoavat monelta osin samankaltaisia ratkaisumalleja vastuun jakamisesta palveluntuottajan ja asiakkaan kesken. Esimerkiksi pilvialustansa turvallisuuden varmistaminen edellyttää palveluntuottajalta paljon valvontaa, raportteja sekä reagointikyvyn ylläpitämistä. Asiakkaan on puolestaan huolehdittava turvallisuudesta pilvessä. Tämä käsittää heidän käyttämiensä palvelukomponenttien asetukset ja konfiguroinnin, datan yhtenäisyyden ja salauksen, tietoliikenteen suojauksen sekä käyttäjien ja käyttöoikeuksien hallinnan. Lisäksi asiakkaan vastuulle kuuluu omalla pilvialustalla suoritettavien järjestelmiensä ja sovellustensa turvallisuuden varmistaminen. (Vaahtera 2022, 28–29.) Kyberturvallisuuskeskuksen listaamia pilviturvallisuuskäytäntöjä ovat pilvipalveluympäristön erottaminen muusta ympäristöstä ja sen jakaminen segmentteihin, kontrolloitu pilvipalvelun käyttöoikeuksien hallinta, kirjattu pilven kattava tietoturvakäytäntö, relevantti IT-turvallisuusosaaminen, toimivat pilven hallinnointikäytännöt, järjestelmän ja sen käytön monitorointi sekä lopuksi osallistava turvallisuuskulttuuri. Näillä käytännöillä saadaan parempi ote kokonaisturvallisuudesta. Yksi hyödyllinen malli pilvipalvelujen turvallisuuden arvioimiseksi on Jerichon neliulotteinen pilvikuutiomalli. Tämä malli tarjoaa kokonaisvaltaisen näkemyksen pilvipalveluiden turvallisuudesta neljän ulottuvuuden kautta: palvelujen ja tietojen sijainti (paikallisuus), tietoturvakäytännöt, palvelujen saatavuus sekä liiketoimintamallit. Näiden ulottuvuuksien avulla organisaatiot voivat arvioida pilvipalvelujen soveltuvuutta omiin tarpeisiinsa ja tunnistaa mahdolliset riskitekijät. (Tulisalmi-Eskola 2020, 17.)

3.4.4 Pilvipalveluiden parissa esiintyvät turvallisuusuhat

Kyberturvallisuusosaamisen merkitys korostuu entisestään, kun syvennytään tarkastelemaan tietoturvan ja kyberturvallisuuden keskeisiä tekijöitä pilvipalveluiden kontekstissa. Pilvipalveluiden monimutkainen luonne edellyttää uhkien havainnoinnin sekä uhkavektorien tunnistamisen kannalta pilviympäristön

erityispiirteiden huomioimista. Kyberturvallisuuskeskuksen julkaisema pilviturvallisuuden arviointikriteeristö on hyödyllinen, koska se on laadittu pilvessä korostuvien uhkavektorien Suomen kansallisten tarpeiden näkökulmasta. Lisäksi se on suunniteltu laajasti hyödynnettäväksi viranomaisten ja elinkeinoelämän piirissä Suomessa. (Vaahtera 2020, 31.) Holistisen käsityksen saavuttaminen edellyttää aihepiirin laajuuden kartoittamisen lisäksi eri metodien ja lähestymistapojen tutkimista digitaalisen viestinnän ammattilaisen näkökulmasta. On tärkeää ymmärtää, että eri pilvipalvelualustat voivat poiketa teknisiltä ratkaisuiltaan ja arkkitehtuuriltaan, mikä vaikuttaa suoraan niiden turvallisuusuhkiin. Tämä auttaa digitaalisen viestinnän ammattilaisia tunnistamaan ja arvioimaan potentiaalisia riskejä omassa toimintaympäristössään ja varautumaan niihin asianmukaisesti. Traficomin pilvipalvelujen turvallisuuden arviointikriteeristö tarjoaa kätevän oppaan turvallisuustason arviointiin ja suojauksen vahvistamiseen. Kriteeristö kattaa 11 eri osa-aluetta, jotka auttavat suunnittelemaan pilvipalveluihin siirtymistä tai nykyisten palvelujen turvallisuuden arviointia. (Kyberturvallisuuskeskus 2020.) Tämän tutkimuksen tavoitteiden kannalta PiTuKri on konkreettinen esimerkki työkalusta, jonka avulla voidaan arvioida pilvipalveluiden turvallisuutta ja tunnistaa niihin liittyviä riskejä. Sen käytön tapauskohtainen soveltaminen luo vaatimuksia myös käyttäjän kannalta edellyttäen riittävää kyberturvallisuusosaamista. (Vaahtera 2020, 31; Kyberturvallisuuskeskus 2020.)

3.5 Digitaalisen muotoilijan rooli ja tiedontarpeet

Digitalisaation myötä kyberturvallisuuden taidoista on tullut kansalaistaitoihin rinnastettavaa toimintaa, joiden avulla vastuullinen kansalainen pystyy omalla käyttäytymisellään edesauttamaan yhteiskunnan säilymistä turvallisempana. Samalla tavalla digitaalinen muotoilija voi omalla toiminnallaan edistää kyberturvallisuutta omassa vaikutuspiirissään. Olennaista kullekin olisi tiedostaa tärkeimmät kyberturvallisuuden tekijät ja omaksua parhaat toimintatavat omassa roolissaan. Tehokas tapa hahmottaa digitaalisen muotoilijan ammatillisia

vastuualueita suhteessa tietoturvaan ja kyberturvallisuuteen on kartoittaa heidän työtehtäviänsä. Sitä kautta voimme tunnistaa digitaalisen viestinnän ammattilaisten tiedontarpeita ja paremmin ymmärtää, mitä tietoja ja taitoja he tarvitsevat tietoturvan ja kyberturvallisuuden hallintaan.

3.5.1 Digitaalisen muotoilijan monipuoliset vastuualueet

Digitaalisen muotoilijan rooli on tehtäviensä puolesta moniulotteinen, mikä tuo oman haasteensa kokonaisuuden hahmottamiseen. Siihen kuuluu päivittäin toistuvasti erilaisten autentikointi- ja pääsynhallintaprotokollien käyttöä ja pilvipalveluihin kirjautumista. Tämä tarkoittaa esimerkiksi sisäänkirjautumista eri verkkosivustoille ja sovelluksiin käyttäen tunnistautumistapoja, kuten käyttäjänimiä, salasanoja ja kaksivaiheista todennusta. Lisäksi digitaalisen muotoilijan on käytettävä erilaisia tunniste- ja salausavaimia sekä muita turvallisuusprotokollia varmistaakseen tietojen suojan ja turvallisen pääsyn erilaisiin palveluihin.

Pääsääntöisesti digitaalisen muotoilijan vastuualueisiin kuuluu digitaalisen viestinnän suunnittelua, toteutusta ja ylläpitoa. Tämä rooli edellyttää laaja-alaista osaamista eri aloilta, kuten web-kehityksestä, käyttäjäkokemuksen suunnittelusta, käyttöliittymäsuunnittelusta sekä graafisesta suunnittelusta. Tyypillisiä digitaalisen muotoilijan tehtäviä voivat olla verkkosivustojen ja mobiilisovellusten suunnittelu ja toteutus, käyttöliittymäsuunnittelu erilaisiin käyttäjärajapintoihin, digitaalisen sisällön tuottaminen eri kanaviin sekä visuaalisen ilmeen määrittäminen. Lisäksi digitaalisen muotoilijan rooli voi sisältää jatkuvaa yhteistyötä muiden ammattilaisten kanssa, kuten ohjelmistokehittäjien, markkinoijien ja käyttäjäkokemussuunnittelijoiden kanssa. Tavoitteena on varmistaa, että lopputuote täyttää sekä yrityksen että käyttäjän tarpeet ja odotukset. Tämän kaltainen monialainen lähestymistapa edellyttää digitaaliselta muotoilijalta joustavuutta, luovuutta ja teknistä osaamista eri alustoilla ja teknologioissa.

3.5.2 Tietoturvan merkitys digitaalisessa viestinnässä

Digitaalisen viestinnän kontekstissa tietoturva on ensisijaisen tärkeää, koska lähes kaikki nykyaikainen viestintä tapahtuu digitaalisessa muodossa. Sähköpostit, pikaviestit, sosiaalinen media, verkkosivustot ja muut digitaaliset alustat ovat olennainen osa viestintää, ja niiden käyttö ilman asianmukaista tietoturvaa altistaa osapuolet monille riskeille ja mahdollisille väärinkäytöksille. Tietoturva digitaalisessa viestinnässä kattaa laajan kirjon käytäntöjä ja menetelmiä, jotka auttavat suojaamaan tietoja ja järjestelmiä. Näihin kuuluvat muun muassa tietojen salaus, vahvistettu tunnistautuminen, järjestelmänvalvonta ja palomuurit. Ilman asianmukaista tietoturvaa viestintäkanavat voivat altistua monille riskeille, kuten tietovuodoille, identiteettivarkauksille ja tietojärjestelmien vahingoittamiselle.

Digitaalisen viestinnän ammattilaisen on ymmärrettävä tietoturvan merkitys ja osattava soveltaa asianmukaisia käytäntöjä ja menetelmiä omassa työssään. Tämä voi sisältää esimerkiksi tietojen salaamista, tietoturva-aukkojen tunnistamista ja korjaamista sekä käyttäjien koulutusta tietoturva-asioissa. Lisäksi digitaalisen viestinnän ammattilaisen on oltava tietoinen alan uusimmista tietoturvauhkista ja -trendeistä sekä osattava reagoida niihin tehokkaasti ja nopeasti. Tietoturvan huomiointi digitaalisessa viestinnässä on keskeistä sekä yksilölle että organisaatiolle, ja se edellyttää jatkuvaa valppautta sekä panostusta tietoturvaan liittyvään tietoon ja osaamiseen.

4 Teknologia, viestintä ja kyberturva opinnäytetyön kontekstissa

4.1 Teknologia, viestintä ja kyberturva

Digitaalisen viestinnän yleistyminen ja teknologian kehitys ovat yhdessä mullistaneet tapamme kommunikoida ja toimia verkossa. Tämä kehitys on tuonut

mukanaan uusia mahdollisuuksia, mutta myös haasteita, erityisesti tietoturvan ja kyberturvallisuuden näkökulmasta. Tämän osion tarkoituksena on auttaa hahmottamaan teknologian, viestinnän ja kyberturvan välistä yhteyttä sekä niiden merkitystä nykyaikaisessa yhteiskunnassa. Ensiksi avataan tietoturvan ja kyberturvallisuuden määritelmät ja niiden eroja. Sen jälkeen syvennytään keskeisiin käsitteisiin ja periaatteisiin näiden aiheiden kontekstissa. Seuraavaksi keskustellaan digitaalisen viestinnän roolista ja merkityksestä nykyaikaisessa yhteiskunnassa, jonka jälkeen siirrytään tarkastelemaan viestinnän merkitystä organisaatioissa ja yrityksissä. Lopuksi analysoimme lyhyesti teknologian vaikutusta digitaaliseen viestintään, kuten viestintäkanavien monipuolistumisen ja reaaliaikaisen viestinnän vaikutuksia, unohtamatta internetin globaalia aspektia.

4.2 Keskeiset käsitteet ja periaatteet

Tietoturvan ja kyberturvallisuuden määritelmät, niiden merkitys ja erot tulivat alussa läpikäytyä. Niiden ymmärtäminen on olennaista, jotta voidaan paremmin myös hahmottaa muita keskeisiä käsitteitä ja periaatteita aiheen kannalta. Lähempää kybermaailman uhkia tarkasteltaessa on havaittavissa niiden olevan moninaisia ja alati muuttuvia. Kyberuhiksi luokitellaan toimet, joiden tarkoituksena on aiheuttaa vahinkoa tai tuhota tietoverkkoja, -järjestelmiä tai päätelaitteita, tai vaikuttaa niihin siten, että niiden käyttömahdollisuudet tai tietosisällöt kärsivät. Nämä digitaalisen maailman kyberuhat voidaan jakaa viiteen eri ryhmään hyökkääjien motiivien perusteella: kybervandalismi ja haktivismi, kyberrikollisuus, kybervakoilu, kyberterrorismi ja kybersodankäynti. (Pöyhönen 2020, 34–35.) Jyväskylän yliopiston kyberturvallisuuden professori Martti Lehto on esittänyt kuusikerroksisen määritelmän hyökkäysmotiiveille kybermaailmassa. Hän kuvaa tasoilla 1–6 erilaisia toimintamuotoja ja motiiveja kyberhyökkäyksille.

Tason 1 muodostaa kybervandalismi, kuten esimerkiksi hakkerointi ja haktivismi sekä parveilu – tai kyberparveilu. Kyberparveilu viittaa hyökkäykseen, johon

osallistuu useita toisiinsa liitettyjä toimijoita ja jotka toimivat koordinoituna ryhmänä. (Pöyhönen 2020, 34–35.) Parveilu voi viitata esimerkiksi haitallisten ohjelmistojen käyttämään taktiikkaan, jossa useat tartunnan saaneet tietokoneet tai laitteet toimivat yhteistyössä hyökkäysten toteuttamiseksi. Tämän kaltaisen toiminnan tarkoituksena voi olla julkisen huomion saaminen. Näiden vaikutukset ovat yleensä vaarattomia ja lyhytkestoisia. Esimerkkinä tällaisesta toiminnasta ovat Anonymous-hakkeriryhmän suorittamat operaatiot.

Taso 2 puolestaan käsittää kyberrikollisuuden, mikä on rikollista toimintaa, jossa käytetään sähköisiä viestintäverkkoja ja tietojärjestelmiä. EU komission tietoverkkorikollisuus voidaan jakaa kolmeen eri kategoriaan riippuen siitä, millainen rooli digitaalisella maailmalla on rikoksen toteuttamisessa. Niin kutsuttua perinteistä rikollisuutta, jossa esimerkiksi sähköisiä viestintäverkkoja on vain käytetty rikoksen toteuttamiseen, kuten uhkailuun. Toisena sähköisten viestimien hyödyntäminen laittoman sisällön julkaisuun, mistä esimerkkeinä viharikosten tai lapsen seksuaalisen hyväksikäytön jakamiseen. Viimeisenä rikokset, jotka tapahtuvat vain digitaalisessa viitekehyksessä, kuten tietomurrot tai palvelunestohyökkäykset. (Pöyhönen 2020, 34–35.)

Kolmannen tason kybervakoilu saattaa kuulostaa jännittävältä, mutta se on verrattain yleistä toimintaa. Se on vakoilua, joka tapahtuu digitaalisessa maailmassa. Kybervakoilun avulla kerätään salaisia tietoja – (sensitiivinen, yksinoikeudellinen tai turvaluokiteltu) – yksityisistä ihmisistä, kilpailijoista, ryhmistä tai jopa vieraan valtion hallituksesta tavoitteena saavuttaa poliittista, sotilaallista tai taloudellista etua. Tason 4 kyberterrorismi viittaa terrorismiin, jossa hyödynnetään tietoverkkoa kriittisten informaatiojärjestelmien hyökkäyksiin ja hallintaan. Kyberterrorismin motiivit ovat samat kuin perinteisessäkin terrorismissa – tuottaa vahinkoa, levittää pelkoa ja painostaa poliittista johtoa. niiden hyökkäysten kohteeksi valikoituvat usein kriittiset informaatiojärjestelmät. (Pöyhönen 2020, 34–35.)

Tason 5 muodostaa kybersabotaasi, mikä on sotilaallista toimintaa kybermaailmassa tavoitteena epävakauden aiheuttaminen, offensiivisten kyberhyökkäyskykyjen testaaminen, hybridioperaatioiden tai sodan valmistelu. (Pöyhönen 2020, 34–35.) Viimeisen tason 6 muodostaa kybersodankäynti. Vaikka käsitteelle ei olekaan löydetty yleisesti hyväksyttyä määritelmää, se kuvataan usein valtioiden välisenä vihamielisenä toimintana, jossa hyödynnetään tietoverkkoja ja niiden haavoittuvuuksia, kuten Kyberturvallisuuden sanastossa mainitaan (Turvallisuuskomitea 2018). Puhuttaessa varsinainen kybersodankäynnistä on kyseessä valtioiden välinen sotatila, jossa kyberoperaatiot ovat osa muita sotilaallisia operaatioita. (Pöyhönen 2020, 34–35.) Kybersodankäynnin pääluokkia ovat esimerkiksi: strateginen, taktisoperatiivinen sekä kriisejä alemmalla tasolla tapahtuvaa sodankäyntiä. Strateginen kybersodankäynti käsittää pitkäkestoisemmat ja laajemmat tavoitteet, kuten kansallinen turvallisuus ja valtioiden keskinäiset suhteet. Taktisoperatiivinen kybersodankäynti puolestaan tarkoittaa enemmän käytännön toimia ja operaatioita, joiden avulla pyritään saavuttamaan välittömiä taktisia etuja tai vahingoittamaan vastustajaa.

4.3 Digitaalisen viestinnän rooli

Tarinankerronta on nykyaikaisen viestinnän keskeinen tekijä. Sen avulla voidaan vaikeatkin asiat muokata ymmärrettävään muotoon. Digitaalinen tarinankerronta yhdistää tarinankerronnan ja teknologian. Digitaalisen viestinnän rooli on monitahoinen ja sen vaikutukset mittavat, koska se tarkoittaa valtaa osaavissa käsissä. Tämä herättää kysymyksen: miksi on tärkeää kuka ja millainen taho hallitsee tarinan narratiivia? Tarinankerronnan voima piilee sen narratiivissa ja digitaalinen viestintä määrittelee sen roolin. Vastavuoroisesti väärissä käsissä tarinan lahjomattomuus kärsii ja totuus saattaa muuttua kompromissiksi. Näin ollen, digitaalinen viestintä on merkittävä markkinoinnin ja brändinrakennuksen työkalu, kun sitä osataan käyttää oikein. Viestintä ei ole vain informaation välittämistä, vaan parhaimmillaan onnistunutta tarinan kerrontaa.

Tarinaa siitä, miten yritys toimii ja millainen organisaatio on kyseessä, mihin se on matkalla. Kaikki nämä aspektit luovat mielikuvia yrityksestä ja synnyttävät meissä intuitiivisen tunteen kyseisestä brändistä. (Korva 2023, 12.)

4.4 Viestinnän merkitys organisaatioissa

Viestinnän rooli yrityksissä ja organisaatioissa on monitahoinen. Se tarjoaa yritykselle mahdollisuuden rakentaa mainettaan ja lisätä tunnettavuuttaan. Sen avulla voidaan välittää tietoa sidosryhmille, luoda vuorovaikutteisia kokemuksia ja käydä vuoropuhelua näiden kanssa. Lisäksi viestinnällä on taloudellista merkitystä, sillä onnistunut viestintä voi edistää liikevaihdon kasvua. Viestintä on alati jatkuva prosessi, joka sisältää suunnittelun, toteutuksen, seurannan, palautteen ja arvioinnin sekä uuden viestinnän suunnittelun. (Korva 2023, 12.) Ottaen huomioon, että viestinnän resurssit ovat aina rajalliset, on strategisen viestinnän kannalta merkittävää ymmärtää erot eri sidosryhmien kesken. Keskeinen väline strategiseen viestintään onkin sidosryhmäanalyysi. Siihen löytyy erilaisia malleja, mutta yksi tunnetummista on Mitchellin ja muiden sidosryhmien tärkeyden malli (ks. kuvio 1). Kuten sidosryhmien tärkeyden mallista on havaittavissa, niiden keskinäinen hierarkia vaihtelee suhteessa niiden ulottuvuuden mukaan, joita on kolme: valta, oikeutus ja kiireellisyys. Organisaation menestys riippuu siitä, miten hyvin se onnistuu sovittamaan arvonsa ja tavoitteensa yhteen keskeisten sidosryhmiensä tarpeiden ja odotusten kanssa. (Waaramaa & Nissilä 2023, 19.)

Kuvio 1: Sidosryhmien tärkeyden malli (Waaramaa 2023, 20; Mitchell ja muut, 1997, s. 865–868).

Viestinnän tulisi olla tavoitteellista ja hyvin suunniteltua toimintaa. Sisäinen viestintä koetaan yleisesti ottaen yhdeksi suurimmaksi kipukohdaksi, kun puhutaan organisaation toimintatavoista. (Heiska 2020.) Viestintä organisaation sisällä ja sen ulkopuolella ovat keskeisessä asemassa liiketoiminnan sujuvuuden ja maineen rakentamisen kannalta. Sisäinen viestintä varmistaa, että organisaation jäsenet ovat tietoisia tavoitteista, tehtävistä ja päätöksistä. Se luo myös yhteenkuuluvuuden tunnetta ja sitoutumista organisaation arvoihin. Hyvin toimiva sisäinen viestintä vähentää väärinymmärryksiä, parantaa työilmapiiriä ja edistää tehokasta yhteistyötä eri osastojen välillä. (Heiska 2020.)

4.5 Teknologian vaikutus viestintään

Teknologian kehityksen myötä digitaalisen viestinnän rooli ja merkitys ovat jatkuvassa kasvussa. Kasvuun vaikuttavat monet eri tekijät, mutta varmaa on kehityksen mukanaan tuoma muutos. Viestintäkanavien monipuolistuminen on muuttanut vuorovaikutusta merkittävästi. Kehitykseen ovat vaikuttaneet erilaiset teknologiset välineet ja sovellukset, kuten sosiaalinen media, mobiililaitteet ja verkkovideot. Tämä kehitys on muuttanut viestintäkulttuuriamme ja mahdollistanut uusia tapoja vuorovaikutukseen. Vaikka viestinnän ammattilaiset puhuvat paljon tekoälyn ja datan hyödyntämisesti, siihen löytyy verrattain vähän varsinaista viestintätieteiden alan tutkimusta (Kanti-Paul 2019, 7).

Reaaliaikainen viestintä on osaltaan mullistanut vuorovaikutustapojamme, jopa tuoneet valitettavia lieveilmiöitä mukanaan. Teknologian kehityksen myötä nopeammaksi ja reaaliaikaisemmaksi muuttunut viestintä on avannut uusia mahdollisuuksia välittömään vuorovaikutukseen. Samalla se kuitenkin altistanut meitä informaatioähkylle sekä jatkuvuuden vaatimukselle. Teknologian nopea kehitys on aiheuttanut myös haasteita yksityisyydensuojalle ja tietoturvauhkille. Kaiken kaikkiaan tarve tasapainottaa reaaliaikaisen viestinnän edut ja haitat tarkkaan harkitun viestintästrategian avulla on ilmeinen.

Internetin ja digitaalisten välineiden avulla viestintä on muuttunut entistä globaalimmaksi. Se on mahdollistanut kansainvälisen yhteydenpidon, yhteistyön sekä vuorovaikutusmahdollisuudet eri kulttuurien välillä. Sen lisääntyminen on vakiinnuttanut aiempaa globaalimman tavan toimia myös kuluttajatasolla. Koko maailma on muodostunut markkinapaikaksi verkkokaupoille ja asiakkaiden hankintaa tehdä kohdennetusti, mikä lisää kansainvälisen kaupan mahdollisuuksia.

5 Tietoturva ja kyberturvallisuus digitaalisessa viestinnässä

Tietoturva ja kyberturvallisuus ovat keskeisiä digitaalisen viestinnän viitekehyksessä. Kyberturvallisuuden haasteiden laajuutta auttaa hahmottamaan paremmin ymmärtämällä asian luonnetta myös kansallisella tasolla koko yhteiskuntaa koskettavana asiana. Aiheeseen löytyy kattavasti kehitysehdotuksia ja tarkempaa analyysiä Jyväskylän yliopiston Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksen – hankkeen loppuraportista. Liikenne- ja viestintäministeriön Jyväskylän yliopistolta tilaamassa kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksessa selvitettiin laaja-alaisesti kyberturvallisuuteen liittyvän osaamisen määrällisen ja laadullisen kehittämisen kehitysehdotuksia. Kyseisellä tutkimushankkeella huomioitiin ja edistettiin niitä tavoitteita, joita on esitetty EU:n kyberturvallisuusstrategiassa 2020, EU:n digitaalista kehitystä edistävissä ohjelmissa, Suomen kyberturvallisuusstrategiassa (2019) ja sen kehittämisohjelmassa (2021) sekä EU:n ja Suomen osaamisen kehittämisen ohjelmissa.

Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksessa kartoitettiin aihetta tarkemmin. Siinä esiteltiin muun muassa näkökulmia kyberosaamisen kehittämiseen sekä sitä tukevan koulutuksen osaamisen vahvistamiseen. Keskeiset toimenpiteet kyberturvallisuuden parantamisen kannalta nähtiin tarpeelliseksi kohdentaa koko yhteiskuntaa koskettaviksi. Tarvittavan osaamisen lisäksi vahva kansallinen kyberturvallisuus edellyttäisi myös laajaa osallistumista yhteiskunnan kaikilla eri tasoilla, sekä tiivistä yhteistyötä erityisesti julkishallinnon ja elinkeinoelämän välillä. Lisäksi tutkimuksessa nähtiin tarvetta vahvalle kotimaiselle kyberturvallisuusteollisuudelle, joka toisi osaamista digitaalisen yhteiskunnan palveluiden turvaamiselle sekä lisäisi viranomaisten kyberturvallisuuskyvykkyyksiä. Tavoitteena luoda vahvaa pohja koko yhteiskunnan turvallisen toiminnan säilyttämiselle. (Lehto 2022).

Samassa tutkimuksessa nähtiin paitsi huippuluokan osaamisen kehittäminen tärkeänä osana tulevaisuuden kyberturvallisuustarpeisiin vastaamista, myös käytännönläheinen kansalaisten kouluttaminen. Tästä hyvänä esimerkkinä Jyväskylän yliopiston juuri (syksy 2023) päivitetty versio kansalaisen kyberturvallisuuden verkkokurssista. Verkkokurssilta löytyy hyvä kattaus sisältöä aiheen kannalta. Sen suorittamisesta saa Jyväskylän yliopiston antaman virallisen opintosuorituksen ja opintorekisteriotteen perusteella suoritus voidaan merkitä myös Maanpuolustuskoulutus MPK:n järjestelmään. Hyvä kyberturvallisuus on parhaimmillaan yhteiskunnallisesti kattavaa toimintaa, maanpuolustusta unohtamatta. Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa, kuten määritellään Kyberturvallisuuden sanastossa. Se korostaa tietoturvan keskeistä roolia, mutta sisältää laajemman näkemyksen digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuudesta ja niiden vaikutuksesta toimintaan. Kyberpuolustus, jonka vastuu on Puolustusvoimilla, koostuu tiedustelusta, suojaamisesta ja vaikuttamisen suorituskyvyistä (Soikkeli 2021, 10; Kyberturvallisuuden sanasto 2018). Digitaalisen viestinnän kontekstissa tietoturva ja kyberturvallisuus ovat paitsi keskeisiä myös olennainen osa onnistuneen viestinnän kannalta. Aiheen tekee problemaattiseksi sen monitahoinen ja kompleksi luonne. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa (Kyberturvallisuuden sanasto 2018). Tietoturvan merkitys on keskeinen kyberturvallisuuden saavuttamiseksi. Lisäksi laajemmin tarkasteltuna se käsittää digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuuden ja sen vaikutuksen toimintaan. (Soikkeli 2021, 10.)

5.1 Tietoturvan merkitys

Tässä alaluvussa tarkastellaan tietoturvan merkitystä digitaalisessa viestinnässä ja siihen liittyviä käytäntöjä. Tietoturvallisuus osana hyvää tiedonhallintatapaa merkitsee pyrkimystä saavuttaa tilanne, jossa voi luottaa kybertoimintaympäristöön. Tämä edellyttää tietoturvan keskeistä roolia, mutta se käsittää

myös laajemman näkökulman digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuuteen ja niiden vaikutukseen toimintaan. (Soikkeli 2021, 10). Tietoturvan peruskäsitteet ovat keskeisiä Digitaalisessa viestinnässä. Ne ovat periaatteita ja käytäntöjä, joilla varmistetaan, että viestintä on turvallista ja luotettavaa. Ne voivat käsittää esimerkiksi salattujen viestintäkanavien käytön, käyttäjätunnusten ja salasanojen asianmukaisen hallinnan sekä tietoturvallisten verkkoyhteyksien varmistamisen. Noudattamalla näitä periaatteita luodaan edellytykset luotettavalle ja turvalliselle viestinnälle.

Kyberturvallisuus on vaikeasti hahmotettava kokonaisuus, toteaa Soikkeli tutkimuksessaan. Von Solmsin ja van Niekerkin (2013) mukaan tietoturvallisuus, ICT-turvallisuus ja kyberturvallisuus ovat keskinäisessä yhteydessä. ICT-turvallisuus keskittyy teknologian ja tallennetun tiedon turvaamiseen, kun taas tietoturvallisuus huomioi myös tiedon muodon. (Soikkeli 2021, 14). Vuonna 2017 hyväksytty Suomen yhteiskunnan turvallisuusstrategia on valtioneuvoston periaatepäätös, joka yhdenmukaistaa kansallisia varautumisperiaatteita ja ohjaa eri hallinnonalojen varautumista. Suomessa käytössä oleva kokonaisturvallisuuden malli kattaa yhteiskunnan elintärkeät toiminnot (Turvallisuuskomitea 2017, 5).

5.2 Henkilötietojen suojaaminen

Tietoturvan yksi keskeinen osa-alue on henkilötietojen suojaaminen. Se käsittää erilaisia toimenpiteitä ja käytäntöjä, joiden avulla varmistetaan henkilötietojen luottamuksellisuus, eheys ja saatavuus. Lain mukaan yksityisyys on kaikkien perusoikeus ja henkilötietojen suoja tarkoittaa ihmisten yksityisyyden ja siihen liittyvien tietojen suojaamista. Tässä osiossa tarkastellaan erityisesti henkilötietojen suojaamisen merkitystä ja käytännön keinoja sen varmistamiseksi digitaalisessa viestinnässä. Tietosuoja on tarkoitus kulkea mukana osana jokaisen arkea, kuten EU:n perusoikeuskirjan henkilötietojen käsittelyn on tapahduttava tiettyä tarkoitusta varten ja sen on oltava asianmukaista. Tietosuoja-asetuksen

tavoitteena on yhdenmukaistaa henkilötietojen suoja kaikissa EU-maissa ja sovittaa se digitaaliseen ympäristöön. Tämä auttaa parantamaan eurooppalaisten yritysten kilpailukykyä nykyaikaisessa digitaalisessa markkinassa. (Keskuskauppakamari 2018.)

5.3 Luottamuksellisuuden säilyttäminen

Tietojen, kuten salasanojen, ja järjestelmien, kuten sähköpostin, luottamuksellisuuden periaate edellyttää, että ne ovat saatavilla vain niille henkilöille, joilla on niihin oikeus. Eheysperiaate määrittelee, että tiedot ja järjestelmät pysyvät luotettavina, oikeina ja ajantasaisina, eivätkä ne muutu tai ole muutettavissa esimerkiksi laitteisto- tai ohjelmistovirheiden, luonnonkatastrofien tai ihmistoiminnan seurauksena. Eheys voidaan säilyttää esimerkiksi päivittämällä tietoja ja tekemällä säännöllisiä varmuuskopioita. Luottamuksellisuuden säilyttäminen on keskeinen osa tietoturvaa, joka vaikuttaa organisaatioiden tapaan varmistaa, että tietoa käsitellään ja jaetaan vain oikeutetuille henkilöille. Tehokkaat suojausmenetelmät, kuten salaus ja monitasoinen tunnistautuminen varmistavat, että tiedot pysyvät suojattuina ja vain oikeutetuilla käyttäjillä on pääsy niihin. Organisaatiot kohtaavat jatkuvasti uhkia, jotka pyrkivät saamaan haltuunsa arkaluontoisia tietoja. Oikeiden suojausmenetelmien avulla voidaan estää tietovuodot ja vahingot yrityksen maineelle. Hyvin koulutettu henkilöstö tunnistaa paremmin tietoturvariskit ja osaa toimia niiden ehkäisemiseksi ja torjumiseksi. Selkeät ja kattavat turvallisuusohjeet auttavat organisaatiota varmistamaan, että kaikki toimivat yhtenäisten turvallisuuskäytäntöjen mukaisesti.

5.4 Resilienssi ja Zero Trust -periaate

Resilienssi on paljon keskusteluissa viime vuosia esiintynyt termi, joka on tämän tutkimuksen turvallisuuskontekstin kannalta yksi keskeisiä käsitteitä. Sitä

käytetään usein synonyymina kriisinkestävyydelle, muutosjoustavuudelle ja joustokestävyydelle. Turvallisuuskäsitysten muutokset seuraavat muutoksia ympärillämme ja ne muuttuvat samalla, kun maailma ympärillämme muuttuu. Samoin näkökulmat jalostuvat, kun turvallisuuskäsite muuttuu ja tässä tapauksessa laajenee. Digitaalisen viestinnän viitekehys turvallisuuskontekstissa on laaja ja siinä on paljon huomionarvoisia tekijöitä. Resilienssikäsitteen käyttö turvallisuuskontekstissa on lisääntynyt merkittävästi 2020-luvulla. Esimerkiksi ennen koronapandemiaa ja Ukrainan sotaa resilienssistä puhuttiin usein hybridivaikuttamisen yhteydessä tai yleisesti ilman selkeää kriisiyhteyttä. Lisäksi käsitteenä saattaa aiheuttaa hämmennystä yleisössä, koska siihen liitetään eri yhteyksissä erilaisia määritelmiä. (Hiltunen 2023). Resilienssi ja Zero Trust -periaate muodostavat yhdessä keskeisen osan nykyaikaista tietoturvaa. Zero Trust -periaate edustaa nykyaikaista lähestymistapaa tietoturvaan, jossa oletetaan, että verkoston jokainen osa voi olla potentiaalinen hyökkäyksen kohde, ja siksi kaikki verkkoyhteydet ja toimijat tulee varmentaa jatkuvasti. Tämä edistää organisaation resilienssiä, kun se minimoi yksittäisten hyökkäysten vaikutukset ja mahdollistaa nopean toipumisen.

Nykyään yritykset kohtaavat jatkuvasti merkittäviä haasteita, kun ne pyrkivät suojaamaan tietojaan ja verkkoympäristöjään pahantahtoisilta toimijoilta, erityisesti lunnasohjelmilta ja tiedonkalasteluhyökkäyksiltä. Tämä huolenaihe on johtanut strategian käyttöönottoon, jota kutsutaan nimellä Zero Trust, ja se on saanut paljon huomiota tietoturva-alalla, koska sitä sovelletaan laajasti yrityksissä ympäri maailmaa. Tästä huolimatta, vaikka Zero Trust -mallit ovat laajasti käytössä, ne eivät tarjoa kattavia ohjeita kaikilla keskeisillä alueilla, erityisesti tietojen varmuuskopioinnin ja palauttamisen osalta. Tarkemmin sanottuna, tietojen varmuuskopiointi- ja palautusjärjestelmät eivät sisälly yleisesti käytettyihin Zero Trust -kehyksiin. Kuitenkin tietojen varmuuskopiointi- ja palautusjärjestelmät ovat keskeisiä osia yritysten tietotekniikassa ja niitä tulisi kohdella sen mukaisesti. (Garbis 2023.)

5.5 Varautuminen ja ennaltaehkäisy

Lähtökohtaisesti varautuminen mahdolliseen tietoturvahyökkäykseen voi säästää yrityksille aikaa, rahaa ja maineen vahingoittumista pitkällä aikavälillä. Varautuminen ja ennaltaehkäisy ovat osa-alueita kyberturvan kannalta, joiden avulla pyritään estämään ja minimoimaan mahdollisia tietoturvauhkia ja hyökkäyksiä. Luontevinta aiheen kannalta on hyödyntää jo olemassa olevia hyviä käytäntöjä ja niitä julkaisevien alan ammattilaisten ja organisaatioiden ohjeita tehokkaista menetelmistä kyberturvallisuuden edistämiseksi. Tämän tutkimuksen lähtökohtana on kartoittaa parhaita toimintamalleja ja tavoitteena laatia yhteenveto, josta ilmeen lyhytlistaus hyödyllisistä käytännöistä. Toimintansa saaman julkisuuden kautta otsikoihin usein noussut NSA (National Security Agency) on julkaissut oman listansa: NSA:n kymmenen parasta tietoturvauhan lieventämistoimenpidettä. Sen tulisi ainakin heidän resurssiensa puolesta vastata tietoturva-alan parhainta osaamista.

Listan kymmenen kohtaa keskittyy seuraaviin aspekteihin. 1) Päivitä ja päivitä ohjelmistot välittömästi: Hyödynnä kaikkia saatavilla olevia ohjelmistopäivityksiä, automatisoi prosessi mahdollisimman pitkälle ja käytä päivityspalvelua suoraan valmistajalta vähentääksesi uhkatoimijoiden hyökkäysriskiä. 2) Puolusta käyttöoikeuksia ja tilejä: Määrittele käyttöoikeudet riskien mukaan, hyödynnä Privileged Access Management (PAM) -ratkaisua ja toteuta porrastettu hallintaoikeus rajoittaaksesi pääsyä arvokkaisiin resursseihin ja estääksesi uhkatoimijoilta lateraalista liikkuvuutta. 3) Noudata allekirjoitettujen ohjelmistojen suorituskäytäntöjä: Käytä modernia käyttöjärjestelmää, joka tukee allekirjoitettujen ohjelmistojen suorituskäytäntöjä, ylläpidä luotettavien sertifikaattien luetteloa ja hyödynnä sovelluksen valkoista listaa estääksesi ei-toivottujen ohjelmien ja upotetun haitallisen koodin käytön. 4) Harjoittele järjestelmän palautussuunnitelmaa: Luo, tarkista ja säännöllisesti harjoittele järjestelmän palautussuunnitelmaa, jotta voit varmistaa tietojen palauttamisen ja liiketoiminnan jatkuvuuden odottamattomissa tapahtumissa tai haitallisissa uhkissa. 5) Järjestelmien ja asetusten aktiivinen hallinta: Tee kattava inventaario verkkolaitteista ja

ohjelmistoista, poista tarpeettomat tai ylimääräiset laitteet ja ohjelmistot, ja hallitse tarkasti laitteita, sovelluksia, käyttöjärjestelmiä ja turvallisuusasetuksia vähentääksesi altistumista mahdollisille hyökkäyksille ja varmistaaksesi täyden hallinnan toimintaympäristössä. 6) Jatkuva verkkojen tunkeutumisen metsästys: Oletetaan, että kompromissi on tapahtunut, ja käytetään omistautuneita tiimejä havaitsemaan, rajaamaan ja poistamaan uhkatoimijat verkosta. Hyödynnetään passiivisia havaitsemismekanismeja ja toteutetaan aktiivista metsästystä sekä läpäisemistestauksia, kun havaitaan tietoturvaloukkauksia. 7) Tehosta nykyaikaisia laitteiston tietoturvaominaisuuksia: Hyödynnä laitteiston tietoturvaominaisuuksia, kuten UEFI Secure Boot, TPM ja laitteiston virtualisointi, ja aikatauluta vanhat laitteet laitepäivityksiin parantaaksesi käynnistysprosessin eheyttä ja suojataksesi kriittisiä tietoja ja käyttäjätunnistetietoja. 8) Tietoverkkojen erottelu sovellustietoisilla puolustusmekanismeilla: Erottele kriittiset verkot ja palvelut, ja käytä sovellustietoisia verkkopuolustusjärjestelmiä estämään epämuodostunutta liikennettä sekä rajoittamaan sisältöä politiikan ja lainsäädännön mukaisesti. 9) Integroi uhkan maineenpalvelut: Hyödynnä monilähteisiä uhkamaineenpalveluita tiedostoille, DNS:lle, URL-osoitteille, IP-osoitteille ja sähköpostiosoitteille havaitaksesi ja estääksesi haitallisia tapahtumia ja saadaksesi pääsyn laajempaan uhka-analyysiin ja vinkkien antamiseen. 10) Siirry monivaiheiseen tunnistautumiseen: Priorisoi suojausta tilien osalta, joilla on korkeat käyttöoikeudet, etäkäyttöoikeudet tai muuten sisältävät arvokkaita resursseja, sekä käytä fyysisiä tunnuslaitteita, kuten tunnisteita, salasanojen ja PIN-koodien lisäksi, vähentäen näin käyttäjätunnusten varastamisen ja uudelleenkäytön riskiä. Yllä esitetyt kymmenen toimenpidettä ovat olennainen osa kyberturvallisuutta koskevaa keskustelua ja tarjoavat arvokasta ohjausta tietoturvauhkien torjumisessa. On suositeltavaa tutustua tarkemmin NSA:n julkaisemaan listaan voidakseen hyödyntää sen tarjoamia käytännön neuvoja ja suosituksia. Tämä tutkimus suosittelee listan noudattamista parhaana käytäntönä kyberturvallisuuden parantamiseksi. Listan latauslinkki on saatavilla lähdeluettelossa (NSA 2018). Lähdeluettelosta löytyy myös uudempi pilvipalveluiden kyberturvallisuusohjeet (NSA 2024).

6 Digitaalisen muotoilijan rooli tietoturvan näkökulmasta

Tässä osiossa tarkastellaan digitaalisen muotoilijan tehtäviä ja vastuita, erityisesti liittyen tiedontarpeisiin, osaamisvaatimuksiin, jatkuvan oppimisen merkitykseen, käytännön työkaluihin ja viestintäalalla tarvittaviin tietoturvakäytäntöihin. Tämä osio tarjoaa katsauksen siihen, miten digitaalisen muotoilijan rooli liittyy tietoturvaan ja miten ammattilaiset voivat kehittää tietämystään ja taitojaan tässä merkittävässä osa-alueessa. Vastuullisen viestinnän ammattilainen huomioi kyberhygienian merkityksen osaksi oman ammattitaidon ja digitaalisen kypsyysasteen kehittämistä.

6.1 Tiedontarpeet ja osaamisvaatimukset

Tietoturvasta huolehtiminen digitaalisen muotoilijan roolissa ei rajoitu pelkästään käyttöliittymien suunnitteluun, vaan se edellyttää myös monipuolista osaamista ja syvällistä ymmärrystä alan periaatteista ja käytännöistä. Digitaalisen muotoilijan rooli tietoturvan edistäjänä on keskeinen, sillä hänellä on mahdollisuus vaikuttaa suunniteltujen digitaalisten palveluiden turvallisuuteen ja käyttäjäkokemukseen. Digitaalisen muotoilijan on oltava monipuolinen asiantuntija, jolla on vahva ymmärrys käyttöliittymäsuunnittelusta, käyttäjäkokemuksen periaatteista ja tietoturvasta. Hänen tehtävänsä sisältää käyttäjätutkimuksen suorittamisen, prototyyppien luomisen, käyttöliittymäelementtien suunnittelun ja käyttäjätestauksen toteuttamisen. Digitaalinen muotoilija, joka tuntee käytettävät teknologiat, muotoilumallit ja alan käytännöt sekä osaa tulkita vallitsevia trendejä, on asiansa osaava oman alansa ammattilainen (Talasniemi 2020).

Lisäksi digitaalisen muotoilijan tulee hallita graafisen suunnittelun perusteet ja digitaaliset työkalut luodakseen houkuttelevia ja esteettisesti miellyttäviä käyttöliittymiä. Yleinen ymmärrys käytetyistä teknologioista ja teknisen osaamisen merkitys korostuu, vaikka muotoilijan ei tarvitse olla ohjelmointiguru, sillä

perustiedot web- ja mobiiliteknologiasta auttavat kommunikoimaan tehokkaasti kehitystiimin kanssa (Talasniemi 2020). Tietoturvatekijöiden integroiminen suunnitteluprosessiin on tärkeää, ja digitaalisen muotoilijan on osattava suunnitella käyttöliittymiä ja käyttäjäkokemuksia, jotka ovat turvallisia ja suojaavat käyttäjien tietoja ja yksityisyyttä. Jatkuva oppiminen ja halu kehittää omaa osaamistaan ovat välttämättömiä menestyksen kannalta tässä alati muuttuvassa ympäristössä.

6.1.1 Koulutuksen rooli

Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksen hankkeen loppuraportista ilmenee kyberalan koulutuksesta ja vaatimuksista olevan huomattava määrä tutkimusta. Siinä myös vahvistetaan viestit maailmalta kyberalan osaajien puutteesta. Euroopassa tätä ongelmaa vuonna 2017 tutkinut European Cyber Security Organisation (ECSO) vahvistaa osaajista olevan puutetta. ECSO kertoo tuloksissaan kyberturvallisuuskoulutuksen vaatimuksista adaptiivisten koulutusympäristöjen osalta, sekä koulutuksen ajoittamisesta riittävän ajoissa huomioiden molemmat sukupuolet (ECSO 2017). ECSO on myös tehnyt raportin, missä se on esittänyt kyberturvallisuuden osaajilta vaadittavista taidoista, (ECSO 2021). Huomionarvoista kaiken kaikkiaan on osaajien puutteen seurauksena laadulliset ja määrälliset vaatimukset kyberalan koulutukselle. (Lehto 2022, 13.)

6.1.2 Jatkuvan oppimisen merkitys

Digitalisaatio asettaa organisaatioille jatkuvia uudistumishaasteita niiden pyrkiessä säilyttämään kilpailukykynsä nopeasti muuttuvassa ja monimutkaisessa maailmassa. Teknologian rooli tässä laajemmassa muutoksessa korostaa organisaatioiden tarvetta reagoida nopeasti muutoksiin ja oppia hallitsemaan niiden vaikutuksia tehokkaasti. Tämä muutos vaikuttaa kaikkiin osa-alueisiin, johtaen

työtapojen ja organisaatiokulttuurin muutokseen. Ketterät toimintatavat ja lean-ajattelu ovat osoittautuneet tehokkaiksi ratkaisuiksi kompleksisiin ongelmiin samalla, kun kokeilukulttuurin, jatkuvan oppimisen ja uudistumiskyvyn merkitys kasvaa entisestään. (Vitikka 2020, 8.) Jatkuva oppiminen on muodostunut keskeiseksi osaksi työn tekemisen viitekehystä. Kehityksen suunta on muuttanut odotuksia organisaation johtamiskulttuurin ja toimintaympäristön suhteen henkilöstön osalta. Nykyään odotetaan, että molemmat tukevat tiedonhankintaa ja jatkuvaa oppimista. (Vitikka 2020, 8.) Tämän päivän työskentely tapahtuu monissa yrityksissä tiimeissä. Saman mallin mukaisesti erilaisten organisaatioiden toiminta sijoittuu pienryhmiin, tiimeihin tai projekteiksi. Uuden tiedon luominen käsittää yhteisöllisiä prosesseja ja tiedon jakaminen organisaation sisällä edellyttää mahdollisuutta dialogiin, korostaen näin kommunikaation ja sisäisen viestinnän merkitystä. (Vitikka 2020, 44.) Oppiminen organisaatiossa tapahtuu monella tasolla: yksilöiden, tiimien, organisaation ja verkoston tasolla. Yksilötason oppiminen muodostaa perustan ja on lähtökohta muutokselle. (Vitikka 2020, 12) Tiedon luominen ja tiimioppiminen ovat keskeisiä tietotyön aikakaudella. Tiedon rooli liiketoiminnassa on korostunut, ja sen jatkuva uudistaminen, datan käsittely sekä sen tehokas ja laaja-alainen hyödyntäminen ovat keskeisiä kilpailutekijöitä kaikissa organisaatioissa. (Vitikka 2020, 20.)

Omaa pohdintaa/ tekstiä: Digitaalisen muotoilijan rooliin liittyy olennaisesti jatkuva oppiminen, mikä korostuu erityisesti tietoturvan ja kyberturvallisuuden kontekstissa. Digitaalisen viestinnän alalla muutosten nopea tahti edellyttää jatkuvaa päivittymistä, sillä digitaaliset työkalut, verkkoalustat ja toimintaympäristöt kehittyvät jatkuvasti. Lisäksi alati muuttuvassa trendien virrassa voi olla haastavaa hahmottaa eri tekijöiden keskinäisiä suhteita ja priorisoida toimintaa niiden mukaan. Samankaltaisia haasteita kohtaa myös muotoilija, jonka on tietoturvan kontekstissa pystyttävä ottamaan kantaa erilaisiin muuttujiin. Jatkuva oppiminen ja organisaation sisäinen toimintakulttuuri muodostavat yhdessä perustan, jolla toimintaa voidaan kehittää ja sopeuttaa muuttuviin tarpeisiin. Näin ollen aiheen kannalta huomionarvoiseksi muodostuukin organisaation yrityskulttuurin rooli ja merkitys. Kuten aiemmin todettu sen asettamat rakenteet ja niiden tarjoamat

olosuhteet parhaimmillaan tukevat organisaation kompetenssin ylläpitoa ja parantamista. (Vitikka 2020, 52.)

6.1.3 Tietoturvakäytännöt viestintäalalla

Verkkoympäristö on muuttunut huomattavasti ja sen kehitys viime vuosina on ollut vuorovaikutteisempaan suuntaan. Sitä ei voi enää ajatella pelkästään yksisuuntaisena kanavana tiedon välitykseen, kuten 2010-luvun alussa. (Kts. Juholin 2016, 98). Samalla tavalla digitaalisen viestinnän kontekstissa tietoturvan ja kyberturvallisuuden merkitys on asettunut huomionarvoiseen asemaan, johtuen nykyaikaisen viestinnän digitaalisesta luonteesta. Lähes kaikki nykyaikainen viestintä tapahtuu digitaalisesti, kuten sähköpostit, pikaviestit, sosiaalinen media, verkkosivustot ja muut digitaaliset alustat. Tämän kaltaisten viestimien hyödyntäminen ilman asiaan kuuluvaa tietoturvaa ja kyberturvallisuuden palveluita asettaisi viestinnän osapuolet alttiiksi erilaisille uhille ja mahdollisille väärinkäytöksille. Niitä ovat esimerkiksi tietovuodot, identiteettivarkaudet sekä tietojärjestelmien vahingoittaminen. Kaiken digitaalisen viestinnän sekä verkossa tapahtuvan toiminnan kannalta olisikin ensisijaisen tärkeää ymmärtää tietojen ja järjestelmien turvallisuuden varmistamisen merkitys. Soveltamalla parhaita tietoturva- ja kyberturvallisuuskäytäntöjä tehokkaasti on mahdollista luoda hyviä käytäntöjä ja edistää kyberhygieniaa omassa organisaatiossaan itsensä ja muiden suojaamiseksi.

6.2 Empiirinen tutkimus

6.2.1 Kyselytutkimus digitaalisen viestinnän ammattilaisille

Teettämäni kyselytutkimus digitaalisen viestinnän osaajille oli kevyt kyberkartoitus, jossa vastaajien itsearviointikyky korostui. Kyselyn kautta kerättiin tietoa

vastaajien kokemuksista ja käsityksistä aiheen kannalta olennaisten käsitteiden, termien ja tapahtumien merkityksestä. Kyselyyn vastasi 11 digitaalisen viestinnän osaajaa. Kyselytutkimus sisälsi seitsemän osiota. Niiden painotukset olivat sekä toisistaan poikkeavia että kokonaisuuden kannalta myös toisiinsa tukeutuvia (ks. Liite 1). Ensimmäisessä osiossa rajattiin kyselyyn vastanneiden ikäjakauma suhteessa kokemukseen digitaalisesta viestinnästä. Ikäryhmien kartoitus oli myös olennaista aiheen suhteessa nuoren historian kannalta, johtuen digitalisaation nopeasta kehityksestä lyhyen ajan sisällä. Toisen osion kysymysten tarkoituksena oli kartoittaa vastaajan asenteita ja lähtökohtia aiheen tunnettavuuden osalta. Kolmas osio on ensimmäinen varsinainen itsearviointia vaativa osio, missä määriteltiin vastaajan tietotaso aihepiirin suhteen. Itsearviointi on olennaista ja merkittävä osa oman kyberturvallisuuden hahmottamista. Samoin digitaalisen muotoilijan rooli edellyttää asianmukaista kykyä arvioida ja hahmottaa omaa nykytilannetta.

Neljännessä osiossa kohdennettiin huomio aihepiirin olennaisiin termeihin ja käsitteisiin. Tämä osio toimii eräänlaisena tietoluotaimena, koska siinä esitettiin kysymyksiä aihepiirin eri puolilta. Vastauksien perusteella saadaan hahmoteltua karkea käsitys vastaajien tarpeista. Viides osio kohdennettiin osallistuneiden henkilökohtaiseen verkkokäyttäytymiseen. Siinä esiteltiin toimintamalleja hyvän kyberhygienian kannalta. Kuudes osio painotti yksilön tietotason ja asenteen merkitystä. Osion tavoitteena oli rajata pois vähemmän tunnettuja pilvipalveluita. Lisäksi siinä kartoitettiin tiedonlähteistä ja niitä tarjoavista tahoista. Viimeinen ja seitsemäs osio sisälsi kysymyksiä vastaajan omasta suhteesta parhaiden käytäntöjen osalta sekä yleisimmin tunnettujen kyberuhkien tunnettavuudesta vastaajien kesken. Viimeisen osion tavoitteena oli saada palautetta eri viestintämetodien mielekkyydestä suhteessa uuden asian oppimiseen.

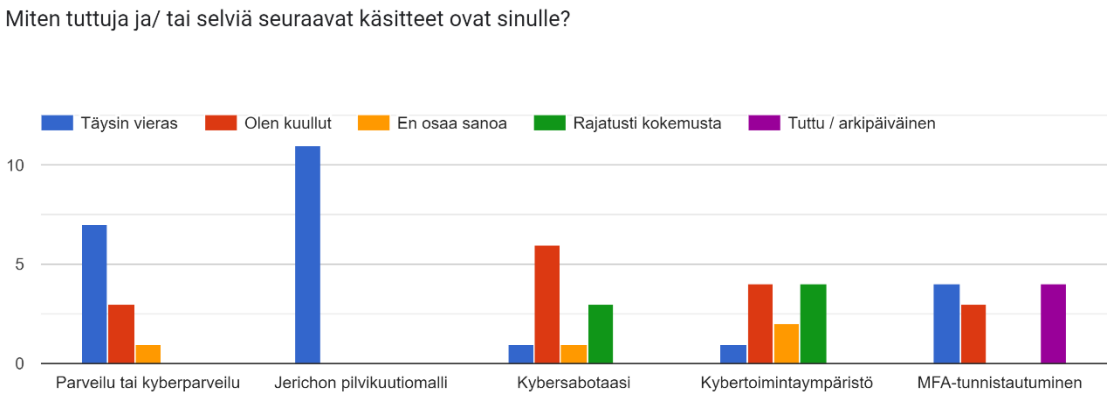
6.2.2 Tietoturvaan liittyvä tietämys ja kokemus

Kyselyn tulokset tukevat käsityksiä koulutustarpeista tietoturvan ja kyberturvallisuuden suhteen. Tämän muuttamiseksi on tehty ja tehdään jatkossakin paljon työtä. Muutoksen saavuttaminen on hidasta ja vaatii resursseja. Sen kannalta myös yksi tämän tutkimuksen päätavoitteista on luotaamisen näkökulmasta saada parempi käsitys tietämyksen tasosta ja ennen kaikkea asenteista digitaalisten muotoilijoiden kollegiaalisessa kontekstissa. Kokemukset muokkaavat asenteita ja tahtotilaa uuden oppimisen kannalta. Aihepiirin arkipäiväistäminen sekä demystifioiminen esimerkiksi avaamalla käsitteitä ja niiden merkityksiä voi herättää uteliaisuutta ja madaltaa kynnystä oppimishalukkuutta kohtaan. Aihe on luonteensa puolesta vakava. Vastassa ovat järjestäytyneet ja korkeasti motivoituneet tahot, kuten ammattirikolliset ja jopa valtiot. Tästä huolimatta perehtyminen voi muodostua mielekkääksi ja voimaannuttavaksi oppimiskokemukseksi. Kyselyn vastaukset tukevat oletettua lähtöasetelmaa aiheen tunnettavuuden kannalta. Kiinnostus ja asenteet aihepiiriä ja sen merkitystä kohtaan ovat joko olleet hyvällä tasolla tai kasvaneet. Tämä on positiivinen ilmiö pohdittaessa ratkaisumalleja tietotason lisäämiseksi. Pohjaan arvioni omaan kokemukseeni sekä saamaani palautteeseen ja reaktioihin, kun olen esittänyt tutkimukseni aiheen ja motiivit niiden taustalla. Motiivini ovat korkeamman tietotason saavuttaminen ja asenteisiin vaikuttaminen kiinnostusta sekä keskustelua herättelemällä. Asenteita aihetta kohtaan on todennäköisesti muokannut siitä yleistynyt ja yhä aktiivisempi viestintä valtavirtamediakanavissa, kun kyberturvan näyttäytyminen uutisotsikoissa arkipäiväisten aiheiden rinnalla on yleistynyt.

6.2.3 Lisäkoulutustarpeet

Tietoturvan ja kyberturvallisuuden suhteen tarpeet lisäkoulutukselle ovat kiistattomat huolimatta siitä, mitä lähteitä tarkastellaan. Huomionarvoinen tekijä lisäkoulutuksen tarpeiden kannalta oli saavuttaa parempi käsitys lähtötilanteesta ja tarpeista. Ne yhdessä määrittävät tarpeen määrän ja tiedon luonteen. Aiemmin

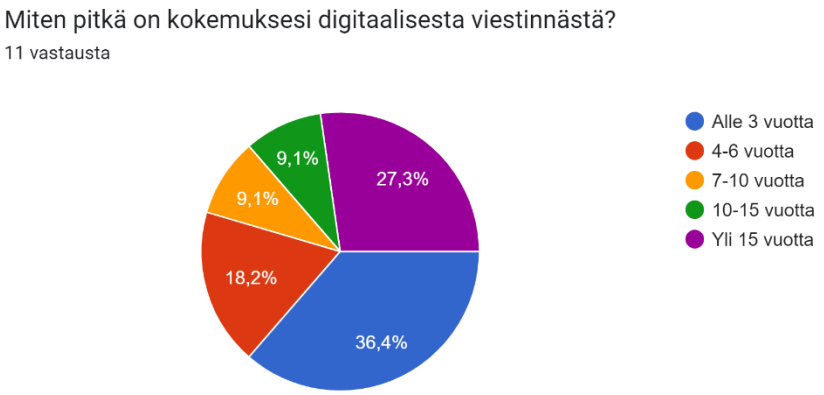
mainittu tarpeen määrä on huomattava. Tietoa aiheesta ei yksinkertaisesti voida jakaa liikaa – juna on jo liikkeessä ja osa matkustajista hämmästelee asemalla. Oikeanlaisen tiedon luonteen ymmärtäminen on olennaista ja sitä kartoitettiin myös tämän tutkimuksen kautta. Tietoturvakysymykset ovat laajoja ja holistista ajattelua edellyttäviä kokonaisuuksia. Ei ole yksinkertaisia ja nopeita ratkaisuja lisäkoulutustarpeidenkaan osalta, mutta jostain on aloitettava. Tämä tutkimus on ollut oma henkilökohtainen päänavaukseni aiheesta, jonka merkitys arjessa on vakava ja välttämätön. Syvällisempi perehtyminen teettämäni kyselytutkimuksen vastauksiin indikoi selkeitä tarpeita lisäkoulutuksen osalta. Analyyttisempi tarkastelu osoitti yhteisiä nimittäjiä osaamisen aukoissa. Yksi selkeä oma osa-alueensa kyberturvallisuuden kontekstissa oli pilvipalvelut ja niitä tarjoavat tahot. Digitaaliset muotoilijat tulevat oman ammatillisen roolinsa puolesta käyttämään pilvipalveluita monipuolisesti. Yhtenä kehityskohteena ja osana digitaalisen viestinnän koulutusta olisi perusteltua kartoittaa suurimmat, yleisimmät pilvipalveluntarjoajat ja niiden mahdolliset erot. Samoin kuvaavaa oli myös kollektiivinen aukko tietämyksessä Jerichon neliulotteisen pilvikuutiomallin suhteen (ks. kuvio 2). Se oli kyselyn ainoa kysymys, joka oli kaikille vieras käsite. Sen tunteminen on olennainen osa pilvipalveluiden hankintaan liittyvää työtä, koska se auttaa tekemään perusteltuja päätöksiä, hallitsemaan riskejä ja varmistamaan palveluiden laadun ja turvallisuuden. Tämä kysymys auttoi luomaan haamurajan tarkastuspisteen vastaajien tietämyksen laajuuden osalta (ks. Liite 1).



Kuvio 2. Kyselytutkimus: neljännen osion toisen kysymyksen Jerichon pilvikuutiomalli oli kaikille vastanneille täysin vieras.

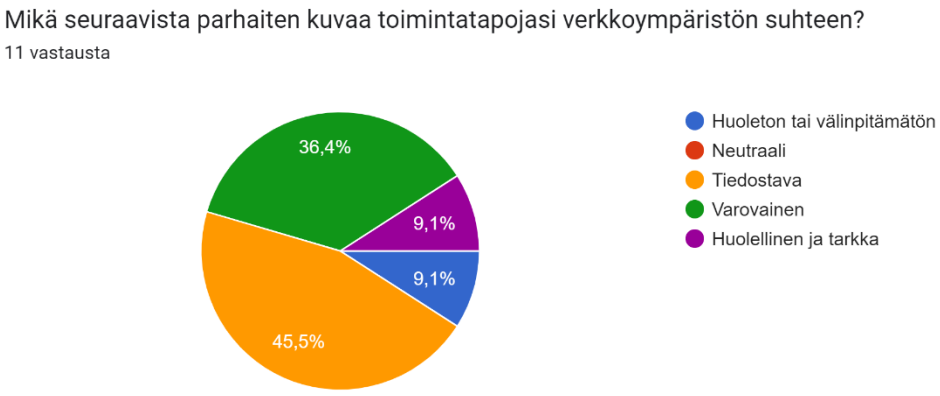
6.2.4 Analyysi ja yhteenveto kyselyn tuloksista

Kvalitatiivisen tutkimusmenetelmän teema-analyysin mukaisesti pyrin tunnistamaan toistuvia teemoja keräämääni kyselytutkimuksen vastauksissa. Yksi toistuva trendi vastauksista on poimittavissa vaikkakin tulkinnanvaraisesti. Sitä kuvaa parhaiten kunnioittava ja asiallinen suhtautuminen aihepiirin kannalta kriittisiin tekijöihin sekä toimintaan verkossa yleisesti. Voidaanko tästä vetää johtopäätös valtavirtajournalismin harjoittaman sensaatio-otsikoiden myynnin ja digitaalisen viestinnän koulutuksen yhteisvaikutuksesta digimaturiteetin osalta? Oli kysymys retorinen tai ei, niin asian vakavuus näyttäisi menneen perille.



Kuvio 3. Kyselytutkimus: pienestä otannasta huolimatta digitaalisen viestinnän kokemuksen suhteen oli hajontaa havaittavissa.

Ensimmäisen osion vastaukset vastaajien ikäjakauman ja kokemuksen osalta digitaalisesta viestinnästä olivat keskenään korreloivia vähemmän kuin osasin ennalta olettaa (ks. kuvio 3). Ikäjakaumien rajat perustuivat arvioon tyypillisestä iästä korkeakouluopintojen suhteen ja olivat toleranssirajoiltaan suuret. Toisessa osiossa oli tarkoitus luoda käsitys vastaajien lähtökohdista suhteessa kyselyn aiheeseen. Saman osion pohjalta voidaan todeta, että asenteissa oli yleisesti vastuullinen toimintamalli verkkokäyttäytymisen osalta. Ainoastaan alle kymmenen prosenttia kuvaili omaa verkkokäyttäytymistään huolettomaksi tai välinpitämättömäksi (ks. kuvio 4). Yli kolmannes vastaajista oli varovaisia ja lähes puolet tiedostavia. Alle kymmenen prosenttia oli huolellisia ja tarkkoja. Otanta viestii tiedostavan varovaisesta tavasta toimia verkkoympäristössä, mikä olisi tulkittavissa tasoltaan tyydyttäväksi tai jopa hyväksi kyberhygieniaksi.



Kuvio 4. Kyselytutkimus: ainoastaan alle kymmenen prosenttia kuvaili omaa verkkokäyttäytymistään huolettomaksi tai välinpitämättömäksi.

7 Johtopäätökset ja pohdinta

Tässä opinnäytetyössäni keskityin tutkimaan, miten viestintävälineet vaikuttavat tietoturvaan ja pyrin kartoittamaan parhaita toimintamalleja niiden käyttämiseen turvallisesti ja vastuullisesti. Edellinen oli itselleni entuudestaan tuttua asiaa, johtuen omasta ammatillisesta kokemuksestani digitaalisesta viestinnästä. Sitä vastoin jälkimmäisestä, viestintävälineiden käyttämistä vastuullisesti, sekä niihin liittyvien hyvien käytäntöjen opiskelu olivat suurelta osin itsellenikin uutta asiaa. Kriteerit lopputuloksen kannalta edellyttävät hyvää kyberhygieniaa ja tiedostavan toiminnan ulottaminen myös ja ensisijaisesti omaan ajatteluun. Tämä opinnäytetyö on ensimmäinen vaihe osana laajempaa kokonaisuutta, kun tarkastellaan työn tavoitteita ja niiden saavuttamista. Tavoitteet tiedon keräämiseen saavutettiin sekä yleisellä tasolla että yksilökohtaisemmin kyselytutkimuksen kohderyhmän kannalta. Kysely tuotti osaltaan myös luotaavan näkökulman, mikä helpottaa perspektiivin asettamista jatkon kannalta.

Kuten alussa todettu on tämä opinnäytetyö konstruktiivinen tutkimus, minkä yhtenä tavoitteena oli luoda konkreettinen tuotos. Työskentelyprosessin kannalta juuri tuo konkreettisen tuotoksen luonne ja muoto otti ajankohtaisemman muodon digitaalisessa kontekstissa. Koska tietoturva ja etenkin kyberturvallisuus ovat aiheina dynaamisia, muutokselle alttiita ja edellyttävät uusinta tietoa niiden ylläpitämiseksi, luontevinta olikin pukea tuo konkreettinen tuotos digitaaliseen kontekstiin sopivaksi. Tämän tutkimuksen yksi ydinkysymyksistä on kyberturva-aiheelle tyypillinen muutos, mikä edellyttää jatkuvaa opiskelua asettaen samalla vaatimuksia lopullisen tuotteen kannalta. Konkretia edellyttää, että tuotoksella pystytään vastaamaan tulevaisuuden muutostarpeille ja tarvittaessa myös mukautumaan niihin. Digitaalinen alusta ja elävä dokumentti voisi olla esimerkiksi verkkosivusto, jonka kautta olisi mahdollisuus ladata ajantasaista tietoa. Tämän probleeman ratkaisemiseksi syntyi verkkojulkaisu nimeltä CyberSub Dispatch Nro. 01–2024 (ks. Liite 2). Se on ensimmäinen julkaisu osana laajempaa verkkojulkaisujen sarjaa. Tähän tarkoitukseen varaamani verkkotunnus: SubmarineSecurity.com tarjoaa kotisataman informaatioliikenteelle sekä täyttää

kriteerit sopivan nimen osalta. Verkkosivustoa ei julkaista osana tätä opinnäytettä. SubmarineSecurity.com -sivuston alustava wireframe-suunnitelma löytyy liitteistä (ks. Liite 3).

Kyselytutkimuksen kautta kerätty tieto ja vastausten reflektointi ovat osaltaan auttaneet paremmin hahmottamaan mahdollisia kipupisteitä. Aihe on laajuudestaan huolimatta jaettavissa pienempiin ja samalla hallittavimpiin osakokonaisuuksiin, mikä helpottaa aiheen kartoittamista. Kevyt kyberkartoitus digiviestinnän osaajille teetettiin anonyymisti. Kyselyn tavoite ja tarkoitus kerrottiin. Siinä mainittiin, että kyselyn avulla on tarkoitus kartoittaa digitaalisen muotoilun ja viestinnän parissa vaikuttavien opiskelijoiden sekä ammattilaisten suhdetta ja tietotasoa tietoturvaan ja kyberturvallisuuteen. Kyselyn kuvausta seurasi tiedonanto ja linkki, mistä voi lukea GDPR-saatteen ja miten vastauksia tullaan analysoimaan, sekä miten pitkään ja kenen toimesta niitä säilytetään. Ennen suostumusta kyselyyn osallistumisesta kerrottiin seitsemään osioon vastaamiseen kuluvan aikaa noin 7–10 minuuttia. Tämän jälkeen pyydettiin kyselyyn osallistuneiden suostumus ennen kyselyn aloittamista. Vastaukset kerättiin hyödyntäen Google Forms -verkkosovellusta. Yhteystietoja ei kerätty missään kohtaa prosessia.

Kyselyn sisältö oli laadittu luotettaviksi koettujen lähteiden pohjalta. Asioiden paikkansa pitävyyttä tarkistettiin käyttämällä useampia eri lähteitä sekä ristiviittausmenetelmää hyödyntäen. Vääristymiä aiheen kannalta tuskin esiintyy merkittävästi, johtuen aihepiirin laaja-alaisen faktapohjaisen tiedon ja tutkimuksen tarjonnasta. Oman lisänsä faktojen tarkastamisen helpottamiseksi on tehnyt viime vuosien selkeä nousujohteinen trendi aihepiiriin liittyvien laadukkaiden julkaisujen osalta. Tämä tutkimus keskittyi kartoittamaan aihetta, jonka laajamittaisempi tarkastelu edellyttäisi monipuolisesti laadittuja jatkotutkimuksia. Tästä syystä aiheen rajaus kohdennettiin digitaalisen viestinnän osaajiin eli digitaalisiin muotoilijoihin. Kvalitatiivisen tutkimusmenetelmän analyyttisen tarkastelumallin teema-analyysiin tukeutuen kyselytutkimuksen vastauksia tulkittiin sen osaamisen pohjalta, mitä aiheesta oli kartutettu ennen prosessia ja sen aikana.

Aalto-yliopiston kyberturvallisuuden työelämäprofessori Jarno Limnéll toteaa verkkosivuillaan suomalaisen yhteiskuntamme sisällä tarpeen sillanrakentajille. Hän näkee sen keskeiseksi tekijäksi yhteisöllisen, menestyvän ja turvallisuudesta huolta pitävän Suomen kannalta. (Limnéll 2024). Limnéll on ollut upseerina puolustusvoimissa, johtotehtävissä liike-elämässä ja professorina yliopistossa, joten hän edustaa ajattelua, mikä on olennaista puhuttaessa kansallisen kyberturvan edistämisestä. Tämän opinnäytteen tavoitteiden taustalla ovat motiivit, joiden pyrkimyksenä on yksilön toimintaa jalostamalla luoda valmiuksia kyberturvan osalta kansallisella tasolla. Kyberturvallisuuden dosentti Jarno Limnéll korostaa teknologian ymmärryksen merkitystä poliittisessa päätöksenteossa ja painottaa tekoälyn sekä kyberturvallisuuden koskettavan jokaisen kansalaisen arkea (STT 2024). Samassa artikkelissa mainittiin ”luottamuspääoma”, jonka merkitys voi olla resurssina keskeinen. Luottamuspääoma viittaa luottamuksen määrään ja laatuun, jota yksilöllä, organisaatiolla tai yhteisöllä on toisiin ihmisiin, instituutioihin tai ryhmiin. Se kuvaa sitä, miten paljon ihmiset luottavat toisiinsa ja millä tavoin tämä luottamus vaikuttaa heidän keskinäiseen toimintaansa.

Luottamuspääoma voi esimerkiksi edistää tietoturvaan ja kyberturvallisuuteen liittyvää toimintaa ja yhteistyötä. Lähtökohtaisesti kaikki pilvipalveluita tarjoavat tahot nauttivat luottamusta, jonka menettäminen olisi heidän toimintansa kannalta kriittistä. Monissa yrityksissä prosesseja optimoivat pilviratkaisut ovat arkipäivää, ja siksi myös niiden tietoturvan tulisi pysyä kehityksen tahdissa (Lehtinen 2022.) Pilvipalveluiden arviointia määrittävät kriteerit olisivatkin suositeltavaa tietoa digitaalisen muotoilijan roolin kannalta. Asenteet yhdessä tiedostavan verkkokäyttäytymisen kanssa ovat suurelta osin ne tekijät, mitkä muodostavat yksilön kyberhygieniatason. Lopuksi on tärkeää muistuttaa yksilön luottamuspääoman ja ajan tasalla olevan tiedon keskinäisestä suhteesta ja merkityksestä. Dosentti Jarno Limnéll lainaa verkkosivuillaan filosofi Senecan sanoja: ”Ihmiset voidaan jakaa kahteen ryhmään: niihin, jotka kulkevat edellä ja saavat jotain aikaan ja niihin, jotka kulkevat jäljessä ja arvostelevat” (Limnéll 2024).

Lähteet

Ali-Yrkkö, Jyrki, Kässi, Otto, Pajarinen, Mika & Rouvinen, Petri 2023. Data, tekoäly ja talouskasvu. Digibarometri 2023. Helsinki, Taloustieto. <https://www.etla.fi/wp-content/uploads/Digibarometri-2023.pdf>

Anderton, Robert, Botelho, Vasco & Reimers, Paul 2023. Working Paper Series, Digitalisation and productivity: gamechanger or sideshow? European Central Bank (ECB), ECB Working Paper Series No 2794 /. <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2794~6911beee80.en.pdf>

Calder, Alan 2022. The Cyber Security Handbook – Prepare for, respond to and recover from cyber-attacks, IT Governance Publishing (ITGP). Ely, United Kingdom: IT Governance Publishing.

Garbis, Jason 2023. Zero Trust Data Resilience, A Secure Data Backup and Recovery Model, Numberline Security. Luettavissa osoitteessa: <https://numberlinesecurity.com/wp-content/uploads/2023/11/2023-11-30-Zero-Trust-Data-Resilience-Research-Whitepaper.pdf> (luettu 23.3.2024).

Heikkinen, Miikka 2022. Etätyön tietoturvajohtamisen kehittäminen pk-yrityksessä. Opinnäytetyö (YAMK), Seinäjoki: Seinäjoen AMK, teknologiaosaamisen johtaminen. Luettavissa osoitteessa: <https://www.theseus.fi/handle/10024/782762> (luettu 3.2.2024).

Heiska, Mikko 2020. Sisäisen viestinnän tutkimus – Tapaustutkimus sisäisen viestinnän käytänteistä. Opinnäytetyö (AMK), Satakunnan ammattikorkeakoulu, liiketalouden koulutusohjelma. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi:amk-2020101821391> (luettu 31.3.2024).

Hiltunen, Mikko 2023. Resilienssin käsite suomalaisessa turvallisuuskeskustelussa, Pro Gradu, Jyväskylä: Jyväskylän Yliopisto, informaatioteknologian tiedekunta. Luettavissa osoitteessa: <http://urn.fi/URN:NBN:fi:jyu-202305313406> (luettu 22.3.2024).

IT Knowledge Zone 2023. How Digital Maturity Improves CyberSecurity. Itknowledgezone.com/ <https://itknowledgezone.com/how-digital-maturity-improves-cybersecurity/> (luettu 13.3.2024).

Juholin, Elisa 2013. Communicare! Kasva viestinnän ammattilaiseksi, 6. uudistettu painos. Helsinki: MIF Management Institute of Finland.

Kanti-Paul, Hanna 2019. Datavetoisuus, tekoäly ja johtajan vuorovaikutusosaaminen organisaatiossa, Datalla johtajan näkemyksiäVaasa: Vaasan yliopisto, markkinoinnin ja viestinnän yksikkö, viestinnän monialainen maisteriohjelma. Luettavissa täällä: <https://osuva.uwasa.fi/handle/10024/9272> (luettu 1.4.2024).

Keskuskauppakamari 2018. Tietoturvaopas yrityksille, Keskuskauppakamari. Luettavissa täällä: <https://kauppakamari.fi/julkaisu/tietoturvaopas-yrityksille/> (luettu 22.2.2024).

Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri), Traficomin julkaisuja 13/2020, PiTuKri – versio 1.1 – maaliskuu 2020. Helsinki, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom. Kyberturvallisuuskeskus.fi Luettavissa täällä: <https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri> (luettu 4.4.2024).

Kyberturvallisuuskeskus 2024. Tietoturva nyt! Kyberturvallisuuskeskuksen viikkokatsaus - 03/2024. Helsinki, Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom. Kyberturvallisuuskeskus.fi <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-032024> (luettu 15.2.2024).

Kääntä, Liisa & Salmela, Eveliina 2018. Näkökulmia viestintätieteisiin – Asiantuntijoiden viestinnästä digitaalisen median mahdollisuuksiin. Vaasan yliopiston raportteja 9, verkkoaineisto. Vaasan yliopisto: markkinoinnin ja viestinnän yksikkö. Luettavissa osoitteessa: <https://osuva.uwasa.fi/handle/10024/8129> (luettu 14.2.2024).

Lehtinen, Saana 2022. Tietoturva voi jopa tehostaa liiketoimintaa.
/ 30.11.2022. Helsinki: Content House, Epressi.com
<https://www.epressi.com/tiedotteet/turvallisuus/tietoturva-voi-jopa-tehostaa-liiketoimintaa.html> (luettu 22.2.2024).

Lehto, Martti 2022. Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti. Jyväskylä: Jyväskylän yliopisto, informaatioteknologian tiedekunnan julkaisuja, no. 93/2022. Luettavissa täällä:
<http://urn.fi/URN:ISBN:978-951-39-9336-8> (luettu 23.2.2024).

Liana Technologies 2023. Viestinnän vastuullisuus ja strateginen merkitys organisaation menestyksen kulmakivinä. LianaTech.fi
<https://www.lianatech.fi/tutustu/blogi/viestinnan-vastuullisuus-ja-strateginen-merkitys-organisaation-menestyksen-kulmakivina.html> (luettu 14.2.2024).

Limnéll, Jarno 2024. Suomen tulevaisuus tehdään yhdessä. JarnoLimnell.fi
<https://www.lianatech.fi/tutustu/blogi/viestinnan-vastuullisuus-ja-strateginen-merkitys-organisaation-menestyksen-kulmakivina.html> (luettu 13.4.2024).

Luoma-aho, Vilma & Pekkala, Kaisa 2019. Osallistava viestintä. ProComma Academic -digikirja. Helsingin yliopisto: ProCom - Viestinnän ammattilaiset ry. Luettavissa osoitteessa: <http://doi.org/10.31885/2019.00008> (luettu 14.2.2024).

NSA 2018. NSA'S Top Ten Cybersecurity Mitigation Strategies. National Security Agency, Central Security Service, Nsa.gov Luettavissa täällä: <https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf > (luettu 24.3.2024).

NSA 2024. NSA Releases Top Ten Cloud Security Mitigation Strategies. National Security Agency, Central Security Service, Nsa.gov Luettavissa täällä: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/> (luettu 24.3.2024).

Perttunen, Anna 2023. Vinkkejä tietoturvalliseen viestintään. MicroMagic.fi <https://micromagic.fi/story/vinkkeja-tietoturvalliseen-viestintaan/> (luettu 22.2.2024).

Pilli, Laura 2023. IT-alan muutostekijät, Digitaalinen transformaatio ja työn murros. Opinnäytetyö (AMK). Jyväskylä: Jyväskylän ammattikorkeakoulu, liiketalouden tutkinto-ohjelma. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi:amk-202304256209> (luettu: 30.3.2024).

Päivän Lehti: uutiset 14.12.2020. Kyberrikollisuus yleistyy ja Suomi kompuroi tietoturvassa – tietovuodot yritysten ongelmana. Tampere, Päivän Lehti Digital Oy. Luettavissa osoitteessa: <https://www.paivanlehti.fi/kyberrikollisuus-yleistyy-ja-suomi-kompuroi-tietoturvassa-tietovuodot-yritysten-ongelmana/> (luettu 11.2.2024).

Pöyhönen, Jouni 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu. Jyväskylä: Jyväskylän yliopisto. Luettavissa osoitteessa: <https://jyx.jyu.fi/handle/123456789/71395> (luettu 31.3.2024).

Rantala, Juuso 2021. Improving the cybersecurity readiness and capabilities of SME-companies in Southwest Finland: implementing a focused cyber threat information sharing service using MISP. Bachelor's thesis. Turku: Turku University Of Applied Sciences, Information and Communications Technology, Cybersecurity. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi:amk-2021110819427> (luettu 2.2.2024).

Salonen, Susanna 2024. Sisäisen digimaturiteetin kasvattaminen julkishallinnossa. Opinnäytetyö (YAMK), Satakunnan ammattikorkeakoulu, johtaminen ja palveluliiketoiminta. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi:amk-202402022420> (luettu 10.3.2024).

Savolainen, Markus 2022. Narratiivinen tutkimus kyberturvallisuuskulttuurista kaupungin hallinto-organisaatiossa. Pro gradu -tutkielma/ maisteritutkielma / lisensiaattitutkimus. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi-fe2022111465575> (luettu 6.2.2024).

Soikkeli, Mikko 2021. Lainsäädäntö tieto- ja kyberturvallisuuden perustana – valtionhallinnon viranomaisen näkökulma. Pro Gradu -tutkielma, Jyväskylä: Jyväskylän yliopisto, informaatioteknologian tiedekunta. Luettavissa osoitteessa: <http://urn.fi/URN:NBN:fi:jyu-202105303303> (luettu 6.2.2024).

Soini, Heikki 2018. Seitsemän asiaa, jotka kaikkien pitää tietää digitaalisen median tulevaisuudesta juuri nyt. Yle.fi/aihe 29.06.2018 Luettavissa osoitteessa: <https://yle.fi/aihe/artikkeli/2018/06/29/seitseman-asiaa-jotka-kaikkien-pitaa-tietaa-digitaalisen-median-tulevaisuudesta> (luettu 7.2.2024).

STT Info 14.12.2020. Kyberrikollisuus yleistyy ja Suomi kompuroi tietoturvassa – osaamispula jarruttaa kehitystä. Helsinki, Suomi: STT Viestintäpalvelut Oy. Luettavissa osoitteessa: <https://www.sttinfo.fi/tiedote/69896266/kyberrikollisuus-yleistyy-ja-suomi-kompuroi-tietoturvassa-osaamispula-jarruttaa-kehitysta?publisherId=3695> (luettu 6.2.2024).

STT Info 26.2.2024. Kokoomuksen Limnell: Todella hienoa, että ehdottamani ”Teknologian maanpuolustuskurssi kansanedustajille” nyt konkretisoituu koulutukseksi. Helsinki, Suomi: STT Viestintäpalvelut Oy. Luettavissa osoitteessa: <https://www.sttinfo.fi/tiedote/70108797/kokoomuksen-limnell-todella-hienoa-etta-ehdottamani-teknologian-maanpuolustuskurssi-kansanedustajille-nyt-konkretisoituu-koulutukseksi?publisherId=69819275&lang=fi> (luettu 13.4.2024).

Taalasmaa, Perttu 2020. Blogi: Moderni digitaalinen muotoilija. Sangre.fi Luettavissa osoitteessa: <https://www.sangre.fi/fi/blog/moderni-digitaalinen-muotoilija> (luettu 14.4.2024).

Turvallisuuskomitea 2017. Yhteiskunnan turvallisuusstrategia. <https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2017/> (luettu 31.3.2024).

Työturvallisuuskeskus 2023. Verkkojulkaisu: Etätyössä turvallisesti. Tt.fi <https://ttk.fi/julkaisu/etatyossa-turvallisesti/#etatyon-taustaa-maaritelma-ja-muodot> (luettu 7.2.2024).

Vaahtera, Jouni 2022. Pilvipalveluiden kyberturvallisuusuhkien automaattisten havainnointikyvykkyyksien kehittäminen kansallisen tason havainnointia varten. Opinnäytetyö (YAMK), XAMK: Tekniikan ylempi ammattikorkeakoulututkinto, kyberturvallisuuden koulutus. Luettavissa osoitteessa: <https://urn.fi/URN:NBN:fi:amk-2022062419122> (luettu14.3.2024)

Vitikka, Minja 2020. Digitaalinen transformaatio haastaa organisaatiot ketteryyteen ja jatkuvaan oppimiseen. Pro Gradu -tutkielma, Jyväskylä: Jyväskylän yliopisto, informaatioteknologian tiedekunta. Luettavissa osoitteessa: <http://urn.fi/URN:NBN:fi:jyu-202006255119> (luettu 9.3.2024).

Vuori, Miikka 2023. Verkkoartikkeli: Onko kaikki orwellilaista? Vai onko orwellilaisuudella enää mitään tekemistä Orwellin 1984:n kanssa? Kulttuuritoimitus.fi <Onko kaikki orwellilaista? Vai onko orwellilaisuudella enää mitään tekemistä Orwellin 1984:n kanssa? - Kulttuuritoimitus> (luettu 12.4.2024).

Waaramaa, Teija & Nissilä, Niina 2023. Verkkoaineisto, Digitalisoituva viestintä muuttuvassa maailmassa. Vaasan yliopisto: Vaasan yliopiston raportteja 41, verkkoaineisto. Luettavissa osoitteessa: <https://urn.fi/URN:ISBN:978-952-395-075-7> (luettu 22.2.2024).

Kuvalähteet

Kuvio 1. Sidosryhmien tärkeyden malli (Waaramaa 2023, 20; Mitchell ja muut, 1997, s. 865–868).

Kuvio 2. Kyselytutkimus: neljännen osion toisen kysymyksen Jerichon pilvikuutiomalli oli kaikille vastanneille täysin vieras.

Kuvio 3. Kyselytutkimus: pienestä otannasta huolimatta digitaalisen viestinnän kokemuksen suhteen oli hajontaa havaittavissa.

Kuvio 4. Kyselytutkimus: neljännen osion toisen kysymyksen Jerichon pilvikuutiomalli oli kaikille vastanneille täysin vieras.

Liitteet

Liite 1. Kyselylomake: Kevyt kyberkartoitus digiviestinnän osaajille, kysymykset

Liite 2. Tietopaketti: CyberSub Dispatch Nro. 01 – julkaisun ensimmäinen nro (PDF)

Liite 3. Verkkosivusto: SubmarinSecurity.com -verkkotunnuksen alustava verkkosivun wireframe-suunnitelma.

Liite 1. Kyselylomake: Kevyt kyberkartoitus digiviestinnän osaajille.

Tervetuloa ja kiitos osallistumisestasi,

Tämän kyselyn avulla on tarkoitus kartoittaa digitaalisen muotoilun ja viestinnän parissa vaikuttavien opiskelijoiden sekä ammattilaisten suhdetta ja tietotasoa tietoturvaan ja kyberturvallisuuteen.

Tämä kysely on osa tutkimusta aiheesta: Tietoturva ja kyberturvallisuus digitaalisessa viestinnässä: Digitaalisen muotoilijan näkökulma ja vastuu.

Tutkimuksen tavoitteena on selvittää tietoturvan ja kyberturvallisuuden merkitystä digitaalisen viestinnän kontekstissa. Aihe on luonteensa puolesta ajankohtainen ja muutosaltis.

Tutkimuksen toteuttaa Metropolia Ammattikorkeakoulun opiskelija osana opinnäytetyötään.

Osallistuminen kyselyyn on täysin vapaaehtoista, ja voit keskeyttää osallistumisesi koska tahansa ilman syytä. Henkilötietojasi ei kerätä ja vastauksia käsitellään anonyymisti eikä sinua voida tunnistaa vastauksistasi.

Tutkimuksen aineistoa säilytetään minun toimestani turvallisesti, ja se tuhotaan automaattisesti tutkimuksen päätyttyä, kuitenkin viimeistään 31.7.2024.

Tutkimukseen vastaaminen vie arviolta 7–10 min aikaa, ja arvostan suuresti osallistumistasi.

Jos sinulla on kysyttävää kyselystä tai tietosuojakäytännöistä, voit ottaa minuun yhteyttä osoitteeseen samuel.kallio@metropolia.fi.

Kiitos, että osallistut tutkimukseeni!

Ystävällisin terveisin,

Samuel Kallio

Kevyt kyberkartoitus digiviestinnän osaajille

Tämän kyselyn avulla on tarkoitus kartoittaa digitaalisen muotoilun ja viestinnän parissa vaikuttavien opiskelijoiden sekä ammattilaisten suhdetta ja tietotasoa tietoturvaan ja kyberturvallisuuteen.

arcticseamanstudio@gmail.com Vaihda tiliä

Ei jaettu

* Pakollinen kysymys

GDPR saatteen löydät tämän >> linkin takaa. Siinä kerrotaan, miten vastauksia analysoidaan ja myös miten pitkään ja kenen toimeista niitä säilytetään.

Kyselyn sisältö ja arvioitu kesto

Tähän kyselyyn vastaamiseen kuluu noin 7-10 minuuttia. Osioita on seitsemän ja kysymyksiä yhteensä 19.

Kyselyn sisältö ja arvioitu kesto
Tähän kyselyyn vastaamiseen kuluu noin 7-10 minuuttia. Osioita on seitsemän ja kysymyksiä yhteensä 19.

Suostumuksesi tähän verkkokyselyyn. Suostutko osallistumaan tähän tutkimukseen? *

- (●) Kyllä, olen lukenut tutkimustiedotteen ja ymmärtänyt sen. Haluan osallistua tähän tutkimukseen.
- ( ) Ei, en halua osallistua tähän tutkimukseen.

Voisitko kertoa ikäsi?

- ( ) Alle 25-vuotias
- ( ) 25-35
- ( ) 36-45
- ( ) 46-55
- ( ) Yli 55-vuotias

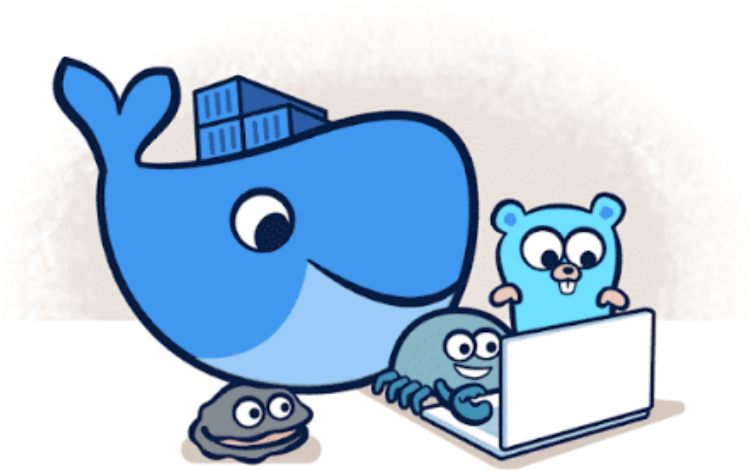
Miten pitkä on kokemuksesi digitaalisesta viestinnästä?

- ( ) Alle 3 vuotta
- ( ) 4-6 vuotta
- ( ) 7-10 vuotta
- ( ) 10-15 vuotta
- ( ) Yli 15 vuotta

Digitaalinen viestintä, palvelumuotoilu ja muu verkkoympäristöön sijoittuva ammatillinen toiminta.

Tämän osion tarkoituksena on luoda käsitys vastaajan omista lähtökohdista suhteessa kyselyn aiheeseen.

Mikä seuraavista parhaiten kuvaa omaa rooliasi digitaaliseen viestintään?



- ◯ Digitaalisen median / palvelumuotoilun opiskelija
- ◯ Viestinnän / digitaalisen median / palvelumuotoilun opinnot suoritettu
- ◯ Viestinnän / digitaalisen median / palvelumuotoilun ammattilainen
- ◯ Muu: _____

Mikä seuraavista parhaiten kuvaa omaa suhdettasi tietoturvaan ja kyberturvallisuuteen?

- ◯ Kokematon
- ◯ Vähäinen käsitys aiheesta
- ◯ Ymmärrän peruskäsitteitä aiheen kannalta
- ◯ Olen suorittanut kurssin (tai useita) aiheeseen liittyen
- ◯ Perehtynyt ja seuraan aktiivisesti
- ◯ Muu: _____

Mikä seuraavista parhaiten kuvaa toimintatapojasi verkkoympäristön suhteen?

- ◯ Huoleton tai välinpitämätön
- ◯ Neutraali
- ◯ Tiedostava
- ◯ Varovainen
- ◯ Huolellinen ja tarkka
- ◯ Muu: _____

Ennaltaehkäisevän toiminnan kannalta oman tietotason määrittäminen on ensisijaisen tärkeää kyberturvan suhteen.

Itsearviointi on digitaalisen viestinnän viitekehyksessä ensisijaisen tärkeää etenkin, kun ammattimainen toiminta edellyttää kykyä hahmottaa nykytilanne sekä kartoittaa tarpeet ja ensisijaiset toimenpiteet.

Miten arvioisit omaa tietämystäsi suhteessa kyberturvaan?

	1	2	3	4	5	
Heikko	○	○	○	○	○	Vahva

Miten hyvin olet sisäistänyt ennalta ehkäisevät toimenpiteet kyberuhkien varautumisen suhteen?

	1	2	3	4	5	
Heikosti	○	○	○	○	○	Hyvin

Miten arvioisit omaa kykyäsi palautua tietoturvahyökkäyksen seurauksista?

	1	2	3	4	5	
Heikko	○	○	○	○	○	Vahva

Miten koet kyselyn aiheen, kiinnostaisiko sen laajempi tuntemus ja ymmärrys?

	1	2	3	4	5	
Vähän	○	○	○	○	○	Paljon

Uudet aihepiirit saavat muodon, kun termit ja käsitteet alkavat hahmottua.

Tämän osion tarkoituksena on kartoittaa olemassaolevia tarpeita digitaalisen viestinnän ammattilaisten keskuudessa.

Miten tuttuja ja/ tai selviä seuraavat käsitteet ovat sinulle?

	Täysin vieras	Olen kuullut	En osaa sanoa	Rajatusti kokemusta	Tuttu / arkipäiväinen
Kyberhygienia	○	○	○	○	○
Hybridivaikuttaminen	○	○	○	○	○
Resilienssi	○	○	○	○	○
Zero Trust -periaate	○	○	○	○	○
Digimaturiteetti	○	○	○	○	○

Miten tuttuja ja/ tai selviä seuraavat käsitteet ovat sinulle?

	Täysin vieras	Olen kuullut	En osaa sanoa	Rajatusti kokemusta	Tuttu / arkipäiväinen
Parveilu tai kyberparveilu	○	○	○	○	○
Jerichon pilvikuutiomalli	○	○	○	○	○
Kybersabotaasi	○	○	○	○	○
Kybertoimintaympäristö	○	○	○	○	○
MFA-tunnistautuminen	○	○	○	○	○

Miten tuttuja ja/ tai selviä seuraavat käsitteet ovat sinulle?

	Täysin vieras	Olen kuullut	En osaa sanoa	Rajatusti kokemusta	Tuttu / arkipäiväinen
Ransomware	○	○	○	○	○
Troijalainen	○	○	○	○	○
Hajautettu palvelunestohyökkäys	○	○	○	○	○
Tietovuoto	○	○	○	○	○
Nollapäivähaavoittuvuus	○	○	○	○	○

Puhuttaessa kyberturvan merkityksestä, jokaisen henkilökohtainen panos vaikuttaa kokonaisuuteen.

Tiesitkö, että kansalaisen oma kyberhygienia osaltaan vahvistaa tai heikentää resilienssiä kansakunnan tasolla eli kykyä vastata poikkeaviin tilanteisiin ja/ tai kriittisiin uhkiin verkkoympäristössä.

Mitkä seuraavista toimenpiteistä koet henkilökohtaisesti tärkeiksi hyvän kyberhygienian saavuttamiseksi.

	Ei lainkaan tärkeä	Ei kovin merkittävä	En osaa sanoa	Merkittävä	Kriittinen
Salasanaholvin käyttö	○	○	○	○	○
Suojatun yhteyden muodostaminen	○	○	○	○	○
Palautumisstrategia - suunnitelma	○	○	○	○	○
Ohjelmistopäivitykset	○	○	○	○	○
Järjestelmien aktiivinen hallinta	○	○	○	○	○

Miten itse toimit suhteessa alla lueteltuihin toimintatapoihin, miten itse käytät tai noudatat niitä?

	En käytä	Harvoin	Joskus	Usein	Aina
Vahvat salasanat	○	○	○	○	○
Haittaohjelmien torjuntaohjelma	○	○	○	○	○
Tietojen varmuuskopiointi	○	○	○	○	○
Tietoinen klikkaaminen	○	○	○	○	○
Varovaisuus julkisia WiFi-verkkoja kohtaan	○	○	○	○	○

Ennaltaehkäisevät toimenpiteet käsittävät toimintaperiaatteita, joita ohjaavat tottumukset, turvallisuusprotokolla ja asenteet.

Tietoturvan ja kyberturvallisuuden taso on suuresti riippuvainen yksilöiden asenteista ja heidän tietotasostaan.

Mitkä luettelon pilvipalveluista ovat henkilökohtaisesti tai työtehtävien kautta tuttuja?

	Ei lainkaan tuttu	Melko vieras	En osaa sanoa	Tuttu	Arkipäiväinen
Microsoft Azure	○	○	○	○	○
Amazon Web Services (AWS)	○	○	○	○	○
Google Cloud Platform (GCP)	○	○	○	○	○
IBM Cloud	○	○	○	○	○
Oracle Cloud	○	○	○	○	○
Alibaba Cloud	○	○	○	○	○
Salesforce	○	○	○	○	○

Mitkä seuraavista julkaisuista, lähteistä, instituutioista tai organisaatioista ovat aiheen kannalta entuudestaan tuttuja tai olet niistä tietoinen?

	En tunnista	Olen kuullut	En osaa sanoa	Tiedän	Tunnen hyvin
Kybersää	○	○	○	○	○
Digibarometri	○	○	○	○	○
Kyberturvallisuuskeskus	○	○	○	○	○
Euroopan hybridiuhkien torjunnan osaamiskeskus	○	○	○	○	○
Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)	○	○	○	○	○

Viimeinen osio on omistettu parhaille vinkeille ja oppimisen mahdollisuudelle.

Loppua kohden kevennykseksi esimerkkejä biisien ja bändien nimiltä kuulostavilta kuuluisista kyberturvahaitoista ja -hyökkäyksistä sekä alan termeistä.

Mitkä seuraavista nimistä tunnistat ja/ tai tiedät kyseisen tapauksen?

	Aivan vieras	Olen ehkä kuullut	En osaa sanoa	Kuulostaa tutulta	Tiedän tapauksen
Akira	○	○	○	○	○
NotPetya	○	○	○	○	○
Heartbleed	○	○	○	○	○
WannaCry	○	○	○	○	○
Stuxnet	○	○	○	○	○
Bug Bounty	○	○	○	○	○
Phishing	○	○	○	○	○

Miten arvioisit näin lopuksi omaa suhdettasi parhaiden käytäntöjen osalta?

	En käytä	Harvoin	En osaa sanoa	Usein	Aina
Kuinka usein päivität käyttöjärjestelmäsi, sovelluksesi ja tietoturvaohjelmasi?	○	○	○	○	○
Käytätkö vahvoja ja ainutlaatuisia salasanoja eri verkkopalveluissa?	○	○	○	○	○
Käytätkö salasanasäilöjää (password manager) salasanojesi hallintaan?	○	○	○	○	○
Tarkistatko sähköpostiviestien lähettäjät ennen liitteiden avaamista tai linkkien napsauttamista?	○	○	○	○	○
Käytätkö monivaiheista todennusta tärkeissä verkkopalveluissa?	○	○	○	○	○
Säilytätkö tärkeitä tiedostoja ja varmuuskopioita turvallisesti?	○	○	○	○	○

Valitse alla olevista vaihtoehdoista ne, jotka tarjoaisivat sinulle parhaan mahdollisuuden kiinnostua ja oppia aiheesta, joka on ajankohtainen ja tärkeä.

	Ei kiitos	Luultavasti ei	En osaa sanoa	Mahdollisesti	Toimii
Uutiskirje sähköpostilla	○	○	○	○	○
Uutiskirje printtinä	○	○	○	○	○
Podcast	○	○	○	○	○
YouTube / Vlog	○	○	○	○	○
Online-peli	○	○	○	○	○
Flash cards	○	○	○	○	○
Mobiilisovellus	○	○	○	○	○

Kiitos!
Arvostamme kovasti osallistumistasi ja tähän käyttämääsi aikaa.
Turvallisemman tulevaisuuden puolesta!

Liite 2. Tietopaketti: CyberSub Dispatch Nro. 01 – verkkojulkaisun ensimmäinen nro (PDF).

SUBMARINE SECURITY

CyberSub Dispatch Nro. 01 – 2024

'Detecting threats before they surface'

Pilvipalvelut

Kyberturvallisuuskeskuksen listaamia pilvi-turvallisuuskäytäntöjä ovat pilvipalvelu-ympäristön erottaminen muusta ympäristöstä ja sen jakaminen segmentteihin, kontrolloitu pilvipalvelun käyttöoikeuksien hallinta, kirjattu pilven kattava tietoturvakäytäntö, relevantti IT-turvallisuusosaaminen, toimivat pilven hallin-nointikäytännöt, järjestelmän ja sen käytön monitorointi sekä lopuksi osallistava turvallisuuskulttuuri.

Kyberghygienia

Kyberhygienia tarkoittaa kyberturvallisuuden kehittämistä ja sen ylläpitämistä, eli omaa ja ympäristön kyberturvallisuutta edistetään säännöllisillä rutiineilla. Kyberhygienian idea on, että turvallisesta toiminnasta tulee osa päivittäistä tekemistä ja tämän takia asiaan tulisi kiinnittää huomiota. Kyberturvallisuus ei ole kaikille ykkösasia, mutta jokaisen tulee tästä huolimatta tiedostaa sen tärkeys ja tehdä välttämätön, jotta pysyy turvassa kybervihol-lisilta. Hyvän kyberhygienian avulla toimimme turvallisesti arjessamme.

Digimaturiteetti

Käsiteltäessä aihetta kyberturvallisuuden näkökulmasta on hyvä tiedostaa, mitä kyber-toimintaympäristö tarkoittaa. Se ei tarkoita vain elektronista irrallista entiteettiä, vaan se koostuu ihmisten, organisaatioiden ja fyysis-ten järjestelmien yhdessä muodostamasta vaikutusympäristöstä. Kybertoimintaympä-ristön näkökulmasta kyberturvallisuus osana digitaalista transformaatiota korostaa digima-turiteetin kasvattamisen merkityksen.

NSA (National Security Agency)

NSA:n kymmenen parasta tietoturvauhan lieventämistoimenpidettä:

1) Päivitä ja päivitä ohjelmistot välittömästi
2) Puolusta käyttöoikeuksia ja tilejä
3) Noudata allekirjoitettujen ohjelmistojen suorituskäytäntöjä
4) Harjoittele järjestelmän palautussuunnitelmaa
5) Järjestelmien ja asetusten aktiivinen hallinta
6) Jatkuva verkkojen tunkeutumisen metsästys
7) Tehosta nykyaikaisia laitteiston tietoturvaominaisuuksia
8) Tietoverkkojen erottelu sovellustietoisilla puolustusmekanismeilla
9) Integroi uhkan maineenpalvelut
10) Siirry monivaiheiseen tunnistautumiseen

Resilienssi & Zero Trust -periaate

Resilienssi ymmärretään suomalaisessa turvallisuuskeskustelussa erilaisina yhdistelminä kyvykkyyksiä tai ominaisuuksia.

Resilienssi ja Zero Trust -periaate muodostavat yhdessä keskeisen osan nykyaikaista tietoturvaa. Zero Trust -periaate edustaa nykyaikaista lähestymistapaa tietoturvaan, jossa oletetaan, että verkoston jokainen osa voi olla potentiaalinen hyökkäyksen kohde, ja siksi kaikki verkko-yhteydet ja toimijat tulee varmentaa jatkuvasti.

Vaikka Zero Trust -mallit ovat laajasti käytössä, ne eivät tarjoa kattavia ohjeita kaikilla keskeisillä alueilla, erityisesti tietojen varmuuskopioinnin ja palauttami-sen osalta.

keywords - avainsanat: kyberhygienia, digimaturiteetti, resilienssi

Kolme kovaa ladattavaa >> [Download | Read | Share]

Uhkien ennakointi käsittää ensisijaisesti ennalta tehtävät toimenpiteet tietoturvan ja kyberturvallisuuden kannalta.
Parhaita käytäntöjä on paljon. Täältä löydät muutamia. Paremman kyberhygienian puolesta.

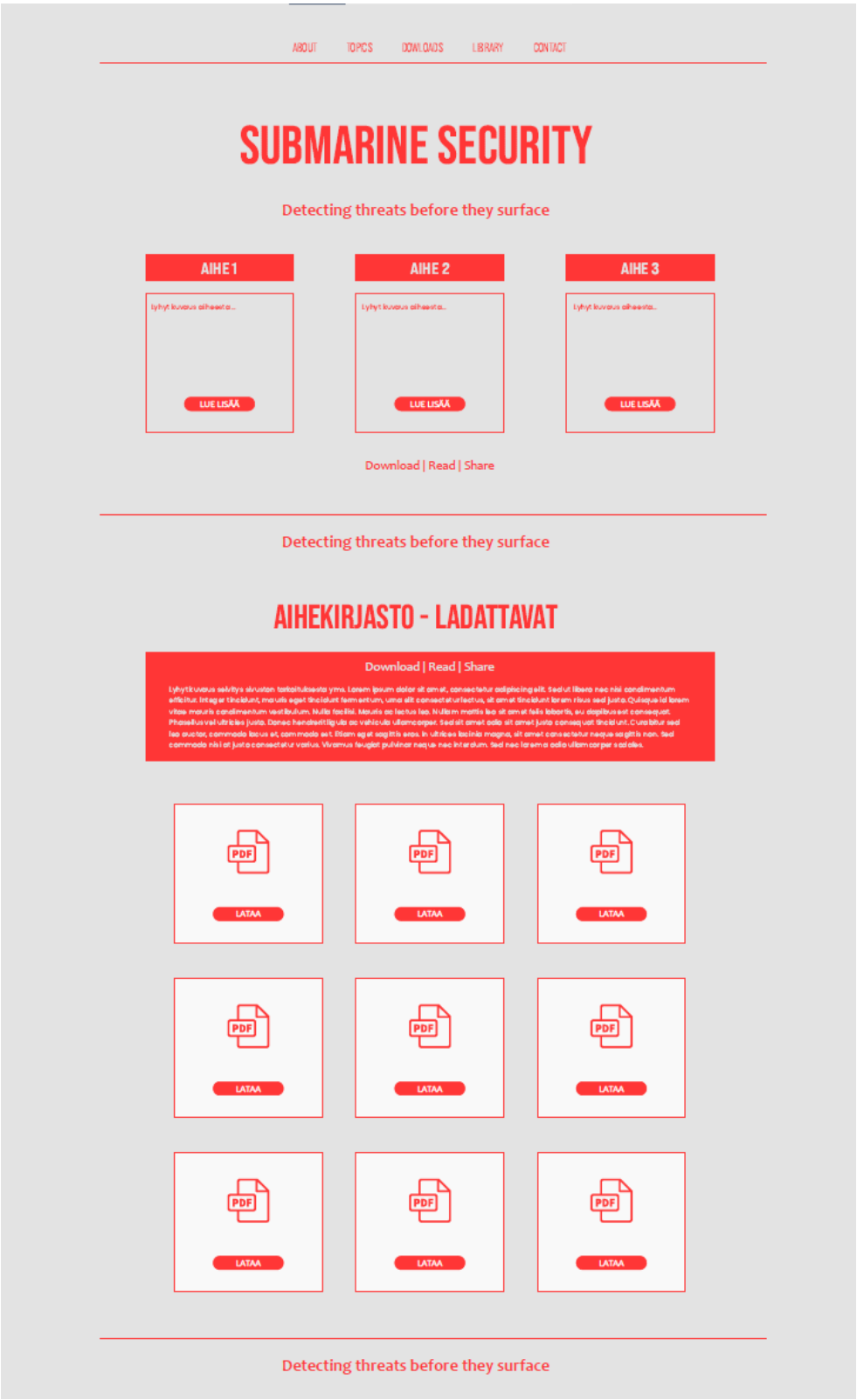
- NSA 2018. **NSA'S Top Ten Cybersecurity Mitigation Strategies.** National Security Agency, Central Security Service
- Kyberturvallisuuskeskus 2020. **Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)**, Traficomin julkaisuja 13/2020
- Kyberturvallisuuskeskus 2024. Tietoturva nyt! **Kyberturvallisuuskeskuksen viikkokatsaus - 03/2024**

Tämän dokumentin, (SubmarineSecurity.com -sivuston), tarkoitus on kerätä oikeaa tietoa kyberturvaan liittyvistä aiheista ja jakaa sitä eteenpäin.
Pyrimme ylläpitämään jakamamme tietoa ajan tasalla julkaisutiheyden sekä päivittämisen kannalta.

SUBMARINE SECURITY

SubmarineSecurity.com | CyberSub Dispatch Nro. 01 – 2024 | Yhteydenotot: dispatcher@submarinesecurity.com

Liite 3. Verkkosivusto: SubmarinSecurity.com -verkkotunnuksen alustava verkkosivun wireframe-suunnitelma.



SHORTLIST - CYBER TIPS

Download | Read | Share

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

Detecting threats before they surface

CYBER STORM BROADCAST

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

UHKAVAROITUS

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

UHKATASO

lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.

UHKARAPORTTI

Lyhyt kuvaus selvitys sivuston tarkoituksesta yms. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed ut libero nec nisi condimentum efficitur. Integer tincidunt, mauris eget tincidunt fermentum, urna elit consectetur lectus, sit amet tincidunt lorem risus sed justo. Quisque id lorem vitae mauris condimentum vestibulum. Nulla facilisi. Mauris ac lectus leo. Nullam mattis leo sit amet felis lobortis, eu dapibus est consequat. Phasellus vel ultricies justo. Donec hendrerit ligula ac vehicula ullamcorper. Sed sit amet odio sit amet justo consequat tincidunt. Curabitur sed leo auctor, commodo lacus et, commodo est. Etiam eget sagittis eros. In ultrices lacinia magna, sit amet consectetur neque sagittis nan. Sed commodo nisl at justo consectetur varius. Vivamus feugiat pulvinar neque nec interdum. Sed nec lorem a odio ullam corper sodales.