VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Jesse Koskinen

INHIMILLISET NÄKÖKULMAT KYBERUHKIIN JA TURVALLISUUTEEN

Liiketalous 2024

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Jesse Koskinen
Opinnäytetyön nimi	Inhimilliset näkökulmat kyberuhkiin ja turvallisuuteen.
Vuosi	2024
Kieli	suomi
Sivumäärä	43 + 1 liitettä
Ohjaaja	Päivi Rajala

Opinnäytetyön tarkoituksena on tutkia kyberuhkien ja -turvallisuuden inhimillisiä näkökulmia. Digitaalisten palveluiden ja teknologisten innovaatioiden jatkuva kehitys asettaa tarpeen syventyä kyberuhkien ymmärtämiseen entistä paremmin, erityisesti keskittyen inhimillisiin ulottuvuuksiin.

Toisessa luvussa tarkastellaan inhimillisten tekijän roolia kyberturvallisuudessa, syventyen psykologisiin näkökulmiin, hyökkäysten motivaatioon ja käyttäjän tietoturvakäyttäytymiseen, erityisesti sosiaalisten tekijöiden ja manipulaation näkökulmista.

Kolmannessa luvussa analysoidaan inhimillisten tekijöiden vaikutusta kyberturvallisuuden strategioihin, kiinnittäen huomiota organisaation kulttuuriin ja koulutuksen merkitykseen. Kyberturvallisuustutkimuksen osalta käsitellään verkkoturvallisuuskyselyn suunnittelua ja sen toteutusta. Tutkimus toteutettiin kyselytutkimuksena.

Yhteenvetoluvussa esitetään tutkimuksen päätulokset, erityisesti ikäryhmien ja opintosuuntien välisten vertailujen osalta. Tutkielma päättyy suositukseen jatkotutkimukselle, avaten näkökulmia kyberturvallisuuden inhimillisten ulottuvuuksien laajempaan ymmärrykseen ja strategiseen kehitykseen.

Avainsanat Kyberturvallisuus, Tietotekniikka, Kyberuhka, Inhimilliset tekijät

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology
Business Information Technology

ABSTRACT

Author	Jesse Koskinen
Title	Human Perspectives on Cyber Threats and Security.
Year	2024
Language	Finnish
Pages	43 + 1 Appendices
Name of Supervisor	Päivi Rajala

The objective of this thesis was to investigate the human perspectives of cyber threats and cybersecurity. The continuous development of digital services and technological innovations necessitates a deeper understanding of cyber threats with a particular focus on human dimensions.

In the second chapter, the role of human factors in cybersecurity is examined, delving into psychological aspects, the motivations behind cyber-attacks, as well as user cybersecurity behavior, especially from the perspectives of social factors and manipulation.

The third chapter analyzes the impact of human factors on cybersecurity strategies, emphasizing organizational culture and the significance of education. Regarding cybersecurity research, the design and implementation of a cybersecurity survey are discussed. The research was conducted as a survey study.

The summary chapter presents the main findings of the research, particularly in terms of comparisons between age groups and study directions. The thesis concludes with recommendations for further research, opening perspectives for a broader understanding and strategic development of the human dimensions of cybersecurity.

Keywords Cybersecurity, Cyberthreat, Human Factors

SISÄLLYS

KUVA- JA TAULUKKOLUETTELO

LIITELUETTELO

1 JOHDANTO

Yhteiskuntamme on siirtynyt yhä enemmän digitaaliseen aikakauteen, jossa teknologian rooli on keskeinen kaikilla elämänaloilla. Tämä digitalisaatio on tuonut mukanaan lukuisia mahdollisuuksia, mutta samalla se on synnyttänyt uusia haasteita, erityisesti kyberturvallisuuden näkökulmasta. Kasvava riippuvuutemme tietotekniikasta ja verkkopalveluista on avannut ovia monenlaisille kyberuhille, jotka voivat uhata paitsi yksilöiden ja yritysten tietoturvaa myös koko yhteiskunnan toimintaa.

Tämä opinnäytetyö keskittyy tutkimaan kyberuhkien ja -turvallisuuden inhimillisiä näkökulmia. Aihevalinta perustuu sen tärkeyteen ja laaja-alaiseen merkitykseen nykypäivän yhteiskunnassa. Digitaalisten palveluiden ja teknologisten innovaatioiden jatkuva kehitys on synnyttänyt tarpeen ymmärtää syvemmin ihmisten kokemuksia ja reaktioita kyberuhkiin. Tämän tutkimuksen tavoitteena on lisätä tietoisuutta siitä, miten ihmiset kokevat kyberuhkat, mitkä ovat heidän turvallisuuskäsityksensä ja millaisia vaikutuksia näillä näkökulmilla voi olla kyberturvallisuuden kehittämisessä.

Aiempi tutkimus on jo antanut arvokasta tietoa teknologian ja tietoturvan välisestä suhteesta, mutta inhimillisten näkökulmien osalta on vielä paljon tutkittavaa. Tämä työ pyrkii täyttämään tämän tutkimusaukon tuomalla esiin yksilöiden, organisaatioiden ja yhteiskunnan näkemyksiä, jotta voimme paremmin ymmärtää, miten ihmiset osallistuvat ja reagoivat kyberuhkiin. Tutkimalla näitä inhimillisiä ulottuvuuksia voimme kehittää tehokkaampia ja käyttäjäystävällisempiä kyberturvallisuuden strategioita, jotka vastaavat paremmin yhteiskunnan tarpeisiin ja odotuksiin.

Tämän tutkimuksen keskiössä ovat teknologian jatkuva kehitys ja yhteiskunnan kasvava digitalisaatio, ja niiden vaikutukset kyberturvallisuuteen sekä inhimillisiin ulottuvuuksiin. Miten nämä muutokset konkreettisesti heijastuvat kyberuhkiin ja -turvallisuuteen, sekä millaisia seurauksia niillä voi olla yksilöille, organisaatioille, sekä yhteiskunnalle.

Teknologian nopea eteneminen ja digitalisaation syveneminen ovat muuttaneet merkittävästi yhteiskunnan toimintamalleja ja rakennetta. Kuitenkin näiden muutosten myötä kyberuhkien monimuotoisuus ja vaarallisuus ovat lisääntyneet. Tutkimuksen tavoitteena on ymmärtää, miten teknologian kehitys ja digitalisaatio vaikuttavat käytännössä kyberturvallisuuteen, erityisesti miten ne näkyvät inhimillisissä kokemuksissa, käyttäytymisessä ja turvallisuuskäsityksissä.

Tämä tutkimuskysymys on poikkeuksellisen ajankohtainen, kun otetaan huomioon digitaalisten järjestelmien keskeinen rooli yhteiskunnassa ja niiden kriittinen merkitys niin taloudellisessa kuin yksilöiden päivittäisessä toiminnassa. Ymmärtämällä paremmin, miten teknologian muutokset vaikuttavat kyberturvallisuuteen ja miten ihmiset reagoivat näihin muutoksiin, voidaan kehittää tehokkaampia strategioita kyberuhkien ennaltaehkäisyyn ja hallintaan.

Tutkimus keskittyy erityisesti inhimillisiin ulottuvuuksiin, kuten ihmisten tietoisuuteen kyberuhkista, heidän turvallisuuskäsityksiinsä sekä siihen, miten teknologian muutokset näkyvät käyttäjien käyttäytymisessä ja päätöksenteossa. Tämä rajaus auttaa meitä saamaan syvällisemmän käsityksen siitä, miten yksilöt ja organisaatiot voivat parhaiten sopeutua kyberuhkiin ja turvata digitaalisen ympäristönsä muuttuvissa olosuhteissa.

Tämän opinnäytetyön ensisijaisena tavoitteena on syventää ymmärrystä siitä, miten teknologian jatkuva kehitys ja yhteiskunnan digitalisaatio vaikuttavat

kyberturvallisuuteen, erityisesti keskittyen inhimillisiin ulottuvuuksiin. Tarkoituksena on selvittää, miten nämä tekijät ilmenevät yksilöiden, organisaatioiden ja laajemmin yhteiskunnan turvallisuuskäsityksissä, käyttäytymisessä sekä päätöksenteossa.

Opinnäytetyössä pyritään tarkastelemaan ilmiötä monitahoisesti ja keräämään empiiristä aineistoa, joka tarjoaa syvällisen kuvan siitä, miten teknologinen muutos ja digitalisaatio heijastuvat käytännössä kyberturvallisuuteen liittyviin inhimillisiin kokemuksiin. Tämä tutkimus on empiirinen laadullinen tapaustutkimus, jonka tarkoituksena on auttaa ymmärtämään syvällisemmin kyberuhkia ja käyttäjien toimintaa sekä saada näkemys tutkittavasta ilmiöstä. Tutkimuksen aineistonkeruumenetelmänä on korkeakouluopiskelijoille suunnattu kysely.

Opinnäytetyön näkökulma on käytännönläheinen ja soveltava. Tarkoituksena on tuottaa tietoa, jonka avulla voidaan parantaa kyberturvallisuutta ja vastata muuttuviin haasteisiin digitalisoituvassa yhteiskunnassa. Tutkimus pyrkii tarjoamaan konkreettisia suosituksia ja ratkaisuja niin yksilöille kuin organisaatioillekin siinä, miten ne voivat tehokkaasti suojautua kyberuhkilta ja sopeutua jatkuvasti muuttuvaan digitaaliseen ympäristöön.

Opinnäytetyö vastaa kehittämistarpeeseen, joka liittyy yhteiskunnan kyberuhkiin liittyvään tietoisuuden lisäämiseen ja kyberstrategioiden parantamiseen. Digitaalisten uhkien monimuotoisuus edellyttää uusia näkökulmia ja tehokkaita toimenpiteitä, ja tämä tutkimus pyrkii täyttämään tätä tarvetta tuomalla esiin inhimillisten ulottuvuuksien merkitystä kyberturvallisuudessa.

Johdannossa esitellään tutkimuksen taustaa ja kontekstia, avataan tutkimuskysymys sekä määritellään tutkimuksen tavoitteet. Tarkoituksena on antaa lukijalle selkeä käsitys tutkimuksen aiheesta ja sen merkityksestä. Luvussa 2 keskitytään

yleisesti kyberturvallisuuden käsitteeseen ja käsitellään kyberuhkien määritelmä ja luokittelu, turvallisuuden käsitteet kyberympäristössä sekä inhimilliset tekijät kyberturvallisuudessa. Kolmas luku syventyy kyberuhkiin liittyviin inhimillisiin tekijöihin. Luvussa käsitellään psykologisia näkökulmia, kyberhyökkäysten motivaatiota, käyttäjien tietoturvakäyttäytymistä sosiaalisissa tilanteissa, sosiaalista manipulointia ja huijauksia sekä kyberuhkien yhteiskunnallisia vaikutuksia. Neljäs luku tarkastelee, miten inhimilliset tekijät vaikuttavat kyberturvallisuuden strategioihin. Keskitytään organisaation kulttuuriin ja sen merkitykseen tietoturvan kannalta, koulutuksen ja tietoisuuden rooliin sekä henkilöstön osallistumiseen ja sitoutumiseen kyberturvallisuustyössä. Viides luku esittelee kyberturvallisuustutkimuksen suunnittelun, toteutuksen ja tulokset. Luvussa selitetään verkkoturvallisuuskyselyn suunnitteluprosessi, kyselytutkimuksen toteutus sekä tuodaan esille saadut tutkimustulokset. Viimeisessä luvussa tehdään yhteenveto tutkimuksen päätuloksista. Käsitellään kyselyn tulosten analysointia, tutkimuksen rajoituksia ja annetaan suosituksia mahdollisille jatkotutkimuksille. Luvussa pyritään kiteyttämään tutkimuksen keskeiset löydökset ja niiden merkitys.

2 KYBERTURVALLISUUS

Kappaleessa 2 käsitellään kyberturvallisuutta monipuolisesti. Ensinnäkin tarkastellaan eri kyberuhkien määritelmiä ja niiden luokittelua, mikä auttaa hahmottamaan digitaalisen ympäristön potentiaalisia vaaroja. Toiseksi pureudutaan turvallisuuden käsitteisiin kyberympäristössä, syventäen ymmärrystä siitä, miten perinteiset turvallisuusnäkökulmat soveltuvat digitaaliseen maailmaan. Lopuksi keskitytään inhimillisiin tekijöihin kyberturvallisuudessa, kuten käyttäjien tietoisuuteen, koulutukseen ja käyttäytymiseen, jotka ovat keskeisiä osatekijöitä digitaalisen ympäristön turvallisuuden ylläpitämisessä.

2.1 Kyberuhkien määritelmä ja luokittelu.

Kyberuhkilla tarkoitetaan kaikkia niitä toimintoja, jotka pyrkivät hyödyntämään tietoverkkoja ja tietojärjestelmiä vahingoittamiseen, tietojen varastamiseen tai palveluiden estämiseen. Tällaiset toimet voivat käsittää tietojärjestelmien haavoittuvuuksien hyväksikäyttöä, haittaohjelmien levittämistä, identiteettivarkauksia ja muita elektronisia hyökkäyksiä.

Päätöksenteko kyberturvallisuuden osalta nojaa perustuu olemassa oleviin uhkiin. Limnell, Majewski ja Salminen (2014, s. 111) määrittelevät uhkakuvaston käsitteen seuraavasti: "Uhkakuvasto, eli niiden uhkien kokoelma, joita organisaatiossa torjutaan ja joilta pyritään suojautumaan, voidaan rakentaa teknisistä lähtökohdista. Tämä käsite korostaa organisaation toimia uhkien tunnistamiseksi ja niihin varautumiseksi teknologisten näkökohtien pohjalta.

ENISA (European Network and Information Security Agency) julkaisee vuosittain uhkaraportin, jossa se on listannut jokaisen vuoden suurimmat kyberuhat. ENISA

on eurooppalainen kyberturvallisuusvirasto, joka perustettiin vuonna 2004. Sen tehtävänä on edistää ja parantaa tietoturvaa sekä tietoverkkojen turvallisuutta Euroopan unionissa. ENISA tarjoaa asiantuntija-apua, neuvoja ja tukea jäsenvaltioille sekä yhteistyötä erilaisten sidosryhmien kanssa edistääkseen tehokasta kyberturvallisuutta Euroopassa. Virasto tukee myös EU:n toimielimiä ja organisaatioita kyberuhkiin liittyvissä asioissa.

ENISA:n raportin (2023) mukaan tämän hetken suurimmat kyberuhat ovat:

• DDoS-hyökkäykset ja lunnasohjelmat nousevat korkeimmiksi pääuhkiksi, joita seuraavat sosiaalinen manipulointi, tietoon liittyvät uhat, tiedon manipulointi, toimitusketjuun kohdistuvat uhat ja haittaohjelmat.

Pöyhönen (2022) selittää blogissaan ”DDoS hyökkäykset – Mitä ne ovat, miksi niitä tehdään ja kuinka niiltä voi suojautua? ” termin seuraavasti: DDoS (Distributed Denial of Service) hyökkäyksellä tarkoitetaan verkkohyökkäystä, jolla pyritään estämään verkkosivun käyttö, hyökkäys toteutetaan yleensä niin, että palveluun tai laitteisiin kohdistetaan niin paljon liikennettä, että tämä ruuhkautuu niin se kykene palvelemaan asiakkaitaan.

Lunnasohjelmat ovat haittaohjelmia, joka vaativat uhreiltaan lunnaita salauksen purkamiseksi, kun ne ensin salakirjoittavat heidän tiedostojaan tai järjestelmiään. Tämä synnyttää merkittävän turvallisuusuhkan, sillä uhri menettää pääsyn tietoihinsa, ellei suostu maksamaan hyökkääjälle lunnasvaatimuksia. Tämä uhka johtaa taloudellisiin menetyksiin ja voi lisäksi altistaa organisaation mahdollisille tietovuodoille.

Molemmat hyökkäystyypit ovat vakavia uhkia verkkoturvallisuudelle, ja niitä vastaan tarvitaan tehokkaita suojatoimia ja strategioita.

• Havaittavissa on uhkatoimijoiden ammattimaistumisen kasvu heidän tarjoamissaan "as-a-Service"-ohjelmissa. He käyttävät uusia taktiikoita ja vaihtoehtoisia menetelmiä tunkeutuakseen ympäristöihin, painostaakseen uhreja, kiristääkseen heitä ja kehittääkseen laittomia liiketoimintojaan.

• ETL 2023 tunnisti julkishallinnon kaikkein eniten kohdistetuksi sektoriksi (~19 %), perässään yksittäiset kohteet (~11 %), terveydenhuolto (~8 %), digitaalinen infrastruktuuri (~7%) sekä valmistus, rahoitus ja liikenne. ETL (Extract,Transform,Load) on tietojenkäsittely prosessi, joka koostuu kolmesta vaiheesta, hanki, muunna, sekä lataa. Hankintavaiheessa tiedot kerätään erilaisista lähteistä, esimerkiksi tietokannoista ja sovelluksista. Muuntovaiheessa hankitut tiedot käydään läpi, puhdistetaan, yhdistetään ja muokataan sopivaan muotoon varastointia varten. Lataus vaiheessa tiedot siirretään tietovarastoon, jossa niitä voidaan käyttää analytiikassa tai raportoinnissa.

• Venäjän hyökkäyksessä Ukrainaa vastaan informaation manipulointi on noussut keskeiseksi elementiksi.

• Valtion-nexus-ryhmät säilyttävät jatkuvan kiinnostuksen kaksikäyttötyökaluihin (jotta pysyvät havaitsemattomina) ja tunkeutuvat tunnettuihin ohjelmistopaketteihin troijalaistamalla niitä. Valtion Nexus -ryhmät tarjoavat foorumin eri virastojen ja organisaatioiden väliselle yhteistyölle ja tiedonvaihdolle näillä aloilla, edistäen näin kansallista turvallisuutta ja tehokasta resurssien käyttöä.

Kaksikäyttötyökalut (dual-use tools) viittaavat työkaluihin tai teknologioihin, jotka voivat palvella sekä rauhanomaisia että sotilaallisia tarkoituksia. Näiden työkalujen ominaisuudet voivat olla sellaisia, että niitä voidaan soveltaa laillisesti esimerkiksi teollisuudessa tai tutkimuksessa, mutta ne voivat myös tarjota mahdollisuuden väärinkäyttöön sotilaallisessa tai kyberhyökkäyksissä.

Kaksikäyttötyökalujen säilyttäminen jatkuvan kiinnostuksen kohteena valtion Nexus -ryhmissä viittaa siihen, että nämä ryhmät seuraavat aktiivisesti ja hyödyntävät sellaisia työkaluja, jotka voivat palvella sekä puolustuksellisia että hyökkääviä tarkoituksia. Tämä voi sisältää teknologioita tai ohjelmistoja, jotka voivat olla alun perin suunniteltu toiseen tarkoitukseen mutta voidaan muuntaa troijalaisohjelmien avulla saavuttamaan epärehellisiä tavoitteita, kuten tietojen varastamista tai verkkojen murtamista.

Tämä strategia voi olla osa valtion Nexus -ryhmien pyrkimyksiä pysyä havaitsemattomina ja toteuttaa tiedustelu- tai hyökkäystoimia tunnettujen ohjelmistopakettien sisällä. Näiden ryhmien käyttäessä kaksikäyttötyökaluja voi olla vaikeampaa havaita niiden toimintaa ja reagoida tehokkaasti, mikä lisää niiden kykyä toimia huomaamattomasti ja tehokkaasti edistäen kansallista turvallisuutta omien etujensa mukaisesti.

Kyberrikolliset kohdistavat yhä enemmän pilvi-infrastruktuureja, heillä on geopolitiikkaan liittyviä motiiveja vuonna 2023 ja he ovat lisänneet kiristyshyökkäyksiään, ei vain lunnasohjelman kautta, vaan myös suoraan käyttäjiä vastaan.

• Sosiaalisen manipuloinnin hyökkäykset kasvoivat merkittävästi vuonna 2023, ja tekoäly (AI) ja uudet tekniikat tulivat esiin, mutta kalastelu pysyy edelleen yleisimpänä hyökkäystapana.

ENISA:n (European Network and Information Security Agency) vuotuinen kyberuhkaraportti vuodelta 2023 osoittaa, että DDoS-hyökkäykset ja lunnasohjelmat muodostavat keskeisimmät kyberuhat. Raportti paljastaa myös huomattavaa ammattimaistumista uhkatoimijoiden tarjoamissa "as-a-Service"-ohjelmissa, joissa käytetään uusia taktiikoita ja vaihtoehtoisia menetelmiä ympäristöihin tunkeutumiseksi ja uhrien painostamiseksi. Julkishallinto on tunnistettu pääkohteeksi,

seuraavana yksittäiset kohteet, terveydenhuolto, digitaalinen infrastruktuuri, sekä valmistus, rahoitus ja liikenne. Raportti huomauttaa myös Venäjän hyökkäyksen Ukrainaan keskittyvän informaation manipulointiin ja korostaa valtio-nexus-ryhmien kiinnostusta kaksikäyttötyökaluihin. Pilvi-infrastruktuurit, geopolitiikkaan liittyvät motiivit ja kiristyshyökkäysten lisääntyminen suoraan käyttäjiä vastaan ovat muita raportissa esiin nostettuja trendejä. Sosiaalisen manipuloinnin hyökkäykset kasvoivat vuonna 2023, ja vaikka tekoäly ja uudet tekniikat tulivat esiin, kalastelu säilyi yleisimpänä hyökkäystapana.

2.2 Turvallisuuden käsitteet kyberympäristössä

Turvallisuuden käsitteet, kuten tietoturvallisuus ja kyberturvallisuus, ovat keskeisiä termejä nykyaikaisessa digitalisoituneessa ympäristössä. Järvisen (2018, s. 14) mukaan näitä termejä käytetään usein ristiin, mutta niillä on kuitenkin selkeä ero tavoitteissaan, vaikka molemmat liittyvät datan suojaamiseen ja tietojärjestelmien toiminnan varmistamiseen.

Tietoturvallisuus keskittyy perinteisesti tietojärjestelmien suojaamiseen ja datan eheyden, saatavuuden sekä luottamuksellisuuden varmistamiseen. Tämä käsite liittyy laajemmin tietoturvaan organisaatiossa ja sen pyrkimykseen suojata fyysisiä ja virtuaalisia resursseja, estää tietovuodot sekä varmistaa tietojen oikeellisuus ja luotettavuus. Tietoturvallisuuden fokus on perinteisesti ollut laajempi, sisältäen myös esimerkiksi fyysisen turvallisuuden ja tietosuojan näkökulmat Rousku (2014, s47) määrittelee kirjassaan termin "Tietoturvallisuus" seuraavasti: ”Tietoturvallisuus on laaja käsite. Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja saatavuuden takaamista”.

Kyberturvallisuus puolestaan on käsite, joka on noussut esiin digitalisaation myötä. Se korostaa erityisesti tietoverkkojen ja digitaalisten järjestelmien

suojaamista kyberuhkia vastaan. Kyberturvallisuus keskittyy enemmän teknologiseen puoleen, kuten tietoverkkojen, tietokoneiden ja ohjelmistojen suojaamiseen haittaohjelmilta, tietomurroilta ja muilta kyberhyökkäyksiltä. Kyseessä on siis tarkemmin määritelty osa-alue, joka on osa laajempaa tietoturvallisuuden käsitettä. Conongian ja Mandarinon (2014) mukaan kyberturvallisuus viittaa taitoon turvata tiedon yhteiskunnan olemassaolo ja jatkuvuus kyberavaruudessa. Termi kattaa laaja-alaisesti tiedon, omaisuuden ja kriittisen infrastruktuurin suojelemisen ja turvaamisen digitaalisessa ympäristössä. Kyberturvallisuuden tavoitteena on varmistaa tehokas suojaus ja hallinta kyberuhkien vaikutuksilta sekä ylläpitää kykyä toimia kyberavaruudessa

Vaikka tietoturvallisuus ja kyberturvallisuus liittyvät vahvasti toisiinsa, niiden käytössä on terminologinen ero, joka heijastaa niiden erilaista painotusta. Tietoturvallisuus peittää laajemman kentän, kun taas kyberturvallisuus keskittyy nimenomaan tietotekniikan ja tietoverkkojen turvallisuuteen digitaalisessa ympäristössä.

Kokonaisuutena näiden käsitteiden ymmärtäminen on olennaista organisaatioille, jotka haluavat varmistaa turvallisuutensa nykyaikaisessa digitaalisessa toimintaympäristössä. Molemmissa käsitteissä keskiössä on kuitenkin pyrkimys suojaamiseen ja luottamuksellisuuden varmistamiseen, ja ne muodostavat vahvan perustan kokonaisvaltaiselle turvallisuudelle.

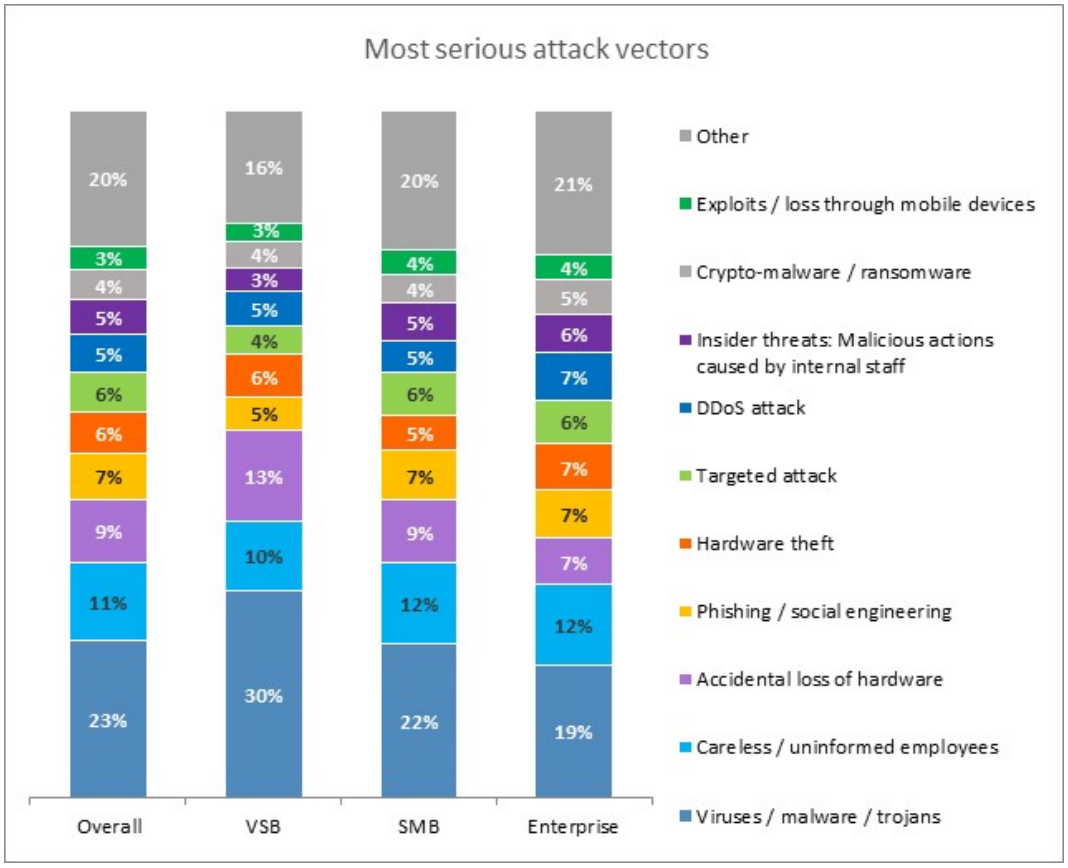
2.3 Inhimilliset tekijät kyberturvallisuudessa

Ray Stantonin analyysin mukaan nykyisin yritysten tietoturvallisuus on äärimmäisen haavoittuvainen, ennennäkemättömällä tasolla. Hänen argumenttinsa

kiteytyy siihen, että jokainen yksilö on joutunut keskelle taistelutantereita, joissa varkaat, hakkeroijat, ja jopa valkohattuhakkerit käyvät jatkuvaa, monimutkaista sotaa. Tämä tilanne on syntynyt modernin digitalisaation myötä, kun elämämme siirtyvät yhä syvemmin verkkoon. Tämä kehitys asettaa meidät alttiiksi jatkuvasti kasvaville turvallisuusriskeille (Kearney, 2016, s. 5).

Ray Stantonin huomio tietoturvallisuuden kasvaneista riskeistä nykyaikaisessa digitaalisessa ympäristössä on merkittävä. Yritysten ja yksilöiden altistuminen varkauksille, hakkereille ja kyberuhille on lisääntynyt digitalisaation myötä. Elämämme siirtyy entistä enemmän verkkoon, mikä luo jatkuvasti kasvavia haasteita tietoturvalle.

Yksilöinä meidän on myös tiedostettava henkilökohtainen vastuumme tietoturvasta. Tietoisuus digitaalisen ympäristön riskeistä ja hyvien turvakäytäntöjen noudattaminen ovat avainasemassa omien tietojemme ja yksityisyytemme suojelemisessa. Stantonin näkemys korostaa, että tietoturvasta on tullut entistä olennaisempi osa päivittäistä elämäämme, ja sen merkitys vain korostuu tulevaisuudessa. Inhimilliset virheet, kuten kalastelusähköpostien linkkien painaminen, heikot salasanat, vahingossa vuodetut datat, jopa linja-autoon unohtuneet yrityksen tietokoneet muodostavat yrityksille suuremman uhan, kuin salaperäisen hakkerijärjestön kyberhyökkäys.



Kuva 1. Vaarallisimmat uhkatekijät: (Kaspersky Lab, 2017).

Kaspersky Labin (2017) järjestämän tutkimukseen tulokset osoittavat, että yrityksillä on todellakin hyvä syy olla huolissaan työntekijöiden osuudesta kyberuhkiin. Henkilöstö saattaa tehdä virheitä, jotka asettavat yrityksen tiedot tai järjestelmät vaaraan - joko huolimattomuudesta ja vahingossa lipsahtaen tai siksi, että heillä ei ole tarvittavaa koulutusta käyttäytyäkseen asianmukaisesti ja suojellakseen työnantajayritystään.

Huolimattomat tai tietämättömät työntekijät ovat esimerkiksi toiseksi todennäköisin vakavan tietoturvaloukkauksen syy, heti haittaohjelmien jälkeen. Lisäksi 46

prosenttia viime vuoden aikana tapahtuneista tietoturvaloukkauksista on johtunut huolimattomista tai tietämättömistä työntekijöistä.

Henkilöstön inhimillinen virhe ei ole ainoa 'hyökkäysvektori', jonka kohteeksi yritykset joutuvat. Hyökkäysvektori on väline, jota käyttämällä pyritään hyökkäämään tietojärjestelmään tai -verkkoon. Nämä vektorit hyödyntävät tietoverkon tai -järjestelmän heikkouksia tai haavoittuvuuksia. Esimerkkejä hyökkäysvektoreista ovat haittaohjelmat, sähköpostin liitetiedostot, verkkosivut ja ponnahdusikkunat, jotka toimivat väylinä hyökkäyksille.

Viimeisen vuoden aikana yrityksen oma henkilökunta on myös aiheuttanut turvallisuusongelmia omilla ilkeillä toimillaan, ja 30% viimeisen 12 kuukauden aikana ilmoitetuista turvatapahtumista liittyy henkilöstön toimiin, jotka ovat suunnattu omia työnantajiaan vastaan.

Kaspersky labin (2017) Tutkimuksen mukaan yritykset, jotka kokivat tietoturvaloukkauksia viimeisen vuoden aikana, ilmoittivat, että kymmenesosa (11%) vakavimmista tapauksista liittyi huolimattomiin työntekijöihin. Tutkimukseen osallistui yli 5000 yritystä ympäri maailmaa.

3 INHIMILLISET TEKIJÄT KYBERUHKIEN TAUSTALLA

3.1 Psykologiset näkökulmat

Kyberuhkien taustalla vaikuttavat monimutkaiset psykologiset tekijät, jotka käsittävät käyttäytymismallit, tietoisuuden ja päätöksenteon. Organisaatioiden tietoturvallisuuteen vaikuttavat merkittävästi työntekijöiden psykologiset ominaisuudet ja toimintatavat.

Käyttäytymismallit ovat keskeinen tekijä, kun arvioidaan tietoturvan riskitekijöitä organisaatioissa. Työntekijöiden tietoisuus kyberuhkista ja tietoturvakäytännöistä vaikuttaa suoraan heidän kykyynsä tunnistaa ja välttää mahdollisia riskejä. Psykologiset tekijät voivat myös vaikuttaa päätöksentekoon, kun työntekijät joutuvat tekemään valintoja tietoturvaan liittyvissä tilanteissa.

3.2 Kyberhyökkäysten motivaatio

Kyberhyökkäyksiä voidaan toteuttaa useista eri syistä. Hyökkäyksien motivaationa voi olla henkilökohtaisen hyödyn tavoittelu, valtion puolesta vakoilu, tai kyberterrorismi.

Taulukko1. Esimerkkejä kyberhyökkäysten motivaatioista Limnell,Majewski & Salminen (2017,s112)

Motivaatio	Toimijat	Kohde
Kybersota	Poliittinen/sotilaallinen	Valtiot
Kyberterrorismi	Pelonlietsonta/poliittiset muutokset	Terroristit
Kybervakoilu	Tiedon varastus	Valtiot, yritykset
Kyberrikollisuus	Taloudellinen hyöty	Rikolliset
Haktivismi	Poliittinen muutos/omien taitojen esittely	Aktivistit, haktivistit, yksilöt

Taulukossa 1 on esitetty esimerkkejä kyberhyökkäysten motivaatioista ja se tarjoaa monipuolisen katsauksen eri hyökkäystyyppeihin ja niiden motiiveihin. Kybersota korostaa poliittisia ja sotilaallisia tarkoitusperiä, joissa valtiot käyvät taistelua kriittisten infrastruktuurien, kuten lentokenttien ja sähkönjakelukeskusten, hallinnasta. Kyberterrorismi keskittyy pelonlietsontaan ja poliittisiin muutoksiin terroristiryhmien toimesta, iskien infrastruktuuriin ja julkisiin kohteisiin. Kybervakoilussa valtiot ja yritykset pyrkivät tiedon varastamiseen, kun taas kyberrikollisuus on taloudellisesti motivoitunutta, suunnattuna yrityksiin ja yksilöihin. Haktivismi yhdistää poliittisen muutoksen tavoittelun ja omien taitojen esittelyn, jossa aktivistit ja haktivistit haastavat hallituksia ja yrityksiä, vaikuttaen yksilöihin laajemmin.

3.3 Käyttäjien tietoturvakäytös

Käyttäjien tietoturvakäytös on olennainen osa organisaation kokonaistietoturvaa. Käsite viittaa siihen, miten organisaation työntekijät ja käyttäjät toimivat ja

suhtautuvat tietoturvaan päivittäisissä toiminnoissaan. Käyttäjillä on merkittävä rooli omassa tietoturvassaan, ja yksinkertaisilla käytännön toimenpiteillä he voivat parantaa niin omaa tietoturvansa kuin samalla myös yrityksen tietoturvaa.

Tietomurrot tai vuodot voivat johtua joko teknisistä tai inhimillisistä virheistä. Teknisten virheiden korjaukset saattavat aiheuttaa merkittäviä kustannuksia, , mutta inhimilliset virheet voivat olla haastavampia korjata. Käyttäjien koulutuksella ja tietoisuuden lisäämisellä voidaan kuitenkin vähentää inhimillisten virheiden riskiä, mikä on elintärkeää organisaation tietoturvan kannalta. Täten panostaminen käyttäjien tietoturvaosaamiseen ja valistukseen on strateginen toimenpide, joka voi vahvistaa organisaation puolustuskykyä tietoturvauhkia vastaan. Hyppönen (2021, s. 102) käsittelee teoksessaan "Internet" erilaisia virheitä, joita käyttäjät tekevät altistuessaan tietoturvauhkille. Nämä virheet on esitetty kirjan sivulla 102, ja ne kattavat laajan kirjon riskialttiita toimintatapoja. Esimerkkejä näistä virheistä ovat muun muassa saman salasanan käyttäminen kaikissa palveluissa, hämärien apuohjelmien ja selainlaajennusten lataaminen verkosta, kaikkien sähköpostin liitetiedostojen avaaminen ilman tarkistamista, sekä Office-tiedoston avaaminen ja sisällön käyttöön ottaminen verkosta saadun ohjeen perusteella. Lisäksi käyttäjät saattavat syöttää vahingossa kirjautumistietonsa huijaussivustoille. Hyppösen esittämät näkökulmat korostavat käyttäjien vastuuta omasta tietoturvastaan ja antavat arvokasta tietoa siitä, miten välttää yleisiä ansoja internetin käytössä.

Kaspersky Lab (2017) on listannut artikkelissaan *”Mitä kyberrikokset ovat? Miten voit suojautua kyberrikoksilta?”* ohjeita, joilla yksityishenkilö voi suojata laitteensa ja henkilötietonsa:

1. Pidä ohjelmistot ja käyttöjärjestelmä päivitettyinä.

2. Käytä virustorjuntaohjelmaa ja pidä se päivitettynä.

3. Käytä vahvoja salasanoja.
4. Älä koskaan avaa roskaposteissa olevia liitteitä.
5. Älä napsauta roskapostiviestien tai epäluotettavien sivustojen linkkejä.
6. Älä anna henkilötietoja, ellei sitä voi tehdä turvallisesti.
7. Ota yhteyttä suoraan yritykseen, jos saat epäilyttäviä pyyntöjä.
8. Ole tarkkana sivustojen URL-osoitteiden suhteen.
9. Seuraa pankin tiliotteita.

Sosiaaliset tekijät kyberturvallisuudessa ovat ihmisten käyttäytymiseen ja vuorovaikutukseen liittyviä elementtejä, jotka voivat vaikuttaa tietoturvaan. Sosiaalinen manipulointi ja huijaukset muodostavat olennaisen osan tietoturvan laajaa spektriä, keskittyen strategisesti ihmisten harhauttamiseen paljastamaan arkaluonteisia tietoja, kuten salasanoja tai henkilökohtaisia tunnistetietoja. Tämä käyttäytymisen muoto on tyypillisesti taktinen ja perustuu psykologisiin vaikuttimiin sekä hienostuneisiin sosiaalisiin tekniikoihin. Keskeisenä tavoitteena on manipuloida yksilöiden kognitiivisia ja emotionaalisia reaktioita, luoden siten otollisen ympäristön tietoturvaan liittyvien uhkien onnistuneelle hyödyntämiselle.

Sosiaalisen manipuloinnin ja huijausten strategiat voivat vaihdella monipuolisesti, käsittäen esimerkiksi kalastelun (phishing), sosiaalisen tekniikan, valepuhelut, huijausviestit ja -puhelut, sosiaalisen median huijaukset sekä identiteettivarkauden. Näitä taktiikoita yhdistää pyrkimys hyödyntää inhimillisiä heikkouksia, kuten uteliaisuutta, hätätilanteessa toimimista tai luottamusta tunnistettuihin tahoihin. Näistä kaikista keinoista yleisin tapa päästä käsiksi organisaation tietoihin on kalastelu (phising).

Kyseisten hyökkäysten tehokkuus perustuu siihen, että ne eivät suoraan hyödynnä tietoturvainfrastruktuurin haavoittuvuuksia, vaan käyttävät hyväkseen inhimillisiä ja sosiaalisia elementtejä, jotka voivat olla vaikeampia tunnistaa ja torjua. Siksi tietoturvastrategiat eivät voi olla pelkästään teknisiä, vaan niiden on myös kohdistuttava käyttäjien kouluttamiseen ja tietoisuuden lisäämiseen, jotta nämä voivat tunnistaa ja vastustaa näitä huijausyrityksiä tehokkaasti.

3.4 Yhteiskunnalliset vaikutukset

Yhteiskunnalliset vaikutukset ovat olennainen osa tietoturvan kokonaiskuvaa, ja niiden laaja-alaisuus ilmenee monipuolisesti eri yhteiskunnan tasoilla. Tietoturvan heikko tila tai onnistunut tietoturvastrategia voi heijastua voimakkaasti niin talouteen, infrastruktuuriin kuin yksilöiden arkeenkin. Morganin (2020) artikkeli "*Cybercrime to Cost the World $10.5 Trillion Annually By 2025*" tarjoaa huomattavaa perspektiiviä kyberrikollisuuden vaikutuksiin, kun hän korostaa, että vuonna 2021 kyberrikollisuuden aiheuttamat taloudelliset menetykset kohosivat noin 6 miljardiin dollariin maailmanlaajuisesti.

Hänen vertauksensa kyberrikollisuuden potentiaalisesta asemasta valtiona, joka sijoittuisi maailman kolmanneksi suurimmaksi taloudelliseksi toimijaksi Yhdysvaltojen ja Kiinan jälkeen, avaa silmiä laajuudelle, jolla kyberrikollisuus voi vaikuttaa kansantalouksiin. Euroopan parlamentin (2021) arvioima 5,5 tuhatta miljardia euroa kyberrikosten aiheuttamista taloudellisista vahingoista vuonna 2020, mikä on kaksinkertainen määrä vuoteen 2015 verrattuna, viittaa siihen, että kyberuhkien kasvu on ilmiö, joka ei tunne kansallisia rajoja.

Tämä havainnollistaa kyberrikollisuuden laajuutta ja sen vaikutusta maailmantalouteen. Kyberrikollisuus ei ole vain tekninen ongelma, vaan sillä on syvällisiä yhteiskunnallisia seurauksia. Se vaikuttaa paitsi yrityksiin ja valtioihin myös tavallisiin kansalaisiin, jotka voivat joutua identiteettivarkauksien uhreiksi tai kärsiä taloudellisesti kyberhyökkäysten seurauksena. Tällainen laajamittainen vaikutus edellyttää kokonaisvaltaista lähestymistapaa, joka yhdistää teknologiset, lainsäädännölliset ja yhteiskunnalliset näkökulmat tietoturvaan. Lisäksi tämä korostaa tarvetta yhteisille kansainvälisille ponnisteluille kyberrikollisuuden torjumiseksi ja tietoturvan vahvistamiseksi maailmanlaajuisesti.

4 INHIMILLISTEN TEKIJÖIDEN VAIKUTUS KYBERTURVALLISUUDEN STRATEGIOIHIN

4.1 Organisaation kulttuuri ja tietoturva

Organisaation kulttuuri ja tietoturva ovat keskeisiä tekijöitä, jotka vaikuttavat siihen, kuinka tehokkaasti tietoturvapolitiikat ja -käytännöt noudatetaan organisaatiossa. Organisaation kulttuuri muodostaa pohjan sille, miten työntekijät suhtautuvat tietoturvaan ja millaisena he näkevät sen merkityksen osana päivittäistä toimintaa.

Organisaation tavoittelema tietoturvataso ja siihen liittyvät näkemykset esitetään yleisesti organisaation tietoturvapolitiikassa. Tämä asiakirja, yhdessä säännöllisesti päivitettävien toimintastrategioiden ja -politiikan kanssa, muodostaa perustan organisaation käytännön tietoturvaohjeiden laatimiselle ja vahvistamiselle. (Andersson & Koivisto, 2013, s. 34). Tietoturvapolitiikan sisältöä käsitellään myös tietoturvaan liittyvissä standardeissa.

Alla esimerkkejä eri standardeista kuvauksineen SFS Suomen Standardit sivustolta.

ISO/IEC 27000 Tietoturvallisuuden standardisarja

Suomen Standardoimisliitto SFS ry (2024) standardi ISO/IEC 27000 on tietoturvallisuuden standardisarja, jolla organisaatiosi suojaa tieto-omaisuuttaan. Tietoturvallisuuden johtamisjärjestelmän rakentamisessa tukena on standardisarja ISO/IEC 27000, joka tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin.

ISO/IEC 27001:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietotuvallisuuden hallintajärjestelmät. Vaatimukset

Suomen Standardoimisliitto SFS ry (2024) on julkaissut standardin "ISO/IEC 27001:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät - Vaatimukset". Tässä keskeisessä tietoturvallisuuden hallintajärjestelmän standardissa määritellään vaatimukset sen luomiselle, toteuttamiselle, ylläpitämiselle ja jatkuvan parantamisen varmistamiselle. Standardi sisältää myös organisaation tarpeisiin räätälöityjä vaatimuksia tietoturvariskien arviointiin ja käsittelyyn. Nämä vaatimukset on muotoiltu yleisluonteisiksi, jotta ne soveltuisivat kaikenkokoisille ja -tyyppisille organisaatioille. Tämä standardi toimii perustana tietoturvallisuuden hallintajärjestelmien kehittämiselle, tavoitteena varmistaa korkea tietoturvan taso organisaation toiminnassa.

SFS-EN ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot.

SFS-EN ISO/IEC 27002:2022 standardi on tarkoitettu käytettäväksi standardiin ISO/IEC 27001 perustuvan tietoturvallisuuden hallintajärjestelmän toteuttamisprosessissa. Se sopii myös ohjeistukseksi yleisesti hyväksyttyjen tietoturvallisuuden hallintakeinojen toteuttamiseen. Suomen Standardoimisliitto SFS ry (2024)

Standardia voidaan hyödyntää toimiala- tai organisaatiokohtaisten tietoturvallisuuden hallintaohjeiden kehittämisessä, sillä siinä otetaan huomioon toimialaa tai organisaatiota koskevat tietoturvallisuuden riskiympäristöt. Suomen Standardoimisliitto SFS ry (2024)

ISO/IEC 27005:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan.

ISO/IEC 27005:2022 standardissa esitetään ohjeita tietoturvariskien hallintaan. Ohjeet soveltuvat kaikentyyppisille organisaatioille. Suomen Standardoimisliitto SFS ry (2024)

4.2 Koulutuksen ja tietoisuuden merkitys

Koulutuksen ja tietoisuuden rooli organisaation tietoturvassa korostuu merkittävänä tekijänä. Näissä konteksteissa koulutus viittaa käyttäjien valistamiseen ja opettamiseen, kun taas tietoisuuden lisääminen käsittää käyttäjien tarkkuuden ja ymmärtämyksen tietoturvallisuuden riskeistä ja parhaista käytännöistä. Näitä panostuksia pidetään keskeisinä tekijöinä organisaation tietoturvan kokonaisvaltaisessa vahvistamisessa.

Koulutuksen avulla käyttäjät voivat oppia tunnistamaan erilaisia tietoturvauhkia, kuten huijausyrityksiä, haittaohjelmia ja sosiaalista manipulointia. Tämä lisää heidän kykyään toimia varovaisesti ja vastuullisesti verkossa. Samalla tietoisuuden lisääminen auttaa käyttäjiä ymmärtämään, kuinka heidän omat toimintansa voivat vaikuttaa organisaation tietoturvatilanteeseen.

Koulutusohjelmat voivat suuntautua painottamaan salasanojen vahvuuden ylläpitämistä, ohjelmistojen säännöllisten päivitysten merkitystä ja muita keskeisiä turvallisuuskäytäntöjä.Ihmisten täytyy tunnistaa kalastelun ja huijausyritysten merkit, jotta he eivät lankeaisi huijausyrityksiin ja välttäisivät riskitilanteet.

Kun organisaatiot siirtyvät yhä enemmän pilvipalvelujen käyttöön, salasanojen merkitys korostuu entisestään. Pirisen (2021) esittämä näkemys korostaa erityisesti kaksivaiheisen tunnistautumisen (MFA) merkitystä. Pilvipalveluihin voi kirjautua mistä tahansa milloin tahansa, mikä lisää riskiä, että hyökkääjä voi käyttää

salasanaa saadakseen pääsyn organisaation arkaluonteisiin tietoihin milloin tahansa. Pirisen mukaan käyttäjille tulisi tarjota koulutusta salasanahygienian perusteista, sillä hänen näkemyksensä mukaan ei ole enää realistista odottaa, että käyttäjät pystyvät muistamaan kaikki vahvat salasanat ulkoa ilman niiden kirjaamista ylös.

Ensinnäkin työntekijöitä tulisi ohjeistaa salasanojen laatuvaatimuksista, jotta he voivat luoda vahvoja ja turvallisia salasanoja. Lisäksi heidän tulisi saada selkeät ohjeet siitä, miten salasanoja tulisi säilyttää, mukaan lukien mahdollisten salasananhallintasovellusten käyttö.

Toiseksi työntekijöille tulee opettaa, miten tunnistaa oikea sivusto, jolla syöttää käyttäjätunnus ja salasana, erityisesti pilvipalveluiden yhteydessä. Tämä auttaa ehkäisemään kalastelu- ja huijausyrityksiä.

Lisäksi työntekijöitä ohjeistetaan siitä, miten toimia, jos he epäilevät oman käyttäjätunnuksensa ja salasanansa mahdollista paljastumista. Tämä osa koulutusta auttaa varmistamaan nopean ja asianmukaisen reagoinnin tietoturvapoikkeamien tapauksessa.

Koulutus voi sisältää ohjeita hätätilanteisiin reagoimiseen ja tietosuojakäytäntöjen noudattamiseen. Tällainen holistinen lähestymistapa luo vahvan pohjan, jonka avulla organisaatio voi parantaa tietoturvakulttuuriaan ja vähentää riskiä tietoturvahyökkäyksille. Holistisella lähestymistavalla tarkoitetaan kyberturvallisuudessa kokonaisvaltaista lähestymistapaa kyberuhkien ja tietoturvan hallintaan, jolloin otetaan huomioon tietotekninen infrastruktuuri, organisaation prosessit ja käytännöt, ihmisten toiminta ja ulkoisten tekijöiden väliset vuorovaikutukset. Tässä mielessä koulutus ja tietoisuuden lisääminen ovat avaintekijöitä organisaation tietoturvan parantamisessa.

5 KYBERTURVALLISUUSTUTKIMUS

5.1 Verkkoturvallisuuskyselyn suunnittelu

Tutkimuksessa tarkastellaan teknologian kehityksen ja digitalisaation käytännön vaikutuksia kyberturvallisuuteen, keskittyen erityisesti inhimillisiin kokemuksiin, käyttäytymiseen ja turvallisuuskäsityksiin. Tämän kyselyn kohderyhmänä toimivat Vaasan ammattikorkeakoulun opiskelijat, ja tämän kontekstin huomioiminen on olennainen osa verkkoturvallisuuskyselyn suunnittelua.

Verkkoturvallisuuskyselyn suunnittelussa on ensisijaisen tärkeää ottaa huomioon opiskelijoiden ainutlaatuiset tarpeet, osaaminen ja kokemukset. Kielen valinnassa tulisi pyrkiä selkeyteen ja ymmärrettävyyteen, välttäen liiallista teknistä terminologiaa, jotta kyselyn sisältö olisi saavutettavissa kaikille opiskelijoille, huolimatta heidän teknologisesta taustastaan.

Kyselyn kohderyhmänä ovat opiskelijat, joiden arjen huomioiminen edellyttää kysymysten kohdentamista käytännön tilanteisiin. Kysymyksissä tarkastellaan miten opiskelijat käyttävät tietotekniikkaa opiskelutilanteissa, sosiaalisessa elämässä ja vapaa-ajallaan. Lisäksi kysely peilaa opiskelijoiden turvallisuuskäsityksiä ja -käytäntöjä.

Kyselyssä arvioidaan myös opiskelijoiden tietämystä verkkoturvallisuudesta, sisällyttäen kysymyksiä esimerkiksi siitä, millaisia turvallisuusratkaisuja he hyödyntävät ja millaisia odotuksia he asettavat teknologian rooliin omassa turvallisuudessaan.

5.1 Kyselytutkimuksen toteutus

Tutkimuksen kyselytutkimus toteutetaan anonyymisti käyttäen Google Forms -kyselylomaketta, ja kohderyhmänä toimivat Vaasan ammattikorkeakoulun opiskelijat. Kyselylinkki lähetetään osallistujien sähköpostiosoitteisiin, ja kysely koostuu 30 kysymyksestä. Anonyymiyden varmistamiseksi vastaajien henkilötietoja ei tallenneta missään vaiheessa, ja osallistujat voivat vastata kysymyksiin täysin nimettömänä.

Kohderyhmän oikeellisuuden varmistamiseksi käytetään Vaasan ammattikorkeakoulun sisäistä sähköpostijärjestelmää, mikä mahdollistaa osallistumisen vain opiskelijoille. Tämä lisää tutkimuksen luotettavuutta ja varmistaa, että kyselyyn vastaavat todella ne henkilöt, joille se on suunnattu.

Google Forms -alusta tarjoaa kätevän ja helpon tavan kerätä vastauksia. Osallistujat voivat vastata kyselyyn missä tahansa, mikä lisää osallistumisen joustavuutta ja tekee tutkimuksesta saavutettavamman opiskelijoille. Tutkimuksen tällainen toteutustapa mahdollistaa tehokkaan datankeruun samalla kun huolehditaan vastaajien yksityisyyden suojasta.

Vastaajilta pyydettiin kyselyssä tietoa kahdesta pääasiallisesta näkökulmasta: ikä ja opintosuunta. Tämä tiedonkeruu mahdollistaa tulosten tarkastelun ikäryhmittäin ja opintosuunnan perusteella, syventäen analyysiä ja tarjoten arvokasta tietoa eri ryhmien välisistä mahdollisista eroista.

Ensinnäkin ikätiedon kysyminen tarjoaa mahdollisuuden tarkastella vastauksia eri ikäryhmissä. Tällainen demografisten tietojen keruu voi tuoda esiin ikään liittyviä trendejä tai eroavaisuuksia esimerkiksi tietoturvakäyttäytymisessä. Ikäryhmittäinen analyysi voi olla hyödyllinen strategisten päätösten ja toimenpiteiden

suunnittelussa, joiden tarkoituksena on vastata eri ikäryhmien mahdollisiin tietoturvahaasteisiin.

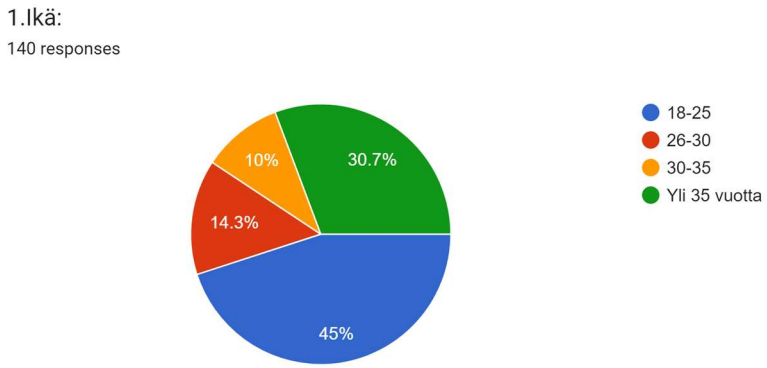
Toiseksi opintosuunnan kysyminen on tärkeää, koska eri opintosuunnilla voi olla erilaisia tarpeita ja haasteita tietoturvaan liittyen. Opiskelijat eri aloilla saattavat olla eri tavoin alttiita erityyppisille tietoturvaongelmille tai olla eri tasoisia tietoturvaosaamisessaan. Tämä tieto voi auttaa kohdentamaan resursseja ja kehittämään opetusohjelmia, jotka vastaavat paremmin opiskelijoiden tarpeita eri opintosuunnilla.

Kyselyn aikarajoituksella (16.2.2024 - 1.3.2024) varmistettiin, että vastaajilta kerättävät tiedot olisivat mahdollisimman ajantasaisia ja vastaisivat tutkimuksen tarkoitusta. Lisäksi aikavälille asetettu rajoitus antaa riittävästi aikaa tulosten kattavalle analysoinnille ja mahdollisille toimenpiteille ennen tulosten julkistamista tai raportointia.

6 KYBERTURVALLISUUSTUTKIMUKSEN TULOKSET JA ANALYYSI

6.1 Kyselytutkimuksen tulokset

Kyberturvallisuuskyselyyn vastasi 140 opiskelijaa, ja vastauksista (Kuva 2.) ilmeni seuraava ikäjakauma: 45 % oli 18–25-vuotiaita, 30.7 % yli 35-vuotiaita, 14.3 % 26–30-vuotiaita ja 10 % 30–35-vuotiaita. Huomionarvoista on yli 35-vuotiaiden vastaajien suuri osuus, mikä yllätti tutkimuksen tekijän odotettua korkeampana. On kuitenkin tärkeää huomauttaa, että otanta kattaa laajan ikäkirjon, mikä antaa monipuolisen kuvan opiskelijoiden näkemyksistä kyberturvallisuudesta eri ikäryhmissä.



Kuva 2. Vastaajien iät.

Kyselyyn vastaajia pyydettiin myös kertomaan opintosuuntansa (kuva 3), jotta eri opintoryhmien väliset vertailut onnistuisivat. Kuvassa 3 näkyy vastaajien prosentuaalinen jakauma opinto suunnittain. Kyselyyn eniten vastanneet osallistujat

olivat tekniikan opiskelijoita. Huomioon ottaen, että tietotekniikan ja tietojenkäsittelyn opintosuunta kuuluu tekniikan alaan, yli puolet vastaajista (52,2 prosenttia) edusti tätä opiskelualaa. Terveys- ja sosiaalialan opiskelijat muodostivat noin viidenneksen vastaajista (22,2 prosenttia), kun taas liiketalouden opiskelijat olivat noin neljännes kaikista vastaajista (25,7 prosenttia).

6.1.1 Ikäryhmien välinen vertailu

Tutkimuksen tavoitteena oli analysoida eri ikäryhmien välisiä eroja liittyen verkkoturvallisuuteen. Alkuperäisenä hypoteesina oli, että nuoremmat opiskelijat kokisivat itsensä itsevarmemmiksi verkossa verrattuna vanhempiin opiskelijoihin, jotka puolestaan saattaisivat kokea itsensä epävarmemmiksi. Oletuksena oli myös, että nuoremmilla olisi parempi salasanojen hallintataito, suurempi luottamus tekoälyyn ja parempi kyky havaita kalasteluyritykset.

Tutkimustulosten mukaan jopa 70 % kaikista vastaajista käyttää samaa salasanaa useissa eri palveluissa, kun taas vain 25 % ei tee niin. Tämä ilmiö jakautui melko tasaisesti eri ikäryhmien kesken, sillä suurin osa jokaisesta ikäryhmästä ilmoitti käyttävänsä samaa salasanaa useassa palvelussa. Mielenkiintoista oli havaita, että erityisesti ikäryhmissä 18–25 ja 26–30 vuotta monet vastaajista kirjasivat salasanansa ylös puhelimen muistiinpanoihin tai paperille. Esimerkiksi 83 vastaajasta näissä ikäluokissa peräti 17 vastaajaa kirjasi salasanansa paperille, kun taas vain 26 vastaajaa käytti salasanojen hallintasovelluksia. Sen sijaan yli 35-vuotiaiden ikäryhmässä havaittiin yllättävän suuri hallintasovellusten käyttö, sillä 18 vastaajaa 43:sta käytti jonkinlaista hallintaohjelmaa salasanoilleen.

Vaikka ikäryhmät osoittivat melko tasaisesti huolta turvallisuudestaan verkossa, suurin osa vastaajista ei pitänyt tietoturvaan liittyviä riskejä niin suurina, että ne estäisivät heitä katsomasta uutisia verkossa. Lisäksi suurin osa vastaajista arvioi

oman tietoturvaosaamisensa tason olevan hyväksi tai melko hyväksi, kun taas vain 9 vastaajaa kaikista ikäryhmistä ilmoitti kokevansa tietoturvaosaamisensa heikoksi. Kaikki ikäluokat kokivat olonsa melko turvalliseksi verkossa, mutta samalla yli puolet jokaisesta ikäluokasta ilmaisi huolensa henkilökohtaisten tietojensa väärinkäytöstä. Kaikki ikäryhmät ovat myös tasaisesti tietoisia julkisten WI-Fi-verkkojen riskeistä.

Tulokset osoittivat myös selkeitä eroja suhtautumisessa tekoälyn kehitykseen eri ikäluokissa. Nuoremmat ikäluokat pitivät tekoälyn kehitystä enimmäkseen positiivisena, kun taas suuri osa yli 35-vuotiaista vastaajista koki sen uhkana. Tästä voidaan päätellä, että eri ikäryhmät suhtautuvat eri tavoin tekoälyn rooliin verkkoturvallisuudessa.

Tutkimuksen tavoitteena oli arvioida eri ikäryhmien välisiä eroja verkkoturvallisuutta koskevissa asenteissa ja käyttäytymisessä. Alkuperäinen hypoteesi oletti, että nuoremmat opiskelijat saattaisivat kokea itsensä itsevarmemmiksi verkossa kuin vanhemmat opiskelijat. Samalla odotettiin, että nuoremmilla olisi parempi salasanojen hallintataito, suurempi luottamus tekoälyyn ja kyky havaita kalastelu-yritykset olisi kehittyneempi.

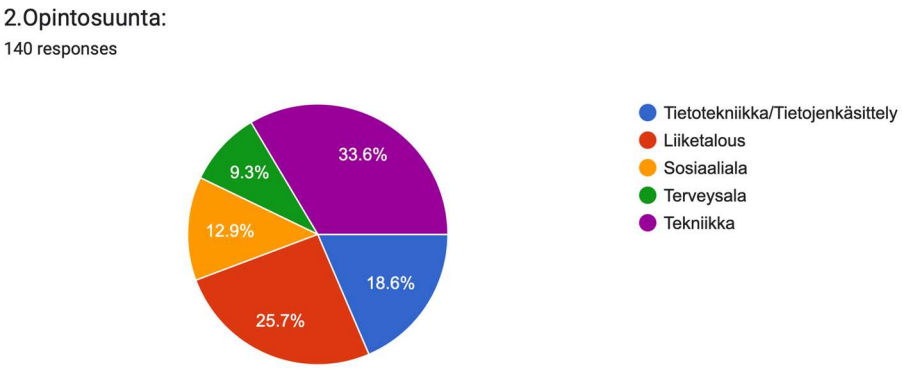
Tutkimustulokset paljastivat, että huolimatta ikäryhmästä suurin osa vastaajista käytti samaa salasanaa useissa eri palveluissa. Nuoremmat ikäryhmät 18–25 ja 26–30 vuotta näyttivät luottavan enemmän perinteisiin tapoihin hallita salasanojaan, kuten kirjaamiseen muistiinpanoihin puhelimessa tai paperille. Yli 35-vuotiaiden ikäryhmässä sen sijaan havaittiin korkeampi hallintasovellusten käyttö salasanojen säilyttämisessä.

Vaikka kaikki ikäluokat ilmaisivat huolensa turvallisuudestaan verkossa, suurin osa vastaajista ei kokenut tietoturvaan liittyviä riskejä esteenä uutisten katsomiselle verkossa. Myös itsearvioitu tietoturvaosaaminen oli pääosin myönteistä kaikissa ikäluokissa. Vaikka kaikki ikäryhmät tunsivat olonsa melko turvalliseksi verkossa, yli puolet ilmaisi huolensa henkilökohtaisten tietojen väärinkäytöstä.

Selkeitä eroja ilmeni suhtautumisessa tekoälyn kehitykseen eri ikäluokissa. Nuoremmat ikäluokat näkivät tekoälyn pääasiassa positiivisena, kun taas yli 35-vuotiaat kokivat sen enemmän uhkana. Tämä osoittaa, että eri ikäryhmät arvioivat ja tulkitsevat tekoälyn roolia verkkoturvallisuudessa eri tavoin.

6.1.2 Opintosuuntien välinen vastausten vertailu

Tutkimuksessa vertailtiin myös vastauksia eri opintosuuntien välillä. Hypoteesina oli, että tietotekniikan ja tietojenkäsittelyn opiskelijat kokisivat olonsa kaikkein turvallisimmiksi verkossa, heillä olisi parempi salasanan hallinta, tunnistaisivat erilaiset uhat, sekä käyttäisivät VPN palvelua enemmän kuin muiden alojen opiskelijat.



Kuva 3. Opintosuunnat.

Tutkimustulosten mukaan 98 vastaajaa käyttää samaa salasanaa useammassa eri palvelussa. Tietotekniikan ja tietojenkäsittelyn opiskelijoista 15 käyttää, ja 10 ei käytä samaa salasanaa, prosentuaalisesti kuitenkin he käyttävät eniten eri salasanoja eri palveluissa.

Kyselyn kysymyksessä 10 vastaajilta kysyttiin, ovatko he jakaneet vahingossa henkilökohtaisia tietoja. Vastausten analysoinnin jälkeen tulos yllätti, sillä tarkasteltaessa vastausten suhteellisia osuuksia voidaan päätellä, että tietotekniikan ja tietojenkäsittelyn alan opiskelijoiden vastauksissa merkittävästi suurin prosentuaalinen osuus niistä, jotka ilmoittavat jakaneensa henkilökohtaisia tietojaan ajattelemattomasti (30.77 %). Sosiaalialan opiskelijat sijoittuvat toiseksi korkeimmaksi prosenttiosuudellaan (27.78 %), kun taas liiketalous on kolmantena (25 %).

Kyselyn kysymyksen 11 perusteella eri aloilla on havaittavissa eroja tietoturvaosaamisen arvioinneissa. Liiketalousalan opiskelijat kokevat oman tietoturvaosaamisensa korkeaksi, kun taas sosiaalialalla esiintyy enemmän vaihtelua arvioinneissa. Tekniikan ala näyttää erottuvan vahvimpana, kun taas terveysalalla

vallitsee kohtuullinen tietoturvaosaaminen. Tietotekniikka ja tietojenkäsittelyala arvioi oman tietoturvaosaamisensa otannassa vahvimmaksi kaikista aloista.

Liitteen 1 kysymyksessä 18 vastaajilta kysyttiin, kuinka usein he päivittävät henkilökohtaisia laitteitaan. Henkilökohtaisten laitteistojen ja ohjelmistojen turvallisuuspäivitysten päivitystiheyttä arvioitaessa voidaan huomata, että kaikilla tarkastelluilla aloilla on havaittavissa säännöllisiä päivityskäytäntöjä. Liiketalousala ja sosiaaliala päivittävät laitteistonsa ja ohjelmistonsa turvallisuuspäivitykset melko säännöllisesti. Tekniikan ala, terveysala ja erityisesti tietotekniikka/tietojenkäsittely-ala erottuvat päivitystiheydessään, sillä ne ilmoittavat päivittävänsä laitteistonsa ja ohjelmistonsa turvallisuuspäivitykset erittäin säännöllisesti. Tietotekniikka/tietojenkäsittely-ala näyttää olevan otannassa erityisen tarkka turvallisuuspäivitysten suhteen.

Henkilökohtaisen tietoturvan huomioimista päätöksenteossa verkossa arvioitaessa voidaan havaita seuraavaa:

Liiketalousalalla tietoturvaan kiinnitetään huomiota laajalti, erityisesti edistyneissä vaiheissa, kuten vaiheissa 3 ja 4. Sosiaalialalla puolestaan tietoturva otetaan huomioon päätöksenteossa, vaikkakin todennäköisesti harvemmin verrattuna liiketalouteen. Kysymys, johon vastattiin, oli seuraava: "Kuinka usein harkitset henkilökohtaisen tietoturvasi vaikutusta verkossa tekemiisi päätöksiin, kuten tiedon jakamiseen?" Vaihtoehdot olivat: 1) en koskaan, 2) joskus, 3) melko usein, 4) usein, 5) aina. Terveysala harkitsee tietoturvaa tasaisesti päätöksissään, vaikka vastausten määrä onkin hieman pienempi.

Tietotekniikka/tietojenkäsittely-ala osoittaa aktiivista tietoturvan harkintaa, erityisesti tasolla 3 ja tasolla 4. Kaiken kaikkiaan kaikilla aloilla ilmenee tiettyä tietoisuutta henkilökohtaisen tietoturvan merkityksestä verkossa, mutta tekniikan ja tietotekniikan aloilla harkinta näyttää olevan erityisen korkealla tasolla.

Tutkimuksen perusteella voidaan todeta, että tietotekniikan ja tietojenkäsittelyn opiskelijat erottuvat monessa suhteessa muiden alojen opiskelijoista. Ensinnäkin heillä on merkittävästi parempi salasanan hallinta, sillä vain 15 opiskelijaa 98:sta käyttää samaa salasanaa useissa palveluissa. Toiseksi tietotekniikan ja tietojenkäsittelyn opiskelijat ilmoittavat kokemansa tietoturvaongelmat verkkoympäristössä yleisesti ottaen muita aloja useammin. Erityisesti henkilökohtaisten tietojen jakamisen osalta he ovat muita aloja edellä, jossa heillä on merkittävästi suurin prosentuaalinen osuus niistä, jotka ovat jakaneet henkilökohtaisia tietojaan ajattelemattomasti.

Lisäksi tietotekniikan ja tietojenkäsittelyn opiskelijat arvioivat omaa tietoturvaosaamistaan korkeimmaksi kaikista opintosuunnista. He myös päivittävät laitteistonsa ja ohjelmistonsa turvallisuuspäivitykset erittäin säännöllisesti, erottuen selvästi muiden alojen opiskelijoista. Tämä osoittaa, että tietotekniikan ja tietojenkäsittelyn opiskelijat ovat aktiivisimpia ja tietoisimpia henkilökohtaisen tietoturvansa ylläpitämisessä ja kehittämisessä verrattuna muihin opintosuuntiin.

6.2 Suositukset jatkotutkimukselle

Tarkempi syventyminen salasanojen hallintaan eri ikäryhmissä: Vaikka tutkimuksessa havaittiin, että suuri osa vastaajista käyttää samaa salasanaa useissa palveluissa, tulevat jatkotutkimukset voivat syventyä tarkastelemaan salasanojen

hallintaa tarkemmin. Esimerkiksi voitaisiin selvittää, mitkä tekijät vaikuttavat salasanojen valintaan ja miten eri ikäryhmät suhtautuvat salasanojen hallintasovelluksiin.

Tietoturvaosaamisen syvällisempi analyysi opintosuunnittain: Tutkimuksessa havaittiin, että tietoturvaosaamisen arviot vaihtelevat eri opintosuuntien välillä. Jatkotutkimuksissa voitaisiin syvällisemmin analysoida, mitkä tekijät vaikuttavat opiskelijoiden tietoturvaosaamiseen eri aloilla ja miten tämä vaikuttaa heidän käyttäytymiseensä verkossa.

Tekoälyn roolin syvällinen tutkimus verkkouhkien torjunnassa**:** Tutkimus osoitti, että eri ikäryhmät suhtautuvat eri tavoin tekoälyn rooliin verkkoturvallisuudessa. Jatkotutkimuksissa voitaisiin tutkia syvällisemmin, miten eri ikäryhmät hahmottavat tekoälyn roolin verkkouhkien torjunnassa ja miten tämä vaikuttaa heidän turvallisuudentunteeseensa verkossa.

Tietoisuus ja käyttäytyminen julkisissa Wi-Fi-verkoissa**:** Tutkimus osoitti, että kaikki ikäryhmät ovat tietoisia julkisten Wi-Fi-verkkojen riskeistä. Jatkotutkimuksissa voitaisiin tutkia syvemmin, miten käyttäjät suojaavat tietonsa julkisissa verkoissa ja miten eri ikäryhmät reagoivat erilaisiin turvallisuusriskitilanteisiin.

Opintosuuntien vaikutus henkilökohtaiseen tietoturvaan**:** Tutkimuksessa havaittiin, että tietotekniikan ja tietojenkäsittelyn opiskelijat erottuvat useilla tietoturvaan liittyvillä mittareilla. Jatkotutkimuksissa voitaisiin syvemmin selvittää, miten opintosuunta vaikuttaa opiskelijoiden tietoturvakäyttäytymiseen ja -asenteisiin sekä mitkä tekijät vaikuttavat näihin eroihin.

7 YHTEENVETO JA POHDINTA

Tutkimus keskittyi kyberturvallisuuden inhimillisiin tekijöihin, tarkastellen niiden roolia, motivaatiota ja vaikutusta turvallisuusstrategioihin. Kyberuhkien luokittelu ja turvallisuuden käsitteiden syventäminen kyberympäristössä tarjosivat teoreettisen perustan tutkimukselle.

Inhimillisten tekijöiden taustalla vaikuttavat psykologiset näkökulmat, kyberhyökkäysten motivaatio, käyttäjien tietoturvakäyttäytyminen ja yhteiskunnalliset vaikutukset. Tutkimus osoitti, että nämä tekijät muodostavat monimutkaisen verkoston, joka vaikuttaa kyberturvallisuuteen monin eri tavoin.

Vaikutus kyberturvallisuuden strategioihin tarkasteltiin organisaation kulttuurin ja koulutuksen merkityksen kautta. Tutkimus korosti, että onnistunut turvallisuusstrategia edellyttää organisaation vahvaa turvallisuuskulttuuria ja koulutuksen jatkuvaa painotusta.

Kyberturvallisuustutkimuksen osalta keskityttiin verkkoturvallisuuskyselyn suunnitteluun ja toteutukseen. Tutkimusprosessiin liittyvät metodologiset valinnat vaikuttivat merkittävästi tulosten luotettavuuteen ja informatiivisuuteen.

Ikäryhmien ja opintosuuntien väliset vertailut paljastivat merkittäviä eroja tietoturvakäyttäytymisessä. Suositukset jatkotutkimukselle kohdistuvat erityisesti näiden erojen syvemmän ymmärtämisen ja niiden perusteella kehitettävien kohdennettujen turvallisuuskoulutusohjelmien suuntaan.

Tämän tutkimuksen perusteella korostuu inhimillisten tekijöiden merkitys kyberturvallisuudessa, jatkotutkimusten avaten mahdollisuuksia syvemmälle ymmärrykselle ja käytännön sovelluksille.

LÄHTEET

Al-Hashem, N., & Saidi, A. (2023). The Psychological Aspect of Cybersecurity: Understanding Cyber Threat Perception and Decision-Making. *International Journal of Applied Machine Learning and Computational Intelligence, 13*(8), 11–22. Noudettu 19.02.2024 osoitteesta: https://neuralslate.com/index.php/Machine-Learning-Computational-I/article/view/41

Andersson, & Koivisto. (2013). *Tietoturvaa toteuttamassa*. Tietosanoma Oy, Helsinki.

Canongia, C., & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. In *Crisis Management: Concepts, Methodologies, Tools and Applications*. Hershey, PA: IGI Global.

European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA Threat Landscape 2023*. Noudettu 22.2.2024 osoitteesta: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Hyppönen, M. (2021). *Internet*. Helsinki: WSOY.

Järvinen, P. (2018). *Kyberuhkia ja somesotaa*. Docendo Oy, Jyväskylä.

Kaspersky Daily. (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Noudettu 15.02.2024 https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kaspersky Lab. (2017). *Mitä kyberrikokset ovat? Miten voit suojautua kyberrikoksilta?* Noudettu 24.02.2024, osoitteesta https://www.kaspersky.fi/resource-center/threats/what-is-cybercrime

Kearney, P. (2016). *Security: The Human Factor*. IT Governance Ltd, Cambridge.

Limnell, T., Majewski, J., & Salminen, M. (2014). *Kyberturvallisuus tekijät*. Docendo Oy, Jyväskylä.

Morgan, S. (2020). Cybercrime to Cost the World $10.5 Trillion Annually By 2025. Noudettu 25.2.2024 osoitteesta https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Pirinen, A. (2021). *Organisaatioiden tietoturvallisuus, - lyhyt oppimäärä*. Noudettu 25.2.2024 osoitteesta https://www.sytyke.org/tietoturva/organisaation-tietoturvallisuus-lyhyt-oppimaara/

Pöyhönen,S.(2022) . *DDoS hyökkäykset – Mitä ne ovat, miksi niitä tehdään ja kuinka niiltä voi suojautua?* Noudettu 12.3.2024 osoitteesta: https://www.tnnet.fi/blogi/ddos-hyokkaykset-mita-ne-ovat-miksi-niita-tehdaan/

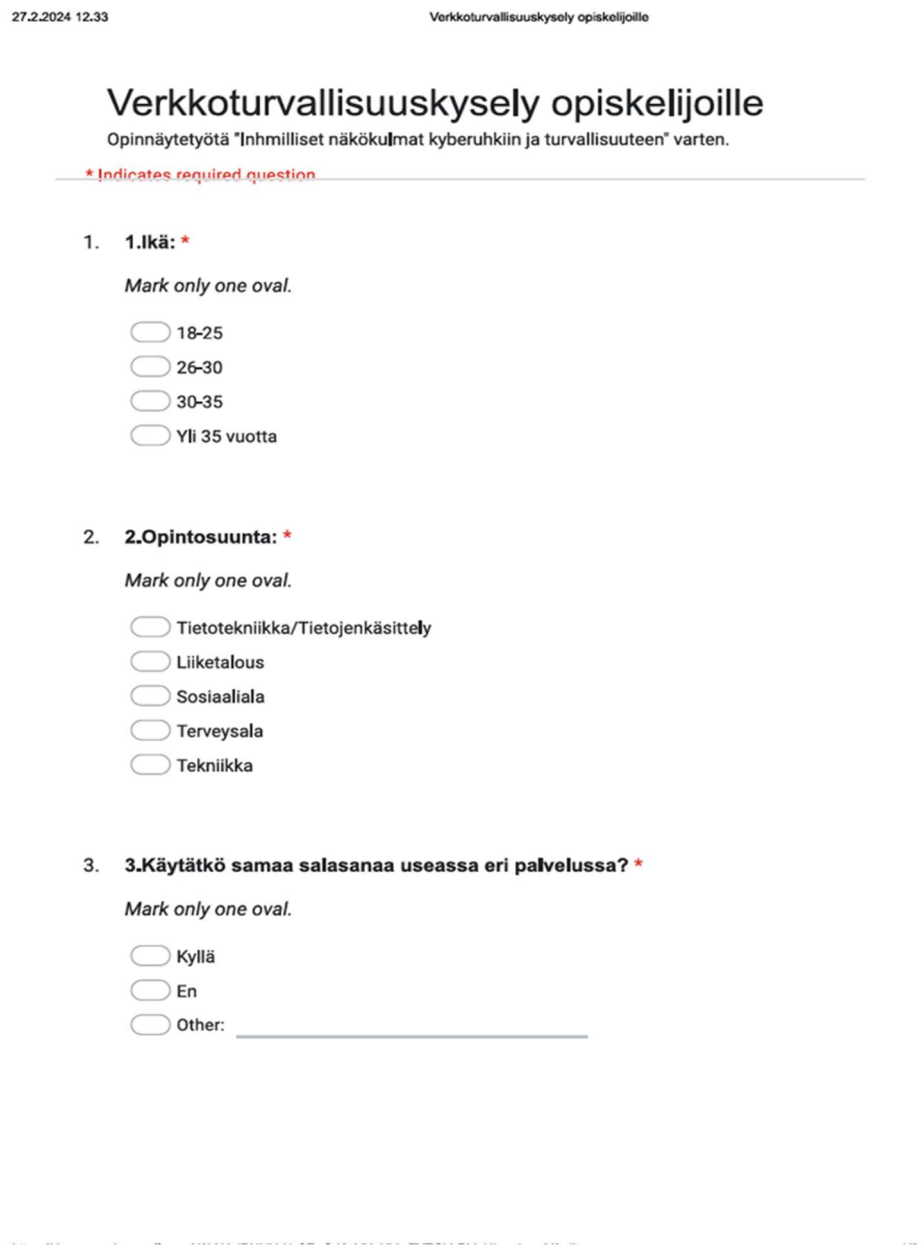
Rousku, K. (2014). *Kyberturvallisuusopas, tietoturvaa kotona ja työpaikalla*. Talentum Media Oy.

SFS Suomen Standardit. *ISO/IEC 27000 Tietoturvallisuuden standardisarja*. Noudettu 2.3.2024 osoitteesta https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

europarl.europa.eu. (2021). *Miksi kyberturvallisuus on tärkeää EU:lle?* Noudettu 10.2.2024 osoitteesta https://www.europarl.europa.eu/topics/fi/article/20211008STO14521/miksi-kyberturvallisuus-on-tarkeaa-eu-lle

LIITTEET

LIITE 1
VERKKOTURVALLISUUSKYSELY OPISKELIJOILLE



27.2.2024 12.33 Verkkoturvallisuuskysely opiskelijoille

Verkkoturvallisuuskysely opiskelijoille

Opinnäytetyötä "Inhmilliset näkökulmat kyberuhkiin ja turvallisuuteen" varten.

* Indicates required question

1. **1.Ikä:** *

   Mark only one oval.

   - 18-25
   - 26-30
   - 30-35
   - Yli 35 vuotta

2. **2.Opintosuunta:** *

   Mark only one oval.

   - Tietotekniikka/Tietojenkäsittely
   - Liiketalous
   - Sosiaaliala
   - Terveysala
   - Tekniikka

3. **3.Käytätkö samaa salasanaa useassa eri palvelussa?** *

   Mark only one oval.

   - Kyllä
   - En
   - Other: _____

4. **4.Oletko kertonut henkilökohtaisen käyttäjätunnuksesi ja salasanasi toiselle henkilölle?** *

Mark only one oval.

- ◯ Kyllä
- ◯ En

5. **5.Oletko huolissasi henkilökohtaisten tietojesi väärinkäytöstä verkossa?** *

Mark only one oval.

- ◯ Kyllä
- ◯ En

6. **6.Oletko tietoisesti vältellyt lukemasta tai katsomasta uutisia tietoturvaan liittyvistä riskeistä, koska ne saattavat aiheuttaa huolta tai stressiä?** *

Mark only one oval.

- ◯ Kyllä
- ◯ En

7. **7.Käytätkö salasanojen hallintasovelluksia (Esim. Keepass)** *

Mark only one oval.

- ◯ Kyllä
- ◯ En
- ◯ Käyttäisin, mutta en tiedä miten ne toimivat
- ◯ Kirjoitan salasanat paperille/puhelimen muistiinpanoihin
- ◯ Muu tapa

8. **8.Onko sinulla käytössä tietoturva sovelluksia? (Esim F-Securen virustentorjuntaohjelma, palomuurit yms)** *

Mark only one oval.

- ◯ Kyllä
- ◯ Ei

9. **9.Käytätkö VPN Palveluita turvallisuussyistä? (Esim F-Securen Freedom VPN)** *

Mark only one oval.

- ◯ Kyllä
- ◯ En
- ◯ En tiennyt, että se suojaa internet yhteyttäni.

10. **10.Oletko joskus huomannut, että olet jakanut henkilökohtaisia tietojasi verkossa ajattelemattomasti?** *

Mark only one oval.

- ◯ Kyllä
- ◯ En

Monivalintakysymyksiä asteikolla 1-5

11. **11.Miten arvioisit oman tietoturvaosaamisesi tasoa?** *

Mark only one oval.

	1	2	3	4	5	
Eritt	◯	◯	◯	◯	◯	Erittäin hyvä

12. **12.Kuinka usein vaihdat salasanasi?** *

Mark only one oval.

	1	2	3	4	5	
En k	◯	◯	◯	◯	◯	Erittäin usein

13. **13.Kuinka turvalliseksi koet olosi verkossa?** *

Mark only one oval.

	1	2	3	4	5	
Eritt	◯	◯	◯	◯	◯	Erittäin turvalliseksi

14. **14.Miten arvioisit omaa kykyäsi tunnistaa ja välttää verkko huijauksia?** *

Mark only one oval.

	1	2	3	4	5	
Eritt	◯	◯	◯	◯	◯	Erittäin hyväksi

15. **15.Kuinka usein harkitset henkilökohtaisen tietoturvasi vaikutusta päätöksissäsi verkossa, esimerkiksi tiedon jakamisessa?** *

Mark only one oval.

	1	2	3	4	5	
En k	◯	◯	◯	◯	◯	Aina

16. **16.Kuinka paljon luotat siihen, että opiskelijayhteisössäsi noudatetaan yhteisiä tietoturvakäytäntöjä?** *

Mark only one oval.

	1	2	3	4	5	
En l	◯	◯	◯	◯	◯	Luotan täysin

17. **17.Koetko, että opiskelijoita on ohjeistettu riittävästi tietoturvallisuuteen liittyvissä asioissa?**

Mark only one oval.

	1	2	3	4	5	
Eritt	◯	◯	◯	◯	◯	Erittäin hyvin

18. **18.Kuinka usein päivität henkilökohtaiset laitteistosi (esim. tietokone, älypuhelin) ja ohjelmistosi (käyttöjärjestelmä, sovellukset) turvallisuuspäivitysten osalta?** *

Mark only one oval.

	1	2	3	4	5	
En k	◯	◯	◯	◯	◯	Aina kun uusi päivitys on saatavilla

Avoimet kysymykset

Voit vastata kysymyksiin muutamalla sanalla,tai pidemmällä vastauksella.

19. **19.Mitä suojautumiskeinoja käytät suojataksesi yksityisyyttäsi sosiaalisessa mediassa ja muissa online-palveluissa?**

20. **20.Oletko tietoinen julkisten Wi-Fi-verkkojen riskeistä ja miten suojaudut niitä vastaan esimerkiksi matkoilla ollessasi?** *

21. **21.Oletko koskaan joutunut verkkohuijauksen uhriksi? Jos olet, niin millaisen?**

22. **22.Jos saat tuntemattomalta sähköpostiviestin, jossa pyydetään klikkaaman linkkiä, miten toimit?** *

23. **24.Onko sinulla huolia liittyen yksityisyyteen ja turvallisuuteen sosiaalisen median käytössä?** *

24. **24.Mitä ajatuksia herää, kun pohdit teknologian vaikutuksia ihmisten turvallisuuteen verkossa?** *

25. **25. Oletko huolissasi tekoälyn kehityksestä, ja sen vaikutuksista verkon turvallisuuteen?** *

26. **26.Miten olet havainnut yhteiskunnan digitalisaation vaikuttavan arkipäivän elämääsi?** *

27. **27.Minkälaisia eettisiä haasteita ja kysymyksiä tekoälyn käyttöön liittyy turvallisuuden ja yksityisyyden kannalta?** *

28. **28.Kuinka tärkeänä pidät eettisten ohjeistusten ja sääntelyn kehittämistä tekoälyn käytölle turvallisuuden varmistamiseksi?** *

29. **29.Miten uskot teknologian käytön vaikuttavan henkilökohtaiseen turvallisuuteesi?** *

30. **30.Oletko osallistunut kyberturvallisuus koulutuksiin, jos olet, niin mitä opit?**