Koronaviruksen vaikutus suomalaisten yritysten kyberturvallisuuteen

Jonas Kivikoski

2020 Laurea

Laurea-ammattikorkeakoulu

Koronaviruksen vaikutus suomalaisten yritysten kyberturvallisuuteen

Jonas Kivikoski

Tietojenkäsittely

Opinnäytetyö

Joulukuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tradenomi (AMK)

Jonas Kivikoski

Koronaviruksen vaikutus suomalaisten yritysten kyberturvallisuuteen

Vuosi 2020 Sivumäärä 20

Opinnäytetyön tarkoituksena oli selvittää, miten koronavirus on vaikuttanut suomalaisten yritysten kyberturvallisuuteen. Opinnäytetyön tavoitteena oli tuottaa tietoa, minkälaisia uhkia koronavirus on tuonut ilmi kyberturvallisuuden näkökulmasta yrityksille.

Tämä opinnäytetyö toteutettiin laadullisena eli kvalitatiivisena tutkimuksena. Aineistonkeruumenetelmänä käytettiin haastatteluja ja aineistolähteitä rinnakkain. Haastatteluiden pohjana käytettiin kyselylomaketta, minkä tarkoituksena oli ohjata haastattelua oikeaan suuntaan.

Tutkimuksen tarkoituksena oli selvittää, minkälaisia uhkia koronavirus oli lisännyt suomalaisissa yrityksissä, mitä mahdollisia kyberturvallisuusriskejä etätyöskentely sisältää ja olivatko yritykset lisänneet resursseja kyberturvallisuuteen vuonna 2020.

Saatujen tutkimustulosten perusteella voitiin todeta, että koronavirus on lisännyt kyberturvallisuusriskejä suomalaisissa yrityksissä. Etätyöskentelyyn siirtyminen on luonut uusia huomioon otettavia riskejä sekä koronavirukseen liittyvät kalasteluviestit ja haittaohjelmat ovat lisääntyneet.

Asiasanat: Kyberturvallisuus, koronavirus, haittaohjelma, etätyö

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Jonas Kivikoski

The Impact of Coronavirus on the Cyber Security of Finnish Companies

Year 2020 Pages 20

The purpose of the thesis was to find out how coronavirus has affected the cyber security of Finnish companies. The aim of the thesis was to produce information about what kind of threats coronavirus has revealed for the companies from cyber security perspective.

The thesis used a qualitative research method. The interviews and literature sources were used in parallel. The interviews were based on a questionnaire with the purpose of guiding the interview into the right direction.

The purpose of the study was to find out what kinds of threats the coronavirus has imposed upon Finnish companies, what possible cyber security risks remote work involves and whether the companies had increased their resources related to cyber security in 2020.

Based on the obtained research results, it can be stated that the coronavirus pandemic has indeed increased the risks related to cyber security in the Finnish companies. The shift to remote working created new type of risks to consider. In addition, the number of phishing messages and different types of malware threats related to coronavirus has also increased.

Keywords: Cyber security, coronavirus, malware, remote work

Sisällys

1 Johdanto 6
1.1 Tutkimuskysymykset ja tavoitteet 6
2 Teoreettinen viitekehys 7
2.1 Kyberturvallisuus 7
2.2 Haittaohjelma 8
2.3 Tietojenkalastelu 9
2.4 Kiristyshaittaohjelma 10
2.5 Petokset ja huijaukset 10
2.6 Disinformaatio 10
2.7 Etätyöskentely 11
3 Tutkimusmenetelmä 12
3.1 Tiedonkeruumenetelmät 12
3.2 Analysointimenetelmät 12
4 Tutkimuksen toteutus 13
5 Tutkimustulokset 14
6 Johtopäätökset 16
Lähteet 17
Kuviot 20

1 Johdanto

Koronaviruksen aiheuttama pandemiakriisi on vaikuttanut elämäämme ja muuttanut monia päivittäisiä rutiinejamme huomattavan lyhyessä ajassa. Koronavirus on tuonut mukanaan niin teknisiä kuin organisatorisia haasteita yrityksille, ja nämä haasteet edellyttävät kyberturvallisuuden eri osa-alueiden perusteellista ymmärtämistä ja uudelleenarviointia yrityksiltä.

Koronavirus on vahvistanut ja muuttanut yhteiskuntamme riippuvuutta tieto -ja viestintätekniikasta sekä internetistä etätyön lisääntymisen takia. Myös kyberrikolliset ovat nopeasti sopeutuneet näihin muutoksiin, mikä on puolestaan muuttanut rikollisten toimintatapoja ja menetelmiä.

Etätyön lisääntymisen myötä työntekijät käyttävät yrityksen laitteita vapaa-ajallaan ja tämä lisää uusia tietoturvahaasteita yrityksille. Videoneuvottelutyökaluista on tullut ensisijainen tapaamisympäristö torjuakseen koronaviruksen leviämisen. Yritysten VPN-verkot ovat lisääntyneet sekä pilvipalveluiden käyttö kasvanut. Kyberrikolliset ovat kohdistaneet huomionsa näihin poikkeustoimiin ja pyrkivät löytämään tätä kautta heikkouksia yritysten järjestelmistä. Kyberrikolliset voivat esiintyä hallituksen organisaatioina, terveysministeriöinä, terveyskeskuksina, it-tukena tai muina tärkeinä tahoina naamioidakseen itsensä luotettaviksi lähteiksi.

Joulukuussa 2019 Kiinassa todettiin tuntematon koronavirus, SARS-Cov-2, mikä aiheutti keuhkokuumetapauksia. Koronavirus on nimetty SARS-koronaviruksen mukaan ja sitä kutsutaan nimellä COVID-19. COVID-19 tulee sanoista corona, virus, disease. Uusi koronavirus arvioidaan olevan lähtöisin yksittäisestä tartunnasta eläimen ja ihmisen välillä. Koronavirus on perimältään läheistä sukua SARS-koronaviruksen ja lepakoilta löydettyjen koronavirusten kanssa (Terveyden ja hyvinvoinnin laitos 2020).

1.1 Tutkimuskysymykset ja tavoitteet

Opinnäytetyön tavoitteena on selvittää koronaviruksen vaikutus suomalaisten yritysten kyberturvallisuuteen ja onko tietyn tyyppiset uhat lisääntyneet pandemian seurauksena. Tarkoituksena on verrata tilannekuvaa maailmalla ja selvittää suomalaisiin yrityksiin kohdistuneita hyökkäyksiä.

2 Teoreettinen viitekehys

Erilaiset kyberriskit ovat kasvaneet räjähdysmäisesti vuonna 2020 hyödyntäen maailman väestön tarpeita ja pelkoja. Maaliskuussa koronaviruksen alkuvaiheessa erilaiset huijaukset lisääntyivät 400% helmikuusta. Huijaukset kohdistuivat yksilöihin sekä organisaatioihin. Kriisien aikana on todennäköisempää, että ihmiset etsivät ajankohtaisia toimintaohjeita ja joutuvat todennäköisemmin haitallisten linkkien ja liitteiden uhreiksi (O'Donoghue, Splittgerber, Thomas, Womersley Smith & Bateman 2020).

Google kertoi torjuvansa huhtikuun aikana 18 miljoonaa päivittäistä koronavirukseen liittyvää kalasteluviestiä ja haittaohjelmaa (Kumaran & Lugani 2020).

Paloalton julkaisemassa tutkimuksessa kävi ilmi, että keskimäärin 1767 haitallista verkkosivua luodaan päivittäin (Chen 2020).

Iso-Britanniassa lopetettiin 471 verkkokauppaa, jotka myivät vilpillisiä koronavirukseen liittyviä tuotteita (Palmer 2020).

Työttömyysasteen noustessa ihmiset, jotka ovat joutuneen jäämään kotiin ilman tulonlähdettä, ovat alkaneet etsiä uusia elinkeinonlähteitä. Cybernewsin tehdyn tutkimuksen mukaan hakkerointiin ja muihin tietoverkkorikollisuuksiin liittyvät haut ovat lisääntyneet. Lisäksi vierailut suosittuihin hakkereiden verkkosivustoihin ja foorumeille lisääntyivät maaliskuussa jopa 66% (Mikalauskas 2020).

2.1 Kyberturvallisuus

Kyberturvallisuus tarkoittaa ennaltaehkäiseviä tekniikoita ja toimia, joita käytetään verkkojen, ohjelmien ja tietojen eheyden suojaamiseen hyökkäyksiltä tai luvattomalta käytöltä. Kyberturvallisuudella pyritään turvaamaan liiketoiminnan jatkuvuus yrityksissä ja organisaatioissa (Paloaltonetworks 2020).

Kyberturvallisuus liittyy kaikkiin aktiivisiin tai passiivisiin toimiin, jotka on toteutettu järjestelmien, verkkojen, ohjelmien tai muun digitaalisen omaisuuden suojaamiseksi. Kyberturvallisuuden hallinta koostuu erilaisista työkaluista, parhaista käytännöistä, palveluista, tekniikoista ja koulutuksesta (IBM 2020).

Karspersky jakaa kyberturvallisuuden seuraaviin osa-alueisiin:

- Verkkoturvallisuudesta puhutaan silloin kun halutaan käytännössä suojata tietoverkko tunkeilijoilta, olivatpa kyseessä kohdistetut hyökkäykset tai haittaohjelmat

- Sovellusturva keskittyy ohjelmistojen ja laitteiden turvaamiseen. Vaarantunut sovellus voi tarjota pääsyn tietoihin, mitkä se on suunniteltu suojaamaan.
- Tietoturva suojaa tietojen eheyttä ja yksityisyyttä niin tallennettaessa kuin siirrettäessä.
- Operatiivinen turvallisuus sisältää prosessit ja päätökset tietovarojen käsittelystä sekä suojaamisesta.
- Katastrofi ja toiminnan jatkuvuus määrittävät miten organisaatio reagoi kyberturvallisuushäiriöön. Poikkeaman sattuessa palautumiskäytännöt määräävät, miten organisaatio palauttaa toimintansa ja varmistaa toimintakapasiteettinsa eli liiketoiminnan jatkuvuuden.
- Loppukäyttäjien koulutus käsittelee kaikkein arvaamattomimman kyberturvallisuustekijän eli ihmiset. Käyttäjien opastus on elintärkeää minkä tahansa organisaation turvallisuudelle (Kaspersky 2020).

2.2 Haittaohjelma

Haittaohjelmaksi voidaan luokitella mikä tahansa ohjelma tai tiedosto, mikä on haitaksi tietokoneen käyttäjälle. Haittaohjelmatyyppejä ovat muun muassa tietokonevirukset, madot, Troijan hevoset ja erilaiset vakoiluohjelmat. Edellä mainitut haitalliset ohjelmat voivat suorittaa erilaisia toimintoja, kuten arkaluontoisten tietojen varastamista, salaamista, poistamista tai tarkkailla mitä käyttäjä tekee tietokoneella (Rouse 2020).

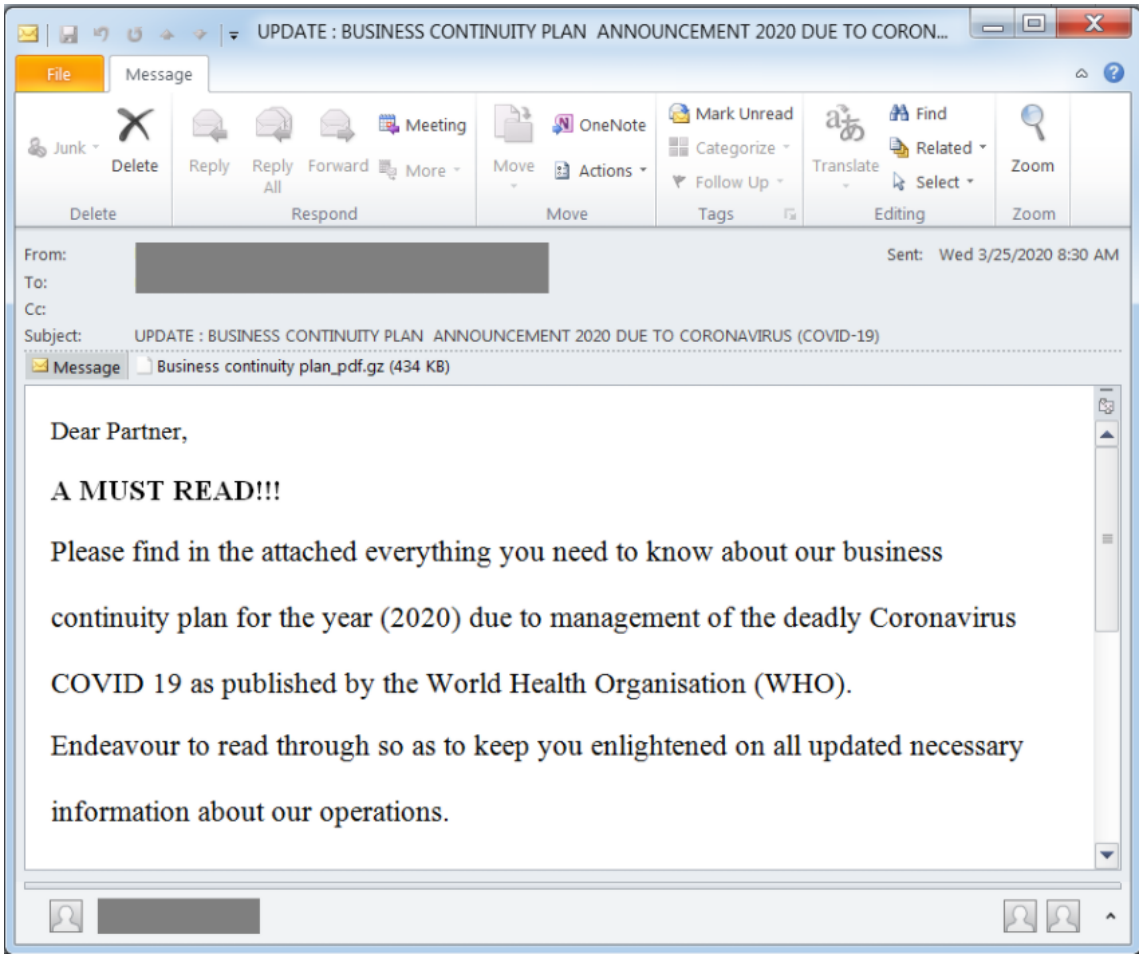
Haittaohjelma on suunniteltu usein tartuttamaan verkkoja ja laitteita sekä vahingoittamaan näitä tai niiden käyttäjiä jollain tavalla. Haittaohjelman aiheuttamat vahingot voivat olla monenlaisia ja ilmetä käyttäjälle eri tavalla. Joissakin tapauksissa haittaohjelman vaikutus on suhteellisen lievä, kun taas joissakin tapauksissa se voi olla tuhoisa. Haittaohjelman tarkoituksesta riippumatta kaiken tyyppiset haittaohjelmat on suunniteltu hyödyntämään laitteita käyttäjän kustannuksella ja haittaohjelman suunnitellun tahon hyödyksi (Rouse 2020).

Haittaohjelmien levittämiseen käytetään niin fyysisiä kuin virtuaalisia keinoja. Haitalliset ohjelmat voivat päätyä järjestelmään esimerkiksi USB-aseman, liitetiedostojen tai haitallisten linkkien kautta ilman käyttäjän suostumusta tai tietämystä. Edistyneimmissä haittaohjelmahyökkäyksissä käytetään usein komento -ja hallintapalvelinta, joka antaa kyberrikolliselle mahdollisuuden kommunikoida tartunnan saaneiden järjestelmien kanssa. Näin tunkeutuja voi saada käsiinsä arkaluontoisia tietoja ja jopa hallita etäkäytön avulla olevaa laitetta tai palvelinta (Rouse 2020).

2.3 Tietojenkalastelu

Tietojenkalastelu on yksi kyberrikollisuuden muotoja. Tietojenkalasteluhyökkäykset ovat väärennettyjä viestejä, jotka näyttävät tulevan luotettavasta lähteestä. Tarkoituksena on huijata uhria luovuttamaan luottamuksellista tietoa rikollisille. Viestit usein sisältävät myös haitallisia liitteitä ja linkkejä, joilla voidaan ladata mahdollinen haittaohjelma käyttäjän tietokoneelle. Käyttäjän virhearvio viestin aitoudesta voi käynnistää tapahtumaketjun, mikä pahimmassa tapauksessa voi vaarantaa koko yrityksen tietoturvallisuuden. Tietojenkalastelijat käyttävät usein hyödyksi vastaanottajan tunteita, kuten pelkoa, uteliaisuutta ja kiirettä. Pyrkimyksenä on saada vastaanottaja avaamaan liitetiedostot tai klikkaamaan haitallisia linkkejä (Cisco, 2020).

Tietojenkalastelijat käyttävät koronaviruksen luomaa poikkeustilannetta hyödyksi ja lähettävät esimerkiksi yrityksen työntekijöille viestejä koskien yritystoiminnan jatkuvuutta (kuvio 1). Viestin liitetiedosto sisältää haittaohjelman, mikä pystyy kaappaamaan käyttäjätunnuksen ja salasanan selaimesta (Pilkey 2020).



Kuvio 1: Kalasteluviesti

2.4 Kiristyshaittaohjelma

Kiristyshaittaohjelmat ovat yksi internetin suurimmista tietoturvaongelmista ja yksi suurimmista tietoverkkorikollisuuden muodoista, joita organisaatiot kohtaavat tänä päivänä. Kiristyshaittaohjelma on haittaohjelman muoto, joka salaa tiedostot ja asiakirjat mistä tahansa yhdestä tietokoneesta aina koko verkkoon, palvelimet mukaan lukien.

Kiristyshaittaohjelman uhreille jätetään usein vain vähän vaihtoehtoja. He voivat joko saada takaisin pääsyn salattuun verkkoonsa maksamalla lunnaita kiristyshaittaohjelman takana oleville rikollisille tai palauttaa varmuuskopioista menetetyt tiedot (Palmer 2020). Alankomaiden poliisin tietotekniikkarikosyksikkö, Europolin verkkorikostorjuntakeskus, Kaspersky ja McAfee on perustanut yhteisen hankkeen salattujen tietojen takaisin saamiseen lunnaita maksamatta. Yleinen suositus on, ettei lunnaita pidä maksaa (Nomoreransom, 2020).

Syyskuun loppupuolella Yhdysvaltojen yhteen suurimmista terveydenhuollon tarjoajista sairaalaketju Universal Health Services (UHS) kohdistui Ryuk-kiristyshaittaohjelma. Kiristyshaittaohjelma lamautti sairaalan it-järjestelmät ja toimintaa jouduttiin jatkamaan ilman tietokoneita. Virallisen lausuntonsa mukaan potilaita pystyttiin kuitenkin hoitamaan eikä potilastietoja tai muuta arkaluonteista dataa ollut vaarantunut (Whittaker 2020). Vastaavia tapauksia on havaittu ympäri maailman.

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) ja Department of Health and Human Services (HHS) laativat yhteisen kyberturvallisuus ohjeistuksen terveydenhuollon suojaamiseksi. Ohjeistuksessa kuvataan tekniikat ja menettelytavat, Kuinka kyberrikolliset tartuttavat järjestelmät erityisesti Ryuk ja Conti kiristyshaittaohjelmien avulla saavuttaakseen taloudellisen hyödyn (Cybersecurity and Infrastructure Security Agency 2020).

2.5 Petokset ja huijaukset

Koronavirukseen liittyvät tuotteet ja huijaukset ovat lisääntyneet verkkomarkkinoilla. Myyjät pyrkivät hyödyntämään julkista pelkoa tarjoamalla tuotteita, jotka väitetään toimivan esimerkiksi virustesteinä tai rokotteina. Palvelun rajoitettu saatavuus saa käyttäjän tekemään hätiköidyn ostopäätöksen. Nämä tuotteet eivät kuitenkaan ole millään tavalla todellisia ja pyrkimyksenä on huijata ostajilta rahaa (The Cyber Threat Impact of COVID-19 to Global Business 2020, 7-8.)

2.6 Disinformaatio

Tietoja koskien koronavirusta tulee internettiin kaikkialta maailmasta, hallitukset mukaan lukien, lehdistöltä, sosiaalisesta mediasta, terveydenhuollon ammattilaisilta sekä verkkorikollisilta. Kuten minkä tahansa kriisin tai sodan nojalla rikolliset ovat löytäneet

tapoja hyödyntää ihmisten tietämättömyyttä koronaviruksen havaitsemisesta, testaamisesta ja hoidosta myymällä erilaisia tuotteita ja palveluita, joiden väitetään auttavan tai parantavan ihmisiä. Sosiaalinen media on täynnä huijauksia, myyttejä ja salaliittoteorioita, siitä mistä virus on alkanut, kuka on syyllinen, miten se leviää väestön keskuudessa ja miten se voidaan havaita (The Cyber Threat Impact of COVID-19 to Global Business 2020, 10.) Internetissä levisi myös haittaohjelman sisältävä koronakartta, mistä näki reaaliaikaisen tilanteen koronavirustartunnan saaneista. ”Corona-Virus-Map” ohjelman ladattua, käyttäjä sai asennettaessa AZORult haittaohjelman tietokoneeseensa (University of Virginia, 2020).

2.7 Etätyöskentely

Etätyöllä tarkoitetaan työtä, mitä tehdään muualla kuin työnantajan toimitiloissa, esimerkiksi kotona tai mökillä. Etätyöstä on yleensä sovittava työnantajan kanssa etukäteen (Tilastokeskus 2020).

Etätyössä käytetään yleensä VPN, eli virtuaalista erillisverkkoyhteyttä. VPN tulee sanoista virtual private network. VPN:n luo turvallisemman ympäristön verkon käytölle (Donald 2020).

Koronaviruksen takia yritykset joutuivat reagoimaan nopeasti uuteen tilanteeseen ja siirtämään työntekijöitä etätöihin, työtehtävien niin salliessa. Eurofoundin teettämän tutkimuksen mukaan Euroopassa jopa 40% kaikista työntekijöistä siirtyi tekemään kokoaikaisesti etätöitä. Suomessa tutkimuksen mukaan noin 30% työntekijöistä on tehnyt kokoaikaisesti etätöitä pandemian aikana (Eurofound 2020, 31-33.)

Etätyön mahdollistava teknologia on ollut olemassa jo pitkään, mutta käyttöönotto on ollut hidasta. Nopea siirtyminen etätöihin ja yritysten niukat resurssit ovat mahdollisesti altistaneet yrityksiä tietoturvauhkille.

Yksi suurin uhka yritysten tietoturvalle on työntekijöiden virheet ja huolimattomuus. Tessianin laatimassa tutkimuksessa kysyttiin 2000 eri alan ammattilaisen tekemistä virheistä töissä Yhdysvalloissa ja Iso-Britanniassa. 57% vastaajista sanoi olevansa hajamielisempiä työskennellessään kotona ja tekevän virheen todennäköisemmin kuin toimistolla. Joka neljäs kyselyyn vastanneista sanoi klikanneensa kalasteluviestin linkkiä urallaan (Tessian 2020).

IBM:n teettämän kyselyn mukaan 76% etätyöntekijöistä on sitä mieltä, että kotona työskentely vie enemmän aikaa tietovuodon havaitsemiseen ja hillitsemiseen (IBM 2020).

Mutune nostaa tietoturvariskeiksi etätyössä muun muassa sen, että kotona käytettävät verkkoyhteydet eivät ole suojattuja samalla tavalla kuin yritysten verkkoyhteydet, ja tämä voi altistaa erilaisille tietoturvauhkille. Etätyöskennellessä myös jaetaan useammin tärkeitä tiedostoja suojaamattoman verkon kautta (Mutune 2020).

3 Tutkimusmenetelmä

Tässä opinnäytetyössä on käytetty laadullista eli kvalitatiivista tutkimusmenetelmää. Laadullisessa tutkimuksessa usein tarkastellaan ilmiötä tutkimuksen kohteena olevien henkilöiden näkökulmasta. Menetelmälle tyypillistä on pyrkimys tuottaa yksityiskohtaista ja monipuolista tietoa tutkitusta ilmiöstä (Puusa & Juuti 2020, Johdanto).

Laadullisen tutkimusmenetelmän lähestymistavaksi valikoitui tapaustutkimus. Tapaustutkimus on usein käytännönläheistä ja siinä hyödynnetään määrällistä sekä laadullista aineistoa ja erilaisia analyysitapoja (Eriksson & Koistinen 2014, 2).

Eriksson ja Koistinen (2014, 22) mukaan keskeisimpiä työvaiheita tapaustutkimuksen tekemisessä on tutkimuskysymysten muotoilu, tutkimusasetelman jäsentäminen, tapausten määrittely sekä valinta ja teoreettisten käsitteiden ja näkökulmien määrittäminen.

Selittävässä tapaustutkimuksessa pyritään selvittämään, miksi tapaus on kehittynyt juuri tietyllä tavalla tai miksi tapaus on juuri sellainen kuin se on. Selittävässä tapaustutkimuksessa painotetaan teorian hyödyllisyyttä, jos sen koetaan auttavan tutkijaa antamaan selityksen havaituille käytännöille (Eriksson & Koistinen 2014, 13).

3.1 Tiedonkeruumenetelmät

Eriksson ja Koistinen (2014, 30) pitävät tyypillisimpinä tiedonkeruumenetelminä haastatteluja, tilastoja, havainnointia, dokumentteja sekä media-aineistoja. Tapaustutkimuksessa aineistoja ja aineistolähteitä käytetään rinnakkain. Laadullisen aineiston ohella voidaan käyttää myös määrällistä aineistoa. Määrälliseen aineistoon luetaan tilastot, survey-aineistot tai aikasarja-aineistot.

Opinnäytetyön tiedonkeruumenetelmänä käytetään haastattelua ja hyödynnetään aineistolähteitä rinnakkain. Haastatteluiden tukena käytettiin lyhyttä kyselylomaketta.

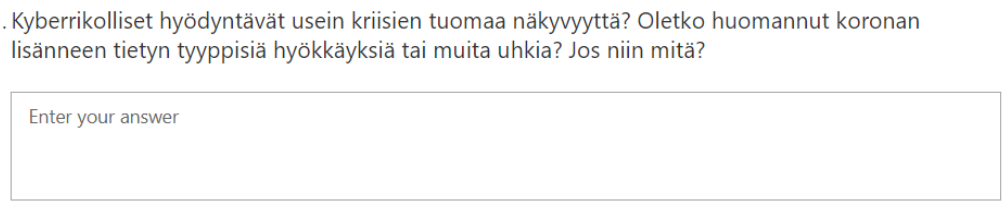
3.2 Analysointimenetelmät

Aineiston analysoimisessa tavoitteena on järjestää aineisto yhtenäiseksi kokonaisuudeksi luokittelemalla tai tyypittelemällä. Aineistosta tehdyille havainnoille annetaan merkitys ja niiden välille pyritään rakentamaan yhteyksiä ja selviä johtopäätöksiä (Eriksson & Koistinen 2014, 33).

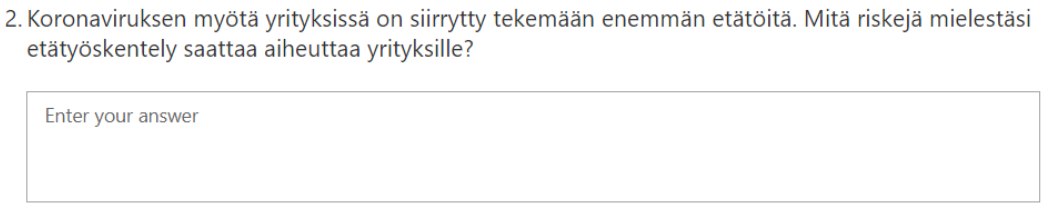
4 Tutkimuksen toteutus

Tutkimusta varten haastateltiin kyberturvallisuusalan ammattilaisia. Haastatteluiden pohjana käytettiin kyselylomaketta. Kyselylomakkeen tarkoitus oli ohjata haastattelua oikeaan suuntaan, mutta muuten haastattelu oli avointa keskustelua. Kyselylomakkeeseen vastasi 9 henkilöä. Haastattelut järjestettiin etänä koronavirustilanteen takia Microsoft Teams viestintäalustan avulla.

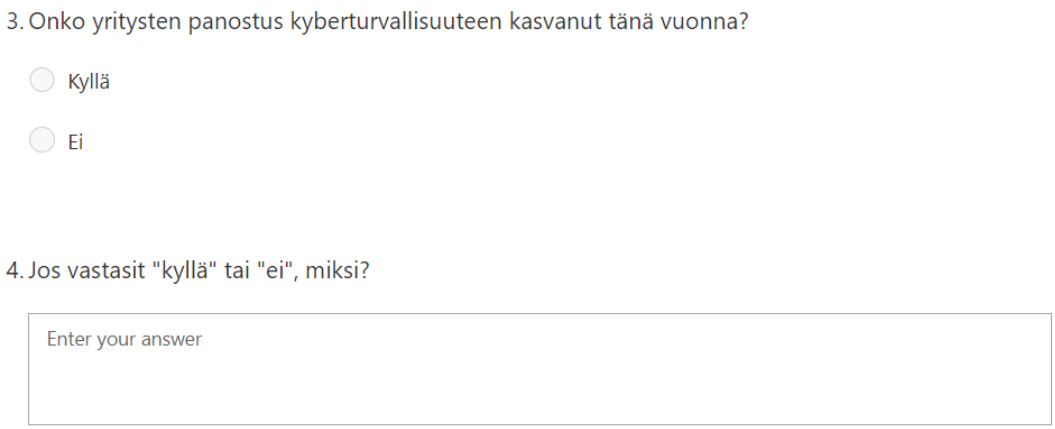
Haastattelu rakentui viidestä kysymyksestä, joista kolme oli avointa kysymystä.



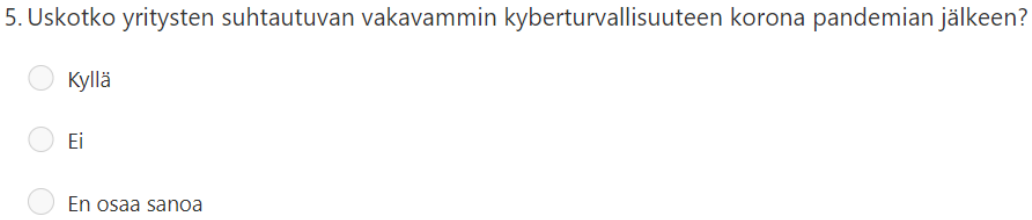
Kuvio 2: Kysymys 1



Kuvio 3: Kysymys 2



Kuvio 4: Kysymys 3 & 4



Kuvio 5: Kysymys 5

5 Tutkimustulokset

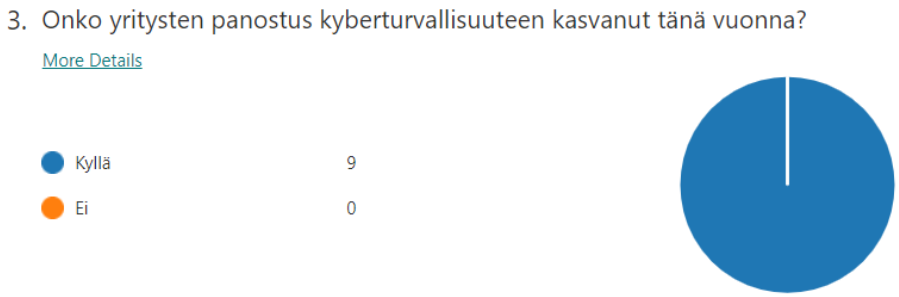
Ensimmäisen kysymyksen tavoitteena oli tarkastella ovatko tutkimukseen vastanneet havainneet tietyn tyyppisten uhkien lisääntyneen pandemian aikana suomalaisissa yrityksissä. 7 vastaajista mainitsi kalasteluviestien lisääntyneen huomattavasti. Neljä vastaajista mainitsi erityisesti korona-aiheisten kalasteluviestien lisääntyneen. Yksi vastanneista mainitsi kiristysohjelmien kasvun osana kyberrikollisuutta.

Toisessa kysymyksessä haluttiin selvittää mitä riskejä etätyöskentely mahdollisesti aiheuttaa yrityksille. Viisi vastanneista nosti yhdeksi suurimmaksi riskiksi yrityksen tietokoneen käytön vapaa-ajalla. Työntekijät saattavat ladata ei työhön liittyviä tiedostoja tietokoneille, mikä voi mahdollistaa jopa haittaohjelmien pääsyn yrityksen verkkoon.

Kolme henkilöä mainitsi VPN-yhteyksien ja kotiverkon turvallisuuden puutteet. Tämä voi esimerkiksi selittyä sillä, että yrityksellä ei ollut resursseja reagoida muuttuneeseen tilanteeseen tarpeeksi nopeasti.

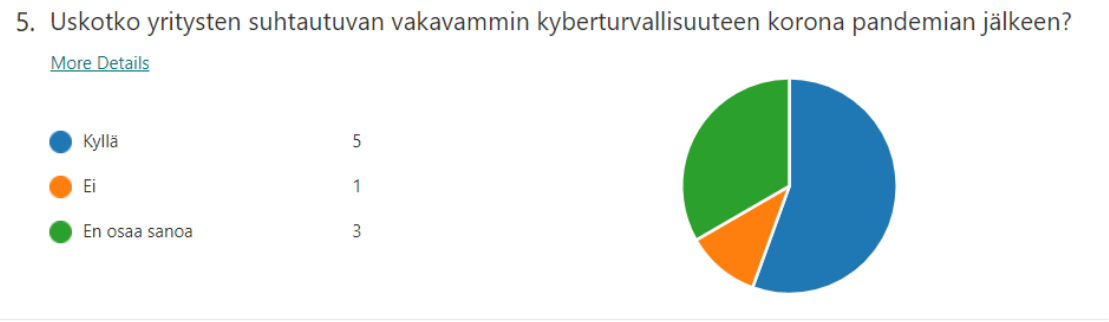
Kaksi henkilöä piti fyysisiä laitevarkauksia todennäköisempinä etätyönteossa kuin toimistolla työskennellessä. Yksi vastanneista mainitsi yksintyöskentelyn lisäävän riskiä sortua kalasteluviestin uhriksi, kun informaation kulku on hitaampaa, eikä uusimmat tiedot tai varoitukset saavuta työntekijöitä saman tien.

Kolmannessa kysymyksessä kysyttiin ovatko tutkimuksessa olleet henkilöt havainneet yritysten lisänneen resursseja kyberturvallisuutta kohti vuonna 2020. Kaikki 9 vastanneista oli sitä mieltä, että yritysten panostus kyberturvallisuutta kohtaan oli lisääntynyt. Neljä henkilöä piti syynä etätyöskentelyyn siirtymistä. Kaksi mainitsi mediassa esillä olleen Vastaamoon liittyvän tietomurron, mikä on herättänyt yrityksissä huolen omasta kyberturvallisuuden tilasta. Kolme vastaajista mainitsi kyberturvallisuuden trendinä ja jatkuvasti olevan kasvussa.



Kuvio 6: 3 kysymyksen jakautuminen

Viimeisessä kysymyksessä selvitettiin mielipiteitä yritysten suhtautumisesta kyberturvallisuuteen pandemian jälkeisenä aikana. Tämä kysymys jakoi mielipiteitä. Viisi vastanneista oli kuitenkin sitä mieltä, että yritykset todennäköisesti tulevat panostamaan kyberturvallisuuteen enemmän tulevaisuudessa. Kolme vastasi ”en osaa sanoa” ja yksi vastanneista ei odottanut yritysten suhtautuvan vakavammin pandemian jälkeen kyberturvallisuuteen.



Kuvio 7: 5 kysymyksen jakautuminen

6 Johtopäätökset

Saatujen vastauksien perusteella voidaan todeta, että kyberrikolliset ovat hyödyntäneet koronaviruksesta johtuvaa tilannetta jonkin verran. Suomessa näkyvyys ei ole ollut niin merkittävää kuin muualla maailmassa.

McAfeen laatiman raportin mukaan Yhdysvalloissa ja Espanjassa on havaittu eniten koronavirukseen liittyviä haitallisia tiedostoja. Näissä maissa on myös todettu hyvin paljon koronavirustartuntoja (McAfee, 2020). Vaikuttaisi siltä, että kyberrikollisuuden näkyvyys on verrannollinen tartuntamääriin tämänhetkisen tiedon perusteella.

Etätyöskentely tulee varmasti lisääntymään tulevaisuudessa, mikä pakottaa yrityksien kohdistamaan lisää resursseja kyberturvallisuuteen. Yksittäisen työntekijän toimet voivat olla suuri riski yrityksen tietoturvallisuudelle ja näin henkilöstöä pitäisi kouluttaa tunnistamaan mahdolliset riskitekijät. Kyberturvallisuuden tulisikin olla pysyvä osa jokaisen yrityksen kulttuuria.

Lähteet

Painetut

Eriksson, P. & Koistinen, K. 2014. Monenlainen tapaustutkimus. Helsinki: Kuluttajatutkimuskeskus

Sähköiset

Chen, J. 2020. COVID-19: Cloud Threat Landscape. Viitattu 1.12.2020. https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/

Cisco 2020. What Is Phishing? Viitattu 25.11.2020. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Cybersecurity and Infrastructure Security Agency. 2020. Alert (AA20-302A). Ransomware Activity Targeting the Healthcare and Public Health Sector. Viitattu 2.12.2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Donald 2020. Cybercrime rates surge during the COVID-19 pandemic. Viitattu 3.12.2020. https://cyberexperts.com/cybercrime-rates-surge-during-the-covid-19-pandemic/

Eurofound 2020. Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg. Viitattu 3.12.2020. https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20059en.pdf

Kaspersky 2020. What is Cybersecurity? Viitattu 25.11.2020. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kumaran, N. & Lugani, S. 2020. Protecting businesses against cyber threats during COVID-19 and beyond. Viitattu 28.11.2020. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

IBM 2020. What is Cybersecurity? Viitattu 25.11.2020. https://www.ibm.com/topics/cybersecurity

IBM 2020. IBM Security Cost of a Data Breach Report 2020. Viitattu 30.11.2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

McAfee 2020. COVID-19 Related Malicious File Detections. Viitattu 3.12.2020. https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html

Mikalauskas, E. 2020. Data suggests unprecedented interest in hacking and cybercrime during pandemic. Viitattu 2.12.2020. https://cybernews.com/security/data-suggests-unprecedented-interest-in-cybercrime-during-pandemic/

Mutune, G. 2020. Work from Home Cyber Risks. Viitattu 2.12.2020. https://cyberexperts.com/work-from-home-cyber-risks%EF%BB%BF/

No More Ransom, 2020. Viitattu 10.12.2020. https://www.nomoreransom.org/fi/about-the-project.html

O'Donoghue,C., Splittgerber, A., Thomas, P. Womersley Smith, H. & Bateman, K. 2020. Coronavirus is now possibly the largest-ever security threat - here's how we may be able to tackle it. Viitattu 28.11.2020. https://www.reedsmith.com/en/perspectives/2020/03/coronavirus-is-now-possibly-the-largest-ever-security-threat

Rouse, M. 2020. Malware. Viitattu 26.11.2020. https://searchsecurity.techtarget.com/definition/malware

Paloaltonetworks 2020. What is Cybersecurity? Viitattu 26.11.2020. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

Puusa, A. & Juuti, P. 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. E-kirja. Gaudeamus.

Pilkey, A. 2020. Coronavirus spam update: watch out for these emails. Viitattu 27.11.2020. https://blog.f-secure.com/coronavirus-spam-update-watch-out-for-these-emails/

Tilastokeskus 2020. Etätyö. Viitattu 3.12.2020. https://www.stat.fi/meta/kas/etatyo.html

Terveyden ja hyvinvoinnin laitos 2020. Koronavirus Covid-19. Viitattu 22.11.2020. https://thl.fi/fi/web/infektiotaudit-ja-rokotukset/taudit-ja-torjunta/taudit-ja-taudinaiheuttajat-a-o/koronavirus-covid-19

Tessian 2020. Psychology of human error. Viitattu 1.12.2020. https://f.hubspotusercontent20.net/hubfs/1670277/%5BTessian%20Research%5D%20The%20Psychology%20of%20Human%20Error.pdf?__hstc=170273983.3ca31fe6a9bd3fbf4df8356b4498939c.1595357368274.1595357368274.1595357368274.1&__hssc=170273983.1.1595357368274&__hsfp=2623516125&hsCtaTracking=f5dae75c-eda9-4caa-9175-b4afb88be295%7Cf0cafcb0-1663-44c9-ab7d-b15cd7cd4423

The Cyber Threat Impact of COVID-19 to Global Business, 2020. Disinformation. Viitattu 27.11.2020. https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf

The Cyber Threat Impact of COVID-19 to Global Business, 2020. Fraud and Hoaxes. Viitattu 27.11.2020. https://wow.intsights.com/rs/071-ZWD-900/images/Cyber%20Threat%20Impact%20of%20Covid19.pdf

University of Virginia, 2020. Fake Coronavirus Map Delivers AZORult malware. Viitattu 10.12.2020. https://security.virginia.edu/fake-coronavirus-map

Palmer, D. 2020. 2,000 coronavirus scammers taken offline in major phishing crackdown. Viitattu 1.12.2020. https://www.zdnet.com/article/2000-coronavirus-scammers-taken-offline-in-major-phishing-crackdown/

Palmer, D. 2020. What is ransomware? Everything you need to know about one of the biggest menaces on the web. Viitattu 1.12.2020. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

Whittaker, Z. 2020. Healthcare giant UHS hit by ransomware attack, sources say. Viitattu 30.11.2020. https://techcrunch.com/2020/09/28/universal-health-services-ransomware/?guccounter=1

Kuviot

Kuvio 1: Kalasteluviesti 9
Kuvio 2: Kysymys 1 13
Kuvio 3: Kysymys 2 13
Kuvio 4: Kysymys 3 & 4 14
Kuvio 5: Kysymys 5 14
Kuvio 6: 3 kysymyksen jakautuminen 15
Kuvio 7: 5 kysymyksen jakautuminen 16