Tampereen yliopisto

Niko Rantala

INFORMAATIOTEKNOLOGIAN AIHEUTTAMAT KYBERTURVALLISUUSRISKIT KULUTTAJALLE

Kandidaatintyö

Tekniikan ja luonnontieteiden tiedekunta
Kandidaatintyö
Joulukuu 2019

TIIVISTELMÄ

Niko Rantala: Informaatioteknologian aiheuttamat kyberturvallisuusriskit kuluttajalle
Kandidaatintyö
Tampereen yliopisto
Tietojohtaminen
Joulukuu 2019

Tämän kandidaatintyön tutkimusongelmana oli selventää, millaisia riskejä ja väärinkäyttöä informaatioteknologia aiheuttaa kuluttajien kyberturvallisuudelle, miksi näin tehdään ja miten väärinkäyttöä voisi torjua. Tarkoituksena oli saada vastaukset kyseisen ongelman lisäksi siihen, mitä ovat yleisimmät riskityypit, kuinka merkittäviä uhat ovat ja kuinka juuri kuluttaja selviytyy kyseisistä riskeistä. Kysymyksiä lähdettiin purkamaan osiin ja käsittelemään niitä systemaattisesti yhdistäen lopulta vastaukset tiiviimmäksi yhteenvedoksi ja tarkastelemalla nykytilaa sekä tulevaisuudennäkymiä.

Kandidaatintyön tutkimusmenetelmänä toimii kirjallisuustutkimus. Se toteutetaan etsimällä järjestelmällisesti tietoa eri tietokannoista ja yhdistelemällä sekä analysoimalla näitä oman tekstin tukemiseksi. Tutkimusaineistoa etsitään eri tietokantojen sisältöä tutkimalla. Työssä hyödynnettäviä tietokantoja ovat muun muassa Andor, Emerald, Proquest, Scopus sekä Web of Science. Tutkimuksen keskeisinä käsitteinä toimivat informaatioteknologia, sen väärinkäyttö, eli toisin sanoen tietoturvariskit painottuen kuluttajiin kohdistuviin riskeihin, kyberturvallisuus sekä kuluttaja. Lisäksi työtä tukevana teoriana on tietojohtaminen, joka liittyy vahvasti tietoturvaan ja sitä kautta teknologiaan, tarjoten sisempiä teorioita ja malleja tiedonhallintaan ja työn kokoamiseen.

Tutkimuksen myötä syntyi tietoa muun muassa yleisimmistä kuluttajiin kohdistuvista tietoturvariskeistä, kuten mitä ne ovat, kuinka yleisiä ne ovat ja miten niiltä voi suojautua. Lisäksi syntyi tietoa siitä, millaisia säännöksiä tällä hetkellä kuluttajien suojaksi on olemassa ja miten kuluttajansuojan pitäisi kehittyä tulevaisuudessa. Odotuksena on, että tulosten myötä työn lukija herää itsekin pohtimaan kyseisiä ongelmia ja riskejä omalta kantiltaan, tajuaa oman roolinsa osana kokonaisuutta tietoturvan rakentamisessa ja muuttamaan omia tapojaan informaatioteknologian hyödyntämisen suhteen kyseiset tietoturvariskit paremmin huomioiden, mikäli sille on tarvetta. Nykyisellä laajuudellaan tutkimuksen tieteellinen kontribuutio ei ole kovin merkittävä, sillä se ei varsinaisesti luo uutta tietoa, mutta se sitoo ja yhdistää aiempia tutkimuksia yhteen tiiviimmäksi ja helppolukuisemmaksi paketiksi, jollaista toista täysin vastaavaa ei tietokantoja tutkittaessa tullut vastaan.

ALKUSANAT

Tämä kandidaatintyönä on tehty osana Tampereen yliopiston tietojohtamisen tutkinto-ohjelman kandidaatintutkintoa syyslukukaudella 2019. Haluan kiittää ohjaajaani ja kandidaatintyöni tarkastajaa Miikka Palvalinia, jolta sain suuresti apua ja ymmärrystä työni tekemiseen. Haluan myös kiittää saman pienryhmän opiskelijoita vertaistuesta sekä kaikkia muita, jotka auttoivat minua kandidaatintyön tekemisessä.

Tampereella, 8.12.2019

Niko Rantala

SISÄLLYSLUETTELO

1. JOHDANTO

Tässä luvussa pohjustetaan tutkimusta tutustuttamalla lukija aiheeseen. Ensin kerrotaan tutkimuksen taustasta, minkä jälkeen esitellään tutkimusongelma ja -kysymykset sekä keskeiset käsitteet. Lopuksi käydään läpi työn rakenne.

1.1 Tutkimuksen taustat ja merkitys

Tämän kandidaatintyön ensimmäisenä aiheena oli teknologian käytön pimeä puoli, jota päätin sen laajuuden vuoksi hieman rajoittaa käsittelemään informaatioteknologian väärinkäyttöä taloudellisen hyödyn tavoittelemiseksi. Aihe oli sellaisenaankin vielä aivan liian laaja, joten päätin aiheanalyysin jälkeen rajoittaa sitä lisää kattamaan vain kuluttajiin kohdistuvat riskit. Päätin myös pudottaa erikseen mainittavan taloudellisen aspektin pois, sillä lähes kaikkien väärinkäytösten taustalla on taloudellinen motiivi. Rajausvaihtoehtoja oli muitakin, mutta uskoin pääseväni kyseisellä rajauksella itseäni tyydyttävään lopputulokseen.

Opiskelen sivuaineena tietoliikennetekniikkaa, johon olen valinnut laajasti mukaan tietoturvallisuuteen liittyviä kursseja ja koen tämän aiheen tukevan hyvin näitä opintoja sekä näiden opintojen tukevan vastavuoroisesti tätä työtä. Opintoihini kuuluu laajasti myös teollisuustalouden opintoja, joiden uskon olevan vastaavalla tavalla hyödyksi. Lisäksi aihe on muutenkin mielestäni varsin mielenkiintoinen ja koen, että sitä on erittäin hyödyllistä tutkia tietoturvan kehittymisen vuoksi, jotta riskejä voitaisiin tunnistaa paremmin ja näin estää taloudellisia tappioita.

Informaatioteknologian mahdollistamat riskit saattavat johtaa suurinkiin taloudellisiin tappioihin, mikäli riskeihin ei ole varauduttu kunnolla. Esimerkiksi viime vuonna kaikista tietomurroista syntyi arviolta jopa 45 miljardin euron lasku, joista suurin osa kohdistui luonnollisesti yrityksiin, mutta myös kuluttajat kärsivät ankarasti. Lisäksi vielä hälyttävämpää oli samassa tutkimuksessa ilmennyt seikka, että jopa 95 % kyseisistä tietomurroista olisi ollut estettävissä. (Internet Society 2018)

Juuri kuluttajiin kohdistuvia riskejä ei ole tutkittu läheskään niin paljon, kuin yrityksiin kohdistuvia riskejä, joten koen tämän tutkimuksen olevan tärkeä niin oman, kuin muidenkin kuluttajien tietoturvan parantamisen suhteen. Aiheesta on kuitenkin jonkin verran tehty tutkimusta, varsinkin kuluttajille suunniteltujen tietoturvaohjelmistojen kehittäjien puolesta, joten en onneksi aivan alusta joudu tutkimusta aloittamaan. Työn tarkoituksena onkin enemmän sitoa aiempia tutkimuksia yhteen tiiviimmäksi ja helppolukuisemmaksi

paketiksi. Lisäksi aihe kiinnostaa itseäni suuresti niin tietoteknisen kuin taloudellisenkin puolen osalta, joka osaltaan vaikutti myös aiheen valintaan.

1.2 Tutkimusongelma ja rajaukset

Työssä tehtävän tutkimuksen tarkoituksena on selventää, millaisia riskejä ja väärinkäyttöä informaatioteknologia aiheuttaa kuluttajien kyberturvallisuudelle, miksi näin tehdään ja miten väärinkäyttöä voisi torjua. Tutkimuskohteet määräytyvät aiheen sekä omien rajausteni perusteella.

Tutkimusongelma oli alkuun aivan liian laaja, joten päätin ensin rajata sitä kattamaan kaikkien teknologian aiheuttamien riskien sijaan vain informaatioteknologian aiheuttamiin riskeihin. Tämäkin osoittautui vielä liian laajaksi aiheeksi, joten päätin aiheanalyysin jälkeen rajata aihetta lisää kattamaan vain kuluttajiin kohdistuvat riskit kyberturvallisuuden toimintaympäristössä. Tutkimusongelmaksi muodostui siten informaatioteknologian aiheuttamat kyberturvallisuusriskit kuluttajalle.

Päätutkimuskysymyksenä on:

- Millaisia riskejä informaatioteknologia aiheuttaa kuluttajien kyberturvallisuudelle ja miten niitä voi torjua?

Alakysymyksiä ovat:

- Mitä ovat yleisimmät riskityypit, kuinka merkittäviä uhat ovat ja kuinka juuri kuluttaja selviytyy kyseisistä riskeistä?

Muita tutkimukseen liittyviä kysymyksiä ovat muun muassa, millainen tilanne on nyt sekä, millaiset tulevaisuudennäkymät sillä on.

1.3 Keskeiset käsitteet ja teoriatausta

Tutkimuksen keskeisinä käsitteinä toimivat informaatioteknologia, sen väärinkäyttö, eli toisin sanoen tietoturvariskit painottuen kuluttajiin kohdistuviin riskeihin, kyberturvallisuus sekä kuluttaja. Lisäksi työtä tukevana teoriana on tietojohtaminen, joka liittyy vahvasti tietoturvaan ja sitä kautta teknologiaan, tarjoten sisempiä teorioita ja malleja tiedonhallintaan ja työn kokoamiseen.

Informaatioteknologia on varsin laaja-alainen termi, jota voidaan kuvata muun muassa näin: ”Insinöörityön osa-alue, johon kuuluu tietokonepohjaiset laitteisto- ja ohjelmistojärjestelmät ja kommunikaatiojärjestelmät, joilla mahdollistetaan tiedon hankinta, esitys, varastointi, välitys ja käyttö” (Sage 2019).

Informaatioteknologiaa voidaan väärinkäyttää muun muassa jonkin tasoiseen hyökkäykseen It-resursseja vastaan, jonka tavoitteena on yleensä taloudellinen hyöty tai vain naiiviudesta johtuvaan tietoturvariskiin esimerkiksi arveluttavan sähköpostin liitettä avatessa (Tarafdar et al. 2015).

Kyberturvallisuus tarkoittaa niin ihmisten kuin datankin suojaamista liittyen digitaalisessa muodossa olevan datan käsittelyyn ja sen päätarkoitus on estää luvaton pääsy tähän dataan (Jenab & Moslehpour 2016).

Kuluttajansuojalain mukaan kuluttaja on luonnollinen henkilö, joka hankkii kulutushyödykkeen pääasiassa muuhun tarkoitukseen kuin harjoittamaansa elinkeinotoimintaa varten (Finlex 2019).

Tietojohtamista voidaan kuvata monella eri tapaa. Johtamisen kenttään se tarjoaa käsitteitä ja malleja, joiden avulla voidaan kuvata ja ymmärtää tiedon eri muotoja sekä tiedon roolia osana organisaation toimintaa. Se tarjoaa myös johtamisen malleja, joiden avulla tietoa voidaan hallita. Lisäksi tietojohtaminen tuo teknistä järjestelmäosaamista tietojohtamisen käytännön toteutukseen. (Laihonen et al. 2013)

1.4 Työn rakenne

Tutkimus etenee suoraviivaisesti aiheen taustasta ongelmien ja kysymysten sekä pääkäsitteiden määrittelyn kautta itse tutkimukseen. Aluksi kerrotaan myös, miten aihetta aiotaan tutkia ja mitä näkökulmia tarkastellaan. Sisällys alkaa johdantokappaleella, jossa avataan tutkimusongelmaa ja motiiveja sen tutkimiseen. Johdannon jälkeen avataan tutkimuksen toteutusta kertomalla tutkimusmenetelmistä ja esittelemällä aineisto. Tämän jälkeen pureudutaan alatutkimuskysymyksiin ja pohditaan ensin niitä tarkemmin ennen päätutkimuskysymykseen siirtymistä. Näin nidotaan kysymykset yhteen päätutkimuskysymystä käsitellessä pohjustuksena päätelmille sekä lopputuloksille. Lopussa ovat päätelmät sekä tulosten esittely. Aivan tutkimuksen lopuksi tulevat siinä hyödynnetyt lähteet.

2. TUTKIMUKSEN TOTEUTTAMINEN

Tässä luvussa kerrotaan yleisesti tutkimuksen toteutuksesta. Ensin avataan tutkimusmenetelmää ja sen jälkeen siirrytään tutkimusaineiston esittelyyn.

2.1 Tutkimusmenetelmä

Kandidaatintyön tutkimusmenetelmänä toimii kirjallisuustutkimus. Se toteutetaan etsimällä järjestelmällisesti tietoa eri tietokannoista ja yhdistelemällä sekä analysoimalla näitä oman tekstin tukemiseksi. Apuna tässä toimii kirjaston järjestämä tiedonhakukoulutus ja lisäksi järjestelmällisen kirjallisuuskatsauksen tukena käytetään Finkin mallia (Fink 2005, Salminen 2011 mukaan), joka koostuu seitsemästä kohdasta:

1. Tutkimuskysymyksen asettelu
2. Bibliografian tietokantojen ja www-sivujen valinta
3. Hakutermien valinta
4. Käytännön seulan asettaminen
5. Metodologisen seulan asettaminen
6. Katsauksen suorittaminen
7. Synteesin tekeminen tuloksista.

Tutkimusaineistoa etsitään eri tietokantojen sisältöä tutkimalla. Työssä hyödynnettäviä tietokantoja ovat muun muassa Andor, Emerald, Proquest, Scopus sekä Web of Science. Jotta voi löytää haluamaansa aineistoa, pitää hakua ensin rajata. Rajaaminen toimii helpoimmin erottelemalla tutkimuskysymyksestään peruskäsitteet ja jakamalla nämä käsitteet vielä alakäsitteisiin. Näitä käsitteitä yhdistelemällä Boolen operaattoreilla saadaan esiin enemmän ja vähemmän osuvampia tuloksia, joita voidaan jatkojalostaa muuttamalla käsitteitä sekä operaattoreita, joko rajaavammiksi tai sallivammiksi. Hakutuloksia voidaan rajata lisäksi myös esimerkiksi julkaisuvuoden ja -formaatin perusteella.

Taulukossa 1 on listattuna tutkimuksen päätutkimuskysymys sekä siitä johdettavat käsitteet ja alakäsitteet, joita hyödynnetään aineiston haussa. Käsitteitä etsitään niin englanniksi kuin suomeksikin haun kattavuuden takaamiseksi ja käsitteitä voidaan myös hieman muotoilla uusiksi.

Taulukko 1: *Haettavat käsitteet*

Päätutkimuskysymys	Mitä ovat informaatioteknologian aiheuttamat kyberturvallisuusriskit kuluttajalle?		
Tärkeimmät käsitteet	informaatioteknologia	tietoturvariski	kuluttaja
Alakäsitteet	teknologia	tietoturva	ihminen
	tietojärjestelmä	riski	hyödyke
	tietotekniikka	rikos	tietotaito
	ohjelma	raha	riskinotto

Tutkimusaineistoa löytyy niin fyysisesti kirjastoista kirjojen ja lehtien muodossa, kuin digitaalisesti tallennettuna artikkeleina, tutkimuksina, konferenssijulkaisuina ja e-kirjoina. Aineisto valitaan sen sopivuuden mukaan sekä sen luotettavuuden ja ajankohtaisuuden perusteella. Apuna tässä toimivat muun muassa vertaisarviot sekä siteerausten määrä.

Tärkeimmillä käsitteillä löytyy seuraavanlaisesti tuloksia aiemmin mainituista tietokannoista hakemalla mahdollisimman laajasti ilman mitään lisärajauksia, kuten julkaisuajankohta, taulukossa 2:

Taulukko 2: *Pääkäsitteiden tietokantahaku*

Hakusana	**Andor**	**Emerald**	**Proquest**	**Scopus**	**Web of Science**
”information technology”	10 995 615	yli 161 000	5 058 437	198 866	102 704
”cybersecurity risk”	47 720	445	9 699	240	98
consumer	62 461 404	yli 95 000	24 653 125	422 402	544 014

Kuten taulukosta 2 voi nähdä, yksittäisiä käsitteitä hakemalla tuloksia syntyy aivan liikaa, joten Boolen operaattoreiden käyttö on lähes ehdotonta tulosten rajaamiseksi. Sopivia hakulausekkeita ovat muun muassa:

- ”information technology” AND (cybersecurity OR ”cyber security”) AND risk AND consumer
- (cybersecurity OR ”cyber security”) AND risk AND consumer
- ”information technology” AND consumer AND risk
- information OR cyber AND consumer AND risk
- information AND security AND consumer

Lisäksi hakua rajataan kattamaan vain viisi viime vuotta, koska tietotekniikan saralla kyseinen aika on jo varsin pitkä. Osa vastaantulevista vanhemmistakin lähteistä saattaa silti olla vielä käyttökelpoisia. Tutkimuksessa pyritään myös käyttämään enimmäkseen vertaisarvioituja ja runsaasti siteerattuja lähteitä mahdollisuuksien mukaan lähteiden luotettavuuden takaamiseksi.

Suorittamalla uusi haku hyödyntäen aiemmin mainittuja hakulausekkeita ja asettamalla julkaisuvuosiksi viimeiset viisi vuotta saadaan seuraavanlaisia tuloksia taulukossa 3:

Taulukko 3: *Muutaman hakulausekkeen tietokantahaku*

Hakulauseke	Andor	Emerald	Proquest	Scopus	Web of Science
”information technology” AND (cybersecurity OR ”cyber security”) AND risk AND consumer	31 735	726	35 224	6	3
(cybersecurity OR ”cyber security”) AND risk AND consumer	136 510	778	90 354	57	82
”information technology” AND consumer AND risk	303 209	yli 15 000	220 872	142	439

Hakulausekkeita hyödyntämällä saatiin selvästi tarkempia tuloksia, joka näkyy hyvin taulukossa 3 hakutulosten vähentyneenä määränä. Näin hakutulosten joukosta on jo selvästi tehokkaampaa valita tutkimukselle olennaiset lähteet. On myös suotavaa tehdä vielä lisärajauksia muun muassa lukuoikeuksien suhteen, sillä osa nyt löydetyistä materiaaleista saattoi olla maksullisia tai muuten tavoittamattomissa. Scopuksen ja Web of Sciencen kohdalla on kuitenkin syytä muuttaa hakukriteereitä laajemmiksi, sillä alle 10 tulosta on aivan liian vähän.

2.2 Tutkimusaineisto

Tutkimusta varten löytyi useita relevantilta vaikuttavia lähteitä, joista muutama toimii kattavampana lähteenä, eli niitä on mahdollista hyödyntää useampaankin otteeseen ja näiden lisäksi useita muita, ei välttämättä niin olennaisia lähteitä, mutta jotka kuitenkin tukevat tutkimusta ja toivottavasti auttavat luomaan keskustelua lähteiden välille tuomalla esille eri mielipiteitä ja kantoja. Ohessa esiteltynä muutama tutkimuksessa hyödynnettävistä lähteistä:

Miedema (2018) kuvaa artikkelissaan *Engaging Consumers in Cyber Security* kuluttajien tietoturvan sääntelyn nykytilaa sekä kuinka kuluttajat saataisiin kiinnostumaan enemmän tietoturvasta. Lopputuloksena oli, että olemme juuri käännekohdassa, jossa selviää kuinka kyseiset säännökset oikeasti toimivat jatkuvan eksponentiaalisen digitaalisen kehityksen myötä. (Miedema 2018b)

Tarafdar et al. (2015) kertovat artikkelissaan *The Dark Side of Information Technology* Informaatioteknologian pimeästä puolesta kuvaten sen haittavaikutuksia työntekijöille ja työnantajille. Artikkelin tutkimusten yhteenvetona oli, että kyseisiä haittavaikutuksia kyetään torjumaan parhaiten ylimmän johdon, IT-päälliköiden sekä HR-päälliköiden holistisella ja integroidulla lähestymistavalla. (Tarafdar et al. 2015)

Jenab & Moslehpour (2016) avaavat julkaisussaan *Cyber Security Management* laajasti useita eri tietoturvaan liittyviä aiheita ja riskejä. Julkaisusta löytyykin lähes kaikki merkittävimmät teemat, kuten palvelunestohyökkäykset, virukset sekä vakoiluohjelmat. (Jenab & Moslehpour 2016)

Miedema (2018) kertoo hänen toisessa tässä työssä hyödynnettävässä julkaisussaan *Consumer Protection in Cyber Space and the Ethics of Stewardship* kuinka eri säädökset ja lait suojaavat kuluttajia kyberavaruudessa. Tutkimuksen tuloksena syntyi ajatus siitä, että kuluttajien pitäisi ajatella olevan ikään kuin internetin kanssahoitajia tai isännöitsijöitä (co-steward). (Miedema 2018a)

Salahdine, & Kaabouch (2019) antavat laajan katsauksen työssään *Social Engineering Attacks: A Survey* kuinka käyttäjän manipulointia (social engineering) väärinkäytetään hyökkäyksiin henkilökohtaista dataa vastaan sekä kuinka suojautua siltä. Lopputuloksena oli, että näiltä hyökkäyksiltä on hankalaa suojautua ilman riittäviä vastatoimenpiteitä, joten tietoturvan koulutus nousee hyvin tärkeäksi. (Salahdine, & Kaabouch 2019)

Aineistoa analysoidaan tutkimalla sen sisällöstä ensin tiivistelmän, otsikoiden ja yhteenvedon perusteella materiaalin sopivuus omiin tarpeisiin ja sitten, joko sisällysluettelon tai selaimen hakutoiminnon avulla etsien tarkemmin tutkimukseen soveltuvan sisällön.

3. INFORMAATIOTEKNOLOGIA JA SEN AIHEUTTAMAT RISKIT KYBERTURVALLISUUDEN SUHTEEN

Tässä luvussa käsitellään informaatioteknologiaa määritellen se ensin käsitteenä ja sitten syventymällä sen aiheuttamiin merkittävimpiin riskeihin kyberturvallisuuden suhteen.

3.1 Informaatioteknologia

Informaatioteknologia on varsin laaja-alainen termi, jota voidaan kuvata hieman eri tavoin riippuen ajankuvasta sekä katsontakannasta. V.A. Izvozchikov (1991) määrittelee informaatioteknologian koneen teknologiana (tietokoneen käyttönä) prosessoidessa, siirtäessä ja jakaessa informaatiota sekä tietojenkäsittelyn luonnissa ja ohjelmistotyökalujen informatiikassa (Izvozchikov 1991, Odintsova 2013 mukaan). I.V. Robert (2008) käsittää informaatioteknologian kokoelmana tarkoituksia ja keinoja informaation keräämiseksi, tallettamiseksi sekä prosessoimiseksi (Robert 2008, Odintsova 2013 mukaan). Uusi luokiteltu viitesanakirja tarjoaa seuraavan määritelmän: Informaatioteknologia on kokoelma keinoja, tekniikoita ja työkaluja informaation tallettamisen, prosessoinnin, siirtämisen ja näyttämisen tarjoamiseksi tarkoituksena työvoiman tehokkuuden ja tuottavuuden lisääntyminen (Voroyskiy F.S. Informatika 2001, Odintsova 2013 mukaan).

3.2 Kyberturvallisuus

Kyberturvallisuus tarkoittaa niin ihmisten kuin datankin suojaamista liittyen digitaalisessa muodossa olevan datan käsittelyyn ja sen päätarkoitus on estää luvaton pääsy tähän dataan (Jenab & Moslehpour 2016). Kyberturvallisuus kehittyy jatkuvasti digitalisaation myötä ja uudenlaisia riskejä ilmenee koko ajan. Tässä työssä kyberturvallisuutta tarkastellaan kuluttajiin kohdistuvien riskien kannalta.

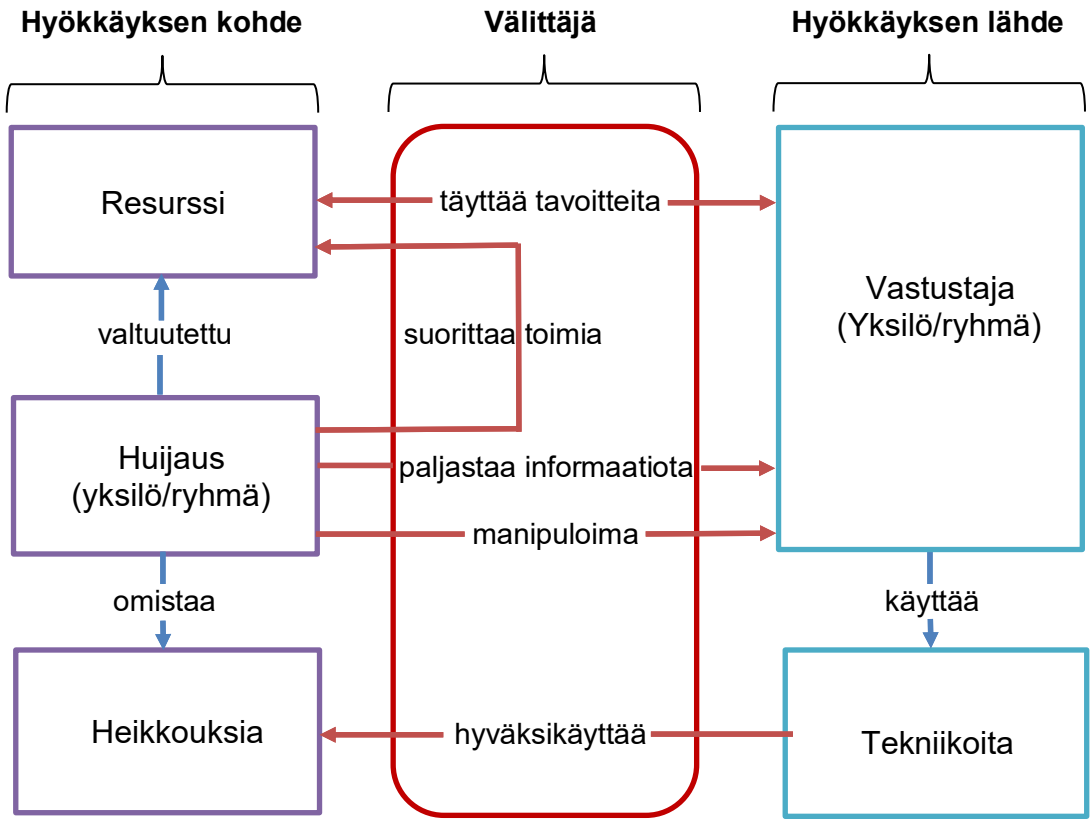
3.3 Merkittävimpiä riskejä

Salahdine & Kaabouch (2019) hyödyntävät ”käyttäjän manipulointi” (social engineering) termiä kuvatessaan ihmisten vuorovaikutuksella tapahtuvia kyberturvallisuusriskejä. Heidän mukaansa käyttäjän manipuloinnin hyökkäykset ovatkin juuri kaikkein suurimpia uhkia kyberturvallisuudelle. (Salahdine & Kaabouch 2019) Kyseiset uhat voidaan tunnistaa, mutta ei pysäyttää (Libicki 2018, Salahdine & Kaabouch 2019 mukaan). Käyttäjien manipuloijat hyväksikäyttävät uhrejaan hankkimalla arkaluontoista informaatiota heistä,

joita he hyödyntävät joko itse johonkin tiettyyn tarkoitukseen tai myyvät sen eteenpäin mustassa pörssissä anonyymejä verkostoja hyödyntäen (Salahdine & Kaabouch 2019).

Kuvassa 1 on luotu yleiskuva sosiaalisen manipuloinnin elementeistä sekä sen kulusta kuvaamalla hyökkäyksen kohteen ja sen lähteen välisiä vuorovaikutuksia.

Kuva 1: *Yleiskuva sosiaalisen manipuloinnin elementeistä ja kulusta (Fan et al. 2017)*

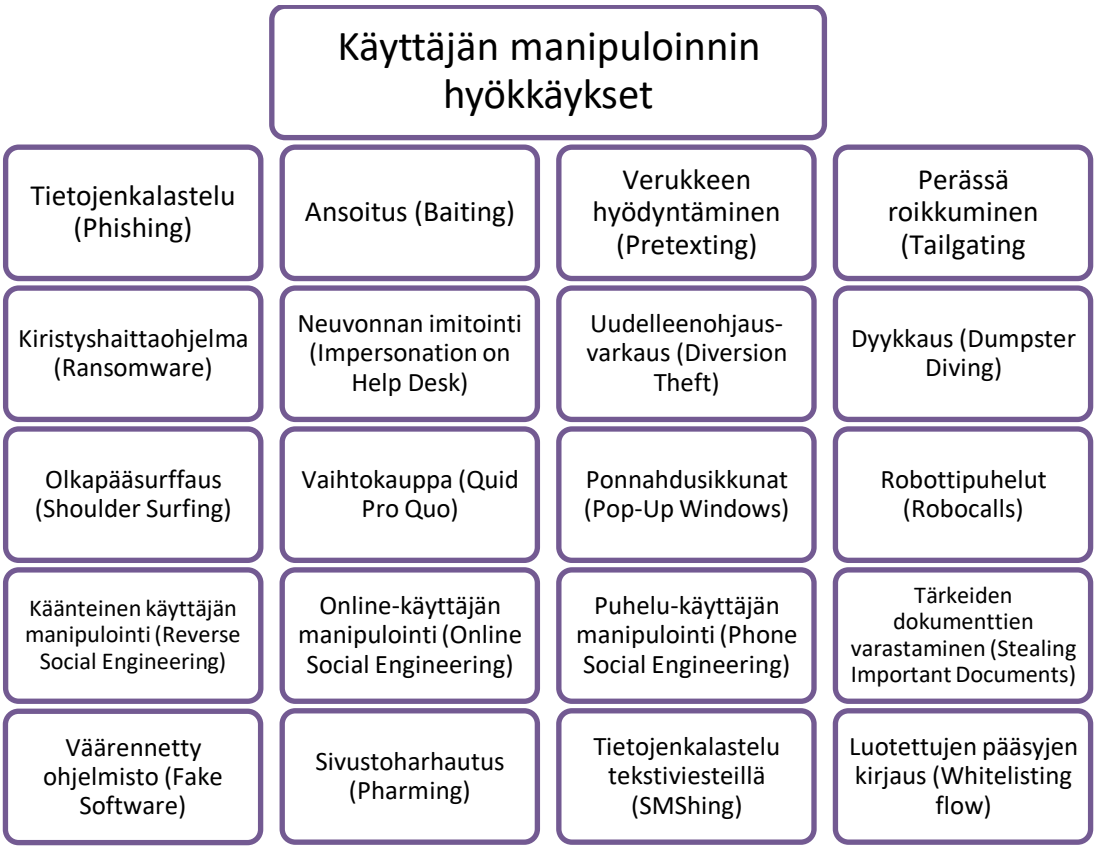


Sosiaalisen manipuloinnin hyökkäykset voidaan jakaa kahteen kategoriaan: ihmisperusteisiin ja tietokoneperusteisiin. Ihmisperusteisissä hyökkäyksissä hyökkääjä kohdistaa hyökkäyksen suoraan tiettyyn kohteeseen haluamansa informaation keräämiseksi ja voi siten vaikuttaa vain rajalliseen määrään uhreja. Tietokoneperusteisissa hyökkäyksissä hyödynnetään yleensä ohjelmistoja ja niillä voidaan hyökätä sekunneissa useiden eri laitteita käyttävien uhrien kimppuun. Hyökkäykset voivat kuitenkin yhdistellä myös eri aspekteja kummastakin kategoriasta. (Salahdine & Kaabouch 2019)

Salahdine & Kaabouch (2019) ovat jakaneet yleisimmät hyökkäystyypit luokkiin niiden ominaisuuksien perusteella sen mukaan, ovatko ne ihmis- vai tietokoneperusteisia, sekä onko hyökkäystapana sosiaalinen, tekninen vai fyysinen hyökkäys (Salahdine & Kaabouch 2019). Kyseiset hyökkäystyypit luokiteltuina ylhäältä alaspäin ovat nähtävissä kuvassa 2. Käsitteet ovat karkeasti suomennettuina, sillä virallisia käännöksiä löytyy vain

yleisimmille termeille ja niiden osalta on hyödynnetty Kyberturvallisuuden sanastoa (Turvallisuuskomitea, 2018).

Kuva 2: *Käyttäjän manipuloinnin hyökkäystyypit (Salahdine & Kaabouch 2019)*



Tarkastellaan seuraavaksi tarkemmin joitain yleisimpiä hyökkäyksiä, joista ensimmäisenä kaikkein yleisin, eli tietojenkalastelu (phishing) (Gupta et al. 2016, Salahdine & Kaabouch 2019 mukaan). Ne tähtäävät vilpillisesti hankkimaan yksityistä ja luottamuksellista tietoa tarkoituksellisilta kohteilta useimmiten puhelun tai sähköpostin välityksellä. Uhreja johdetaan luovuttamaan arkaluontoisia tietoja väärennettyjen internetsivujen, sähköpostien, tarjousten, palkintojen, maksulinkkien ja mainosten sekä muiden mahdollisten portaalien kautta. Näiden kautta saatetaan kysyä muun muassa maksu- tai osoitetietoja, joita voidaan myöhemmin väärinkäyttää uhrin kustannuksella. (Salahdine & Kaabouch 2019)

Verukkeen hyödyntäminen (Pretexting) koostuu väärennettyjen ja uskottavien skenaarioiden luomiselle tarkoituksena varastaa uhrin henkilökohtaista informaatiota. Ne perustuvat verukkeisiin, joilla uhri saadaan uskomaan ja luottamaan hyökkääjään. (Ghafir 2016, Salahdine & Kaabouch 2019 mukaan). Hyökkäys toteutetaan puhelun, sähköpos-

tin tai fyysisen median välityksellä. Hyökkääjät hyödyntävät julkisia informaatioita verukkeissaan ja saattavat tarjota jotain palvelua tai pyytää apua johonkin kysyen samalla henkilökohtaisia tietoja uhriltaan (Salahdine & Kaabouch 2019).

Ansoitushyökkäykset ovat tietojenkalasteluhyökkäyksiä, joissa käyttäjiä pyydetään klikkaamaan jotain linkkiä saadakseen ilmaista tavaraa. Ne toimivat kuin Troijan hevoset siten, että hyökkäys toteutetaan hyväksikäyttämällä suojaamattomia materiaaleja kuten USB-tikkuja, jotka sisältävät haittaohjelmaa, ja jotka jätetään esimerkiksi kahvilaan sopivan uhrin löydettäväksi. Kun hyväuskoinen uhri asettaa tikun koneeseensa, se alkaa toimia kuin tosielämän Troijan hevonen ja suorittaa kaikenlaisia haitallisia toimia taustalla uhrin huomaamatta. (Salahdine & Kaabouch 2019)

Perässä roikkuminen (Tailgating), kutsutaan myös nimellä ”reppuselkäily” (Piggybacking) tai fyysinen pääsy, tarkoittaa pääsyä jollekin rajoitetulle alueelle tai kohteeseen seuraamalla jotakin henkilöä, jolla on kulkuoikeus kyseiseen paikkaan. Näin hyökkääjät pääsevät käsiksi heille muuten luvattomiin kohteisiin. Hyökkääjä saattaa esimerkiksi pyytää uhria avaamaan oven hänelle sanomalla unohtaneensa kulkukortin ja täten päästä luvatta sisälle rakennukseen. Toisessa esimerkissä hyökkääjä voi pyytää puhelinta tai tietokonetta lainaan jotain pientä asiaa varten, mutta sen sijaan tehdäkin haittaa uhrille esimerkiksi asentamalla jonkin haittaohjelman. (Xiangyu et al. 2017, Salahdine & Kaabouch 2019 mukaan)

Kiristyshaittaohjelma (Ransomware) rajoittaa ja/tai estää pääsyn uhrin dataan ja tiedostoihin salaamalla ne. Jotta uhri saisi tiedostonsa takaisin, hänen pitää maksaa lunnaat tai kyseiset tiedot lähtevät leviämään tai ne katoavat kokonaan. Kyseinen maksu pitää yleensä suorittaa Bitcoineilla, joka on säätelemätön digitaalinen valuutta, jota on hankala jäljittää. (Kim et al. 2017, Segovia et al. 2017, Salahdine & Kaabouch 2019 mukaan). Kiristyksen jälkiseuraukset saattavat tulla kalliimmiksi kuin itse lunnasvaatimus (Wang et al. 2018, Salahdine & Kaabouch 2019 mukaan), joten kyseiset hyökkäykset ovat varsin tehokkaita varsinkin yrityksiä kohtaan, joilla on useampia merkittäviä liikesalaisuuksia tai yksityishenkilöitä kohtaan, joilla on jotain muita salaisuuksia tai arkaluontoisia tietoja hallussaan.

4. KULUTTAJA INFORMAATIOTEKNOLOGIAN KÄYTTÄJÄNÄ KYBERTOIMINTAYMPÄRISTÖSSÄ

Tässä luvussa käsitellään kuluttajaa informaatioteknologian käyttäjänä määritellen ensin mitä kuluttaja tarkoittaa ja sitten siirtymällä uhkien yleisyyden kautta siihen, kuinka kuluttajaa suojataan sekä kuinka kuluttaja voi itse suojautua kyberturvallisuuteen liittyviltä uhilta.

4.1 Kuluttaja

Kuluttajansuojalain mukaan kuluttaja on luonnollinen henkilö, joka hankkii kulutushyödykkeen pääasiassa muuhun tarkoitukseen kuin harjoittamaansa elinkeinotoimintaa varten (Finlex 1978). Ilman kuluttajia ei olisi myöskään palveluntarjoajia ja siten kuluttajat ovat elintärkeässä roolissa kaupankäynnissä sekä jakeluketjussa.

4.2 Uhkien ja niiltä suojautumisen yleisyys

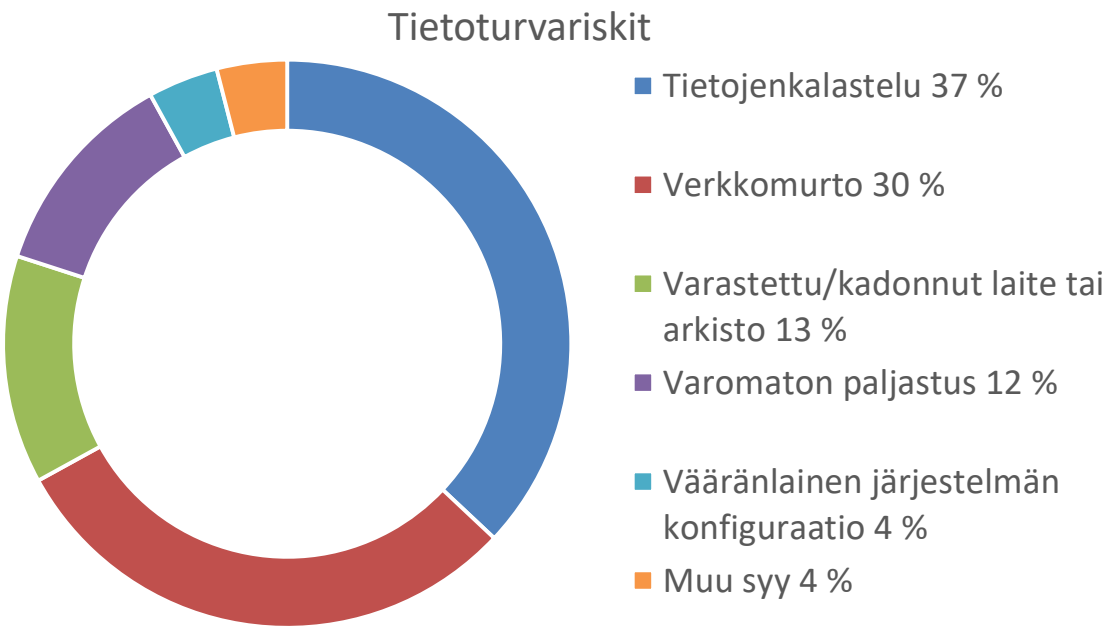
Arvioiden mukaan vuonna 2017 jopa viisi miljardia arkistoa joutui paljastetuiksi eri murtojen seurauksena. Murtojen määrä väheni 3,2 % edellisestä vuodesta, joka on varsin positiivista, mutta hälyttävintä on se, että jopa 95 % näistä murroista olisi ollut estettävissä oikeanlaisella tietoturvastrategialla. (ISOC 2018, RBS 2018, Internet Society 2018 mukaan). Suurimman osan kyseisistä luvuista muodostavat yritykset ja muut organisaatiot, mutta tietoturvariskit koskevat yhtä lailla myös kuluttajia.

Merkittävin uhka kyberturvallisuudelle on välinpitämättömyys sen suhteen ja riskien arvioiminen liian pieniksi. Tenablen vuonna 2017 teettämän tutkimuksen mukaan 94 % yhdysvaltalaisista oli kuullut uutisia tietomurroista viimeisen vuoden aikana, mutta silti 43 % ei ollut muuttanut mitenkään tapojaan toimia verkossa. Lisäksi vain 12 % ilmoitti henkilökohtaisten tietojensa vuotamisesta, mutta todellisten vuotomäärien valossa luku on paljon tuota suurempi. On siis kyse laajasta tietämättömyydestä ja sen lisäksi myös välinpitämättömyydestä, sillä vaikka suurimmat online-palveluntarjoajat ja tietoturvaekspertit kaikki suosittelevat kaksivaiheista tunnistautumista hyvin vahvasti, vain 25 % kertoi käyttävänsä sitä. Lisäksi vain 56 % kertoi lukinneensa tietokoneensa salasanalla ja vain 45 % puhelimensa PIN-koodilla viimeisen vuoden aikana. Biometriikkaa, eli esimerkiksi sormenjälkitunnistusta kertoi hyödyntävänsä myös vain 19 %. (Jonhson 2017)

Rubican sponsoroiman tutkimuksen mukaan suurimpia riskejä tietoturvan suhteen ottavat miehet sekä nuoret. Samassa tutkimuksessa vertailtiin myös muun muassa tietoturvaohjelmistojen, virtuaalisten erillisverkkojen (VPN), salasanan hallintajärjestelmien, ja varmuuskopioinnin yleisyyttä. Tietoturvaohjelmistoja tietokoneella kertoi hyödyntävänsä 82,4 %, mutta puhelimella tai tabletilla vain 37,1 %. Merkittävimpiä tekijöitä sen käytön valinnassa olivat kokemukset sen hyödyllisyydestä sekä hinta. Salasanan hallintajärjestelmää kertoi hyödyntävänsä tietokoneella vain 33,3 % ja puhelimella tai tabletilla vain 28,7 %. Syinä epäsuosioon olivat mielipiteet sen heikosta tehokkuudesta sekä liian suuresta ajankulutuksesta. Varmuuskopiointia kertoi hyödyntävänsä tietokoneella 45,50 % ja puhelimella tai tabletilla 46,60 %. Lopuista suurin osa koki sen liian työlääksi. VPN-yhteyden hyödyntäminen ei ollut kovin suosittua (18,9 % tietokoneella ja 27,4 % puhelimella tai tabletilla) verrattuna muihin keinoihin johtuen kokemuksista sen hankalasta asettamisesta. (Dupuis et al. 2019)

Kuvassa 3 on graafisesti havainnollistettuna yleisimmät tietoturvariskit vuodelta 2018. Tietojenkalastus on yhä merkittävin riski ja verkkoon murtautuminen seuraa heti perästä aiempien vuosien tapaan. (BakerHostetler, 2019)

Kuva 3: *Yleisimmät tietoturvariskit vuonna 2018 (BakerHostetler, 2019)*



4.3 Oman tietoturvan hallinta

Kokonaisvaltainen tietoturvastrategia vaatii paljon, mutta jo yksinkertaisillakin toimilla voidaan parantaa omaa turvallisuutta merkittävästi. Tietoturvayhtiö Cipher on listannut seuraavat 10 keinoa, miten parantaa omaa henkilökohtaista kyberturvallisuuttaan:

1. Pidä ohjelmistosi päivitettyinä

Yksi tärkeimmistä keinoista vähentää riskiä kiristyshaittaohjelmien suhteen on päivittää vanhentuneet ohjelmistot niin käyttöjärjestelmän, kuin sovellustenkin osalta. Tämä auttaa poistamaan kriittiset haavoittuvuudet, joita hakkerit voisivat muuten hyödyntää. Eli kytke automaattiset päivitykset päälle, varmista, että selaimesi saa automaattisia tietoturvapäivityksiä ja pidä myös selaimesi laajennukset, kuten Java, Flash ja muut päivitettyinä.

2. Käytä virusturvaa ja palomuuria

Virusturvaohjelmistot ovat olleet jo pitkään hallitsevin muoto haittaohjelmia vastaan taistelussa. Ne estävät haittaohjelmien ja muiden haitallisten virusten pääsyn dataasi. Käytä vain luotettujen tarjoajien ohjelmistoja. Palomuuri auttaa seulomaan hakkerit, virukset ja muut haitalliset toimet internetin välityksellä ja päättää, mikä liikenne saa luvan pääsyyn laitteellesi. Windows ja Mac sisältävät kumpikin palomuurin ja myös reitittimelläsi pitäisi olla se sisäänrakennettuna.

3. Käytä vahvoja salasanoja ja salasanojen hallintatyökalua

Salasanat ovat tärkeitä pitämään hakkerit erossa datastasi. Niiden pitäisi National Institute of Standards and Technology's (NIST) vuoden 2017 suositusten mukaan olla vähintään kahdeksan merkkiä pitkiä, sisältää ainakin yksi pieni ja isokirjain, yksi numero ja neljä symbolia, mutta ei seuraavia: &%#@_. Valitse se niin, että muistat sen, älä käytä sitä useampaan paikkaan, resetoi se, jos unohdat sen, vaihda se ainakin kerran vuodessa ja älä kerro sitä tai jätä mitään vihjettä siitä julkisesti nähtäville. Jos haluat helpottaa salasanojen muistamista ja hallintaa, kannattaa alkaa hyödyntämään jotain salasananhallintatyökalua.

4. Käytä kaksi- tai useampi vaiheista tunnistautumista

Kyseinen palvelu lisää turvakerroksia tavalliseen salasanalla tunnistautumiseen verrattuna. Tavallisesti syöttäisit vain käyttäjätunnuksen ja salasanan, mutta kaksivaiheisessa tunnistautumisessa sinua pyydetään syöttämään jokin toinenkin tunnistautumiskeino. Tämä voi olla esimerkiksi toinen salasana tai koodi, joka monesti lähetetään puhelimeesi tai sähköpostiisi, kun olet läpäissyt ensimmäisen tunnistautumisen. NIST:n mukaan tekstiviestin välityksellä lähetettävää koodia ei kuitenkaan pitäisi käyttää, sillä matkapuhelinverkkoja vastaan voidaan hyökätä haittaohjelmalla tai muuten murtautua verkkoon ja näin menettää dataa.

5. Opi tietojenkalastelusta ja ole epäileväinen sähköposteja, puheluita ja mainoslehtisiä kohtaan

Tietojenkalastelussa hyökkääjä yrittää tekeytyä joksikin toiseksi ja tällä tavalla huijata uhria luovuttamaan tietojaan, klikkaamaan haitallista linkkiä tai avaamaan haittaohjelman sisältävän liitteen. Tämä saattaa johtaa kiristyshaittaohjelmalla hyökkäykseen ja 90 % niistä alkaakin tietojenkalastelulla. Eli älä avaa tuntemattomia sähköposteja eikä linkkejä ennenkö tiedät mihin se johtaa, ole muutenkin epäileväinen sähköposteja kohtaan ja tutki sen luotettavuutta esimerkiksi kielioppivirheiden suhteen sekä muista, että haitalliset linkit saattavat tulla myös luotetuilta lähteiltä, mikäli hekin ovat saaneet jonkin haittaohjelman itselleen.

6. Suojele arkaluontoista henkilökohtaista tunnistettavaa informaatiotasi

Kyseinen informaatio on mitä tahansa informaatiota, jota kyberrikollinen voi käyttää identifioimaan tai paikallistamaan yksittäisen henkilön. Informaatiota voi olla esimerkiksi nimi, osoite, puhelinnumero, sosiaaliturvatunnus tai syntymäaika. Itsestään pitäisi verkossa pitää näkyvissä mahdollisimman vähän ja myös pitää huoli yksityisyydenasetuksista siitä, kellä kaikilla on oikeus tarkastella tietojasi. Jokainen vääriin käsiin joutuva informaatio lisää tietomurron riskiä dramaattisesti.

7. Käytä mobiililaitteitasi turvallisesti

Aseta hankala pääsykoodi, ei syntymäaikaa tai pankin PIN-koodia, asenna sovelluksia vain luotetuista lähteistä, pidä laitteesi päivitettynä, vältä henkilökohtaisten tietojen lähettämistä viestien ja sähköpostien välityksellä, käytä hyödyksi puhelimen löytämistoimintoa estääksesi sen katoaminen tai varkaus sekä varmuuskopioi tietosi säännöllisesti.

8. Varmuuskopioi tietosi säännöllisesti

Varmuuskopiointi jätetään usein huomioimatta, mutta kiristys- tai muunlaisen haittaohjelman uhriksi joutuessa usein ainoa tapa palauttaa tiedostonsa on pyyhkiä ensin kaikki tiedot ja sitten palauttaa ne varmuuskopiosta. Varmuuskopioinnissa kannattaa hyödyntää 3-2-1 sääntöä, eli pidä kolmea eri kopiota tiedoistasi kahdella eri mediaformaatilla ja yhtä erikseen pilvipalvelussa.

9. Älä käytä julkista Wi-Fiä

Älä käytä julkista langatonta verkkoa ilman virtuaalista erillisverkkoa (VPN), joka salaa yhteytesi laitteen ja erillisverkon oman serverin välillä ja siten vaikeuttaa huomattavasti kyberrikolliselle tietoihisi käsiksi pääsemistä. Jos et voi hyödyntää sitä, käytä mieluummin operaattorin tarjoamaa dataa turvallisuuden vuoksi.

10. Tarkista tunnuksesi sekä luottotietosi säännöllisesti

On tärkeää turvata tunnuksensa sekä tarkastella luottotietojaan säännöllisesti epäilyttävien muutosten varalta, jotta niihin voi reagoida ajoissa. Hyvä keino luottotietojensa turvaamiseksi on käyttää erillistä PIN-koodia, joka luottotapahtuman yhteydessä niin, että kortilla ei voi tehdä ostosta ilman sitä. (Cipher 2018)

Huomion arvoisin asia kyberturvallisuuden suhteen onkin juuri henkilökohtainen toiminta, sillä suurin osa tietomurroista ja niiden yrityksistä liittyy jollain tavalla inhimillisiin ihmisten tuottamiin virheisiin. Siksi valistus asian suhteen on ensiarvoisen tärkeää. (Cipher 2018).

4.4 Suojaavat säännökset ja lait sekä uusi kehityssuunta

Kuluttajien kasvanut aktiivisuus verkossa on myös lisännyt kuluttajien haavoittuvuutta erilaisille huijauksille, hakkeroinnille sekä haittaohjelmille. Samaan aikaan vastavuoroisesti tietämättömät kuluttajat muodostavat riskin internetille; haittaohjelmat saattavat ottaa hyväuskoisen ja huonosti suojatun kuluttajan tietokoneen haltuunsa. Täten he voivat joutua tiedostamattaan osaksi bottiverkkoa, joka saattaa hyödyntää kyseistä tietokonetta roskapostin lähettämisessä tai palvelunestohyökkäyksessä. Bottiverkko tarkoittaa haittaohjelman kautta haltuun saatujen tietokoneiden verkkoa, jotka seuraavat robotin lailla verkon johtajan toimia ilman, että koneiden käyttäjät itse edes tiedostavat asiaa. Palvelunestohyökkäys toteutuu, kun uhriksi valikoituneen kohteen internetsivu tai -palvelu ylikuormittuu siihen johtavasta useasta lähteestä tapahtuvasta liikenteestä niin, että kyseinen sivu tai palvelu niin sanotusti kaatuu ja muuttuu ei saatavilla olevaksi muille käyttäjille. (Miedema 2018a)

Vaikka tietokoneita on ollut jo vuosikymmeniä, on julkinen internet suhteellisen uusi ilmiö. Koko sen historian ajan hallitukset ja lainsäädännöt ovat kamppailleet pysyäkseen siihen liittyvän teknologisen kehityksen perässä. Tämän seurauksena kuluttajansuojanhallinnot kehittyvät vieläkin ja jotkin sen alaiset toimenpiteet ovat hyvin vaillinaisia. Internetin kontekstiin liittyvät kuluttajansuojan ongelmat voidaan jakaa neljään eri kategoriaan: yksityisyys, esteettömyys, turvallisuus ja omaisuus. Jokaisessa kategoriassa niitä säätelevät viitekehykset keskittyvät suojelemaan kuluttajien kiinnostuksen kohteita, vaikka kyseinen suojelu saattaisi kaivata tuekseen muitakin tärkeitä asioita, kuten verkkopalvelujentarjoajien ja muiden sidosryhmien kiinnostuksen kohteet. Ajatus siitä, että muutkin sidosryhmät, kuten juuri verkkopalvelujentarjoajat tai jopa hallitus, saattaisivat tarvita suojelua kuluttajien haittaohjelmilla saastuneita koneita vastaan ei ole vielä yleinen tai keskeinen piirre kuluttajansuojanhallinnossa. (Miedema 2018a)

Nykyhetkellä tyypillinen kuluttajansuojanhallinto on luonteeltaan vertikaalista niin, että hallituksella on ylin vastuu valvomaan ja asettamaan toimenpiteitä kuluttajien turvaamiseksi ja kuluttajat nähdään pääosin passiivisina vastaanottajina näille toimenpiteille. Infrastruktuuri ja palveluntarjoajat hoitavat valtion ja kuluttajien välimaaston ja hoitavat valtaosan velvollisuuksista kuluttajien kiinnostusten kohteiden suojelemiseksi. Tälle vertikaaliselle mallille voidaan tunnistaa ainakin kolme erilaista lähestymistapaa: toimenpiteitä kuluttajien suojelemiseksi verkossa, toimenpiteitä saada kuluttajat itse osallistumaan näihin toimiin sekä toimenpiteitä saada kuluttajat osaksi tietoyhteiskuntaa. (Miedema 2018a)

Kuluttajansuojanlainsäädäntö on pitkään keskittynyt kieltämään tietynlaisia häikäilemättömiä keinoja ja säätelemään niitä, kuten harhaanjohtava mainostaminen, sääntöjä riitatilanteista, kauppakelpoisuudesta, tuotteiden turvallisuudesta ja suoranaisista vilpeistä. Internetin myötä on tullut uusia uhkia, joista osa on päätynyt kyseisen lainsäädännön piiriin ja osa muun muassa rikoslakiin sekä yksityisyyttä käsittelevään lainsäädäntöön. Yhtenä suurimmista kuluttajien huolista internetaikana onkin juuri yksityisyydensuoja, jota kuluttajansuojahallinnot yrittävät laajoin toimin turvata. (Miedema 2018b). Vuonna 2018 voimaan tullut GDPR (General Data Protection Regulation) toi tähän laajoja muutoksia koko EU:n tasolla asettamalla tarkat säädökset siitä, kuinka liiketoimenharjoittajien pitää suojata ja hallinnoida kuluttajien yksityisiä tietoja oikealla tavalla turvatakseen kuluttajien oikeuksia (Gough 2018).

Vaikka kuluttajiensuojalainsäädäntö kehittyy koko ajan, yllättäen suurin osa valtioista ei ole omassa kyberturvallisuusstrategiassaan ottanut huomioon kuluttajien roolia riittävän laajasti, vaan kyberturvallisuudesta huolehtiminen on jätetty pääasiassa yksityisen sektorin johdettavaksi ja kuluttajien osuus on ollut vain tulla koulutetuiksi oikeista toimintatavoista. Kuluttajille ei ole säädetty mitään juridisia velvollisuuksia haittaohjelmilta ja muilta hyökkäyksiltä suojautumiseen eikä säädöksiä, miten toimia, kun kuluttaja huomaa joutuneensa tämän kaltaisen hyökkäyksen kohteeksi. Useat organisaatiot, kuten Kansainvälinen televiestintäliitto ITU ja Euroopan unionin verkko- ja tietoturvavirasto ENISA ovat kannustaneet valtioita ottamaan tehokkaammin kuluttajien roolin huomioon kyberturvallisuusstrategioissaan ja käsittelemään kuluttajia yhdenvertaisena sidosryhmänä osana sitä. Muutamat valtiot ovatkin tunnistaneet ongelman ja ryhtyneet toimenpiteisiin sen parantamiseksi muun muassa luomalla käsitteen kyberhygieniasta ja kuinka kansalaisten pitäisi toteuttaa sitä. (Miedema 2018b)

Taulukossa 4 on kuvattu sitä, kuinka yleistä julkinen tietoisuus, keskustelu ja median näkyvyys on kyberongelmille. Aihetta tarkastellaan vertaamalla kyseisten tekijöiden vahvuutta niitä hyödyntävien maiden määrään Aasia-Oseania alueella.

Taulukko 4: *Kybertietoisuuden yleisyys ja taso Aasia-Oseania alueen maissa (ASPI 2017, Miedema 2018b mukaan)*

Onko kyberongelmista julkista tietoisuutta, keskustelua ja median näkyvyyttä?	Vähän tai ei yhtään julkista tietoisuutta. Mahdollisuus laajalle valikoimalle koulutuksellisia, sitä pidemmälle ulottuvia sekä kapasiteettia rakentaville toimille kyberongelmien suhteen.	Jotain tietoisuutta kyberongelmista, pääasiassa rajoittunut uuteen mediaan (blogit, sosiaalinen media). Mahdollisuus auttaa kansalaisten ymmärryksen rakentamisessa kyberongelmien suhteen.	Vahva julkinen tietous kyberongelmista uusien ja vanhojen medialähteiden kautta. Kybertietoiset loppukäyttäjät ja laaja digitaalisen median omaksunta tarjoavat vahvoja mahdollisuuksia liiketoimien ja kuluttajien välille.
Maiden lukumäärä Yhteensä: 25	11	7	7

Uuden kehityssuunnan kuluttajansuojassa verkkouhkia vastaan pitäisi ottaa paremmin huomioon kuluttajan rooli myös uhkien aiheuttajana muille sidosryhmille. Täten nykyisen vertikaalisen kuluttajansuojanhallinnon valtion ja kuluttajan välillä suojelijana ja suojeltavana pitäisi tasoittua niin, että kuluttajat ovat suoremmin mukana turvaamassa omat kiinnostuksen kohteensa sekä myös muiden sidosryhmien kiinnostuksenkohteet. Internetin luonteen takia sitä hyödyntävät kuluttajat pitäisi ymmärtää yksittäisten kuluttajien sijasta ikään kuin internetin kanssaisännöitsijöinä ja siten tunnistaa tähän liittyvät vastuut internetin terveyden ja toimivuuden ylläpidosta globaalina lähteenä. (Miedema 2018a)

5. INFORMAATIOTEKNOLOGIAN KYBERTURVALLISUUSRISKIT KULUTTAJAN KANNALTA

Tähän mennessä on käsitelty kuluttajan kyberturvallisuuteen liittyviä riskejä, niiden esiintyvyyttä, miten niiltä voi suojautua sekä mitä säädöksiä tähän liittyy. Tässä luvussa yhdistetään kyseiset kokonaisuudet tiiviimmäksi esitykseksi.

5.1 Nykytila

Tietoturvaan kohdistuvat hyökkäykset ovat vieläkin turhan yleisiä, mutta suurin osa tämän hetkisistä riskeistä on tunnistettu tai tunnistettavissa ja lähes niille kaikille on olemassa jokin vastakeino (Jenab & Moslehpour 2016). Tällä hetkellä yleisimpänä riskinä ovat tietojenkalastelu ja verkkomurrot (BakerHostetler, 2019). Merkittävin tekijä on kuitenkin inhimillinen tekijä (Cipher 2018), joten koulutusta tietoturvan merkityksestä niin itselle kuin sitä kautta koko yhteiskunnalle tarvitaan yhä enemmän, jotta tietoturvasta huolehtimasta ei ylenkatsottaisi ja siksi turhaan altistuttaisi näille riskeille (Miedema 2018a).

Nykyinen lainsäädäntö koskien kuluttajansuojaa kyberturvallisuuden suhteen tulee koko ajan hieman jäljessä, mutta se on ottanut jo monia tärkeitä askelia, kuten GDPR ja kehittyy koko ajan vastaamaan paremmin tietotekniikan kehitystä (Gough 2018, Miedema 2018a). Tällä hetkellä säädäntö on kuitenkin hieman liikaa jakaantunut niin, että valtio valvoo ja ohjaa toimenpiteitä, jotka kuluttajat vain passiivisesti ottavat vastaan. (Miedema 2018b,

5.2 Tulevaisuuden näkymät

Tulevaisuudessa alati lisääntyvän digitalisaation ja tietoteknisen kehityksen myötä uhat lisääntyvät ja muuttavat muotoaan, joka asettaa useita eri haasteita tietoturvan kehittymiselle. Nähtäväksi jää kehittyvätkö vastatoimet yhtä nopeasti kuin uhat ja hyökkäykset sekä onnistutaanko kuluttajia kouluttamalla lisäämään yksilöiden kiinnostusta ja aktiivisuutta tietoturvasta huolehtimiseen.

Lainsäädännön pitää myös ottaa harppauksia pysyäkseen mukana tässä kehityksessä ja sen pitää ottaa vahvemmin myös kuluttaja osaksi tarkasteluun valtion oman kyberturvallisuusstrategian suunnittelussa. Valtiota ja kuluttajaa ei enää pidä käsitellä eri tasoilla olevina suojelijana ja suojeltavana ja vaan ne pitää tuoda lähemmäksi toisiaan ja huomioida myös kuluttajien rooli kyseisten uhkien aiheuttajana sekä levittäjänä valtiolle.

6. PÄÄTELMÄT

Viimeisessä luvussa esitellään ja arvioidaan tutkimuksen tuloksia sekä sen onnistuneisuutta ja merkitystä sekä pohditaan, miten aihetta kannattaa tutkia tulevaisuudessa.

6.1 Tutkimuksen tulokset

Tutkimuksen tavoitteena oli selvittää, millaisia riskejä ja väärinkäyttöä informaatioteknologia aiheuttaa kuluttajien kyberturvallisuudelle ja odotettuina tuloksina oli vastaukset ainakin näihin kysymyksiin.

Tutkimuksen myötä syntyi tietoa muun muassa yleisimmistä kuluttajiin kohdistuvista tietoturvariskeistä, kuten mitä ne ovat, kuinka yleisiä ne ovat ja miten niiltä voi suojautua. Lisäksi syntyi tietoa siitä, millaisia säännöksiä tällä hetkellä kuluttajien suojaksi on olemassa ja miten kuluttajansuojan pitäisi kehittyä tulevaisuudessa.

Odotuksena on, että tulosten myötä työn lukija herää itsekin pohtimaan kyseisiä ongelmia ja riskejä omalta kantiltaan, tajuaa oman roolinsa osana kokonaisuutta tietoturvan rakentamisessa ja muuttamaan omia tapojaan informaatioteknologian hyödyntämisen suhteen kyseiset tietoturvariskit paremmin huomioiden, mikäli sille on tarvetta.

Nykyisellä laajuudellaan tutkimuksen tieteellinen kontribuutio ei ole kovin merkittävä, sillä se ei varsinaisesti luo uutta tietoa, mutta se sitoo ja yhdistää aiempia tutkimuksia yhteen tiiviimmäksi ja helppolukuisemmaksi paketiksi, jollaista toista täysin vastaavaa ei tietokantoja tutkiessani tullut vastaan.

6.2 Tulosten arviointi

Tieteellistä kirjallisuutta juuri kuluttajien tietoturvasta ei tuntunut erityisemmin tietokannoista löytyvän, joten monet lähteet hyödynsivät erinäisten tietoturvapalveluja tarjoavien yritysten teettämiä tutkimuksia. Lisäksi työn alussa varsin hyvältä vaikuttanut lähteiden määrä jäi melko pitkälti sille tasolle, koska käyttökelpoisia lähteitä ei vain yksinkertaisesti löytynyt enempää asettamillani hakukriteereillä ja tämän seurauksena kokonaisuuksien yhdistäminen jäikin pitkälti omille harteilleni eikä lähteiden välille syntynyt toivotunlaista keskustelua.

Ottaen huomioon lähteiden vähäinen määrä, pitää tuloksiin suhtautua varsin kriittisesti. Tutkimuskysymyksiin löydettiin kuitenkin vastaukset ja tutkimuksen tuloksena syntyi tiivis

paketti kuluttajan tietoturvan parantamiseksi, jollaista ei toista täysin samanlaista tullut vastaan, joten tutkimusta voidaan ainakin tältä osin pitää kuitenkin onnistuneena.

6.3 Tarve jatkotutkimukselle

Aiheen tutkimus yleisellä tasolla on hyvin merkityksellistä tietoturvan kehittämisen ja parantamisen kannalta, joten tarvetta jatkotutkimukselle on selvästi. Yritysten ja muiden organisaatioiden tietoturvan hallinnasta on olemassa kohtuullisen hyvin tieteellistä kirjallisuutta, mutta juuri kuluttajiin kohdistuvista tietoturvariskeistä ei tietokannoista tuntunut löytyvän paljon mitään kirjallisuutta, joten varsinkin tämä olisi hyvä rajaus myös jatkotutkimusta ajatellen.

LÄHTEET

BakerHostetler, 2019, 2019 Data Security Incident Response Report, Viitattu 7.12.2019, Saatavissa: https://f.datasrvr.com/fr1/019/33725/2019_BakerHostetler_DSIR_Final.pdf

Cipher, 2018, 10 Personal Cyber Security Tips — #CyberAware, Viitattu: 7.12.2019, Saatavissa: https://cipher.com/blog/10-personal-cyber-security-tips-cyberaware/

Dupuis, M., Geiger, T., Slayton, M. & Dewing, F. 2019, The use and non-use of cybersecurity tools among consumers: Do they want help?, SIGITE 2019 - Proceedings of the 20th Annual Conference on Information Technology Education, pp. 81.

Fan, W., Lwakatare, K. & Rong, R. 2017, Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations, International Journal of Computer Network and Information Security, vol. 9, no. 1, pp. 1.

Finlex, 1978, Kuluttajansuojalaki 20.1.1978/38, Viitattu: 10.11.2019, Saatavissa: https://www.finlex.fi/fi/laki/ajantasa/1978/19780038

Gough, O. 2018, GDPR 2018: What is GDPR? What does GDPR stand for?, Express (Online), London (UK).

Internet Society, 2018, 2018 Cyber Incident & Breach Trends Report, Viitattu: 10.11.2019, Saatavissa: https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/

Jenab, K. & Moslehpour, S. 2016, Cyber Security Management: A Review, Business Management Dynamics, vol. 5, no. 11, pp. 16-39.

Johnson, J. 2017, New Study: Many Consumers Lack Understanding of Basic Cyber Hygiene, Tenable, Viitattu: 7.12.2019, Saatavissa: https://www.tenable.com/blog/new-study-many-consumers-lack-understanding-of-basic-cyber-hygiene

Laihonen, H. & Hannula, M. & Helander, N. & Ilvonen, I. & Jussila, J. & Kukko, M. & Kärkkäinen, H. & Lönnqvist, A. & Myllärniemi, J. & Pekkola, S. & Virtanen, P. & Vuori, V. & Yliniemi, T. 2013, Tietojohtaminen, Tampereen teknillinen yliopisto, Tietojohtamisen tutkimuskeskus Novi, Tampere.

Miedema, T.E. 2018a, Consumer Protection in Cyber Space and the Ethics of Stewardship: Journal of Consumer Policy, Journal of Consumer Policy, vol. 41, no. 1, pp. 55-75.

Miedema, T.E. 2018b, Engaging Consumers in Cyber Security, Journal of Internet Law, vol. 21, no. 8, pp. 3-15.

Odintsova, S.A., Kenesova, N.T. & Sarsekeyeva, Z.E. 2013, Information Technology: Definition, Essence and Content of the Concept, Education and Science Without Borders, vol. 4, no. 7, pp. 107-109.

Sage, Andrew P. 2019, Information Technology, AccessScience, McGraw-Hill Education.

Salahdine, F. & Kaabouch, N. 2019, Social Engineering Attacks: A Survey, Future Internet, vol. 11, no. 4.

Salminen, A. 2011, Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin, Vaasan yliopisto, Vaasa.

Tarafdar, M. & D'Arcy, J. & Turel, O. & Gupta, A. 2015, The Dark Side of Information Technology, MIT Sloan Management Review, vol. 56, no. 2, pp. 61-70.

Turvallisuuskeskus 2018, Kyberturvallisuuden sanasto, Sanastokeskus TSK ry, Helsinki, Viitattu: 6.12.1019, Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf