
# Käyttäjälähtöiset tietoturvauhat organisaatiossa ja niiden hallinta

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytiede
LuK-tutkielma
Iiso Kramsu
20.12.2021

# Tiivistelmä

Digitalisoituminen on johtanut siihen, että organisaatioiden on tärkeä ylläpitää omaa tietoturvaansa. Tärkeimmässä roolissa ovat organisaatiossa liikkuvat ja työskentelevät ihmiset, jotka käyttävät päivittäin erilaisia omia ja organisaation laitteita työskennellessään. Organisaation etu ja mahdollinen uhka ovat nämä työntekijät ja laitteet, jotka voivat joutua tietoturvahyökkäyksen uhriksi.

Tutkielman alussa kerrotaan tietoturvasta, määritelmistä, historiasta ja tulevaisuudesta yleisesti. Tutkielmassa selvitetään yleisimmät käyttäjälähtöiset tietoturvauhat ja niiden hallintatavat organisaatioympäristössä. Näistä tietoturvauhista ja hallintatavoista annetaan organisaatioihin liittyviä esimerkkejä. Tutkielma toteutettiin kirjallisuuskatsauksena ja tutkimuksen tulokset pohjautuvat suoraan lähdekirjallisuuteen.

Lähdekirjallisuuden pohjalta nousseita tietoturvauhkia ovat: käyttäjien sosiaalinen manipulointi, tietojenkalastelu, käyttäjien laitteiden haittaohjelmat, käyttäjien laitteiden varkaudet ja palvelunestohyökkäykset. Tutkielmassa käsiteltävät tietoturvauhat ovat tämän päivän ongelmia erilaisille organisaatioille ja heidän työntekijöilleen.

Tutkielmassa esitellään seuraavat toteutukset tietoturvauhkien hallintaan: haittaohjelmien-, sosiaalisen manipuloinnin- ja palvelunestohyökkäyksen hallinta. Tutkielma esittää hyviä keinoja organisaation tietoturvanhallintaan. Tutkimuksen tuloksena esitetään kokonaiskuva käyttäjälähtöisistä organisaation tietoturvauhkista ja niiden hallintakeinoista.

*Avainsanat*
Tietoturva, tietoturvauhka, tietojenkalastelu, haittaohjelma

*Ohjaaja*
FT, yliopistonlehtori, Leena Arhippainen

# Lyhenteet

| | |
|---|---|
| AAA | Authentication, Authorization, Accounting |
| CIA | Confidentiality, Integrity, Availability |
| DDoS | Distributed Denial of Service |
| IBM | International Business Machines Corporation |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| SGL | Structured Query Language |
| USB | Universal Serial Bus |
| WLAN | Wireless Local Area Network |

# Sisällysluettelo

# 1. Johdanto

Syksyllä 2021 Oulun yliopisto joutui laajamuotoisen tietojenkalastelun uhriksi, kun opiskelijat ja henkilökunta vastaanottivat sähköpostiviestin, jossa pyydettiin vaihtamaan salasana omalle yliopiston sähköpostille. Huijaussähköpostiviesti lähettiin tuhansille ihmisille ja noin 700 opiskelijaa ja 50–60 henkilökunnan jäsentä joutuivat sen uhriksi. He menivät vaihtamaan salasanansa, jolloin vanha salasana joutui tietojenkalastelijan käsiin. Hyökkäys oli toteutettu erittäin hyvään aikaan, koska uudet opiskelijat olivat aloittaneet juuri opinnot ja salasanan vaihto toteutetaan vuosittain syksyllä. Tulevaisuudessa vastaavanlaiset hyökkäykset voidaan eliminoida kaksivaiheisella todennuksella, joka on eri paikoissa käytössä laajasti estämässä vastaavanlaisia tietojenkalasteluhyökkäyksiä. (Keski-Heikkilä, 2021.)

Suomessa on esiintynyt viime aikoina laajasti FluBot-haittaohjelman lähettämiä huijausviestejä, josta kyberturvallisuuskeskus on antanut varoituksen. Huijausviestejä on lähetetty kymmenille tuhansille suomalaisille. FluBot-haittaohjelma on kohdistettu Android-käyttöjärjestelmän käyttäjille, joilla on käytössä matkapuhelinliittymä. Haittaohjelma lähettää kohdekäyttäjille tekstiviestejä, joissa väitetään, että käyttäjä on saanut ääniviestin tai ilmoituksen matkapuhelinoperaattorilta ja pyydetään avaamaan viestissä oleva linkki. Linkki ei itsessään sisällä haittaohjelmaa, vaan se pyytää käyttäjältä luvan asentamiseen. FluBot-haittaohjelmalle tyypillistä toimintaa on ollut käyttäjätietojen varastaminen ja laitteesta uusien haittaohjelmaviestien lähetys seuraaviin laitteisiin. Kyberturvallisuuskeskuksen mukaan FluBot-ohjelma on lähettänyt arviolta 70 000 viestiä 25. marraskuuhun 2021 mennessä. (Siikaluoma, 2021.)

Digitalisoituminen on muuttanut organisaatioiden käyttäjäpohjaisia tietoturvauhkia. Organisaatioiden yksi suurimmista tietoturvaan vaikuttavista uhkatekijöistä on työntekijät, jotka työskentelevät organisaation sisällä. Aikaisemmin organisaatioiden työntekijät ovat käyttäneet eri laitteita ja eri salasanoja omissa ja organisaation laitteissa. Laitteiden fyysisen koon pienentyessä ja tehon kasvaessa käyttäjät käyttävät yhtä ja samaa laitetta työhön ja henkilökohtaiseen käyttöön. Tämä mahdollistaa huomattavasti paremman joustavuuden ja tehokkuuden laitteiden päivittäisessä käytössä. He käyttävät päivittäin omia laitteitaan ja organisaation dataa töissä ja töiden ulkopuolella. Välillä kuva siitä, mitä omalla tai organisaation laitteella voi ja ei voi tehdä saattaa hämärtyä ja tämä voi altistaa organisaation mahdolliselle tietoturvariskille. (Annansingh, 2020.)

Tutkielman tarkoituksena on selvittää yleisimmät käyttäjälähtöiset tietoturvauhat ja niiden hallintatavat organisaatio ympäristössä. Tutkielmassa kuvataan perinteisempiä organisaatioiden tilanteita ja toimia, jolloin organisaation tietoturva voi olla uhattuna. Tutkielmassa kuvataan myös tietoturvauhkien hallintakeinot, joita organisaatio voi kohdata käyttäjien toimesta. Tutkielma pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

Tutkimuskysymys 1: Mitä erilaisia tietoturvauhkia organisaatiot voivat kohdata käyttäjien toimesta?

Tutkimuskysymys 2: Millaisilla toimilla voidaan parantaa organisaation tietoturvaa?

Tutkielmassa esitellään tietoturvaan liittyvät perusteet ja mitä on tietoturva yleisesti, jonka pohjalta käydään läpi organisaatioympäristössä kohdattavat tietoturvauhat käyttäjien toimesta, joita ovat: käyttäjien sosiaalinen manipulointi, tietojenkalastelu ja haittaohjelmat.

Käyttäjäpohjaisista organisaation tietoturvauhkien hallintamuodoista tutkielmassa esitellään seuraavat: haittaohjelmien-, sosiaalisen manipuloinnin-, tietojenkalastelun-, ja palvelunestohyökkäysten hallinta.

Tutkielman tutkimusmenetelmänä käytettiin kirjallisuuskatsausta, jonka lähdeaineistona toimii aiheeseen liittyvät kirjallisuus, tiedejulkaisut ja raportit. (Snyder, 2019). Tutkielman lähdekirjallisuusuutta on kerätty seuraavista palveluista: Google Scholar (http://scholar.google.fi/) ja Scopus tietokannasta (https://www.scopus.com). Lähdekirjallisuuden valinnassa otettiin huomioon kirjoittajan tunnettavuus ja lähdetiedon alkuperä.

# 2. Tietoturva

Tietoturva on monessa tilanteessa laajasti käytetty termi, jolle on nimetty monia eri määritelmiä riippuen kontekstista. Tästä johtuen tietoturvan yksi yleinen määritelmä puuttuu kokonaan. Tietoturva on erittäin moniulotteinen ja laajalti eri konteksteissa käytetty termi. (Craigen ym., 2014.)

## 2.1 Tietoturvan historiaa

Tietoturvaan liittyvät kysymykset eivät ole uusi keksintö. Sillä on kestänyt puoli vuosisataa kehittyä tähän pisteeseen, missä tänä päivänä olemme. Se oli jo vuosikymmeniä olemassa ollut tieto, joka huomioitiin tarkemmin 1990-luvun puolessa välissä, kun suuret tahot alkoivat tunnistaa sen vaikutuksia sen aikaiseen laitteistoon ja tietoliikenteeseen. (Warner, 2012.)

Puolijohteiden kehittymisen myötä ihmiset ovat saaneet käyttöönsä sellaista laskentatehoa, josta ei voitu edes unelmoida vuosisataa aiemmin. Samanaikaisesti tietoliikenneyhteydet ovat yhdistäneet miljardit ihmiset toisiinsa maailmanlaajuiseen viestintään. Näiden asioiden kasvu on johtanut myös tietoturvahaavoittuvuuksien nopeaan nousuun. (Warner, 2012.)

Tietokoneiden kommunikointi toistensa kanssa verkkojen sisällä alkoi 1960-luvulla. Siihen aikaan oli hyvin tavanomaista, että useimmat ihmiset eivät olleet nähneet varsinaista tietokonetta. Tietokoneet olivat tuolloin suuria fyysiseltä kooltaan ja kalliita käyttää, koska ne vaativat paljon tehoa toimiakseen ja tietäviä asiantuntijoita niiden käyttämiseen. Tähän aikaan tietokoneet säilöttiin suuriin konesaleihin ja halleihin suuren kokonsa vuoksi. Koneiden vuokraus oli myös hyvin yleistä tähän aikaan suuren hinnan vuoksi ja tietoturvasta pidettiin huolta siten, että tietokoneella ei voinut nähdä toisen käyttäjän toiminnassa olevia ohjelmia tai tietoja. (Warner, 2012.)

1970-luvulla otettiin käyttöön uusia innovaatioita, kuten järjestelmänvalvojan oikeudet, tiedostojen järjestelmäluvat, salauksella toimivat hajautetut salasanat ja tietokoneiden välillä kulkevan tiedon salaus. IBM aloitti kaupallisella puolella ensimmäiset pankkisiirtojen salaukset ja tarjosi siihen käyttämäänsä algoritmia Yhdysvaltojen kauppaministeriön alaiselle teknologian kehityksen virastolle NIST:lle. Tämän jälkeen tiedonsalaus-standardi otettiin käyttöön suuressa mittakaavassa NSA:n eli kansallisen turvallisuusviraston toimesta. (Warner, 2012.)

1980-luvulla tietokoneiden väliset verkot yleistyivät globaalisti ja samanaikaisesti alkoi tietokoneiden ja ohjelmistojen laajempimuotoinen hakkerointi ja virusten levitys. Tietoturva-asiantuntijat tiesivät tuohon aikaan nämä haavoittuvuudet ja miten ne tulisivat leviämään verkon välityksellä ja paikallisesti esimerkiksi. yritysten sisäpiirissä. (Warner, 2012.)

1990-luvulla tietoisuus tietoturvan merkityksestä levisi maailmalla, kun Morris matohaittaohjelma hidasti internettiä 1988 vuoden loppupuolella ja 1992 Michaelangelo-virushaittaohjelma saastutti ja levisi käyttöjärjestelmien sisällä. Ensimmäiset julkisesti tunnetut palvelunestohyökkäykset käynnistyivät 1996 New Yorkissa, kun PANIX-hyökkäys toteutui. Näiden tietoturvaan liittyvien hyökkäysten johdosta suuri laitteiden ja tietoverkkojen käyttäjäyleisö, sai varoituksen siitä, miten tärkeä tietoturva tulisi olemaan jatkossa. (Warner, 2012.)

## 2.2 Tietoturvan määritelmiä

Kirjallisuudesta löytyy monia määritelmiä tietoturvasta. Esimerkiksi Kemmereren (2003) mukaan tietoturva koostuu enimmäkseen puolustusmekanismeista, joita käytetään havainnoimaan mahdollisia tunkeilijoita. Esimerkkinä tällaisesta tunkeilijasta on Sapphire/Slammer SQL -mato.

Tietoturva antaa tietoverkoille, laitteille ja niiden sisältävälle tiedolle suojan haittaohjelmia ja murtoa vastaan. Tietoverkkojen käytön yleistyessä yhdeksi merkittävimmistä osista valtion toimintaa ja liiketoimintaa on suojauksen oltava kunnossa, jotta säästytään vakavilta seurauksilta virastoille, yksityishenkilöille ja yrityksille. (Lewis, 2006.) Amoroson (2006) mukaan tietoturvan tulee vähentää riskiä haittaohjelmien hyökkäyksiltä ohjelmistoihin, laitteisiin ja tietoverkkoihin.

Tietoturva on myös erilaisten työkalujen yhdistämistä, jotta voidaan suojata organisaation ja käyttäjän ympäristöä mahdollisia riskejä vastaan. Tietoturvaan liittyvien tekniikoiden tavoitteena on saavuttaa järjestelmälle tai laitteelle seuraavia asioita: tiedon saatavuus, tiedon eheys, tiedon oikeus ja tiedon luottamuksellisuus Tietoturvan pääasiallinen tehtävä on luoda turvaa eri sidosryhmille. (ITU, 2009.) Tietoturva on myös toimenpide, joka turvaa sähköisten tietojen tai tietokantojen luvattoman käytön. (Craigen, 2014).

Craigen ym., (2014) ovat kehittäneet tietoturvalle uuden kokonaisvaltaisemman käsitteen tutkimuksissaan. Tietoturva pitäisi määritellä seuraavalla tavalla: Tietoturva tulee käsitellä kokonaisuutena, joka sisältää siihen liittyvät prosessit, resurssit ja rakenteet, jotka mahdollistavat järjestelmien ja verkkojen suojauksen erilaisilta uhkatekijöiltä.

## 2.3 Tietoturvan osa-alueet

Tietoturva on voitu vuosien ajan jakaa kolmeen osa-alueeseen CIA-mallin avulla: luottamuksellisuus (*Confidentiality)*, eheys (*Integrity)* ja saatavuus (*Availability)*. Luottamuksellisuus tarkoittaa tietoturvallisuuden osalta sitä, että tietylle henkilölle tai organisaatiolle kuuluva tieto on hallinnassa oikeilla ihmisillä ja järjestelmillä. Eheydellä tarkoitetaan tiedon eheyttä eli sen tulee pysyä muuttumattomana, kun sitä vastaanotetaan, luetaan, lähetetään ja siirretään. Saatavuudella tarkoitetaan tiedon käsiksi pääsyä tarvittaessa. CIA-malli on ajateltu myös vanhanaikaiseksi, joten on kehitetty muita vastaavia tietoturvan osa-alueiden malleja. (Ham, 2021.)

AAA-malli (*Authentication, Authorization, Accounting)* jakautuu kolmeen osa-alueeseen. Ensimmäisenä on todennus, jolla todistetaan, että olet oikea henkilö pääsemään tietoon käsiksi. Todennus vaatii sen, että täytät esimerkiksi jonkun näistä kolmesta: salasana, sormenjälki tai kaksivaiheinen tunnistautuminen. Toiseksi on valtuutus eli sinulla pitää olla tietyt käyttöoikeudet laitteelle, ohjelmalle tai prosesseille. Vääränlaiset tehtävän ei vaativat käyttöoikeudet altistavat helpommin mahdollisille rikkomuksille liittyen luotettavuuteen, eheyteen ja saatavuuteen. Kolmantena on kirjanpito, joka tarkoittaa tietoa siitä, mitä käyttäjät tekevät ollessaan järjestelmään kirjautuneena. Kirjanpidon merkitys tietoturvarikkomuksen jäljityksen onnistumisessa on todella suuri. (Nweke, 2017.)

## 2.4 Tietoturvan tulevaisuus

Tekoälyn ja koneoppimisen käytön kiihtyminen viime vuosina on alkanut vaikuttaa kaikkiin eri teknologian käyttäjien osapuoliin. Samanaikaisesti tietoturvaan liittyvien hyökkäysten torjunta on vaikeutunut ja niiden tunnistaminen on haastavampaa. Ratkaisuna uudenlaisiin tietoturvahyökkäyksiin tulevaisuudessa voi olla koneoppiminen, jonka avulla aikaisempaa tietoturvahyökkäyksen dataa keräämällä pystytään tehokkaammin torjumaan uudet uhat. Toinen merkittävä tietoturvallisuudessa käytettävä työkalu tulee olemaan tekoälyjärjestelmät, jotka pystyisivät tunnistamaan tulevat tietoturvahyökkäykset ja torjumaan ne tehokkaimmalla oikealla tavalla. Tämä myös säästäisi esimerkiksi organisaatioiden IT-henkilöstön resursseja muihin tärkeämpiin tehtäviin. Tekoälyjärjestelmien hyvänä ominaisuutena tietoturvan parantamiseen on myös virheiden vähäinen määrä tietoturvahyökkäysten torjunnassa. (Geluvaraj, Satwik & Kumar, 2019.)

# 3. Käyttäjälähtöiset tietoturvauhat organisaatiossa

Seuraavaksi käydään läpi erilaisia organisaatioihin kohdistuvia tietoturvauhkia, joille organisaation työntekijät ja itse organisaatio voivat altistua.

## 3.1 Käyttäjän sosiaalinen manipulointi

Sosiaalinen manipuloinnin pääasiallinen tarkoitus on saada tietoa hyökkäyksen kohteeksi joutuneesta organisaatiosta sen työntekijän avulla. Tällöin hyökkäystä ei kohdenneta suoraan organisaation järjestelmiin tai laitteisiin. Hyökkäys tapahtuu epäsuorasti organisaation työntekijän kautta ja yleisesti kohteena ovat vaikutusvaltaiset henkilöt organisaatiossa. Näillä ihmisillä on useasti arkaluontoisempaa tietoa ja pääsy useaan organisaation kohteeseen, josta tietoa voidaan saada. Hyökkääjien tehtävänä on manipuloida työntekijä luovuttamaan arkaluontoisia salattuja ja luotettuja tietoja. He voivat myös manipuloida työntekijän suorittamaan jonkun toimenpiteen, jolloin työntekijä tekee itse hyökkäyksen kohdeorganisaatioon tietämättä asiasta. (Krombholz, Hobel, Huber, & Weippl, 2015.)

Sosiaalisen manipuloinnin ensimmäisessä lähestymistavassa hyökkääjä suorittaa fyysisen hyökkäyksen, jossa se etsii kohteena olevasta käyttäjästä henkilötietoja ja työskentelyorganisaation liittyviä tietoja. Hyvin yleisesti käytetty fyysinen hyökkäys on etsiä tietoa kohdehenkilön roskalaatikosta (Cranger, 2001). Tällaisessa hyökkäyksen muodossa hyökkääjä kaivaa kohdehenkilön tai organisaation roskalaatikkoa löytääkseen, jotain arvokasta ja herkkäluontoista tietoa. Tällaisia tietoja ovat organisaation henkilötiedot, dokumenttipaperit, kalenterit, käyttäjätunnukset ja salasanat. Tilanteessa, jossa fyysinen hyökkäys tapahtuu suoraan organisaation tiloihin hän voi mahdollisesti löytää vielä salatumpia tietolähteitä. Sosiaalisen manipuloinnin hyökkääjällä on myös mahdollisuus toteuttaa hyökkäys, joka sisältää esimerkiksi kohdeorganisaation kiristystä sen työntekijän välityksellä. (Krombholz ym., 2015.)

Käänteinen sosiaalinen manipulointi tekee hyökkäyksestä nimensä mukaan käänteisen. Tässä tilanteessa hyökkääjä on suoraan yhteydessä kohteena olevan organisaation työntekijään ja hänen tavoitteenansa on olla uskottava taho, jota kohdehenkilö uskoisi ilman epäilyksiä. Käänteinen sosiaalinen manipulointi koostuu kolmesta siihen liittyvän tekniikan osa-alueesta: sabotointi, mainostaminen ja avustaminen. (Krombholz ym., 2015.)

Ensimmäisenä hyökkääjän tehtävänä on sabotoida kohdeorganisaation järjestelmä tai laite. Tällainen sabotointi voidaan toteuttaa esimerkiksi kytkemällä kohdeorganisaatio pois verkosta tai vaikuttaa sen järjestelmiin ja ohjelmistoihin. Tämän vian ilmentymisen jälkeen hyökkääjä lähestyy organisaation kohdehenkilöä ja tarjoaa omia palveluitaan auttaakseen ongelman ratkaisussa. Tilanteessa, jossa hyökkäyksen kohde hyväksyy avun ongelman korjaukseen, tilanteeseen astuu sosiaalinen manipuloija, joka tulee korjaamaan itse aiheutetun ongelman. Tässä tilanteessa sosiaalisella manipuloijalla on mahdollisuus saada kohdeorganisaatioon liittyvä salasana tai pääsy johonkin sen järjestelmään. Täten hyökkääjä voi hyötyä saamistaan tiedoista. (Krombholz ym., 2015.)

## 3.2 Tietojenkalastelu

Tietojenkalastelu tavoittelee yleensä suurta kohdeyleisöä ja sen tarkoituksena on houkutella kohteena olevia kohdeorganisaation henkilöitä syöttämään heidän arkaluonteisia tietojansa, kuten esimerkiksi salasanoja, tunnuksia, ja pankki- tai luottokortin numeroita. Nämä hyökkääjä varastaa väärennettyjen verkkosivujen avulla, joihin sillä on hallinta. Käyttäjätietojen avulla hyökkääjä voi saada käyttöönsä monet eri tiedot, joilla voi olla pääsy esimerkiksi organisaation tietokantaan. Kohdeorganisaation työntekijän tiedot voidaan kerätä esimerkiksi sosiaalisten verkostojen avulla, josta saadaan helposti perustiedot, kuten nimi, sähköpostiosoite ja puhelinnumero. Tietojenkalastelusähköposteissa hyökkääjän tavoitteena on vakuuttaa kohdehenkilö klikkaamaan haitallisia linkkejä tai muita liitetiedostoja, joka mahdollistaa hyökkäyksen kohteena olevalle koneelle haittaohjelman asennuksen tai tunnuksien ja salasanojen varastamista. (Krombholz ym., 2015.)

Tietojenkalastelutavat kohdennetaan erilaisilla tekniikoilla. Keihäsmainen tietojenkalastelu kohdistaa tietojenkalastelun sähköpostin välityksellä tietylle kohderyhmälle, eikä vain lähetä tietojenkalastelusähköpostiviestejä satunnaisesti valituille käyttäjille. Keihäsmaisen tietojenkalastelun toteuttamiseksi hyökkääjän tulee etsiä potentiaaliset hyökkäyksen kohteet, jonka jälkeen hyökkäys toteutetaan siten, että se näyttää tulevan luotettavalta lähteeltä. Keihäsmaisen tietojenkalastelun yksi muoto on Whaling, jossa kohdehenkilöiksi valitaan korkean tason henkilöitä. Näitä ovat esimerkiksi yritysten toimitusjohtajat ja virkamiehet. (Chaudhry, Chaudhry & Rittenhouse, 2016.)

### 3.2.1 Linkkien avulla tietojenkalastelu

Tietojenkalastelun toteutuksista yksi yleisimmistä tavoista on suurien sähköpostiviestimäärien lähetys, jotka sisältävät jonkunlaisen linkin tietojenkalastelijan itse luomalleen sivustolle. Hyökkäyksen toimivuus perustuu sähköpostin ja sivuston linkin huoliteltuun ulkonäköön, jota hyökkäyksenä oleva henkilö tai organisaatio ei epäile millään tasolla. (Moore & Clayton 2007.)

Tutkimuksessa, jossa seurattiin 62 000 työntekijän tietojenkalastelusähköposteja kuuden viikon ajalta voitiin todeta, että kohdehenkilöt painoivat suuremmalla todennäköisyydellä saamaansa sähköpostiviestin linkkiä, jos he olivat sillä hetkellä oman organisaation tiloissa, jossa oli myös samanaikaisesti heidän muita työntekijöitä. Työntekijä painoi myös linkkiä suuremmalla todennäköisyydellä, jos hänellä oli kiireinen tilanne töissä. (Williams, Hinds & Joinson, 2018.)

### 3.2.2 Väärennetyt verkkosivut

Väärennettyjen verkkosivujen luominen toimii yleisenä tietojenkalastelun muotona. Tässä tietoa kalastetaan kohdekäyttäjältä siten, että hänet vakuutetaan menemään verkkosivustolle, jossa käyttäjän tai organisaation henkilökohtaista tietoa kerätään. Väärennettyjen verkkosivujen tehokkuus perustuu sivuston nimen muotoon, joka on hyvin lähellä olemassa olevaa sivustoa. Esimerkkinä verkkosivujen väärentäjä luo sivuston nimeltään www.mooddle.fi, jossa kirjaimia muokkaamalla sivusto näyttää nopeasti katsottuna oikeanlaiselta, mutta todellisuudessa se ei sitä ole. (Hong, 2012.)

### 3.2.3 Evil twin -tiedonkalastelu

Evil twin eli paha kaksonen tietojenkalasteluhyökkäys toteutetaan WLAN-verkossa, jossa yksi langattoman verkon piste kalastelee tietoa kohdekäyttäjältä. Tukiaseman pystyttäjä on muokannut sen näyttämään täysin luotettavalta langattoman verkon lähteeltä, mutta samanaikaisesti hyökkääjä voi seurata verkossa tapahtuvaa liikennettä. Hyökkäyksen tehokkuus perustuu siihen, että hyökkääjä voi mennä julkisen verkon kohteeseen esimerkiksi lentoasemalle. Paikan päällä hyökkääjä asettaa julkisen verkon toimintaan omalla tietokoneella tai puhelimella ja käyttää siinä samaa verkkotunnusta ja yhteyden taajuutta lentoaseman verkon kanssa. Kohteena oleva käyttäjä kohdistuu helposti hyökkäykselle, koska se on asettanut laitteensa etsimään saatavilla olevia verkkoja esimerkiksi lentoaseman tietyllä verkkotunnuksella ja taajuudella tietämättään. Tällöin hyökkääjän on vain annettava vahva signaali kohdekäyttäjän läheltä ja hän joutunut tietojenkalastelun uhriksi. Manuaaliset verkon valitsijat joutuvat myös helposti vääränlaiseen langattomaan verkkoon, koska he valitsevat useasti signaalin vahvuuden perusteella verkon. (Song, Yang & Gu, 2010.)

### 3.2.4 Clickjacking-tiedonkalastelu

Clickjacking eli klikkausten tahallinen kaappaus tiedonkalasteluhyökkäyksen tarkoituksena on saada kohteena oleva henkilö suorittamaan toiminto, jota käyttäjä ei alun perin aikonut suorittaa. Tälle voi altistua graafista sisältöä sisältävien sivustojen käyttäjät. Nykyaikaiset verkkosivut sisältävät useasti tällaista graafista sisältöä, joita voivat olla esimerkiksi käyttöliittymän päällä olevat elementtikuvakkeet. Klikkausten kalastelussa käytetään myös kursoriin liittyvää kaappausta, jossa kohdekäyttäjä luulee näkevänsä kursorinsa oikeassa kohdassa, mutta painaa sivustolla samanaikaisesti eri kohdasta. (Jamwal & Sharma, 2018.)

## 3.3 Käyttäjän tietokone ja mobiililaitteiden haittaohjelmat

Erilaisten sovelluksien ja ohjelmiston helppo saatavuus käyttäjien mobiililaitteille lisää riskiä saada latauksen mukana haittaohjelma ja mahdollinen hyökkäys laitetta vastaan. Samaan aikaan mobiililaitteilla on heikompi suojaus mahdollisia hyökkäyksiä ja haittaohjelmia vastaan, jonka takia ne houkuttelevat hakkereita ja haittaohjelmien tekijöitä hyökkäyksen kohteeksi. Mobiililaitteen saastuessa haittaohjelmalla se voi aiheuttaa: häiriöitä käyttäjän suorittamiin operaatioihin laitteella, vahingoittaa laitteen järjestelmää, tietojen menetystä ja vuotaa laitteesta esimerkiksi organisaation tai käyttäjän tietoja. (Peng, Yu, & Yang, 2014.)

Erilaiset haittaohjelmat jaetaan kolmeen kategoriaan niiden toimintatavan perusteella (Sanford, 2010.):

1. Haittaohjelma, joka kopioi itsensä ja luo uusia kopioita. Käyttäjä voi tietämättään luoda uuden haittaohjelman passiivisesti.
2. Käyttäjien kasvuun perustuva haittaohjelma, joka ei luo itsestään kopioita, vaan toiset käyttäjät luovat uuden luonnoksen siitä tietämättään.
3. Parasiittihaittaohjelma, joka käynnistää itsensä, kun jokin toinen ohjelma laitetaan suoritukseen.

Haittaohjelman perimmäinen tarkoitus on vahingoittaa tai häiritä järjestelmää tai laitetta. Haittaohjelmia ovat seuraavat: virus, troijalainen, vakoiluohjelma, mato, rootkit, backdoor ja Botnet. (Peng ym., 2014.)

### 3.3.1 Virus- ja mato-haittaohjelmat

Virus haittaohjelmana toimii siten, että se siirtyy käyttäjän laitteelle jonkun laitteiston tai ohjelmiston kautta ilman, että käyttäjä tietää tästä. Virus ensin kopioi itsensä käyttäjän laitteelle, jonka jälkeen se alkaa toteuttamaan sille ohjelmoituja tehtäviä. Näitä tehtäviä ovat esimerkiksi tietovauriot, ohjelmistovauriot ja palvelunestohyökkäykset. (Peng ym., 2014.)

Matohaittaohjelman tarkoituksena on siirtyä käyttäjän laitteelle ja sen järjestelmiin ilman laitteen omistajan huomaamista. Matohaittaohjelma eroaa viruksesta siten, että se ei tarvitse laitteen käyttäjään levitäkseen vaan se suorittaa leviämisoperaation automaattisesti laitteelta toiselle. Sillä on myös ominaisuus luoda itsestään moninkertaisia kopioita ja sen jälkeen lähettämään niitä esimerkiksi sähköpostin välityksellä. Mato haittaohjelman vaikutukset voi olla hyvinkin tuhoisia niiden nopean ja itsenäisen leviämiskyvyn takia. (Peng ym., 2014.)

### 3.3.2 Vakoilu ja kiristys

Vakoiluun käytettävä haittaohjelma, jonka tarkoituksena on henkilökohtaisten ja esimerkiksi käyttäjän organisaation tietojen keräys. Tällaisia varastettavia tietoja voivat olla luottokorttitunnukset, salasanat, käyttäjätunnukset ja sähköpostiosoitteet. Vakoiluohjelmalla voidaan myös seurata käyttäjän laitteen toimia verkon välityksellä. Vakoiluohjelma tulee laitteelle salattuna tiedostomuotona, joka on hankalasti tunnistettavissa. (Peng ym., 2014.)

Ramsonwaren eli kiristyshaittaohjelman tarkoituksena on päästä kohdekäyttäjän laitteelle ja luoda satunnainen salausavain. Tämä jälkeen se salaa käyttäjän käyttöjärjestelmän tietoja, kuten tiedostoja ja kuvia salausavaimen avulla. Lopputuloksen kohdekäyttäjän laite on täysin lukossa ja käyttäjä saa oikeudet eli salausavaimen takaisin maksamalla kiristyksessä vaadittava määrä rahaa. Salausavaimen takaisinsaanti maksun jälkeen ei ole aina varmaa, vaan siihenkin liittyy riski tulla huijatuksi. Yleensä maksu tapahtuu bitcoin kryptovaluutan avulla. (Lopez, Moon & Park, 2016.)

### 3.3.3 Troijalainen ja Takaovi

Troijalainen haittaohjelmana toimii siten, että käyttäjä ohjataan ohjelman asennuksen läpi ja se ei ulkoisesti näytä epäilyttävältä ohjelmalta käyttäjälle. Ohjelman asennuksen jälkeen troijalainen aloittaa hyökkäykset laitteella. Hyökkäyksiä ovat muun muassa pop-up ikkunat, tiedostojen poistamista, tiedostojen varastamista ja muiden erilaisten haittaohjelmien levittämistä ja aktivointia. Troijalaisilla on myös ominaisuus luoda takaovia käyttäjän laitteelle ja näiden avulla muut haittaohjelmat saavat pääsyn laitteelle. Troijalaisesta esimerkkinä on Android-laitteille suunnattu Soundminer, joka voi tallentaa yksityisiä tietoja käyttäjän mobiililaitteen ääniantureista. (Peng ym., 2014.)

Backdoor eli takaovi-haittaohjelmaa käytetään käyttäjän laitteen etähallintaan. Takaovi haittaohjelman avulla hyökkääjät saavat käyttäjän laitteen etäkäytön ja näin pystyvät hallitsemaan laitetta verkon ylitse. Hyökkääjät toteuttavat etähallinnan käyttämällä laitteen järjestelmäkoodissa olevia dokumentoimatta jääneitä prosesseja. (Peng ym., 2014.)

### 3.3.4 Rootkit- ja Botnet-haittaohjelmat

Rootkit eli piilohallintaohjelma, joka pystyy piiloutumaan järjestelmään ilman, että laitteen käyttäjä huomaa sitä. Se ei näytä laitteen käyttäjälle yhteyksiä, joita se suorittaa. Näitä ovat esimerkiksi meneillään olevat prosessit, käytetyt tiedostot ja verkkoon olevat yhteydet. Tämä haittaohjelma pystyy saavuttamaan nämä prosessit muokkaamalla käyttöjärjestelmän ydintä sille omiin tarkoituksiin sopivaksi. (Peng ym., 2014.)

Botnet-haittaohjelman tarkoituksena on laitteiden etäkontrolli. Tätä haittaohjelmaa käytetään usein suurempien verkkohyökkäysten toteutukseen, joka voi olla esimerkiksi hajautettu palvelunestohyökkäys tai massiivinen roskapostilähetysoperaatio. (Peng ym., 2014). Esimerkkinä tällaisesta suuren luokan hyökkäyksestä oli syksyllä 2021 Oulun yliopistoon kohdistunut käyttäjätunnusten ja salasanojen tietojenkalastelu. (Keski-Heikkilä, 2021).

## 3.4 Käyttäjän laitteiden katoaminen ja varkaus

Erilaisten tietokoneiden ja mobiililaitteiden ollessa pieniä ja helposti mukana kulkevia ne ovat helpommin alttiita joutua varastetuksi. Varkaudet suoritetaan yleensä paikoilla, missä liikkuu paljon ihmisiä. Esimerkiksi lentokentät, kirjastot, kahvilat ym. Laitteiden katoaminen tarkoittaa käyttäjän henkilökohtaisten ja mahdollisesti käyttäjän työpaikan tietojen katoamista ja leviämistä niille kuulumattomien tahojen käsiin. (Latheef, Ramadas, Cheruthuruthy, Antony, 2014.)

Pienissä mobiililaitteissa on useasti irrotettava pieni muistikortti, johon on voitu tallentaa suuri määrä dataa. Muistikortin helppo ja nopea varastaminen laitteesta altistaa datan helposti vääriin käsiin. (Halpert, 2004.)

## 3.5 Palvelunestohyökkäykset käyttäjän laitteelle

Palvelunestohyökkäyksessä tarkoituksena on ylikuormittaa, häiritä palveluita ja tuottaa verkkoyhteysongelmia, joka rajoittaa pääsyn hyökkäyksen kohteena olevaan palveluun tai laitteiseen, jolla palvelua käytetään. (Douligeris & Mitrokotsa 2004).

Palvelunestohyökkäykset eli DDoS hyökkäykset ovat suuri kokonaisuus monista eri lähteistä tulevista verkkoliikenteen pakettivirroista, jotka kuluttavat suuria määriä verkon ”isäntä” palvelimen resursseja. Tämä johtaa siihen, että verkonpalvelut eivät enää toimi niitä tarvitsevilla asiakkailla ja käyttäjillä. Kokonaisverkon kuormitus palvelunestohyökkäyksen aikana on niin kuormittunutta, että verkon palveluntarjoajan on haastava tunnistaa oikeat palvelunkäyttäjien pakettipyynnöt verkkoliikenteen seasta. Palvelunestohyökkäyksistä voi aiheutua: järjestelmien sulkeutumista, tiedostojen tuhoutumista ja palvelujen sulkeutumista. (Douligeris & Mitrokotsa, 2004.)

# 4. Käyttäjälähtöisten tietoturvauhkien hallinta

Seuraavaksi käydään läpi erilaisia organisaatioiden tietoturvauhkien hallintakeinoja, joilla voidaan estää ja ennaltaehkäistä tietoturvaan liittyviä riskejä.

## 4.1 Haittaohjelmien hallinta

Allekirjoitukseen perustuva haittaohjelmien torjuntakeino on virustorjuntaohjelmistojen käyttämä menetelmä tunnettujen uhkien tunnistamiseen ja torjumiseen käyttäjän laitteelta. Näitä virustorjuntaohjelmistoja ovat esimerkiksi MacAfee (n.d.), F-Secure (n.d.) ja Malwarebytes (n.d.). Allekirjoituksella tunnistaminen ja torjuminen toimii siten, että tunnettu haittaohjelma saa lyhyen tavukoodin, joka on yksilöity erikseen jokaiselle tunnetulle haittaohjelmalle. Tämän jälkeen virustorjunta käyttäjän laitteella voi tunnistaa tulevan haittaohjelman hyvin pienillä käyttöresursseilla ja virhenopeudella, jonka jälkeen haittaohjelman toiminta laitteella estetään. (Ye, Li, Adjeroh & Iyengar, 2017.)

Heuristinen tunnistus, jossa haittaohjelmat tunnistetaan allekirjoitukseen perustuvalla suojauksella. Heuristinen suojaus pohjautuu asiantuntijoiden määrityksiin hyvä- ja pahalaatuiset tiedostomuodot siinä vaiheessa, kun ne tulevat järjestelmään. (Ye ym., 2017.)

Pilvipalvelupohjainen haittaohjelmien tunnistus toimii seuraavanlaisesti (Ye, ym., 2017):

1. Käyttäjä luo uuden tiedoston sähköpostin kautta.
2. Uusi tiedosto menee automaattiseen skannaukseen.
3. Tiedoston tiedot lähetetään pilvipalveluun.
4. Pilvipalvelun sisällä tiedostot käydään läpi ja jos niissä on jotain haitallista, niin merkitään haittaohjelmat.
5. Pilvipalvelussa skannattujen tiedostojen tiedot lähetetään takaisin käyttäjän laitteelle ja ilmoitetaan mahdolliset uhat.
6. Pilvipalvelua käyttävä haittaohjelmien tunnistus ja torjunta hyödyttää käyttäjää seuraavilla tavoilla: nopea tietoturvaratkaisu ja viimeisimmät suojausratkaisut.

## 4.2 Työntekijöiden sosiaalinen manipulointi ja tietojenkalastelun hallinta

Organisaatioiden sisällä tulee olla tarkasti laadittu turvallisuuspolitiikka, jotta vältetään omien työntekijöiden kautta tulevat sosiaalisen manipuloinnin ja tietojenkalastelun yritykset. Näillä voi olla mittavia tuhoja organisaation sisällä. Organisaation sisällä turvallisuuspolitiikan testauksia pitää suorittaa määräajoin, jotta saadaan selville työntekijöiden ja organisaation oma tietoturvan tietoisuus. (Saleem & Hammoudeh, 2018.)

Fyysisen työntekijöiden turvallisuuden hallinnan avulla vältetään tai pienennetään mahdollisuuksia joutua sosiaalisen manipuloinnin tai tietojenkalastelun kohteeksi. Työyhteisön tehtävänä on muistuttaa omia työntekijöitään, että he eivät laita omia tai saatuja USB-laitteita tai muita vastaavia laitteita organisaation työkoneisiin tai palvelimiin kiinni. Kaikki käytettävät laitteet tulee kierrättää tietoturva asiantuntijoiden testauksen kautta käyttöön, jotta voidaan olla varmoja niiden tietoturvallisuudesta.

Työntekijöillä on myös velvollisuus ilmoittaa kaikki kohtaamansa epäilyttävä toiminta ja käytös, jotta voidaan maksimoida turvallisuus. (Saleem & Hammoudeh, 2018.)

Organisaation sisäinen- ja digitaalinen tietoturva on haittaohjelmien- ja palvelunestohyökkäysten torjuntaa, palomuurien ylläpidon toimenpiteitä ja mahdollisten muiden uhkien seurausta listausta käyttäen. Nämä kaikki tietoturvaan liittyvät hallintakeinot voidaan silti ohittaa hyvinkin helposti murtautumalla fyysisesti organisaatioon tai kulkemalla laitteen niin sanotun takaoven kautta. Tämän takia on kehitetty vaihtoehtoisia keinoja organisaation tietoturvan suojelemiseksi. Ensimmäinen suojauskeino on käyttää hiekkalaatikkomenetelmää, jossa erillinen virtuaalikone suojaa muun muassa koko organisaation verkon haittaohjelmilta ja sen, että organisaation työntekijä ei kytke omia laitteita työpaikan koneisiin kiinni. Toisena keinona organisaation sisällä työntekijöiden sosiaalista manipulointia vastaan on aktiivinen laitteiden seuranta tekoälyn avulla, jossa järjestelmä havaitsee käyttäjän epänormaalit toimenpiteet organisaation laitteella. Esimerkkinä tällaisesta tekoälyjärjestelmästä on vektoritekoälyyn perustuva koneoppimisjärjestelmä, jonka tehtävänä on tunnistaa käyttäjän sähköpostiin tulevat ”spear fishing” tietojenkalasteluun liittyvät viestit. (Saleem & Hammoudeh, 2018.)

## 4.3 Palvelunestohyökkäysten hallinta käyttäjätietoturvan parantamiseksi

Yleensä parhaaksi todettu keino palvelunestohyökkäyksen estämiseen on ennaltaehkäisy. Seuraavana esitellään tällaisia ennaltaehkäisyn keinoja eli tässä tilanteessa suodattimia, joilla voidaan estää palvelunestohyökkäyksen käynnistyminen. (Latheef ym., 2014).

Ingressisuodatus, jossa organisaation reititin määritetään siten, että se ei salli sellaisia saapuvia paketteja, joilla on huonoksi määritetyt lähdeosoitteet. Ingressisuodatus poistaa tietoliikenteestä IP-osoitteet, jotka eroavat domain-osoitteen etuliitteestä. Tällä tavalla saadaan estettyä suuri määrä IP-osoite huijaukseen perustuvia palvelunestohyökkäyksiä. Ainoa huono puoli tässä menetelmässä on se, että se voi vahingossa estää oikean yhteyspyynnön verkkoon. (Latheef ym., 2014.)

Egressisuodatuksessa varmistetaan se, että organisaation verkosta poistuu vain ennalta määritetyt ja varatut IP-osoitteet. Tämän suodatuksen tarkoitus on suojata muita verkon lähdeosoitteita mahdollisilta tulevilta palvelunestohyökkäyksiltä. Ingressi- ja Egressisuodatuksen toimintaperiaatteet ovat samanlaiset, mutta ne on ohjelmoitu toimimaan eri vaiheissa. (Latheef ym., 2014.)

Reititykseen perustuva pakettien suodatus, jossa suodatetaan suurin osa vääristä verkkoon tulevista IP-osoitteiden paketeista ja estetään mahdollinen virheellisten pakettien toiminta organisaation tai käyttäjän laitteella. Näitä IP-paketteja pystytään hallitsemaan verkon reittitietojen avulla. Ongelmallista reittipohjaiselle pakettiensuodatukselle on se, että verkon reitit muuttuvat ajan kuluessa. (Ramadas ym., 2014.)

## 4.4 Laitevarkauksien hallinta

Kaikilla mobiililaitteilla, jotka käsittelevät organisaation herkkäluontoista dataa tulisi käyttää erilaisia suojauskeinoja laitevarkauksia vastaan. Suojauskeinoja, joita mobiililaitteella käytetään ovat vahva salasana, laitelukitus ja organisaation laitehallintapolitiikka. (Halpert, 2004.)

Salasanat ovat useasti ensimmäinen ja ainoa suojaustapa laitteelle, jolloin salasanan täytyisi olla vahva. Monille käyttäjille on normaalina tapana valita oletus salasana tai yleisesti käytetty salasana. Satunnaisesti valitun salasanan muistaminen ilman erillistä salasanan hallintatyökalua altistaa käyttäjän kirjoittamaan salasanan ylös sinne paikkaan, jossa sitä käytetään useasti. Esimerkkinä salasanojen säilyttämispaikkoja ovat: näppäimistön alusta tai näytön alaosassa oleva muistilappu. Hyvän salasanan ominaispiirteitä ovat minimissään kuusi merkkiä sisältäen pieni merkki, iso merkki, numero ja erikoismerkki. Mitä enemmän vaihtelua ja pidempi salasana on sitä paremman suojauksen se antaa laitteelle murtoa vastaan. (Summers & Bosworth, 2004.)

Kolmannen osapuolen ohjelmistoilla voidaan lukita ja tyhjentää mobiililaite, jos laite on ollut tietyn aikaa kadoksissa tai laitteen salasana on syötetty väärin tarpeeksi monta kertaa. (Halpert, 2004).

Organisaatiolla on tärkeä olla oma laitehallintapolitiikka, jonka työntekijät tuntevat käyttäessään eri laitteita työpaikalla ja vapaa-ajallaan. Laitehallintapolitiikalla levitetään tietoa organisaation sisäisten laitteiden mahdollisista tietoturvauhista. (Halpert, 2004.)

# 5. Löydökset ja pohdinta

Tämän tutkielman tavoite oli tutkia organisaation käyttäjälähtöisiä tietoturvauhkia ja hakea vastaukset näiden tietoturvauhkien hallintaan lähdekirjallisuudesta. Tietoturvaan liittyviä hyökkäyskeinoja löydetään ja kehitetään jatkuvasti lisää, joten kaikelta suojautuminen voi olla välillä haastavaa. Monet tietoturvaan liittyvät hyökkäykset ovat useasti myös monimutkaisia ja yhdistävät erilaisia tapoja toteuttaa tietty tietoturvahyökkäys. Samanaikaisesti myös tietoturvanhallintaan tulee uusia suojautumiskeinoja mahdollisimman monipuoliseen tietoturvan toteutukseen.

Tutkielman toisessa luvussa käytiin läpi tietoturvaa, tietoturvan historiaa, tietoturvan määritelmiä, tietoturvan osa-alueita ja tietoturvan tulevaisuutta. Nämä pohjustivat tietoa tietoturvasta yleisesti ja sen ominaisuuksista, jotta seuraavien lukujen läpikäynti olisi mielekkäämpää.

## 5.1 Vastaukset tutkimuskysymyksiin 1 ja 2

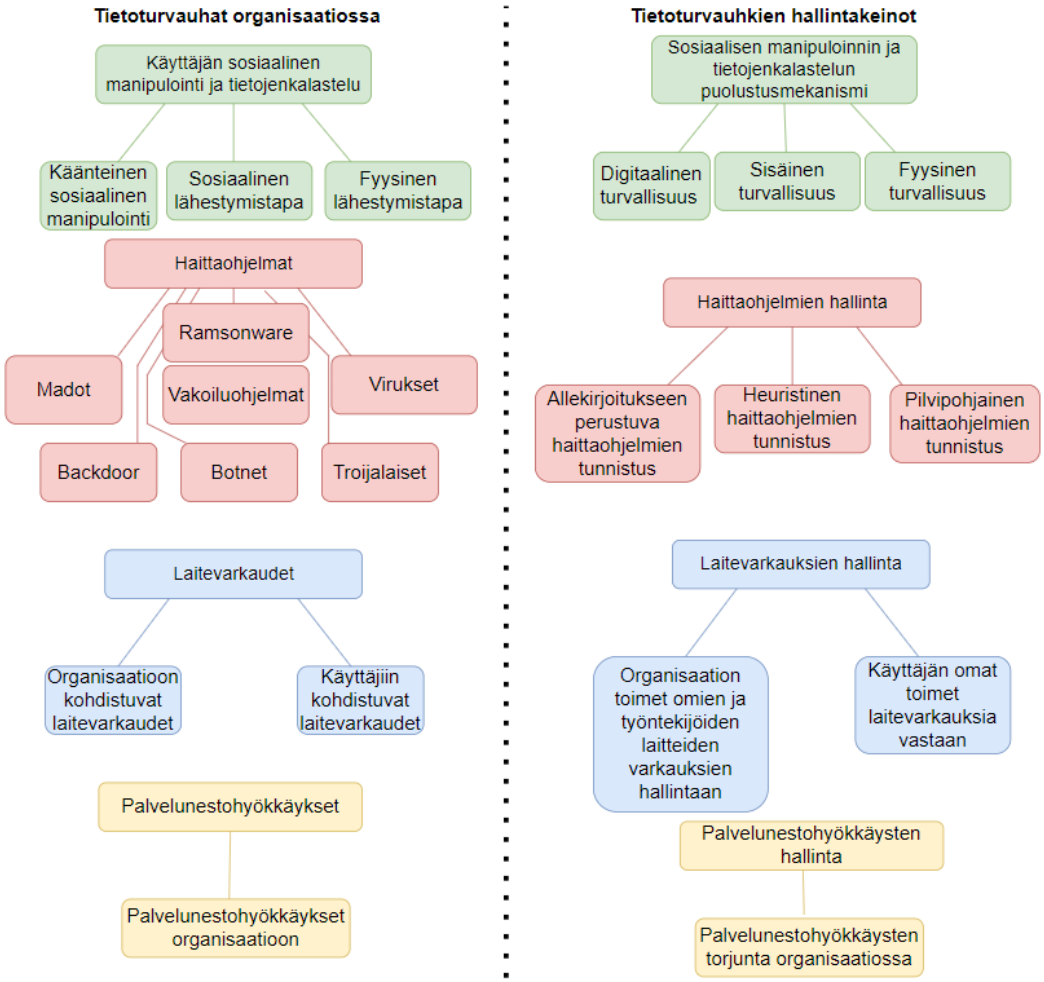
Tutkielman kolmannessa luvussa käytiin läpi sosiaalista manipulointia, tietojenkalastelua, haittaohjelmia, laitevarkauksia ja palvelunestohyökkäyksiä joihin käyttäjät ja organisaatiot voivat kohdata. Nämä vastasivat ensimmäiseen tutkimuskysymykseen: **”Mitä erilaisia tietoturvauhkia organisaatiot voivat kohdata käyttäjien toimesta?”** Sosiaalista manipulointia käytiin läpi fyysisen lähestymistavan, sosiaalisen lähestymistavan ja käänteisen sosiaalisen manipuloinnin muodossa. Tietojenkalastelusta käytiin läpi, miten se kohdennetaan eri tavoin ja mitä erilaisia tietojenkalastelun muotoja on olemassa. Haittaohjelmista käytiin läpi haittaohjelmien kategorointi ja yleisimmät haittaohjelmat. Viimeisenä kolmannessa luvussa käytiin läpi käyttäjien laitevarkauksia ja palvelunestohyökkäyksiä käyttäjän laitteelle.

Tutkielman neljännessä luvussa käytiin läpi haittaohjelmien-, sosiaalisen manipuloinnin-, tietojenkalastelun-, palvelunestohyökkäysten ja laitevarkauksien hallintaa, jota voidaan toteuttaa käyttäjien ja organisaation toimesta. Nämä eri tietoturvan hallinnan keinot vastasivat toiseen tutkimuskysymykseen: **”Millaisilla toimilla voidaan parantaa organisaation tietoturvaa?”** Haittaohjelmien hallintaa käytiin läpi virustorjuntaohjelmistojen muodossa sekä pilvipalvelupohjaisen tunnistuksen kautta. Sosiaalista manipulointia ja tietojenkalastelun hallintaa käytiin läpi organisaation sisäisen menettelyn kautta. Palvelunestohyökkäysten hallintaa käytiin läpi erilaisten suodattimien muodossa. Viimeisenä neljännessä luvussa käytiin läpi laitevarkauksien hallintaan liittyviä torjuntakeinoja.

Tutkimustuloksena saatiin näkemys siitä millaisia tietoturvauhkia organisaatiot kohtaavat ja millä toimenpiteillä niitä torjutaan. Tutkimuksesta on hyötyä itse organisaatioille ja heidän työntekijöilleen, kun mietitään tietoturvaan liittyviä parannuskeinoja.

Tutkimuksen löydöksistä esitellään havainnollistava kuva, joka kokoaa yhteen erilaiset käyttäjälähtöiset tietoturvauhat ja niiden hallintakeinot. Kuvassa on jaoteltu eri tietoturvauhat ja tietoturvauhkien hallintakeinot väreillä kokonaisuuden selkeyttämiseksi. Vihreällä värillä on kuvattuna sosiaalinen manipulointi sekä tietojenkalastelu ja punaisella haittaohjelmat. Sinisellä värillä on erotettuna laitevarkaudet sekä keltaisella palvelunestohyökkäykset.

(Kuva 1).




**Kuva 1.** Tietoturvauhat ja hallintakeinot kokonaisuutena.

## 5.2 Tutkimuksen rajoitukset

Tutkielma rajoittuu kirjallisuuskatsauksen muodossa antamaan käsityksen lukijalle laajemmasta kokonaisuudesta tietoturvaan liittyvistä käyttäjälähtöisistä tietoturvauhista organisaatioissa ja niiden hallintamuodoista. Tutkielmassa olisi voinut tarkastella tietoturvaa eri organisaatioiden näkökulmasta, jotta nähtäisiin esimerkiksi eri alojen, organisaation koon ja ympäristöjen vaikutus organisaation tietoturvaan.

# 6. Yhteenveto

Tutkielmassa käsiteltiin tietoturvaa yleisesti ja organisaation tietoturvauhkia käyttäjälähtöisesti ja näitä olivat seuraavat: käyttäjien sosiaalinen manipulointi, käyttäjien tietokoneiden ja mobiililaitteiden haittaohjelmat, käyttäjän laitteiden katoaminen ja palvelunestohyökkäykset käyttäjän laitteille. Näitä tietoturvauhkia käsiteltiin itse käyttäjän sekä organisaation toimesta, mutta pääasiallinen painotus oli siihen, miten ne voivat vaikuttaa organisaatioon.

Näille tietoturvauhkille käytiin seuraavat hallintakeinot läpi: haittaohjelmien hallinta, palvelunestohyökkäysten hallinta ja sosiaalisen manipuloinnin hallinta. Näin saatiin kokonaiskuva keinoista, joilla parempaa tietoturvaa voidaan toteuttaa organisaation sisällä.

Jatkotutkimuksena voisi toteuttaa empiirisen tutkimuksen liittyen organisaation tietoturvaan esimerkiksi toteuttamalla haastattelututkimuksen yhdessä tai useammassa organisaatiossa. Erilaiset organisaatiot toisivat tähän jatkotutkimukseen myös lisäarvoa. Tämä antaisi kirjallisuuslähteiden lisäksi laadullista materiaalia organisaatio- ja käyttäjänäkökulmista.

# Lähteet


Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

Annansingh, F. (2020). Bring your own device to work: How serious is the risk? *Journal of Business Strategy, ahead-of-print(ahead-of-print).* https://doi.org/10.1108/JBS-04-2020-0069

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *International Journal of Security and Its Applications*, *10*(1), 247–256. http://dx.doi.org/10.14257/ijsia.2016.10.1.23

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13–21. http://doi.org/10.22215/timreview/835

Douligeris C, Mitrokotsa A. (2004) DDoS attacks and defense mechanisms: classification and state-of-the-art, Computer Networks, Volume 44, Issue 5, 2004, Pages 643-666, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2003.10.003

F-Secure (n.d.) Viitattu 7.12.2021 lähteestä: https://www.f-secure.com/fi

Geluvaraj, B., Satwik, P. M., & Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies* (pp. 739-747). Springer, Singapore. https://doi.org/10.1007/978-981-10-8681-6_67

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December 18.

Halpert, B. (2004, October). Mobile device security. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 99-101). https://doi.org/10.1145/1059524.1059545

Ham, J. V. D. (2021). Toward a Better Understanding of "Cybersecurity". *Digital Threats: Research and Practice*, *2*(3), 1-3. https://doi.org/10.1145/3442445

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, July). Reverse social engineering attacks in online social networks. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp 55–74). https://doi.org/10.1007/978-3-642-22424-9_4

ITU. (2009). Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Jamwal, K., & Sharma, L. S. (2018). Clickjacking attack: Hijacking user's click. International Journal of Advanced Networking and Applications, 10(1), 3735-3740.

Haettu osoitteesta: https://www.proquest.com/scholarly-journals/clickjacking-attack-hijacking-users-click/docview/2099845734/se-2

Kemmerer, R. A. (2003). *Cybersecurity.* 25th International Conference on Software Engineering, 2003. Proceedings. doi:10.1109/icse.2003.1201257

Keski-Heikkilä. A. (2021). Oulun yliopisto joutui laajan tietojenkalastelun kohteeksi – yli 750 ihmisen salasanat joutuneet vääriin käsiin. Helsingin Sanomat. 3.9.2021. Viitattu 22.11.2021. Saatavilla: https://www.hs.fi/kotimaa/art-2000008238022.html

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Latheef S, Ramadas S, Cheruthuruthy T, Antony A. (2014). Mobile Device Protection Using Sensors. *International Journal of Computer Applications Technology and Research*. Volume 3- Issue 3, 146-149, ISSN: 2319-8656. Haettu osoitteesta: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1046.173&rep=rep1&type=pdf

Lewis, J. A. (2006). *Cybersecurity and Critical Infrastructure Protection.* Washington, DC: Center for Strategic and International Studies. Haettu osoitteesta: http://csis.org/publication/cybersecurity-and-critical- infrastructure-protection

Lopez, E. M., Moon, S. Y., & Park, J. H. (2016). Ramsonware: Holding your Data Hostage. In *Proceedings of the Korea Information Processing Society Conference* (pp. 304–306). Korea Information Processing Society. https://doi.org/10.3745/PKIPS.y2016m04a.304

MacAfee (n.d.) Viitattu 7.12.2021 lähteestä: https://www.mcafee.com/fi-fi/index.html

Malwarebytes (n.d.) Viitattu 7.12.2021 lähteestä: https://www.malwarebytes.com/

Moore, T., & Clayton, R. (2007, June). An Empirical Analysis of the Current State of Phishing Attack and Defence. In *WEIS*. Haettu osoitteesta: https://tylermoore.ens.utulsa.edu/weis07.pdf

Nweke, L. O. (2017). Using the cia and aaa models to explain cybersecurity activities. *PM World Journal*, *6*, 1-2. Haettu osoitteesta: https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf

Peng, S., Yu, S., & Yang, A. (2014). *Smartphone Malware and Its Propagation Modeling: A Survey. IEEE Communications Surveys & Tutorials, 16(2), 925–941.*doi:10.1109/surv.2013.070813.00214

Saleem, J., & Hammoudeh, M. (2018). Defense methods against social engineering attacks. In Computer and network security essentials (pp. 603-618). Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_35

Sanford, M. (2010). *Computer viruses and malware by john aycock.* ACM SIGACT News, 41(1), 44–47. Haettu osoitteesta: https://dl.acm.org/doi/pdf/10.1145/1753171.1753184?casa_token=IACnwmVXfH

wAAAAA:9EL2gAwg1MlqgvjDnACSDMCfeo9mlvAqIWk91kY6GhAe3Mbib0wVUAaisqchB-hzxnW51DMjMnI

Siikaluoma. M. (2021). Kyberturvallisuuskeskus varoittaa jopa satoja tuhansia huijausviestejä lähettäneestä haittaohjelmasta – yrittää huijata käyttäjää avaamaan ääni- tai kuvaviestin. Kaleva. 30.11.2021. Viitattu 7.12.2021. Saatavilla: https://www.kaleva.fi/kyberturvallisuuskeskus-varoittaa-jopa-satoja-tuha/4154461

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Song, Y., Yang, C., & Gu, G. (2010, June). Who is peeping at your passwords at Starbucks? —To catch an evil twin access point. In *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)* (pp. 323-332). IEEE. doi: 10.1109/DSN.2010.5544302

Summers, W. C., & Bosworth, E. (2004). Password policy: the good, the bad, and the ugly. In *Proceedings of the winter international synposium on Information and communication technologies* (pp. 1–6). Haettu osoitteesta: https://www.researchgate.net/profile/Wayne-Summers-2/publication/234799064_Password_policy_The_good_the_bad_and_the_ugly/links/54f204310cf2f9e34eff3d50/Password-policy-The-good-the-bad-and-the-ugly.pdf

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), 781-799. https://doi.org/10.1080/02684527.2012.708530

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2017). A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR), 50(3), 1–40. https://doi.org/10.1145/3073559