

Maria Mäkelä

# KÄYTETTÄVÄ TIETOTURVA ASIAKKUUDENHALLINTA- JÄRJESTELMÄSSÄ

Kandidaatintyö  
Tekniikan ja luonnontieteiden tiedekunta  
Toukokuu 2021

# TIIVISTELMÄ

Maria Mäkelä: Käytettävä tietoturva asiakkuudenhallintajärjestelmässä  
Usable Security in CRM-system  
Kandidaatintyö  
Tampereen yliopisto  
Tietojohdaminen  
Toukokuu 2021

---

Käytettävyyden ja tietoturvan suhde on ollut jo pitkään kiistanalainen, sillä yleisesti ajatellaan, että käytettävyys tekee tietojärjestelmästä helppokäyttöisen, kun taas tietoturva vaikeuttaa sen käyttöä. Tietojärjestelmien käyttäjät ovat kuitenkin olennainen osa järjestelmän tietoturvaa, sillä käyttäjien tekemät virheet, esimerkiksi huonon käytettävyyden takia, saattavat johtaa vakaviin tietoturvariskeihin organisaatiossa. Käytettävyyden ja tietoturvan huomioiminen yhdessä heti tietojärjestelmien suunnittelun alussa on siis tärkeää, jotta tietoturvan taso ei ole heikkoa huonon käytettävyyden takia.

Tutkimuksen tavoitteena oli selvittää, miten voidaan toteuttaa käytettävä ja tietoturvallinen asiakkuudenhallintajärjestelmä. Tutkimus toteutettiin kirjallisuuskatsauksena, jonka aineistoksi valikoitui aiheeseen liittyvät kirjat, tieteelliset artikkelit ja konferenssijulkaisut. Tutkimusaineistoa käytiin läpi systemaattisesti ja sen avulla saatiin muodostettua selkeä kokonaiskuva aiheesta sekä sen osa-alueista. Aineistoa yhdistelemällä ja soveltamalla saatiin muodostettua päätutkimuskysymykseen vastaus.

Tutkimuksessa todettiin, että käyttäjät tekevät usein tahattomasti organisaatioiden tietojärjestelmissä tietoturvariskeihin johtavia virheitä. Käyttäjien tekemiä virheitä voidaan kuitenkin jo järjestelmän suunnitteluvaiheessa pyrkiä estämään noudattamalla käytettävyyssheuristiikkoja ja suunnitteluohjeita. Tutkimuksessa käytettiin pohjana käytettävyyden analysoinnille käytettävyyssiantuntija Jakob Nielsenin kymmentä heuristiikkaa, joita soveltamalla muodostettiin tutkimustulosten keskeisin osa eli tietoturvan näkökulmasta sopivat suunnitteluohjeet asiakkuudenhallintajärjestelmän toteutukselle. Suunnitteluohjeet muodostettiin sillä ajatuksella, että ne minimoivat yleisimmät käyttäjien tietoturvariskeihin johtavat virheet asiakkuudenhallintajärjestelmässä.

Tutkimus osoitti, että tarkemmalle käytettävän tietoturvan tutkimukselle on tarvetta myös tulevaisuudessa. Tämän vahvistaa esimerkiksi selvittämättömät ristiriidat salasanan vaatimusten suhteen ja se, että asiakkuudenhallintajärjestelmän tietoturvaan tai etenkin käytettävään tietoturvaan liittyvää hyväksi katsottua aineistoa ei tämän työn puitteissa löytynyt. Tutkimuksien vähyys saattaa olla selitettävissä sillä, että organisaatiot eivät välttämättä halua tuoda esiin julkisesti tietoa järjestelmiensä heikkouksista. Aiheesta olisi kuitenkin tarvetta saada enemmän tutkimuksia uusien järjestelmien kehitystä varten, joten jatkotutkimusehdotuksena olisikin tehdä asiakkuudenhallintajärjestelmän käytettävistä tietoturvasta kohdeorganisaatiolle empiirinen tutkimus, joka sisältäisi käyttäjät huomioivan käytettävyystestauksen.

Avainsanat: käytettävyys, tietoturva, käyttäjä, asiakkuudenhallintajärjestelmä, käytettävyyssheuristiikat

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

# ALKUSANAT

Tämä kandidaatintyö on toteutettu kirjallisuuskatsauksena Tampereen yliopiston tietojohdamisen tutkinto-ohjelmaan keväällä 2021. Mielenkiinto tietoturvaan liittyvää aihetta kohtaan kasvoi sen ajankohtaisuuden ja kasvavan suosion perusteella. Käytettävyyttä ja tietoturvaa käsiteltiin parilla tutkinto-ohjelman aikana suoritetulla opintojaksolla, josta sain idean tehdä tutkimuksen näiden kahden ristiriitaisen osa-alueen yhdistämisestä.

Haluan kiittää erityisesti kandidaatintyöni ohjaajaa Ilona Ilvosta erinomaisista kehitysehdotuksista, tuesta ja kärsivällisyydestä vastata loputtomiin kysymyksiini. Lisäksi kiitokset kuuluvat myös kandidaatintyöryhmälleni niin seminaareista saaduista opponoinneista kuin viikoittaisista kandikahveistakin. Haluan myös kiittää muita opiskelukavereitani vertaistuesta sekä läheisiäni kannustuksesta ja avusta, jota sain aina pyytäessäni. Erityiskiitoksen haluan antaa opiskelukavereilleni Nelli Rannilalle ja Nea Virralle, joiden kanssa keskittymisen parantamista varten soitetut Teams-puhelut sisälsivät vertaistuen ja kehitysehdotusten lisäksi myös paljon hauskoja hetkiä ja muuta ajateltavaa tutkimusprosessin aikana.

Tampereella, 3.5.2021

Maria Mäkelä

# SISÄLLYSLUETTELO

1. JOHDANTO .....	1
1.1 Tutkimuksen tausta .....	1
1.2 Tutkimusongelma ja rajaukset .....	3
1.3 Tutkimuksen rakenne .....	3
2. TUTKIMUSMENETELMÄ JA -AINEISTO .....	5
2.1 Tutkimusmenetelmä .....	5
2.2 Tutkimusaineisto .....	7
3. KÄYTETTÄVÄ TIETOTURVA .....	9
3.1 Käytettävyyden määritelmä .....	9
3.2 Tietoturvan määritelmä .....	11
3.3 Käytettävän tietoturvan määritelmä .....	13
4. KÄYTTÄJIEN AIHEUTTAMAT TIETOTURVARISKIT ASIAKKUUDENHALLINTA- JÄRJESTELMÄSSÄ .....	16
4.1 Asiakkuudenhallintajärjestelmä .....	16
4.2 Käyttäjien toiminnan vaikutus järjestelmien tietoturvaan .....	18
4.3 Käyttäjien tietoturvariskejä aiheuttavat virheet järjestelmässä .....	19
5. KÄYTETTÄVÄN TIETOTURVAN SUUNNITTELU ASIAKKUUDENHALLINTA- JÄRJESTELMÄSSÄ .....	23
6. YHTEENVETO .....	28
6.1 Tutkimuksen tulokset .....	28
6.2 Tulosten arviointi .....	30
6.3 Jatkotutkimusehdotukset .....	31
LÄHTEET .....	32
LIITE A: TUTKIMUKSEN KESKEISET LÄHTEET .....	36

# KESKEISET KÄSITTEET

## **Asiakkuudenhallintajärjestelmä (engl. CRM-system)**

Asiakkuudenhallintajärjestelmän tarkoituksena on tehdä yritykselle tehokkaammaksi ja tuottavammaksi vuorovaikutus asiakkaiden kanssa. Järjestelmä sisältää yleensä kaikki organisaation asiakastiedot, kuten yhteystiedot, ostohistoria ja aiemmat asiakaspalvelukohtaukset. Järjestelmän kautta voidaan myös usein kommunikoida asiakkaiden kanssa. (Hargrave 2020)

## **Ihmiskeskeinen suunnittelu (engl. human-centered design, HCD)**

Ihmiskeskeisessä suunnittelussa asetetaan etusijalle ihmisten taidot, tarpeet ja käyttäytyminen, joiden perusteella lähdetään toteuttamaan järjestelmän suunnittelua (Norman 2013, s. 8).

## **Käytettävyys (engl. usability)**

Suomen kielessä käytettävyys-käsitteellä on kaksi erilaista merkitystä liittyen tietoturvaan. Käytettävyys, joka on englanniksi 'availability', tarkoittaa tiedon saatavuutta siihen oikeutettujen henkilöiden keskuudessa. Käytettävyys, joka on englanniksi 'usability', tarkoittaa puolestaan ohjelmiston helppokäyttöisyyttä käyttäjän näkökulmasta. (Sanastokeskus TSK ry 2004) Tässä tutkimuksessa käytettävyys-termille käytetään jälkimmäistä merkitystä (engl. usability) poikkeuksetta.

## **Käytettävä tietoturva (engl. usable cybersecurity)**

Tietoturvaohjelma on käytettävä, jos sen käyttäjät tietävät tietoturvaan liittyvät tekijät, esimerkiksi selkeiden ohjeiden avulla, joita heidän pitää noudattaa ylläpitääkseen hyvän tietoturvan tason ja välttääkseen vaaralliset virheet (Whitten & Tygar 1999).

## **Tietoturva (engl. information security)**

Tietoturva koostuu kolmesta osa-alueesta: luottamuksellisuus, eheys ja saatavuus. Tietoturva saavutetaan politiikan, koulutuksen, harjoittelun ja teknologian kautta. (Whitman & Mattord 2012, s. 8)

# 1. JOHDANTO

Työn tavoitteena on tutkia, mitä kannattaa ottaa huomioon käyttäjän näkökulmasta suunniteltaessa käytettävää eli helppokäyttöistä, mutta samalla tietoturvallista asiakkuudenhallintajärjestelmää. Tässä luvussa käydään läpi tutkimuksen tausta ja tutkimusongelma alatutkimuskysymyksineen. Lisäksi esitellään työn rajaukset ja tutkimuksen rakenne.

## 1.1 Tutkimuksen tausta

Lukuisat tapaukset ovat osoittaneet, että tietoturva ei ole organisaatioille enää vain vaillinnainen velvollisuus, vaan siihen täytyy panostaa jatkuvasti entistä enemmän (Furnell et al. 2018). Organisaatioissa tietoturva saatetaan kokea lisäkuluja aiheuttavana tekijänä, joka lähinnä hidastaa järjestelmien käyttöä tai asiakaspalvelutilanteita. Viime vuosina tietoturva on kuitenkin saanut enemmän näkyvyyttä ja siten myös arvostusta osakseen. Suomessa vuoden 2020 uutisoiduin tietomurto kohdistui psykoterapiakeskus Vastaamoon, jossa kymmenien tuhansien asiakkaiden henkilö- ja potilastiedot anastettiin ja osa niistä myös julkaistiin internetin salatussa Tor-verkossa (Yle 2020). Vastaamon tietomurto kosketti useita suomalaisia ja tämä tapaus todisti viimeistään niin yksityisille henkilöille kuin organisaatioillekin tietoturvan merkityksen.

Kyberturvallisuuskeskuksen (2020) mukaan tietoturvan taso on usein sidoksissa organisaation työntekijöiden valvotuneisuuteen ja yksittäinenkin työntekijä voi estää organisaatioon kohdistuvia tietoturvahyökkäyksiä onnistumasta. Tietojärjestelmien käyttäjillä on nykyään suuri vastuu organisaation tietoturvasta ja tietoturvallisuuden taso määräytyykin lähes aina käyttäjien toiminnan mukaan organisaatioissa (Kyberturvallisuuskeskus 2020). Onkin siis tärkeää tarkastella tietoturvariskejä erityisesti tietojärjestelmien käyttäjien näkökulmasta, sillä suurin syy tietoturvan pettämiselle organisaatioissa löytyy yleensä käyttäjien tekemistä virheistä (Whitten & Tygar 1998).

Useimmiten tietojärjestelmien turvallisuutta tarkastellaan edelleen teknisten ratkaisuiden kautta, vaikka heikkouden tietojärjestelmien tietoturvassa aiheuttavat inhimilliset tekijät (Hughes-Lartey et al. 2021). Tietojärjestelmien käyttäjät eivät kuitenkaan aina ole kiinnostuneita tietoturvasta tai ylipäättään teknologian käyttämisestä oikein, mikä on suuri tietoturvariski organisaatiolle. Lisäksi käyttäjät eivät välttämättä ymmärrä datan tai järjestelmien arvoa yritykselle, mikä voi johtaa siihen, että he eivät myöskään tiedosta heidän tekemisiensä aiheuttavan pahimmillaan suuria tietoturvariskejä. (Sasse & Flechais

2005) Tietoturvaa ei voida siis tarkastella omana osa-alueenaan ilman käyttäjän huomioimista. Tämän takia käsitettä käytettävä tietoturva tulisi tutkia vielä enemmän, jotta tulevaisuudessa voitaisiin välttää yhä useammin käyttäjien tekemien virheiden takia syntyvät tietoturvauhat.

Ihmisen ja teknologian välisessä vuorovaikutuksessa on tärkeää ottaa huomioon teknologian tai tietojärjestelmän käytettävyys, joka tarkoittaa helppokäyttöisyyttä käyttäjän näkökulmasta. Helppokäyttöisiä järjestelmiä suunniteltaessa tavoitteena on, että käyttäjä saa tehtävänsä tehtyä ilman ongelmia, esimerkiksi erilaisten näytöllä olevien ohjeiden, vihjeiden tai palautteen perusteella. (Norman 2013, s. 72–73) Käyttäjien virheistä voidaan usein syyttää huonoa käytettävyyttä tietojärjestelmässä käyttäjän sijasta (Norman 2013, s. 162). Helppokäyttöiset tietojärjestelmät pienentävät siis todennäköisyyttä sille, että käyttäjät tekevät tietoturvariskeihin johtavia virheitä, jolloin käytettävyyden suunnittelulla voidaan siis vähentää käyttäjiin kohdistuvien tietoturvahyökkäysten onnistumista. Käytettävyyden ja tietoturvan suhde on kuitenkin hankala, sillä ne mielletään usein toisensa poissulkeviksi tekijöiksi suunniteltaessa uutta tietojärjestelmää organisaatiolle (Nurse et al. 2011). Kun suunnitellaan uusia tietojärjestelmiä organisaatiolle, ihmiskeskeisellä suunnittelulla ja käyttäjän huomioimisella voi olla suuri merkitys tietoturvarisikien ehkäisemisessä. Käytettävyyteen liittyy monia suunnitteluperiaatteita ja heuristiikkoja, jotka ovat myös hyödyllisiä tietoturvasuunnittelussa (Nurse et al. 2011).

CRM-järjestelmä eli asiakkuudenhallintajärjestelmä on nykyään lähes kaikilla organisaatioilla olennaisena osana päivittäistä toimintaa, sillä se auttaa organisaatiota pitämään huolta olemassa olevista asiakassuhteistaan ja luomaan uusia asiakassuhteita organisaation liikevaihdon kasvun takaamiseksi (Dyché 2002). Asiakkuudenhallintajärjestelmä sisältää monta organisaatiolle tärkeää liiketoiminnan osa-aluetta samassa järjestelmässä ja kuuluu osaksi organisaation järjestelmäkokonaisuutta. Asiakkuudenhallintajärjestelmä auttaa organisaatiota käyttämään reaaliaikaisia tietoja asiakkaista liiketoiminnan tukena ja täten muuttaa organisaation tietoon perustuvaksi organisaatioksi. (Kale 2015) Asiakkuudenhallintajärjestelmä sisältää siis organisaatiolle erittäin kriittistä tietoa etenkin asiakkaista, jolloin tietoturvan merkitys korostuu entisestään. Asiakastietojen vuotaminen tietoturvahyökkäyksen yhteydessä voi aiheuttaa asiakkaissa luottamuksen puutteen lisäksi paljon negatiivisia tunteita organisaatiota kohtaan ja siten se voi jopa pilata organisaation maineen lopullisesti, niin kuin yllä mainitussa Vastaamon tietomurrossa (Yle 2020) kävi.

## 1.2 Tutkimusongelma ja rajaukset

Työssä tutkitaan käytettävän tietoturvan toteuttamista asiakkuudenhallintajärjestelmissä. Tutkimuksen aikana perehdytään käytettävyyteen ja tietoturvaan erillisinä käsitteinä sekä tutkitaan, miten nämä kaksi toistensa usein poissulkevaa näkökulmaa voidaan yhdistää suunnitelmassa uutta järjestelmää. Työtä ohjaa yksi päätutkimuskysymys ja kolme sitä ohjaavaa alatutkimuskysymystä. Alatutkimuskysymykset ohjaavat myös tutkimuksen rakennetta ja näin auttavat työn aikana tuloksia vastaamaan alkuperäiseen tutkimusongelmaan. Päätutkimuskysymyksenä on seuraava:

- Miten toteuttaa käytettävä ja tietoturallinen asiakkuudenhallintajärjestelmä?

Päätutkimusta ohjaavina alatutkimuskysymyksinä ovat seuraavat:

- Miten käytettävyys ja tietoturva voidaan yhdistää?
- Miten käyttäjät vaikuttavat toiminnallaan organisaation tietoturvaan?
- Mitkä ominaisuudet helpottavat asiakkuudenhallintajärjestelmän käyttöä ja siten vähentävät tietoturvariskejä?

Käytettävää tietoturvaa voidaan lähteä tutkimaan tässä tapauksessa joko käyttäjien käyttäytymiseen liittyvien mallien avulla tai tietojärjestelmiin liittyvien ominaisuuksien kautta. Tässä työssä näkökulma rajataan tietojärjestelmien suuntaan eli ihmisten kouluttamiseen ja motivointiin liittyvät osa-alueet jätetään tarkoituksella pois tutkimusalueesta. Työssä keskitytään siihen, miten tietojärjestelmistä saadaan suunnittelun aikana käyttäjän näkökulmasta helppokäyttöisiä, jotta tietoturvariskit vähenevät. Tutkimuksessa ei kuitenkaan etsitä tietoa liittyen eri tietojärjestelmien keskinäiseen kommunikointiin ja käytettävyyteen, vaan tarkastellaan nimenomaan ihmisen ja teknologian vuorovaikutusta tietoturvan näkökulmasta. Organisaation asiakaskunnalla, eli koostuvatko asiakkaat yksityishenkilöistä vai yrityksistä, ei ole merkitystä tutkimuksen kannalta, sillä asiakaskunta ei vaikuta asiakkuudenhallintajärjestelmän toteutukseen useimmissa tapauksissa (Oksanen 2010, s. 23). Työ toteutetaan uusien asiakkuudenhallintajärjestelmien suunnittelun näkökulmasta.

## 1.3 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa eli johdannossa esitellään tutkimuksen tausta, tutkimusongelma alatutkimuskysymyksineen ja rajauksineen sekä tutkimuksen rakenne. Toisessa luvussa käydään läpi tutkimusmenetelmät ja -aineisto eli miten tutkimus on

käytännössä toteutettu. Ensimmäisen ja toisen luvun jälkeen aloitetaan varsinainen tutkimus määriteltyjen alatutkimuskysymysten avulla, jotta saadaan vastaus alkuperäiseen tutkimusongelmaan.

Luvussa 3 aloitetaan tutkimus tutustumalla aluksi käytettävyyteen ja tietoturvaan erillisinä käsitteinä, jonka jälkeen perehdytään tarkemmin näiden kahden käsitteen yhdistämiseen ja niiden väliseen suhteeseen. Neljäs luku syventyy tutkimuksen rajauksen olennaiseen osa-alueeseen eli asiakkuudenhallintajärjestelmään. Kyseisessä luvussa käydään aluksi yleisesti läpi käyttäjien vaikutusta organisaation tietoturvaan ja tutustutaan yleisimpiin käyttäjien tekemiin virheisiin järjestelmissä ja uhkiin, joita virheet mahdollisesti aiheuttavat organisaatiossa. Luvun lopussa teoria käyttäjien vaikutuksesta tietoturvaan ja heidän virheistään sovelletaan asiakkuudenhallintajärjestelmän kontekstiin.

Luku 5 yhdistää aiempien teoriakappaleiden tiedot yhteen ja tutkii käytettävän tietoturvan suunnittelua asiakkuudenhallintajärjestelmässä. Kyseisessä luvussa käydään myös läpi Nielsenin (1994) heuristiikoista johdetut suunnitteluohjeet tietoturvallisen asiakkuudenhallintajärjestelmän toteutukseen, ja perustellaan, miten ne minimoivat käyttäjien tietoturvariskejä aiheuttavia virheitä. Kuudennessa eli viimeisessä luvussa käsitellään tutkimuksen tulokset ja toteutetaan niiden arviointi sekä esitellään jatkotutkimusehdotukset.

## 2. TUTKIMUSMENETELMÄ JA -AINEISTO

Tutkimusmenetelmänä työssä oli kirjallisuuskatsaus, jonka tarkoituksena on muodostaa tutkimusongelmaan vastaus luotettavaksi katsotun tutkimusaineiston avulla. Tässä luvussa esitellään, miten tutkimus toteutettiin eli käydään läpi tutkimusmenetelmä sekä käytetyt tietokannat ja hakulausekkeet, joilla saatiin kerättyä luotettava aineisto tutkimuksen toteutusta varten. Lisäksi tässä luvussa esitellään keskeisimmät lähteet tutkimuksen kannalta.

### 2.1 Tutkimusmenetelmä

Tutkimus suoritettiin kirjallisuuskatsauksena aikaisempien julkaisujen ja tutkimuksien perusteella. Tutkimuksessa yhdistettiin eri julkaisujen tuloksia ja vertailtiin niitä toistensa kanssa. Tutkimuksessa noudatettiin Finkin (2019) kirjallisuuskatsauksen prosessimallia, joka koostuu seitsemästä eri vaiheesta:

1. tutkimuskysymyksen asettaminen
2. tietokantojen ja muiden mahdollisten tietolähteiden valitseminen
3. hakulausekkeiden muodostaminen ja valinta
4. käytännön seula: hakukriteerien asettaminen
5. metodologinen seula: lähteiden tieteellisen laadun varmistaminen ja sopivuus
6. hakutulosten katsaus
7. tulosten yhdisteleminen.

Finkin (2019) mukaan tutkimus alkaa tutkimuskysymyksen asettamisella, joka on tehty jo luvussa 1. Prosessimallin toisen vaiheen mukaan valittiin tietokannat ja muut mahdolliset tietolähteet. Tietokantoja, jotka olivat hyväksi katsottuja tämän tieteellisen tutkimuksen kannalta, ovat Tampereen yliopiston tietokannat Andor, ProQuest ja Scopus. Tiedonhaku laajennettiin myös Google Scholarin tiedonhakuportaaliin, kun tietokannoista ei löytynyt tarvittavia tuloksia. Lisäksi työssä hyödynnettiin Tampereen yliopiston SFS Online -standardikokoelmaa käsitteiden määrittelyssä. Käsitteiden kääntämistä varten käytettiin MOT-sanakirjaa.

Seuraavaksi Finkin (2019) prosessimallin kolmannen vaiheen mukaisesti muodostettiin hakulausekkeet tutkimusongelman sekä alatutkimuskysymyksen perusteella. Aluksi päätettiin, että hakusanoiksi valitaan ainoastaan englanninkielisiä sanoja, sillä suurin osa

alan julkaisuista on englanniksi. Ensimmäisessä hakulausekkeessa esiintyvät termit "human error" ja "mistake" viittaavat ihmisten tekemiin virheisiin, joita tutkimuksessa käsiteltiin. Esimerkiksi pelkkä "error" voisi viitata tietokoneen tekemiin virheisiin, jolloin hakusana ei vastaisi odotettuja tuloksia. Tietoturvasta on englanniksi useampia samassa kontekstissa käytettyjä termejä, kuten "information security", "cyber security" tai pelkkä "security". Tämän takia hakulausekkeisiin jätettiin kyseisissä termeissä esiintyvä sana "security", jolloin kaikki termit otettiin huomioon hakuja tehdessä. Hakulausekkeiden muodostamisessa käytettiin apuna Boolean operaattoreita, jotta tietokannoista löytyvät lähteet saatiin vastaamaan haluttua lopputulosta. Hakulausekkeet koostuivat englanninkielisistä sanoista, jotka liittyvät suoraan alatutkimuskysymyksiin. Taulukossa 1 on esitettyinä valitut hakulausekkeet ja ensimmäisen hakukierroksen tulokset tietokannoittain ennen muita rajoituksia.

**Taulukko 1.** Hakulausekkeet ja niistä saadut tulokset tietokannoittain

HAKULAUSEKE	ANDOR	PROQUEST	SCOPUS
("Human error" OR mistake) AND usable security	14 977	16 188	49
("Customer Relationship Management" OR CRM) AND handbook AND usab*	1 590	2 134	0
(Heuristics OR guidelines) AND usable security	32 766	34 085	133
"Human-computer interaction" AND security	33 384	12 265	3 434

Kuten taulukosta 1 voidaan huomata, suurin osa hakulausekkeista tuotti useita tuhansia tuloksia ilman mitään rajoituksia. Seuraavaksi Finkin (2019) prosessimallin neljännen ja viidennen vaiheen mukaan hakutuloksia rajattiin tarkempien tuloksien takaamiseksi sekä käytännön seulan että metodologisen seulan avulla. Käytännön seulassa hakukriteerinä käytettiin englannin kieltä ja julkaisuvuotta, jossa tulokset asetettiin olemaan enintään kaksikymmentä vuotta vanhoja. Myöhemmin tuloksia rajattiin myös julkaisuvuoden mukaan enintään kymmenen vuotta vanhoiksi, kun haluttiin löytää tuoreempia julkaisuja aiheeseen liittyen. Metodologisen seulan vaiheessa lähteiden tieteellisen laadun varmistamiseksi hakukriteereihin lisättiin avoin pääsy aineistoon ja vertaisarviointi tietokan-

noissa, joissa se oli mahdollista. Taulukossa 2 on esitetty aiemmin valitut hakulausekkeet sekä toisen hakukierroksen tulokset tietokannoittain, kun hakukriteerit oli lisätty haakuun mukaan käytännön seulan ja metodologisen seulan perusteella.

**Taulukko 2. Hakulausekkeet ja niistä saadut tulokset tietokannoittain rajauksilla**

HAKULAUSEKE	ANDOR	PROQUEST	SCOPUS
("Human error" OR mistake) AND usable security	758	3 026	13
("Customer Relationship Management" OR CRM) AND handbook AND usab*	123	805	0
(Heuristics OR guidelines) AND usable security	2 988	8 130	30
"Human-computer interaction" AND security	3 571	5 981	667

Vertaamalla taulukkoja 1 ja 2 huomataan, että hakukriteerien asettamisen jälkeen kaikilla hakulausekkeilla saadut tulokset eri tietokannoissa ovat moninkertaisesti pienemmät kuin edellisellä hakukierroksella. Monissa tapauksissa hakutuloksia löytyi silti paljon, joista suurin osa ei kuitenkaan liittynyt aiheeseen. Tietokannoista hakutulosten esitysjärjestys valittiin relevanttiuden mukaan, jolloin tietokannat automaattisesti ehdottivat ensimmäisille sivuille osuvimmat hakutulokset. Tämä helpotti suuren massan läpikäymistä ja hakutuloksista käytiin läpi silmäilemällä muutaman ensimmäisen sivun aineistojen otsikot, sisällysluettelot ja tiivistelmät. Nämä antoivat jo hyvin tietoa julkaisun sisällöstä ja sen sopivuudesta tutkimukseen.

## 2.2 Tutkimusaineisto

Tutkimusaineistoa etsiessä tavoitteena oli löytää tieteellistä, vertaisarvioitua ja tutkimuksen aiheeseen liittyvää aineistoa. Tietokannoista hakemisen lisäksi sopivia lähteitä saatiin Tampereen yliopiston järjestämän kurssin "Ihmisen ja teknologian vuorovaikutus 1: perusteet" kurssiaineistosta, johon sisältyy muun muassa Normanin (2013) kirja "The Design of Everyday Things: Revised and Expanded Edition". Lisäksi lähteitä etsittiin Computers & Security -lehestä, sillä sen julkaisut ovat tietoturva-alalla arvostettuja. Hyväksi todettu käytäntö aineiston etsimiseen ja löytämiseen on myös helmenkasvatus, jossa relevanttia tutkimusaineistoa löydetään muiden aineistojen lähdeviittauksista.

Tutkimusaineisto ja niiden tekijät esitellään taulukkomuodossa tekijän mukaan aakkosjärjestyksessä liitteessä A, jossa on myös lyhyt kuvaus jokaisen julkaisun keskeisestä sisällöstä. Tutkimuksen keskeisimmät lähteet koostuivat kirjoista, tieteellisistä artikkeleista ja konferenssijulkaisuista. Tutkimusaineistosta löytyy sekä vanhempia perusteoksia että tuoreempia ja siten ajankohtaisempia julkaisuja. Perusteoksien perusteella voitiin muodostaa vankka pohja tutkimukselle ja niiden tarkoituksena on siis antaa tietoa tietoturvan, käytettävyyden ja käytettävän tietoturvan perusteista, joita voidaan hyödyntää tutkimuksessa. Toisaalta keskeisestä tutkimusaineistosta löytyy myös suoraan alatutkimuskysymyksiin liittyviä lähteitä, jotka ovat tuoreempia julkaisuja kuin perusteokset. Tuoreemmat julkaisut liittyen suoraan tutkimuskysymyksiin valittiin kymmenen vuoden aikahaarukalla, sillä käytettävyyperiaatteet eivät ole muuttuneet niin paljon viimeisen vuosikymmenen aikana. Mikäli aineisto kuitenkin käsitteli vanhentunutta teknologiaa, otettiin tämä huomioon soveltaessa sitä tutkimuskohteeseen. Näiden avulla voitiin keskittyä suoraan tutkimuskysymyksiin vertailemalla ja soveltamalla niiden sisältöä toisiinsa.

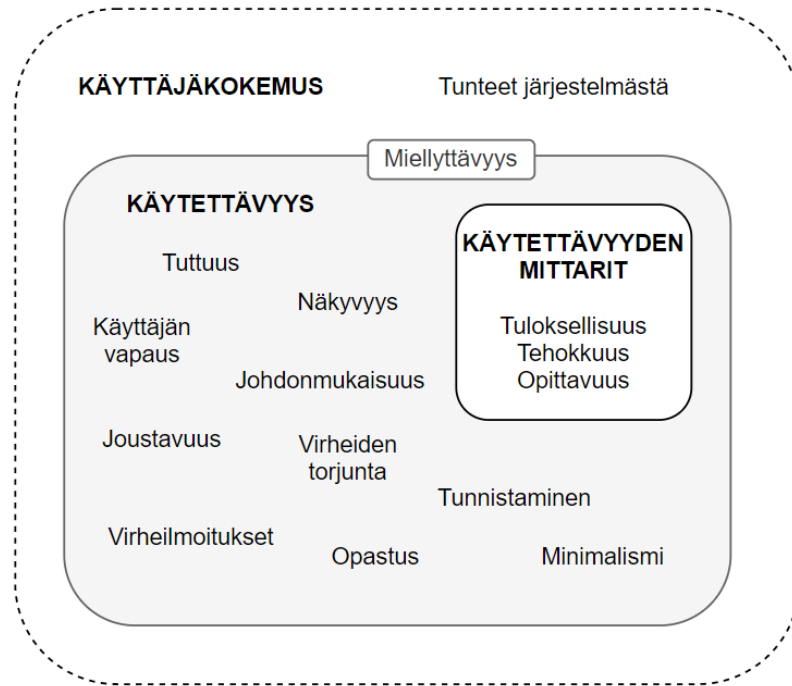
## 3. KÄYTETTÄVÄ TIETOTURVA

Käytettävyys ja käytettävä tietoturva ovat olleet järjestelmien suunnittelun keskiössä, kun käyttäjien on huomattu aiheuttavan tahattomasti tietoturvariskejä organisaatioissa. Käytettävyys ja tietoturva mielletään kuitenkin usein toisensa pois sulkeviksi tekijöiksi järjestelmän suunnittelussa. Seuraavaksi perehdytään siis tarkemmin käytettävyyden ja tietoturvan määritelmiin, joista johdetaan työn keskeisin käsite eli käytettävä tietoturva.

### 3.1 Käytettävyyden määritelmä

Käytettävyydelle löytyy useita eri määritelmiä, joista suurin osa sisältää kuitenkin samoja elementtejä. Käytettävyyden asiantuntija Nielsen (1993, s. 26) painottaa, että käytettävyys ei ole käyttöliittymän yksiuotteinen ominaisuus, vaan se voidaan jakaa viiteen osatekijään: opittavuuteen, tehokkuuteen, muistettavuuteen, virheettömyyteen ja tyydyttävyyteen. Tuoreen ISO/IEC 25010 -standardin (2019) määritelmän mukaan järjestelmän tai ohjelmistotuotteen käytettävyys taas koostuu selkeydestä, opittavuudesta, käytönnästä, käyttövirheiden estämisestä, käyttöliittymän miellyttävyydestä ja esteettömyydestä. Vaikka näiden määritelmien välillä on lähes kaksikymmentä vuotta välissä, samat osa-alueet ovat molemmista määritelmistä havaittavissa. Järjestelmän käytettävyydessä tärkeintä on siis vuosikymmenien ajan ollut opittavuus, virheiden estäminen ja järjestelmän miellyttävä käyttö, jotka tulee ottaa myös jatkossa huomioon järjestelmän suunnittelussa.

ISO 9241-11 -standardin (2018) määritelmän mukaan käytettävyyttä voidaan ajatella mittarina siitä, missä määrin käyttäjä saavuttaa tavoitteensa järjestelmän, tuotteen tai palvelun avulla niin tuloksellisesti, tehokkaasti kuin miellyttävästikin tiettyssä käyttökontekstissa. Rogers et al. (2011, luku 1.6.1) mainitsevat tuloksellisuuden ja tehokkuuden lisäksi käytettävyyden tavoitteiksi myös turvallisuuden, hyödyllisyyden, muistettavuuden ja opittavuuden. Hassan ja Galal-Edeen (2017) tiivistävätkin tutkimuksessaan käytettävyyden mittareiksi kolme tärkeintä eli tuloksellisuuden, tehokkuuden ja opittavuuden. Nämä käytettävyyden mittarit ovat esitetty kuvassa 1, joka tiivistää myös työhön valitun näkökulman käytettävyyden määritelmästä ja suhteesta käyttäjäkokemukseen.



**Kuva 1.** Käytettävyyden määritelmä ja suhde käyttäjäkokemukseen (perustuen Nielsenin 1994; Hassan & Galal-Edeen 2017)

Käytettävyyttä arvioidaan usein heuristisen arvioinnin avulla, jossa arvioijat tunnistavat käytettävyyssongelmia käytettävyyshuristiikkojen avulla (Inostroza et al. 2013). Eri tutkijoiden ja asiantuntijoiden huristiikkoja löytyy useita erilaisia listauksia, joista suurin osa pitää sisällään kuitenkin samoja elementtejä (Nielsen 1994; Bertini et al. 2006; Petrie & Power 2012; Shneiderman et al. 2016). Käytettävyyshuristiikoista yhdet tunnetuimmista ovat Jakob Nielsenin (1994) esittelemät kymmenen huristiikkaa, joita päivitetään jatkuvasti hänen ja toisen käytettävyyshuristiikko Donald Normanin yhteisen yrityksen nettisivuilla (2020). Nettisivujen (Nielsen Norman Group 2020) mukaan nämä kymmenen huristiikkaa tulevat myös tulevaisuudessa toimimaan käyttöliittymien suunnittelun tukena, sillä ne ovat jo viimeiset 26 vuottakin pysyneet muuttumattomina. Alle on listattu Nielsenin (1994) kymmenen huristiikkaa, jotka ovat myös tiivistettynä kuvaan 1 määrittelemään hyvän käytettävyyden piirteitä.

1. **Järjestelmän tilan näkyvyys:** Käyttäjän pitää olla ajan tasalla tapahtumista asi-aankuuluvan ja oikea-aikaisen palautteen avulla.
2. **Järjestelmän ja todellisen elämän vastaavuus:** Järjestelmän tulisi sisältää käyttäjille tuttuja termejä ja käsitteitä ennemmin kuin suunnittelijoiden omia erikoissanoja.
3. **Käyttäjän hallinta ja vapaus:** Käyttäjillä tulisi itsellä olla mahdollisuus perua vahingossa tekemiään virheitä, esimerkiksi ”peruuta” ja ”tee uudelleen” toimintojen avulla.

4. **Yhteneväisyys ja standardit:** Samojen sanojen, tilanteiden ja toimintojen tulisi aina tarkoittaa samaa asiaa, joten suunnittelussa täytyy noudattaa kyseisen toteutusympäristön käyttöstandardeja.
5. **Virheiden estäminen:** Hyvät virheilmoitukset ovat tärkeitä, mutta parempi vaihtoehto on yrittää suunnitella järjestelmä niin, ettei käyttäjä joudu virhetilanteisiin.
6. **Tunnistaminen muistamisen edelle:** Käyttäjän muistikuormaa voidaan minimoida tekemällä järjestelmän toiminnot, käyttöohjeet ja vaihtoehdot näkyviksi.
7. **Käytön joustavuus ja tehokkuus:** Järjestelmä tulisi suunnitella niin kokemattomille kuin edistyneillekin käyttäjille. Kokemattomilta käyttäjiltä voi esimerkiksi piilottaa pikakuvakkeet, jotka helpottavat edistyneiden käyttökokemusta.
8. **Esteettinen ja minimalistinen suunnittelu:** Järjestelmästä kannattaa karsia asiaankuulumattomat ja tarpeettomat tiedot käyttäjän nähtäviltä.
9. **Virhetilanteiden tunnistaminen, ilmoittaminen ja korjaaminen:** Virheilmoitukset täytyy ilmaista selkeästi käyttäjälle sopivalla kielellä, jonka avulla käyttäjät ymmärtävät ongelman ja ratkaisun siihen.
10. **Ohjeet ja dokumentaatio:** Käyttäjälle tulee tarjota konkreettisia, toimintaa tukevia ohjeita, jotka ovat riittävän lyhyitä ja helposti löydettävissä.

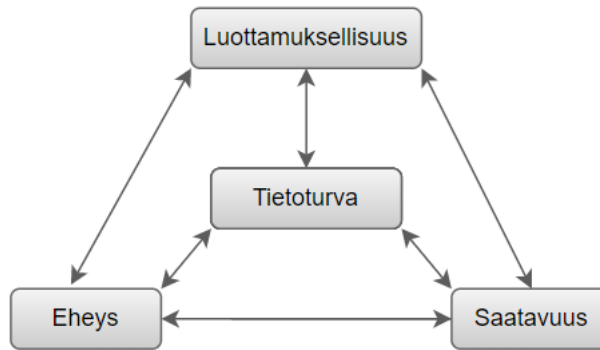
Käytettävyys ja käyttäjäkokemus saattavat käsitteinä mennä helposti sekaisin, ja niiden suhde onkin ollut kiistanalainen tieteellisissä artikkeleissa jo pitkään. Følstad ja Rolfsen (2006) kokoavat kolme erilaista kirjallisuudessa esiintynyttä näkökulmaa käytettävyyden ja käyttäjäkokemuksen suhteelle: käytettävyys ja käyttäjäkokemus täydentävät toisiaan, käytettävyys on käyttäjäkokemuksen mittari sekä käyttäjäkokemus on osa käytettävyyden määritelmää. Neljäs ja myös kirjallisuudessa suosituin näkemys taas painottaa, että käytettävyys on vain yksi osa käyttäjäkokemusta, joka sisältää käytettävyyden lisäksi käyttäjän tunteet käytön aikana (Hassan & Galal-Edeen 2017). Kyseinen näkökulma on valittu suosionsa takia myös tämän työn näkökulmaksi ja kuvaus tästä käytettävyyden ja käyttäjäkokemuksen suhteesta on havainnollistettu kuvassa 1.

### 3.2 Tietoturvan määritelmä

Jokaisella organisaatiolla on tietoa, jota tulee puolustaa erilaisilta uhkilta, kuten hyökkäyksiltä, virheiltiltä ja luonnonilmiöiltä (ISO/IEC 2020). Tietoturva käsitteenä perustuu ISO/IEC 27000 -standardin (2020) mukaan siihen, että tieto on organisaatiolle arvokasta omaisuutta, joka vaatii suojaamista luottamuksellisuuden (engl. confidentiality), saata-

vuuden (engl. availability) ja eheyden (engl. integrity) menettämislä. Useissa julkaisuissa nämä kolme elementtiä muodostavat yhdessä tietoturvan määrittelevän CIA-mallin (Whitman & Mattord 2012, s. 8; Vacca 2017, s. 83; Gupta et al. 2019, s. 257; Chai 2021).

CIA-malli on ollut pitkään käytetty määritelmä tietoturvalle, mutta kirjallisuudessa esiintyy myös muita laajennettuja versioita kyseisestä mallista. Esimerkiksi Bosworth et al. (2014, s. 32) esittelevät tietoturvakehyksen, johon kuuluu CIA-mallin elementtien lisäksi hyödyllisyys (engl. utility), aitous (engl. authenticity) ja hallinta (engl. possession). Myös Whitman ja Mattord (2012, s. 12) tuovat esiin laajennetun CIA-mallin, johon kuuluu Bosworthin et al. (2014, s. 32) määrittelemien elementtien lisäksi virheettömyys (engl. accuracy). Tässä työssä tietoturvaa käsitellään kuitenkin perinteisen CIA-mallin kautta, joka on esitettyä kuvassa 2.



**Kuva 2.** CIA-malli (Gupta et al. 2019, s. 257)

Luottamuksellisuudella tarkoitetaan sitä, kun tiedot on järjestelmässä asetettu vain niiden käyttöön oikeutettujen henkilöiden saataville. Kun ulkopuoliset henkilöt tai järjestelmät pääsevät tarkastelemaan tietoja, luottamuksellisuus on rikkoutunut. (Whitman & Mattord 2012, s. 13) Tietojen salaus on yleisesti käytetty menetelmä luottamuksellisuuden varmistamiseksi (Gupta et al. 2019, s. 257). Saatavuus taas mahdollistaa sen, että valtuutetut käyttäjät tai tietojärjestelmät pääsevät tarkastelemaan tietoja ilman häiriöitä tai esteitä (Whitman & Mattord 2012, s. 12; Gupta et al. 2019, s. 258). Eheydellä puolestaan tarkoitetaan sitä, että tieto ei ole vahingoittunut tai manipuloitu esimerkiksi tietokonevirusten tai muiden haittaohjelmien takia (Whitman & Mattord 2012, s. 13–14). Tietoturvan suunnittelussa ja kehittämisessä tulee siis huomioida jokainen näistä osa-alueista, jotta suojattavat tiedot pysyvät kokonaan turvattuna.

### 3.3 Käytettävän tietoturvan määritelmä

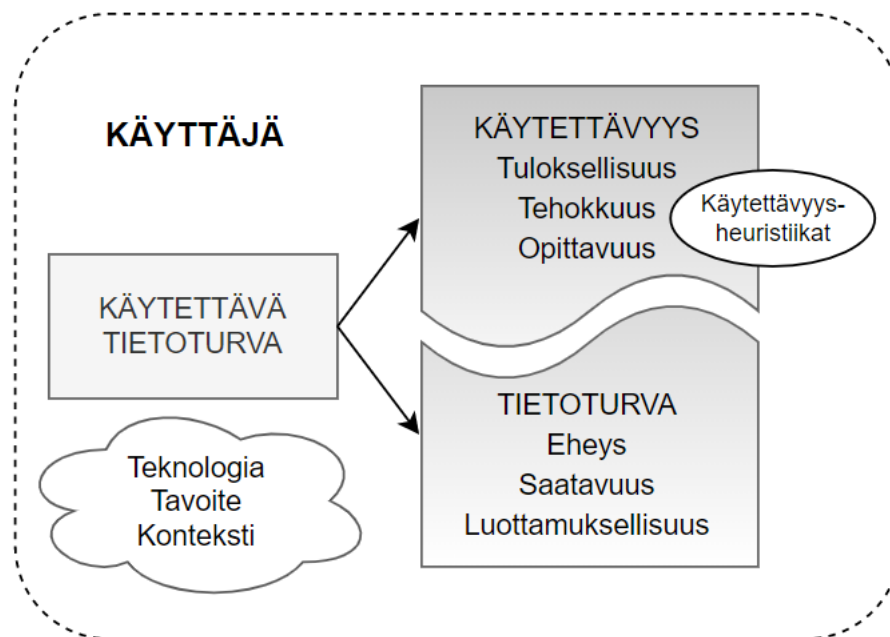
Käytettävä tietoturva käsitteenä sisältää selkeästi kaksi eri osa-aluetta: käytettävyyden ja tietoturvallisuuden. Käytettävyyden ja tietoturvan suhdetta toisiinsa on tutkittu jo monia vuosia, sillä ne nähdään jopa kilpailevina osa-alueina suunniteltaessa tietojärjestelmää (Nurse et al. 2011). Kun suunnitellaan käytettävää tuotetta, pyritään minimoimaan ylimääräiset haasteet ja esteet käyttäjältä hyvän käyttäjäkokemuksen takaamiseksi. Tietoturva taas luo väistämättä käyttäjälle ylimääräisiä haasteita ja esteitä, jotta tuote olisi mahdollisimman turvallinen. (Dourish et al. 2004) Kirjallisuudessa on kuitenkin noussut myös esiin näkökulma siitä, että itse asiassa nämä kaksi usein ristiriidassa olevaa käsitettä saattavat olla toisiaan täydentäviä ominaisuuksia, sillä hyvä käytettävyys voi ehkäistä tietoturvariskejä (Granor & Garfinkel 2004; Yee 2004). Normanin (2009) mukaan käyttäjät kuitenkin saattavat keksiä keinoja kiertää tietoturvaan liittyvät asiat, sillä he kokevat niiden olevan esteenä tehdessään omistautuneena omaa työtään.

Monissa tieteellisissä julkaisuissa käyttäjää pidetään tietoturvan heikoimpana lenkinä (Whitten & Tygar 1999; Guo et al. 2011; Crossler et al. 2013; Willison & Warkentin 2013; Hughes-Lartey et al. 2021). Richter ja Roth (2006) ovat kuitenkin tutkimuksessaan sitä mieltä, että tätä ajattelumallia ei kannata käyttää. Myös Norman (2013, s. 162) painottaa, että ihmisiä ei voi syyttää heidän tekemistään virheistä, vaan syy löytyy aina huonosta suunnittelusta, sillä siinä on silloin keskitytty ainoastaan järjestelmään käyttäjien vaatimusten sijasta. Lisäksi Sasse et al. (2001) on ottanut kantaa siihen, että käyttäjiä on turha syyttää tietoturvariskeihin johtavista virheistä, vaan sen sijaan niistä tulisi oppia ja kerätä havainnot järjestelmän suunnittelijoille. Vaikka käyttäjät aiheuttavat yleensä vakavimmat tietoturvariskit organisaatioiden järjestelmissä, ne voisivat silti olla estettävissä käyttäjät huomioivalla suunnittelulla.

Käytettävästä tietoturvasta puhuttaessa käyttäjät ja inhimillinen tekijä nousee väistämättä esiin. Jopa teknisesti todella turvallinen järjestelmä saattaa epäonnistua turvallisuudessaan, jos käyttäjät eivät osaa tai halua käyttää sitä oikein (Chiasson et al. 2007). Norman (2009) toteaa artikkelissaan, että tietoturvan lisääminen ei kuitenkaan välttämättä tarkoita käytettävyyden heikentymistä, vaikka useimmiten näin onkin. Artikkelissaan Norman käyttää onnistuneena esimerkkinä ovia ja lukkoja, jotka ovat turvallisia ja antavat hyvän suojan kohteelle, mutta niiden vaatima vaivannäkö aktiivisessa käytössä on myös kohtuullinen, jolloin suunnittelun avulla käytettävyys ja tietoturva on saatu yhdistettyä erinomaisesti.

Monet tutkimukset ovatkin osoittaneet, että ristiriidasta huolimatta on mahdollista luoda järjestelmiä, jotka ovat sekä helppokäyttöisiä että turvallisia (Smetters 2008). On kuitenkin selvää, että järjestelmiä suunniteltaessa tietoturvaa ja käytettävyyttä ei voida tarkastella erillisinä osa-alueinaan, vaan molemmat näkökulmat tulee ottaa huomioon suunnittelun alusta alkaen onnistuneen lopputuloksen takaamiseksi. Cranor ja Garfinkel (2004) esittävätkin väitteen siitä, että ihmiset eivät edes käyttäisi helposti käytettävää tietojärjestelmää, jossa on heikko tietoturva, tai tietoturvallista järjestelmää, mikäli se olisi vaikeasti käytettävä.

Järjestelmän käytettävyyttä voidaan tarkastella ihmisen ja tietokoneen välisen vuorovaikutuksen eli HCI:n (engl. human-computer interaction) näkökulmasta. Sasse et al. (2001) tuovat esiin, että HCI ottaa huomioon käyttäjien ja teknologian yhteistyön saavuttaakseen tavoitteen järjestelmässä tietoturvallisesti. He esittelevätkin neljä ulottuvuutta, jotka tulisi ottaa huomioon järjestelmän suunnittelussa tietoturvan ja käytettävyyden näkökulmasta: käyttäjä, teknologia, tavoite ja konteksti. Kuvassa 3 on esitettyä yhteenveto käytettävän tietoturvan käsitteestä ja osa-alueista, jotka otetaan työssä huomioon.



**Kuva 3.** Käytettävän tietoturvan määritelmä ja siihen vaikuttavat tekijät

Käytettävä tietoturva koostuu siis käytettävyyden elementeistä ja mittareista sekä tietoturvan osa-alueista. Näitä voidaankin pitää järjestelmän suunnittelussa tavoitteina, jotta järjestelmästä saadaan sekä käytettävä että tietoturallinen organisaatiolle. Järjestelmän suunnittelussa tulee kuitenkin ensisijaisesti ottaa huomioon käyttäjä, sillä käyttäjällä on suuri vaikutus järjestelmän turvallisuuden tasoon. Tietoturvan näkökulmasta käyttäjä vaikuttaa olennaisesti tietoturvan määrittelemän CIA-mallin (kuva 2) jokaiseen osa-alueeseen.

seen, sillä luottamuksellisuus keskittyy käyttäjien käyttöoikeuksiin, saatavuudella määritellään käyttäjien pääsy vapaasti heille oikeutettujen tietojen pariin ja eheys voi nopeastikin rikkoutua käyttäjien tekemien virheiden takia. Tiedon eheyden varmistamiseksi organisaatioiden tulee huolehtia käyttäjien pääsynhallinnasta, mutta toisaalta ajantasaisella pääsynhallinnalla myös varmistetaan tietoturvan luottamuksellisuus. (Chai 2021) Myös käytettävyys ja sen elementit riippuvat täysin käyttäjästä, sillä ilman käyttäjän kokemusta niitä ei voida arvioida. Lisäksi suunnittelussa tulee ottaa huomioon teknologia, tavoite ja käyttökonteksti, jotka mukautuvat myös käyttäjän tarpeen perusteella. Käytettävä tietoturva on siis laaja ja moneen tekijään vaikuttava osa-alue järjestelmien suunnittelussa, jossa erityisesti käyttäjä täytyy ottaa huomioon päästäkseen tietoturvalliseen, mutta myös käytettävään lopputulokseen.

## 4. KÄYTTÄJIEN AIHEUTTAMAT TIETOTURVARIS- KIT ASIAKKUUDENHALLINTAJÄRJESTEL- MÄSSÄ

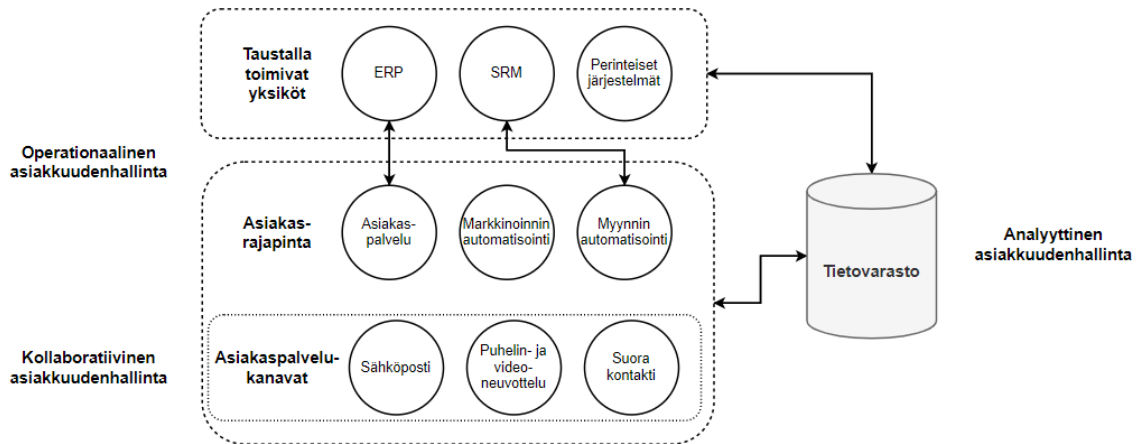
Asiakkuudenhallintajärjestelmä sisältää paljon arkaluontoista tietoa niin asiakkaista ja niiden toiminnasta kuin organisaatiostakin. Tätä tietoa tulee suojella tietoturvahilta, joita valitettavan usein järjestelmän käyttäjät aiheuttavat tahattomasti itse. Seuraavaksi käydään läpi asiakkuudenhallintajärjestelmän toimintaa ja perusominaisuuksia sekä tutustutaan tarkemmin, miten tietojärjestelmien käyttäjät vaikuttavat organisaatiossa olevien järjestelmien tietoturvaan. Lisäksi esitellään yleisiä käyttäjien aiheuttamia tietoturvariskejä ja niistä seuraavia tietoturvahkia tietojärjestelmissä, joista tehdään lopussa yhteenveto asiakkuudenhallintajärjestelmän näkökulmasta.

### 4.1 Asiakkuudenhallintajärjestelmä

Asiakkuudenhallinta (CRM, Customer Relationship Management) kattaa käsitteenä sekä organisaation toimintatavat että tietojärjestelmät liittyen asiakkuudenhallintaan. Lisäksi asiakkuudenhallinta voi tarkoittaa liiketoimintastrategiaa, prosessia ja lähestymistapaa asiakkaiden tunnistamiseen. (Buttle & Maklan 2019, s. 4) CRM-järjestelmä eli asiakkuudenhallintajärjestelmä sisältää kaikki edellä mainitut näkökulmat kyseiseen termiin liittyen, sillä asiakkuudenhallintajärjestelmän tavoitteena on tuottaa kattava kuva asiakkaista, hallita organisaation kaikkia asiakassuhteita eri viestintäkanavissa ja tehostaa prosesseja, jotka liittyvät asiakassuhteisiin (Garrido-Moreno & Padilla-MeléndeZ 2011). Chen ja Popovich (2003) korostavatkin, että asiakkuudenhallintaa ei saa nähdä ainoastaan teknologisenä ratkaisuna organisaatiolle, vaan järjestelmän käyttöönotto vaatii integroidun ja tasapainoisen lähestymistavan, joka huomioi niin teknologiat, prosessit kuin ihmisetkin.

Asiakkuudenhallintajärjestelmät ovat nostaneet jatkuvasti suosiotaan organisaatioissa, ja niitä on nykyään olemassa useita erilaisia. Asiakkuudenhallintajärjestelmien suosio perustuu siihen, että järjestelmä voidaan ottaa käyttöön nopealla aikataululla verrattuna perinteisiin järjestelmiin, vaikka toteutuskustannukset olisivatkin korkeammat (Kale 2015, s. 67). Asiakkuudenhallintajärjestelmät keräävät, varastoivat, ylläpitävät ja jakavat tietoa asiakkaista koko organisaation hyödyksi. Tietojen tehokkaalla hallinnoinnilla onkin erittäin ratkaiseva rooli asiakkuudenhallinnassa. (Chen & Popovich 2003) Asiakkuudenhallintajärjestelmä jaetaan usein kolmeen osaan toimintojensa mukaan: analyyttinen, operationaalinen ja kollaboratiivinen osa (Fayerman 2002; Kale 2015). Kuvassa 4 on

havainnollistettu, mitä eri osa-alueet asiakkuudenhallintajärjestelmässä sisältävät ja niiden suhteita toisiinsa.



**Kuva 4.** Yksinkertaistettu asiakkuudenhallintajärjestelmän rakenne (mukaillen Fayerman 2002; Kale 2015, s. 82)

Asiakkuudenhallintajärjestelmä yhdistää operationaalisessa osassa asiakasrajapinnan (engl. front office), kuten myynnin, markkinoinnin ja asiakaspalvelun, sekä organisaation taustalla toimivat yksiköt (engl. back office), kuten logistiikan, henkilöstöosaston ja taloushallinnon. (Fayerman 2002; Strauss & Frost 2002, Chalmeta 2006 mukaan). Taustalla toimivien yksikköjen tietojärjestelmiä, jotka voidaan yhdistää asiakkuudenhallintajärjestelmään, ovat esimerkiksi toiminnanohjausjärjestelmä (ERP), toimittajasuhteiden hallintajärjestelmä (SRM) ja muut organisaation perinteiset järjestelmät (Kale 2015, s. 82). Asiakkuudenhallintajärjestelmän tarkoituksena on myös integroida eri yksiköiden kosketuspinnat asiakkaisiin, kuten internet, sähköposti, puhelinmyynti ja myymälät, sillä ne ovat usein kontrolloituja erikseen organisaation eri tietojärjestelmissä (Chen & Popovich 2003). Nämä kosketuspinnat ja asiakaspalvelukanavat kuuluvat asiakkuudenhallintajärjestelmän kollaboratiiviseen osaan, jonka tarkoituksena on helpottaa organisaatiossa tapahtuvaa viestintää, koordinoitua ja yhteistoimintaa sidosryhmien kanssa (Kale 2015, s. 82).

Kuvasta 4 voi huomata, että asiakkuudenhallintajärjestelmän keskiössä on analyttisen osan tietovarasto, joka linkittyy jokaiseen järjestelmän osaan. Sen avulla asiakkaiden tietoja voidaan tallentaa, käsitellä, varastoida, erotella, integroida ja raportoida sekä asiakkaan että yrityksen arvon parantamiseksi (Buttle & Maklan 2019 s. 13). Analyttinen asiakkuudenhallinta vastaanottaa ja lähettää jatkuvasti tietojaan operationaalisen osan kanssa, esimerkiksi asiakastiedoista ja heidän toiminnastaan tukeakseen organisaation strategisia prosesseja (Kale 2015, s. 82).

## 4.2 Käyttäjien toiminnan vaikutus järjestelmien tietoturvaan

Organisaatioissa halutaan luonnollisesti kehittää jatkuvasti yhä parempia ja tehokkaampia tietoturvamekanismeja suojaamaan arvokasta tietoa ulkopuolisilta. Tietoturvan tasoa tarkastellaan usein teknologisesti näkökulmasta, jolloin käytettävyyttä ei välttämättä liitetä mukaan tarkasteluun tietoturvan näkökulmasta. Tutkimuksien myötä on kuitenkin havaittu, että käyttäjä on erittäin kriittinen osa tietoturvasuutta (Whitten & Tygar 1999; Smetters 2008; Liginlal et al. 2009; Crossler et al. 2013). Käyttäjät eivät välttämättä ole tarpeeksi tietoisia omien tekojensa seurauksista tietoturvan saralla ja Furnell et al. (2018) nostavatkin esiin sen, että käyttäjät tekevät virheitä usein tahtomattaan ja vahingossa. Schneier (2015, luku 17) tiivistää kirjassaan, että ihmiset eivät kovin tarkkaan ymmärrä tietojärjestelmiä, vaan haluavat vain saada oman tehtävänsä tehtyä välittämättä muusta. Hän listaakin kuusi ihmisiin keskittyvää ongelmaa, jotka vaikuttavat organisaation järjestelmien turvallisuuteen: käyttäjien vähättelevä suhtautuminen riskeihin, taidottomuus järjestelmissä tapahtuvien virheiden käsittelyssä, liika luottamus järjestelmiä kohtaan, turvallisuuteen liittyvien päätöksiä tekeminen, epäluotettavat työntekijät organisaatiossa sekä käyttäjän manipuloinnin yleisyys ja helppous.

Willisonin ja Warketin (2013) mukaan työntekijöiden aiheuttamat tietoturvahukat voivat johtua vahinkojen lisäksi työntekijöiden huonosta koulutuksesta, motivaation puutteesta tai huolimattomuudesta. Nämä piirteet viittaavat osittain myös työntekijöiden epäluotettavuuteen. Toisaalta Richter ja Roth (2006) tuovat esiin julkaisussaan, että suurin osa organisaation työntekijöistä ei koe olevansa potentiaalinen uhri kyberhyökkäykselle, sillä heidän mukaansa kukaan ei voi tehdä mitään heidän tietokoneellansa tai sähköpostillansa. Tämä ajatusmaailma taas viittaa liialliseen luottamukseen järjestelmiä kohtaa. Schneier (2015, luku 17) tuokin kirjassaan esiin, että ihmiset yleensä ajattelevat, että heille ei voisi käydä mitään ja he luottavat tietojärjestelmiin niin paljon, että eivät ole huolissaan järjestelmien turvallisuudesta, jonka takia esimerkiksi varoitusikkunoiden sulkeminen tulee heiltä luonnostaan. Edellä mainitut seikat todistavatkin, että monella on vielä harhainen käsitys siitä, etteikö pienetkin tietoturvirheet kenellä tahansa organisaation jäsenellä voisi aiheuttaa suuria ongelmia ja mahdollisia tietovuotoja organisaatiossa.

Tietoturvariskeihin johtava työntekijöiden tietoturvakäyttäytyminen organisaatiossa voidaan jakaa kahteen luokkaan: tahalliseen ja tahattomaan käytökseen. Molemmissa tapauksissa seuraukset voivat olla yhtä haitallisia, mutta erottelu näiden kahden käyttäytymisen välillä on tärkeää, sillä niiden motiivit eroavat toisistaan. (Crossler et al. 2013) Tietoturvariskeihin johtava tahaton tietoturvakäyttäytyminen tarkoittaa käytännössä sellaisten työntekijöiden käytöstä, jotka jättävät tahallaan organisaation tietoturvapoliittikan

mukaisia ohjeita noudattamatta, esimerkiksi välinpitämättömyyden tai osaamattomuuden takia, mutta heidän tarkoituksenaan ei ole kuitenkaan aiheuttaa organisaatiolle tietoturvariskejä (Guo et al. 2011). Viitaten Yhdysvaltojen CSI:n (Computer Security Institute) tutkimukseen, yksi suurimmista ongelmista organisaatioiden tietoturvassa on nimenomaan tahattomasti tietoturvariskejä aiheuttavat työntekijät (Richardson 2010). Kyseisessä tutkimuksessa yli 16 prosenttia kyselyyn vastanneista organisaatioista arvioi, että lähes kaikki tietoturvan pettämisestä syntyneet tappiot aiheutuivat työntekijöiden tahattomasta tietoturvakäyttäytymisestä.

Etenkin isoissa organisaatioissa työskentelee nykyään tietojärjestelmien parissa eri ikäisiä ja eri tietoteknisillä taustoilla olevia työntekijöitä, joilta saatetaan odottaa kuitenkin saman tasoista tietoturvaosaamista. Gargin et al. (2017) mukaan 1990-luvun lopulla järjestelmien suunnittelussa ei keskitytty paljoakaan käyttäjiin, sillä järjestelmiä tuotettiin massatuotannolla, mutta nykyään käytettävyys on merkittävässä roolissa teknologian suunnittelussa. Viime vuosina on kuitenkin noussut ongelmaksi, että organisaatioissa käyttäjiin kohdistetaan odotuksia itsenäisestä tietoturvaan liittyvien asioiden selvittämisestä, mitä ei kuitenkaan usein tapahdu (Furnell et al. 2018). Käyttäjät eivät yleisesti ole huolissaan tietoturvasta riittävällä tasolla käyttäessään organisaation tietojärjestelmiä, mutta kuitenkin huoli tietoturvasta on jatkuvasti nousussa tietoisuuden kasvaessa (Garg et al. 2017). Tutkimukset ovat myös osoittaneet, että käyttäjien tekemät virheet ovat vähentyneet ja siten tietojärjestelmien yleinen turvallisuus on parantunut, kun organisaatioissa tietoturvallisuusmekanismit on suunniteltu asianmukaisesti käyttäjää tukien (Furnell et al. 2018).

### **4.3 Käyttäjien tietoturvariskejä aiheuttavat virheet järjestelmässä**

Vaikka ihmiset tunnustetaan tietoturvan heikoimpana lenkinä, organisaatiot kärsivät edelleen tietoturvahyökkäyksistä, jotka ovat seurausta ihmisten tekemistä virheistä järjestelmässä (Evans et al. 2019). Monissa julkaisuissa useiden vuosien ajan tietoturvaa uhkaavat käyttäjien virheet liittyvät käyttäjien salasanoihin järjestelmässä (Kraemer & Carayon 2007; Workman et al. 2008; Norman 2009; Guo et al. 2011; Safa et al. 2016; Hadlington 2017). Guo et al. (2011) mukaan työntekijät vaarantavat tietoisesti, mutta eivät kuitenkaan pahantahtoisesti, organisaation tietoturvaa kirjoittamalla salasana muistilapulle tai pitämällä aina samaa salasanaa, vaikka ovatkin tietoisia näiden toimien aiheuttavan tietoturvariskejä. Muita tietoturvariskejä aiheuttavia salasanaan liittyviä käyttäytymismalleja ovat helposti arvattavien salasanojen käyttäminen, salasanan jakaminen kollegoiden kanssa ja saman salasanan käyttäminen useilla nettisivuilla (Hadlington

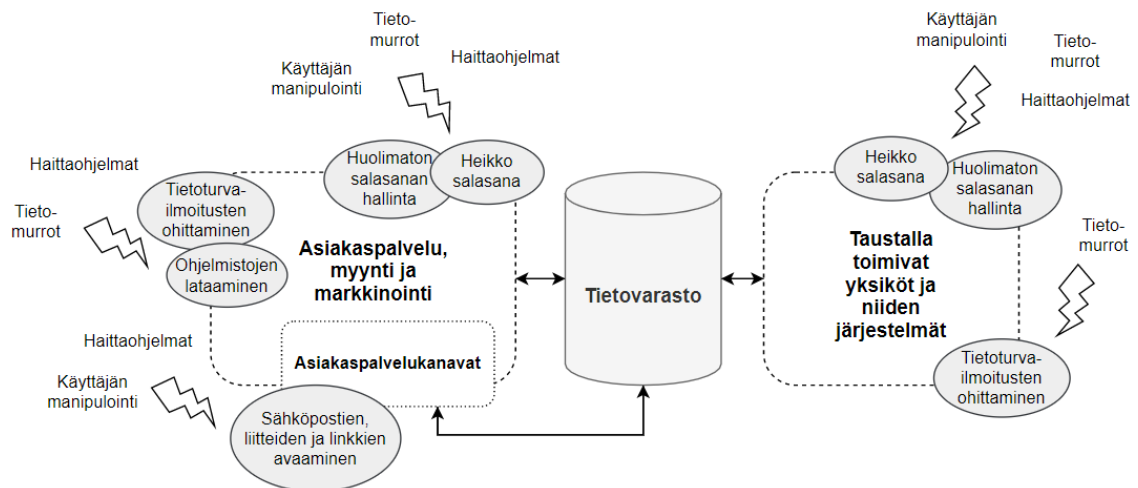
2017). Heikot salasanat antavat mahdollisuuden erilaisten tietoturvahyökkäysten onnistumiselle (Whitman & Mattord 2012, s. 67). Yleinen keino hyökkääjien keskuudessa salasanan varastamiselle on käyttäjän manipulointi, jonka tavoitteena on manipuloida uhria paljastamaan arkaluonteisia tietoja (Mouton 2014). Myös käyttäjien huolimaton salasanan hallinta saattaa antaa vallan haittaohjelmille tai hyökkääjille, jotka käyttävät hyökkäystaktiikkana käyttäjän manipulointia (Kyberturvallisuuskeskus 2021a). Onkin huoletuttavaa, että käyttäjien keskuudessa yksi suurin tietoturvariskin aiheuttaja on salasana, jonka avulla ulkopuolisilla olisi vapaa pääsy monen organisaation järjestelmiin ja niiden sisältämiin tietoihin.

Luvussa 4.2 esitellään Schneierin (2015, luku 17) lista ihmisiin keskittyvistä ongelmista, joista yksi on käyttäjien liian suuri luottamus järjestelmiä kohtaa. Myös tietoturva-asiantuntijoiden ylläpitämä sivusto WeLiveSecurity (2015) listaa yhdeksi vaaralliseksi tietoturvavirheeksi käyttäjien liiallisen luottamuksen, sillä tästä syystä käyttäjät avaavat huolettomasti tuntemattomilta henkilöiltä saaneita sähköposteja ja linkkejä, jotka saattavat sisältää haittaohjelmia. Tietojenkalastelulla hyökkääjät tavoittelevat suomalaisilta tyypillisimmin sähköpostin käyttäjätunnusta ja salasanaa, ja linkki tietojenkalastelusivustolle on voitu piilottaa esimerkiksi organisaation kokouskutsuun tai naamioituun turvapostiin (Kyberturvallisuuskeskus 2021b). Osa organisaation työntekijöistä aiheuttaa suuria tietoturvariskejä sähköpostien ja niiden liitteiden avaamisen lisäksi myös lataamalla verkkosivustoilta hyökkääjien naamioimia ohjelmistoja. Hyökkääjät ovat muun muassa päässeet organisaatioiden tietoihin käsiksi tarjoamalla organisaatioiden työntekijöille harhaanjohtavia ohjelmistoja, kuten väärennetyjä virustentorjuntaohjelmia, jotka ovat sisältäneet todellisuudessa vakoilu- tai haittaohjelmia. (Safa et al. 2016)

Norman (2009) käsittelee artikkelissaan käyttäjiä turvallisuuden vaarantajina, sillä hyvin omistautuneet ja järkevät ihmiset keksivät tahattomasti keinoja kiertää tehtäviä hidastavia, mutta turvallisuuden takaavia esteitä. Hänen mukaansa monien eri varoitusten ja ponnahdusikkunoiden takia käyttäjät klikkaavat kaikki ilmoitukset yleensä pois silmistä häirinnän estämiseksi, jolloin myös tärkeät tietoturvaan liittyvät päivitykset jäävät tekemättä ja järjestelmän turvallisuus heikkenee. Myös Schneier (2015, luku 17) tuo esiin, että käyttäjille on ominaista siirtyessään sivulta toiselle vain kuitata näytöltä ”OK”, vaikka kyseessä olisi varoituksena tietoturvariskistä noussut ponnahdusikkuna. Ihmiset eivät ajattele järkevästi, jos tietoturva tulee esteeksi työlle, joka on tehtävänä (Norman 2009; Schneier 2015, luku 17). Organisaatioiden työntekijöillä on useimmiten kaikilla oma työpaikalta saatu tietokone, ja tiedot järjestelmien päivityksistä saattavat tulla ponnahdusik-

kunana käyttäjälle tietoon. Mikäli järjestelmästä jää käyttäjien huolimattomuuden tai välinpitämättömyyden takia tärkeitä päivitykset tekemättä, järjestelmän tiedot saattavat olla välittömässä vaarassa.

Asiakkuudenhallintajärjestelmä pitää sisällään lähes kaikki tiedot organisaatiosta ja organisaation asiakkaista, joten tietoturvan toimivuus on erittäin tärkeää kyseisessä järjestelmässä. Jos tietoturva peittää asiakkaiden harmiksi ja asiakkaiden tiedot pääsevät sen takia väriin käsiin, luottamus organisaatiota kohtaan voi romahtaa. Asiakkuudenhallintajärjestelmässä kaikista tärkein osa turvata on siis analyttisen osan tietovarasto, johon kuitenkin linkittyy monta eri polkua järjestelmän rakenteessa. Mikäli hyökkääjä saisi pääsyn asiakkuudenhallintajärjestelmän tietovarastoon, voisi asiakkaiden ja organisaation tiedot olla vaarassa levitä eteenpäin tai kadota kokonaan kiristyksen uhalla. Kuvassa 6 on koottuna asiakkuudenhallintajärjestelmän eri osiin kohdistuvia yleisiä tietoturvariskit, jotka aiheutuvat käyttäjien tekemistä virheistä järjestelmässä.



**Kuva 5.** Asiakkuudenhallintajärjestelmään kohdistuvat tietoturvariskit

Asiakkuudenhallintajärjestelmä sisältää käyttäjien myötä useita heikkouksia eri rakenteen osissa, joiden kautta hyökkääjien on mahdollista päästä erilaisten hyökkäystapojen kautta järjestelmään. Kuvasta 6 huomaa, kuinka asiakkuudenhallintajärjestelmän jokaisesta eri osasta linkittyy polku organisaatioiden tarkoin suojaamaan tietovarastoon. Tyyppillisesti monella organisaation jäsenellä on pääsy johonkin asiakkuudenhallintajärjestelmän osaan pelkällä käyttäjätunnuksella ja salasanalla. Mikäli käyttäjä on huolimaton salasanan salaamisessa tai se on muuten helposti arvattavissa, hyökkääjällä on suurempi mahdollisuus päästä tietovarastoon tietomurron, käyttäjän manipuloinnin tai haittaohjelman kautta. Asiakkuudenhallintajärjestelmiä uhkaa myös käyttäjien toiminta silloin, jos he luulevat lataavansa turvallisen ohjelmiston netistä, mutta se onkin valheellinen ja pyrkii ainoastaan pääsemään haittaohjelman avulla käsiksi asiakkuudenhallintajärjestelmään ja sitä kautta arkaluontoiisiin tietoihin käsiksi. Käyttäjät vaarantavat myös silloin

asiakkuudenhallintajärjestelmän tiedot, kun järjestelmä lähettää heille tietoturvaan liittyviä ilmoituksia esimerkiksi päivityksistä, jotka käyttäjät kiireessä ohittavat. Lisäksi etenkin asiakaspalvelukanavien kautta käyttäjät saattavat tiedostamattaan sortua käyttäjän manipulointiin ja aukaista hyökkääjien lähettämiä sähköposteja, niiden liitteitä tai linkkejä, joiden tarkoituksena on ainoastaan saada käyttäjältä arkaluontoista tietoa tai asentaa haittaohjelma järjestelmään.

## 5. KÄYTETTÄVÄN TIETOTURVAN SUUNNITTELU ASIAKKUUDENHALLINTAJÄRJESTELMÄSSÄ

Uutta asiakkuudenhallintajärjestelmää suunniteltaessa yksi olennainen tavoite on tehdä siitä tietoturvallinen. Jotta järjestelmästä saadaan tietoturvallinen, käyttäjien näkökulma voidaan ottaa mukaan suunnitteluprosessiin hyödyntämällä erilaisia käytettävyyshauristiikkoja suunnittelun aikana. Luvussa 3.1 esitellään Nielsenin (1994) kymmenen heuristiikkaa, joita monet alan asiantuntijat hyödyntävät vielä vuosikymmenienkin jälkeen omilla käytettävyystudioissaan. Kyseisiä heuristiikkoja ei ole alun perin suunniteltu vastaamaan tietoturvan tuomiin haasteisiin, joten osa niistä ei ole olennaisia tämän työn kannalta. Tässä luvussa käydään läpi, miten käytettävyyshauristikat huomioiden voidaan suunnitella asiakkuudenhallintajärjestelmä, jossa luvussa 4.3 esitetyt käyttäjien tietoturvariskeihin johtavat virheet voidaan minimoida. Lisäksi esitellään Nielsenin (1994) heuristiikoista johdetut ja sovelletut suunnitteluohjeet tietoturvallisen asiakkuudenhallintajärjestelmän suunnitteluun.

Yksi iso haaste organisaatioissa on käyttäjien heikot salasanat tai niiden huolimaton hallinta. Organisaation työntekijät eivät välttämättä ymmärrä sitä, että taitavat hakkerit saattavat muutamissa sekunneissa hakkeroida heikon salasanan, jolloin heidän mielestään helposti näppäiltävä tai muistettava salasanana voi tuntua jopa loogiselta vaihtoehdolta. Järjestelmässä tulisikin siis olla ohjaileva ominaisuus, jolla tietämätönkin käyttäjä pystyy valitsemaan vahvan salasanan. Onkin tutkittu, että käyttäjän asettaessa tai vaihtaessa salasanansa järjestelmään välitön palaute salasanan vahvuudesta motivoi häntä valitsemaan vahvemman salasanan kuin ilman palautetta (Furnell et al. 2018). Nielsenin (1994) ensimmäinen käytettävyyshauristikka kannustaa oikea-aikaiseen palautteeseen, joka pitää käyttäjä ajan tasalla toiminnastaan. Asiakkuudenhallintajärjestelmässä tulisi siis antaa käyttäjän asettaessa salasanana välittömästi palaute salasanan vahvuudesta, jotta käyttäjä pystyy reagoimaan siihen asianmukaisella tavalla. Esimerkiksi surunaama syötekentän vieressä symboloi käyttäjälle heikkoa ja tietoturvan vaarantavaa salasanana, ja näin motivoi häntä asettamaan vahvemman salasanan (Furnell et al. 2018).

Välittömän palautteen lisäksi salasanan valinnassa olisi hyvä tarjota käyttäjälle selkeä polku tarkempiin ohjeisiin ja dokumentteihin, joista voisi tarkemmin tutustua esimerkiksi vahvan salasanan ominaisuuksiin (Furnell et al. 2018). Nielsenin (1994) kymmenes heuristiikka ohjaa toimintaa tukevien ja helposti saatavilla olevien ohjeiden tarjoamiseen käyttäjälle. Salasanan ominaisuuksiin liittyvä ohje olisi tärkeää tarjota käyttäjälle erityisesti silloin, jos palaute näyttää heikkoa turvallisuuden tasolla. Nykyään organisaatiot

osaavatkin usein vaatia jo tiettyjä ominaisuuksia salasanalta, joita sen tulee sisältää olakseen vaikeampi murtaa. Se aiheuttaa kuitenkin ristiriitaa käytettävyyden kanssa, sillä joskus vaatimukset voivat mennä niin korkeiksi, että käyttäjän on lähes mahdotonta muistaa salasanaansa, jolloin kasvaa todennäköisyys salasanan kirjoittamisesta lapulle tai älypuhelimien muistiinpanoihin. Tämä taas vaarantaa järjestelmän tietoturvan entisestään. Tähän käytettävyyden ja tietoturvan ristiriitaan ei ole yksiselitteistä vastausta vielä löydetty. Onkin kuitenkin selvää, että Nielsenin (1994) ohjeisiin kannustava heuristiikka täytyy ottaa käyttöön myös yleisten salasanan hallintaan liittyvien ohjeiden kohdalla, jotka opastaisivat käyttäjää toimimaan tietoturvallisesti salasanan kanssa.

Tietojenkalastelu ja muu käyttäjien manipulointi on ollut jo pitkään erittäin yleinen keino hyökkääjien keskuudessa päästä organisaatioiden tietoihin käsiksi (Kyberturvallisuuskeskus 2021b). Luvussa 4.3 todetaan, että salasanaan liittyvien ongelmien lisäksi myös tuntemattomilta saadun sähköpostin, liitteen tai linkin avaaminen on tyypillinen virhe organisaation käyttäjiltä. Erinomainen keino välttää tietojenkalastelun onnistumiselta on käyttäjien kouluttaminen, mutta tietojärjestelmän käytettävyydelläkin voidaan vaikuttaa tulokseen. Asiakkuudenhallintajärjestelmän eri osiin vaaditaan yleensä käyttäjältä kirjautumistiedot, jotta voidaan tunnistaa käyttäjän olevan organisaation työntekijä ja näin oikeutettu järjestelmän käyttöön. Kyberturvallisuuskeskus (2019) suosittelee, että järjestelmien kirjautumissivustot kannattaisi räätälöidä organisaatiossa tietyn graafisen ilmeen mukaan, jolloin käyttäjät tunnistavat oikean sisäänkirjautumissivuston hyökkääjän lähettämästä sivustosta ja näin tietojenkalastelun onnistuminen organisaation kirjautumistiedoilla on epävarmempaa. Tämä suositus muistuttaa myös Nielsenin (1994) neljättä heuristiikkaa, jonka mukaan suunnittelussa on tärkeää ottaa huomioon tilanteiden ja toimintojen yhteneväisyys toteutusympäristössä. Tästä voidaankin soveltaa suunnitteluohjeeksi organisaation ulkoasun yhteneväisyys ja standardit, jolloin tietojenkalastelu tekeytymällä organisaation jäseneksi olisi helpompi huomata. Tämä suunnitteluohje noudattaa myös viidettä heuristiikkaa, joka kannustaa virhealttiiden tilanteiden ehkäisemiseen jo suunnitteluvaiheessa.

Asiakkuudenhallintajärjestelmässä osa rakenteesta on usein liitettynä verkkoselaimen, jolloin myös muu selaimen käyttö vaikuttaa asiakkuudenhallintajärjestelmän tietoturvan tasoon. Sähköpostista saatujen linkkien avaamisen lisäksi käyttäjät vaarantavat organisaation tiedot lataamalla selaimesta turvalliselta vaikuttavia ohjelmistoja, jotka kuitenkin saattavat sisältää järjestelmään tunkeutuvia haittaohjelmia (Safa et al. 2016). Niin kuin aiemmin mainittiin, Nielsenin (1994) viides heuristiikka ohjaa järjestelmien kehittäjiä suunnittelemaan järjestelmä niin, että virheitä ei voi tapahtua. Tämän heuristiikan mu-

kaan organisaatio voisi estää työkoneella ohjelmistojen lataamisen netistä kokonaan ilman järjestelmänvalvojan lupaa, etenkin jos tietokone tulkitsee ohjelmiston epäilyttäväksi. Mikäli järjestelmä ei osaa arvioida ohjelmiston turvallisuutta, täytyisi käyttäjälle tulla kuitenkin yhdeksännen heuristiikan (Nielsen 1994) mukainen virheilmoitus, joka vaatii käyttäjän kielellä varmistuksen lataamisen turvallisuudesta. Nämä ominaisuudet voisivat ehkäistä vaarallisten ohjelmistojen lataamisen kokonaan, jolloin ei olisi vaaraa tietomurroista netistä ladattujen ohjelmistojen kautta.

Tietojärjestelmien käyttäjillä on ensisijaisena tavoitteena saada aina oma tavoite tehtyä valmiiksi, jolloin erilaiset epäselvät ponnahdus- tai varoitusikkunat häiritsevät heidän tekemistään, ja ilmoituksen sisältöä tutkimatta ne saatetaan vain hyväksyä tai klikata pois sen enempää välittämättä (Norman 2009; Schneier 2015, luku 17). Nielsenin (1994) yhdeksäs heuristiikka korostaa virheilmoitusten tärkeyttä ja varoitusikkunat itsessään jo toimivat virheilmoituksina käyttäjille, joten niitä ei missään nimessä kannata järjestelmästä poistaa. On kuitenkin suositeltavaa, että asiakkuudenhallintajärjestelmässä ruudulle tulevat varoitusikkunat ja ilmoitukset suunniteltaisiin käyttäjille sopiviksi, jolloin esimerkiksi Nielsenin (1994) toisen heuristiikan mukaan niiden tulisi puhua käyttäjän kieltä eli sisältää tuttuja käsitteitä ammattikielen sijasta. Selkeät ja käyttäjälle tuttua kieltä sisältävät tekstit auttavat käyttäjiä ymmärtämään ilmoituksen sisällön paremmin, jolloin on myös suurempi todennäköisyys sen noudattamiseen sekä tietoturvariskien pienenemiseen.

Aiemmin Nielsenin (1994) ohjeisiin kannustavaa kymmenettä heuristiikkaa sovellettiin palautteen ohella salasanan valintaa vahvistamaan. Salasanan muodostamiseen ja hallintaan liittyvien ohjeiden lisäksi olisi erittäin tärkeää, että käyttäjille olisi jatkuvasti tarjolla ja helposti saatavilla ohjeita ylipäätään tietoturvan ylläpitämiseen. Nämä ohjeistukset tulisi suunnitella Nielsenin (1994) toisen heuristiikan mukaisesti käyttäjän kielelle, jotta työntekijät eivät turhaudu niitä lukiessa siihen, että ohjeet ovat täynnä uusia erikoissanoja liittyen järjestelmän tietoturvaan. Asiakkuudenhallintajärjestelmän käyttäjien tulisi myös tietää, mistä osasta järjestelmää he löytävät tarvittaessa ohjeita esimerkiksi saadessaan epäilyttävän sähköpostin tuntemattomalta henkilöltä. Helposti saatavilla olevien ohjeiden lisäksi organisaatiot voisivat kouluttaa vahvalla tietoturvaosaamisella varustetun tukihenkilön (engl. power user), joka toimisi muille työntekijöille roolimallina ja apukätenä, jolta voisi kysyä tietoturvaan liittyviä kysymyksiä matalalla kynnyksellä (Guo et al. 2011). Mitä helpommin tietoa tietoturvaan liittyen on käyttäjille tarjolla, sitä todennäköisemmin käyttäjät myös käyttävät sitä hyödykseen.

Nielsenin (1994) kahdeksas heuristiikka suosittelee järjestelmän ulkoasusta poistettavan kaikki tarpeettomat tiedot käyttäjän nähtäviltä. Kyseinen minimalistisen suunnittelun

heuristiikka tukee CIA-mallin luottamuksellisuuden osa-aluetta, jonka mukaan järjestelmässä tulee asettaa tiedot vain niiden käyttöön oikeutettujen työntekijöiden saataville (Whitman & Mattord, s. 13). Asiakkuudenhallintajärjestelmässä on monta eri osaa, kuten asiakaspalvelu, myynti ja markkinointi, joiden käyttöoikeuksia voidaan suunnitella juuri työntekijöiden tarpeiden mukaan. Tämä myös parantaisi järjestelmän tietoturvaa, sillä hyökkääjän päästessä yhden työntekijän kautta järjestelmään käsiksi, voi kuitenkin suurin osa tiedoista pysyä turvassa käyttöoikeuksien rajaamisen ansiosta.

Tietojen turvallisuuden kannalta olisi myös tärkeää, että ainoastaan järjestelmän hallinnolla olisi oikeus kaikista kriittisimpiin alueisiin järjestelmässä, jolloin tavalliset käyttäjät eivät vaarantaisi niitä osia vahingossa (Realpe et al. 2016). Lisäksi käyttäjien on minimalistisen ulkoasun avulla mahdollista huomata, mikäli järjestelmässä on jotain normaalia poikkeavaa, joka voisi johtaa mahdollisen hyökkääjän jäljille. Minimalistinen suunnittelu parantaa tietoturvan myös CIA-mallin saatavuuden osa-aluetta, joka mahdollistaa tietoihin pääsyn ilman häiriöitä tai esteitä ilman viivästymistä (Whitman & Mattord 2012, s. 12; Gupta et al. 2019, s. 258).

Tietoturvallisen asiakkuudenhallintajärjestelmän suunnittelussa kannattaa huomioida luvussa 4.3 esitetyt käyttäjien virheet ja pyrkiä minimoimaan ne tiettyjen järjestelmään liitettävien ominaisuuksien tai elementtien avulla. Taulukkoon 3 on koottuna seitsemän olennaista suunnitteluohjetta tietoturvan näkökulmasta, joiden tarkoituksena on vähentää käyttäjistä aiheutuvia tietoturvariskejä asiakkuudenhallintajärjestelmässä. Nämä suunnitteluohjeet on sovellettu Nielsenin (1994) heuristiikoista, joista osa otettiin lähes sellaisenaan suunnitteluohjeisiin, osasta poimittiin tietoturvan kannalta olennaisin ehdotus, kun taas osasta tietoturvaan liittymättömistä heuristiikoista luovuttiin kokonaan.

**Taulukko 3.** Seitsemän olennaista suunnitteluohjetta tietoturvallisen asiakkuudenhallintajärjestelmän suunnitteluun

Suunnitteluohje	Perustelut	Ohjetta tukevat lähteet
<b>Oikea-aikainen palaute</b>	Oikea-aikainen palaute, esimerkiksi vahvan salasanan valintaan, motivoi käyttäjää noudattamaan palautteen antamaa ohjeistusta. Palaute ohjaa käyttäjää tietoturvallisempiin valintoihin ennen kuin vahinkoa on tapahtunut.	Nielsen 1994; Bertini et al. 2006; Petrie & Power 2012; Shneiderman et al. 2016
<b>Käsitteet käyttäjälle tutulla kielellä</b>	Käyttäjät eivät välttämättä ymmärrä tai edes huomioi ilmoituksia tai ohjeita, joiden käsitteet eivät ole tuttuja, vaikka kyseessä olisi tärkeä asia koskien tietoturvaa. Tuttu kieli tekee ohjeista myös helpommin lähestyttävämät.	Nielsen 1994; Bertini et al. 2006; Petrie & Power 2012

<b>Yhteneväisyys ulkoasussa</b>	Työntekijät voivat tunnistaa epäilyttävät organisaation mukaan naamioidut tietojenkalastelusivustot tai -sähköpostit helpommin, jos organisaatiolla on tietty yhtenäinen malli ulkoasussa.	Nielsen 1994; Bertini et al. 2006; Shneiderman et al. 2016
<b>Virhealtiiden tilanteiden ennakoiminen</b>	Kaikki käyttäjille virhealtiit tilanteet kannattaa pyrkiä karsimaan jo suunnitteluvaiheessa. Esimerkiksi järjestelmä voidaan suunnitella alusta alkaen estämään netistä ladattavat ohjelmistot työkoneelle, jotta niiden kautta haittaohjelmat ei pääse organisaation tietoihin käsiksi.	Nielsen 1994; Shneiderman et al. 2016
<b>Järjestelmän minimalistinen ulkoasu</b>	Minimalistinen ulkoasu tukee CIA-mallin luottamuksellisuuden ja saatavuuden osa-alueita sekä helpottaa järjestelmän käyttöä, mikä myös parantaa tietoturvan tasoa.	Nielsen 1994; Petrie & Power 2012
<b>Helposti ymmärrettävät virheilmoitukset</b>	Jokaista virhetilannetta ei voi estää etukäteen, joten virheilmoitukset tulee suunnitella niin, että ne kiinnittävät käyttäjän huomion ja ovat helposti ymmärrettäviä käyttäjälle tutulla kielellä.	Nielsen 1994; Petrie & Power 2012; Shneiderman et al. 2016
<b>Tietoturvaan liittyvien ohjeiden tarjoaminen</b>	Helposti saatavilla olevat ohjeet ja niiden tarjonta etenkin tietoturvaan liittyen antaa käyttäjille mahdollisuuden saada tarvittaessa vastaus kysymykseen ja parantaa käyttäjän tietoturvakäyttäytymistä turvallisemmaksi.	Nielsen 1994; Petrie & Power 2012

Käyttäjien aiheuttamia tietoturvariskejä ei luultavasti voida koskaan täysin estää, vaikka organisaatio kuinka panostaisi kouluttamiseen ja järjestelmien käytettävyyteen. Jatkossa tulisi kuitenkin panostaa uusien järjestelmien suunnittelussa yhä enemmän siihen, että kehittäjiä ja suunnittelijoita koulutettaisiin ajattelemaan järjestelmää käytettävyyden ja etenkin loppukäyttäjien näkökulmasta. Taulukossa 3 esitetyt ja kehittäjille suunnatut suunnitteluohjeet toimivat hyvänä lähtökohtana käyttäjien virheiden minimoimiselle tietoturvan näkökulmasta. Suunnittelussa tulee pitää mielessä se, että käyttäjien tekemät virheet johtuvat usein vain huonosta suunnittelusta eli huolellisella suunnittelulla ja virheiden ennakoimisella voidaan estää monet yksinkertaiset virheet, joiden seuraukset saattaisivat muuten olla organisaatiolle hyvinkin ikävät.

## 6. YHTEENVETO

Asiakkuudenhallintajärjestelmä mahdollistaa organisaation tietojen ja asiakassuhteiden kokonaisvaltaisen hallinnan sekä vuorovaikutuksen asiakkaiden kanssa. Se pitää sisälleen paljon arvokasta tietoa organisaation toiminnasta ja sen asiakkaista, mitä täytyy suojella pahantahtoisilta hyökkääjiltä. Järjestelmän käyttäjien toiminnalla on kuitenkin joskus negatiivinen vaikutus organisaation tietoturvan tasoon ja käyttäjien tietoturvariskeihin johtavia virheitä tulisikin ehkäistä uudessa järjestelmässä huolellisen suunnittelun avulla. Tutkimuksen viimeisessä luvussa esitellään tutkimuksen tulokset ja arvioidaan, miten tutkimus on kokonaisuudessaan onnistunut. Lisäksi käydään läpi tutkimuksen merkitystä ja esitellään mahdollisia jatkotutkimusehdotuksia.

### 6.1 Tutkimuksen tulokset

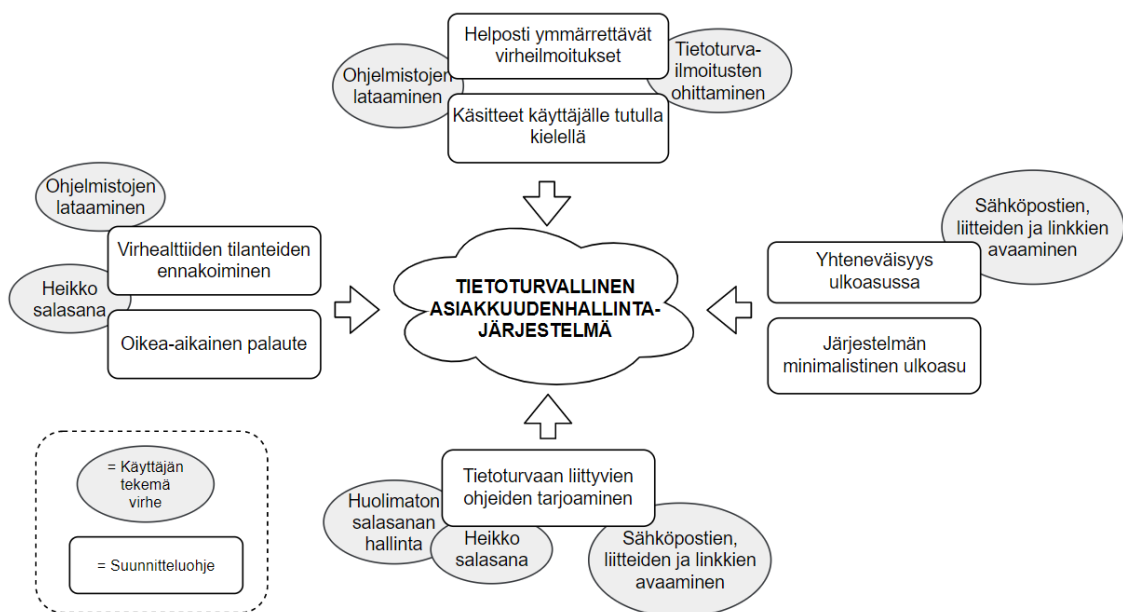
Tutkimuksen tavoitteena oli selvittää kirjallisuuskatsauksena, miten käytettävä tietoturva voidaan toteuttaa asiakkuudenhallintajärjestelmässä. Työssä tutkittiin ensimmäisen alatutkimuskysymyksen avulla käytettävyyden ja tietoturvan käsitteitä sekä niiden suhdetta toisiinsa, jota on jo pitkään pidetty ristiriitaisena. Toisen alatutkimuskysymyksen avulla tutkittiin käyttäjien toiminnan vaikutusta organisaation tietoturvan tasoon ja samalla esiteltiin yleisimpiä tietoturvariskeihin johtavia virheitä, joita käyttäjät tekevät asiakkuudenhallintajärjestelmässä. Kolmannen ja viimeisen alatutkimuskysymyksen vastaus saatiin yhdistämällä edellisten alatutkimuskysymysten pääkohdat, joiden avulla muodostettiin kokonaisuus suunnitteluohjeista, joita asiakkuudenhallintajärjestelmän suunnittelussa kannattaisi ottaa huomioon.

Tutkimuksessa havaittiin, että käyttäjien kouluttaminen on tärkeä osa organisaation tietoturvariskien minimoimista, mutta myös tietojärjestelmien käyttäjäkeskeisellä suunnittelulla voidaan saada käyttäjien tietoturvariskeihin johtavat virheet huomattavasti väheneväksi. Käytettävyyteen ja sen suunnitteluun liittyvissä julkaisuissa viitataan usein käytettävyyden asiantuntijan Jakob Nielsenin (1994) kehittämiin heuristiikkoihin, joista monet ovat toimineet myös muiden asiantuntijoiden kehittämien heuristiikkojen perustana. Myös tässä tutkimuksessa käytettiin Nielsenin heuristiikkoja pohjana käytettävyyden määritelmälle ja uusille suunnitteluohjeille.

Tutkimus osoitti, että tietojärjestelmissä käyttäjien tekemillä virheillä on suuri vaikutus tietoturvan tasoon. Yleisimmät käyttäjien tietoturvariskejä aiheuttavat virheet ovat heikot

salasanat ja niiden huolimaton hallinta, tavallisiksi ohjelmistoiksi naamioitujen haittaohjelmien lataaminen selaimesta, tietoturvailmoitusten ohittaminen sekä epäilyttävien sähköpostien, liitteiden ja linkkien avaaminen. Käyttäjien tekemät virheet vaikuttavat monessa eri asiakkuudenhallintajärjestelmän rakenteen osassa ja ne voivat johtua esimerkiksi heikosta koulutuksesta, huolimattomuudesta, laiskuudesta tai välinpitämättömyydestä.

Luvussa 5 yhdistettiin käytettävän tietoturvan ja asiakkuudenhallintajärjestelmän tietoturvaan liittyvät teoriat, sillä tavoitteena oli löytää ratkaisu asiakkuudenhallintajärjestelmässä esiintyviin virheisiin Nielsenin (1994) käytettävyysheuristiikkojen avulla. Käytettävyysheuristiikoista nostettiin tärkeimmiksi suunnitteluohjeiksi tietoturvan kannalta olennaisimmat osuudet, joista muokattiin vielä tarkemmat kokonaisuudet uusiksi suunnitteluohjeiksi (taulukko 2). Tutkimuksessa tärkeimmiksi suunnitteluohjeiksi korostuivat seuraavat seitsemän ominaisuutta: oikea-aikainen palaute, käsitteet käyttäjille tutulla kielellä, yhteneväisyys ulkoasussa, virhealttiiden tilanteiden ennakoiminen, järjestelmän minimalistinen ulkoasu, helposti ymmärrettävät virheilmoitukset ja tietoturvaan liittyvien ohjeiden tarjoaminen. Kuvaan 7 on koottuna työn keskeisimmät tutkimustulokset.



**Kuva 6.** Käyttäjien virheitä minimoivat suunnitteluohjeet tietoturvalliseen asiakkuudenhallintajärjestelmään

Tutkimuksen keskeisimmät tulokset kattavat yleiset tietoturvariskeihin johtavat käyttäjien tekemät virheet asiakkuudenhallintajärjestelmässä ja suunnitteluohjeet kyseisten virheiden vähentämiseen tai jopa ehkäisemiseen. Nämä suunnitteluohjeet ottavat huomioon

niin käytettävyyden kuin tietoturvan näkökulman eli ne pyrkivät tekemään järjestelmästä helposti käytettävän, jolloin myös tietoturva järjestelmässä paranee. Asiakkuudenhallintajärjestelmässä käytettävän tietoturvan suunnittelu tulee ottaa huomioon jokaisessa järjestelmän osassa, jotta tietoturvariskit saadaan minimoitua ja tietovaraston tiedot pidettyä suojattuna.

## 6.2 Tulosten arviointi

Tutkimuksen päätutkimuskysymyksestä saatiin jaoteltua selkeät alatutkimuskysymykset, jotka auttoivat pitämään työn tavoitteen mielessä selkeästi. Tutkimuksen rakenne muodostui pitkälti alatutkimuskysymyksiä perusteella, jonka ansiosta työ eteni luontevasti teoriakokonaisuus kerrallaan. Aineistoa sekä käytettävään tietoturvaan että käyttäjien vaikutuksesta organisaation tietoturvaan löytyi runsaasti. Tuoretta tutkimusaineistoa perusteoriaan esimerkiksi käytettävyydestä tai tietoturvasta oli haastavaa löytää, sillä monissa artikkeleissa, konferenssijulkaisuissa ja kirjojen luvuissa esiintyivät samat perusteokset tietyiltä tutkijoilta, vaikka suurin osa niistä onkin jopa yli 20 vuotta vanhoja.

Asiakkuudenhallinnasta ja sen eri osa-alueista liiketoiminnassa löytyi hyvin aineistoa eri tietokannoista, mutta suoraan asiakkuudenhallintajärjestelmiin liittyvää aineistoa oli tarjolla huomattavasti vähemmän ja kyseisen järjestelmän tietoturvaan tai käytettävyyteen hyväksi katsottuja lähteitä tämän työn puitteissa ei oikeastaan löydetty lainkaan. Tämä johti siihen, että aineistoa käyttäjien vaikutuksesta organisaation tietoturvaan hyödynnettiin eri konteksteista, jonka jälkeen tietoa sovellettiin asiakkuudenhallintajärjestelmään. Näin myös asiakkuudenhallintajärjestelmässä tapahtuvat virheet on päätelty aineistosta, jotka käsittelevät käyttäjien tekemiä virheitä tietojärjestelmissä yleisesti.

Asiakkuudenhallintajärjestelmä on yleinen ja jatkuvasti suositaan nostanut järjestelmä, joka löytyy monelta organisaatiolta päivittäisestä käytöstä. Tutkimuksien vähyyden asiakkuudenhallintajärjestelmien tietoturvasta saattaa kuitenkin johtua siitä, että organisaatiot eivät ole halukkaita julkisesti tuomaan esiin järjestelmiensä haavoittuvuuksia, jotta hyökkääjät eivät saa tietoa niiden heikkouksista. Tulevaisuudessa aiheesta olisi kuitenkin hyvä saada myös tutkimusaineistoa enemmän julkiseen jakoon, jotta tietoisuus käyttäjien vaikutuksesta järjestelmien tietoturvaan tunnistettaisiin vakavaksi ongelmaksi. Aineiston vähyyteen voikin tulla tulevaisuudessa muutos, sillä keväällä 2018 EU-maissa voimaan astunut tietosuoja-asetus GDPR (General Data Protection Regulation) pakottaa organisaatiot sakkojen uhalla julkistamaan tapahtuneet tietoturvaloukkaukset, kuten hakkeroinnit, kyberhyökkäykset tai haittaohjelmatartunnat, parantaakseen henkilötietojen suojaa ja tietosuojaoikeuksia (Tietosuojavaltuutetun toimisto 2021).

### 6.3 Jatkotutkimusehdotukset

Käytettävyyden ja tietoturvan välinen suhde on jo pitkään ollut kiistanalainen järjestelmien suunnittelussa, eikä kaikkiin ristiriitaisiin tekijöihin ole vielä löytynyt vastausta. Esimerkiksi vahvan salasanan vaatimukset tekevät salasanasta vaikeasti muistettavan, mutta helposti muistettava salasana ei ole taas tietoturallinen. Onkin selvää, että käytettävän tietoturvan ympäriltä löytyy vielä ristiriitaisuuksia eri järjestelmissä, joita voidaan lähteä tutkimaan vielä tarkemmin tulevaisuudessa.

Käytettävään tietoturvaan liittyy vahvasti käyttäjien näkökulma, joka on tässäkin tutkimuksessa ollut keskeisessä osassa. Jatkotutkimuksissa käytettävää tietoturvaa asiakkuudenhallintajärjestelmässä olisi loogista lähteä tutkimaan empiirisen tutkimuksen kautta hyödyntämällä oikeiden käyttäjien mielipiteitä sekä kokemuksia järjestelmästä ja sen ominaisuuksista. Tutkimus voitaisiin siis laajentaa organisaatioon, joka suunnittelee uuden asiakkuudenhallintajärjestelmän hankkimista ja siihen vaadittavia ominaisuuksia. Tutkimus voitaisiin toteuttaa tekemällä organisaation työntekijöille käytettävyydestä joko prototyyppien avulla tai vanhan järjestelmän kanssa, jotta tuloksia pystytään arvioimaan realistisesti oikeassa käyttöympäristössä.

Käytettävän tietoturvan rinnalla olisi hyvä tutkia myös suorituskyvyn näkökulmaa, sillä se saattaa helposti kärsiä, kun keskitytään ainoastaan käytettävyyteen, tietoturvaan tai molempiin. Näiden kolmen suhteesta voisi siis jatkaa tutkimusta ja kehittää asiakkuudenhallintajärjestelmälle suunnitteluohjeet, jotka ottaisivat käytettävän tietoturvan lisäksi suorituskyvyn näkökulman mukaan. Lisäksi käytettävän tietoturvan suunnittelua voisi tutkia organisaatioiden eri järjestelmissä tai yksityishenkilöiden käyttämissä sovelluksissa.

# LÄHTEET

- Bertini, E., Gabrielli, S. & Kimani, S. 2006. Appropriating and Assessing Heuristics for Mobile Computing. Proceedings of the working conference on advanced visual interfaces. ACM. pp. 119–126.
- Bosworth, S., Kabay, M. E. & Whyne, E. 2014. Computer security handbook. 6th edition. Hoboken, New Jersey: Wiley.
- Buttle, F. & Maklan, S. 2019. Customer Relationship Management: Concepts and Technologies. 4th edition. London: Routledge.
- Chai, W. 2021. Confidentiality, integrity and availability (CIA triad). TechTarget. Saatavilla (viitattu 4.4.2021): <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA>
- Chalmeta, R. 2006. Methodology for Customer Relationship Management. The Journal of systems and software. 79 (7), pp. 1015–1024.
- Chen, I. J. & Popovich, K. 2003. Understanding Customer Relationship Management (CRM): People, Process and Technology. Business process management journal. 9 (5), pp. 672–688.
- Chiasson, S., Biddle, R. & Somayaji, A. 2007. Even Experts Deserve Usable Security: Design guidelines for security management systems. SOUPS Workshop on Usable IT Security Management (USM).
- Cranor, L.F. and Garfinkel, S. 2004. Secure or Usable? IEEE Security & Privacy. 2(5), pp. 16–18.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. 2013. Future directions for behavioral information security research. Computers & Security. Vol. 32, pp 90–101.
- Dourish, P., Grinter, R. E., de la Flor, J. D. & Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and ubiquitous computing. 8 (6), pp. 391–401.
- Dyché, J. 2002. The CRM Handbook: A Business Guide to Customer Relationship Management. Boston: Addison-Wesley.
- Evans, M., He, Y., Maglaras, L. & Janicke, H. 2019. HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers & security. Vol. 80, pp. 74–89.
- Fayerman, M. 2002. Customer Relationship Management. New directions for institutional research. (113), pp. 57–68.
- Fink, A. 2019. Conducting Research Literature Reviews: From the Internet to Paper. SAGE Publications. 5th edition. Sage Thousand Oaks.
- Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W. & Li, N. 2018. Enhancing security behaviour by supporting the user. Computers & Security. Vol. 75, pp. 1–9.

- Garg, H., Choudhury, T., Kumar, P. & Sabitha, S. 2017. Comparison between Significance of Usability and Security in HCI. 3rd International Conference on Computational Intelligence & Communication Technology (CICT). IEEE, pp. 1–4.
- Garrido-Moreno, A. & Padilla-Meléndez, A. 2011. Analyzing the impact of knowledge management on CRM success: The mediating effects of organizational factors. *International Journal of Information Management*, 31 (5), pp. 437–444.
- Guo, K. H., Yuan, Y., Archer, N. P. & Connelly, C. E. 2011. Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28 (2), pp. 203-236.
- Gupta, B., Agrawal, D. P. & Wang, H. 2019. *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. Boca Raton: CRC Press.
- Hadlington, L. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*. 3 (7), e00346.
- Hargrave, M. 2020. Customer Relationship Management (CRM). Investopedia. Saatavilla (viitattu 4.3.2021): [https://www.investopedia.com/terms/c/customer\\_relation\\_management.asp](https://www.investopedia.com/terms/c/customer_relation_management.asp)
- Hassan, H. M., & Galal-Edeen, G. H. 2017. From usability to user experience. *International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*. IEEE, pp. 216–222.
- Hughes-Lartey, K., Li, M., Botchey, F. E. & Qin, Z. 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*. 7 (3), e06522–e06522.
- Inostroza, R., Roncagliolo, S., Rusu, C. & Rusu V. 2013. Usability heuristics for touchscreen-based mobile devices: update. *Proceedings of the 2013 Chilean Conference on human - computer interaction*. ACM, pp. 24–29.
- ISO 9241-11. 2018. Ergonomics of human-system interaction. Part 11: Usability: Definitions and concepts.
- ISO/IEC 25010. 2019. Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuARE). System and software quality models.
- ISO/IEC 27000. 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.
- Kale, V. 2015. *Implementing SAP CRM: The Guide for Business and Technology Managers*. Boca Raton, Florida. CRC Press.
- Kraemer, S. & Carayon, P. 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*. 38 (2), pp. 143–154.
- Kyberturvallisuuskeskus. 2019. Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. Saatavilla: <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf>

- Kyberturvallisuuskeskus. 2020. 10 tietoturvanäkymää vuodelle 2020. Saatavilla (viitattu 3.2.2021): <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/10-tietoturvanakymaa-vuodelle-2020>
- Kyberturvallisuuskeskus. 2021a. Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle. Saatavilla (viitattu 3.2.2021): <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-3-uhkaa-ja-3-ratkaisua-jokaiselle>
- Kyberturvallisuuskeskus. 2021b. Kybersää, helmikuu 2021. Saatavilla: [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4\\_helmikuu\\_2021\\_TLP\\_WHITE.pdf](https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_helmikuu_2021_TLP_WHITE.pdf)
- Liginlal, D., Sim, I. & Khansa, L. 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & security*. 28 (3), pp. 215–228.
- Mouton, F., Leenen, L., Malan, M.M. & Venter, H.S. 2014. *Towards an Ontological Model Defining the Social Engineering Domain*. Berlin, Heidelberg: Springer International Publishing.
- Nielsen Norman Group. 2020. 10 Usability Heuristics for User Interface Design. Saatavilla (viitattu 2.4.2021): <https://www.nngroup.com/articles/ten-usability-heuristics/>
- Nielsen, J. 1993. *Usability Engineering*. Academic Press, Boston, USA.
- Nielsen, J. 1994. Enhancing the explanatory power of usability heuristics. *Conference on Human Factors in Computing Systems – Proceedings*, pp. 152–158.
- Norman, D. 2009. When Security Gets in the Way. *Interactions* 16 (6), pp. 60–63.
- Norman, D. 2013. *The Design of Everyday Things: Revised and Expanded Edition*. New York: Basic Books.
- Nurse, J. R. C., Creese, S., Goldsmith, M. & Lamberts, K. 2011. Guidelines for usable cybersecurity: Past and present. *Third International Workshop on Cyberspace Safety and Security (CSS)*. IEEE, pp. 21–26.
- Oksanen, T. 2010. *CRM ja muutoksen tuska: Asiakkuudet haltuun*. Helsinki: Talentum Media.
- Petrie, H. & Power, C. 2012. What do users really care about? A comparison of usability problems found by users and experts on highly interactive websites. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2107–2116.
- Realpe, P. C., Collazos, C. A., Hurtado, J. & Granollers, A. 2016. A set of heuristics for usable security and user authentication. *Proceedings of the XVII International Conference on Human Computer Interaction*, pp. 1–8.
- Rogers, Y., Sharp, H. & Preece, J. 2011. *Interaction Design: Beyond Human-Computer Interaction*. 3rd edition. Chichester: Wiley.
- Safa, N. S., Von Solms, R. & Fitcher, L. 2016. Human aspects of information security in organisations. *Computer fraud & security*. 2016 (2), pp. 15–18.
- Sanastokeskus TSK ry. 2004. *Tiivis tietoturvasanasto*. Helsinki. Saatavilla: <https://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf>

- Sasse, M. A. & Flechais, I. 2005. Usable Security: Why Do We Need It? How Do We Get It? Security and Usability: Designing secure systems that people can use, pp. 13–30.
- Sasse, M. A., Brostoff, S. & Weirich, D. 2001. Transforming the ‘weakest link’ — a human/computer interaction approach to usable and effective security. BT technology journal. 19 (3), pp. 122–131.
- Schneier, B. 2015. Secrets and Lies Digital Security in a Networked World. 15th anniversary edition. John Wiley & Sons.
- Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S. & Elmqvist, N. 2016. Designing the User Interface: Strategies for Effective Human-Computer Interaction. Sixth Edition, Pearson.
- Smetters, D. K. 2008. Cyber security technology usability and management. Wiley Handbook of Science and Technology for Homeland Security: 1-1.
- Tietosuojavaltuutetun toimisto. 2021. Tietoturvaloukkaukset. Saatavilla (viitattu 16.4.2021): <https://tietosuoja.fi/tietoturvaloukkaukset>
- Vacca, J. R. 2017. Computer and Information Security Handbook. 3rd edition. San Francisco: Elsevier Science & Technology.
- WeLiveSecurity. 2015. 11 security mistakes you probably keep on making. Saatavilla (viitattu 9.4.2021): <https://www.welivesecurity.com/2015/07/22/11-security-mistakes/>
- Whitman, M. E. & Mattord, H. J. 2012. Principles of information security. 4th edition. Boston, MA: Course Technology, Cengage Learning.
- Whitten, A & Tygar, J. D. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. USENIX Security Symposium. Vol. 348, pp. 169–184.
- Whitten, A. & Tygar, J. D. 1998. Usability of Security: A Case Study. Carnegie Mellon University School of Computer Science Technical Report CMU-CS-98-155.
- Willison, R. & Warkentin, M. 2013. Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS quarterly 37(1), pp. 1–20.
- Yee, K. P. 2004. Aligning security and usability. IEEE Security & Privacy. 2 (5), pp. 48–55.
- Yle. 2020. Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Saatavilla (viitattu 2.4.2021): <https://yle.fi/uutiset/3-11612399>

## LIITE A: TUTKIMUKSEN KESKEISET LÄHTEET

JULKAISIJA(T)	JULKAISU- VUOSI	JULKAISU	JULKAISUN KESKEINEN SISÄLTÖ
Fayerman	2002	Customer Relationship Management	Julkaisuissa käydään läpi asiakkuudenhallinnan merkitystä ja esitellään asiakkuudenhallintajärjestelmän rakenne, joka koostuu analyyttisestä osasta, operationaalisesta osasta ja kollaboratiivisesta osasta.
Furnell et al.	2018	Enhancing security behaviour by supporting the user	Julkaisussa tutkitaan, miten käyttäjille annettu palaute salasanasta voi vaikuttaa myönteisesti vahvempiin salasana-avalintoihin.
Guo et al.	2011	Understanding Non-malicious Security Violations in the Workplace: A Composite Behavior Model	Julkaisussa tutkitaan järjestelmien käyttäjien motivaatiota tietoturvaohjeiden noudattamiseen ja nostetaan esiin ihmisten tietoturvariskeihin johtava käyttäytyminen organisaatiossa.
Gupta et al.	2019	Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives	Kirja perehtyy tietoturvan moniin eri osa-alueisiin niin teorian kuin käytännönkin tasolla.
Kale	2015	Implementing SAP CRM: The Guide for Business and Technology Managers	Kirjassa tutustutaan asiakkuudenhallintajärjestelmään liittyviin osa-alueisiin ja mitä organisaation tulee ottaa huomioon sen käyttöönotossa.
Nielsen	1994	Enhancing the explanatory power of usability heuristics	Artikkelissa esitellään eri käytettävyysheuristiikkoja, joista tärkeimmät ovat Nielsenin kokoamat kymmenen heuristiikkaa, joita on käytetty jo vuosikymmeniä julkaisun jälkeen pohjana useiden asiantuntijoiden kehittämille suunnitteluohjeille.

Norman	2009	When Security Gets in the Way	Artikkelin mukaan käyttäjakeskeisellä suunnitellulla järjestelmistä voidaan tehdä helpompia käyttää, mikä myös parantaa organisaation tietoturvaa.
Norman	2013	The Design of Everyday Things: Revised and Expanded Edition	Kirjassa korostetaan suunnittelun tärkeyttä, sillä Normanin mukaan käyttäjä pitää ottaa huomioon jo suunnittelussa. Ihminen ei siis ole syyllinen virheisiin, jos käytettävä asia on suunniteltu huonosti.
Safa et al.	2016	Human aspects of information security in organisations	Artikkelissa käydään läpi sitä, että tietoturvatekniikka ei voi taata tietoturvaa kokonaan organisaatiossa, vaan käyttäjien rooli tulee myös huomioida tietoturvan tasoa arvioitaessa.
Schneier	2015	Secrets and Lies Digital Security in a Networked World	Kirjan sisältö perustuu tietoturvallisten tietokoneverkoston rakentamiseen ja sen ympärillä oleviin aihealueisiin, kuten tietoturvauhkat, haavoittuvuudet ja käyttäjien osuus organisaation tietoturvaan.