Käyttäjän manipulointi ja siihen varautuminen yrityksissä

Casper Almén

2022 Laurea

Laurea-ammattikorkeakoulu

Käyttäjän manipulointi ja siihen varautuminen yrityksissä

Casper Almén

Tietojenkäsittely

Opinnäytetyö

Marraskuu 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Casper Almén

Käyttäjän manipulointi ja siihen varautuminen yrityksissä

Vuosi 2022 Sivumäärä 46

Opinnäytetyössä tutkittiin käyttäjän manipuloinnin ilmiötä tietoturvan kontekstissa. Käyttäjän manipulointi tarkoittaa suunniteltua tietoturvahyökkäystä organisaatiota tai yksittäistä ihmistä vastaan, jossa käytetään erilaisia manipulointiin pohjautuvia hyökkäysmetodeja. Työn tavoitteena oli selvittää erilaisia keinoja, joiden avulla yritykset voivat varautua käyttäjän manipuloinnin hyökkäyksiltä. Työssä pohdittiin myös, miten käyttäjän manipuloinnin uhka on muuttunut viime vuosien aikana ja miltä se tulee näyttämään tulevaisuudessa.

Opinnäytetyö on toteutettu narratiivisena kirjallisuuskatsauksena. Aineistoksi valittiin aikaisempia kansainvälisesti julkaistuja tutkimuksia ja asiantuntijakirjallisuutta. Aineistoa analysoitiin hyödyntäen aineistolähtöistä sisällönanalyysiä.

Opinnäytetyön tuloksiksi saatiin, että käyttäjän manipuloinnin varautumiskeinoissa täytyy keskittyä systemaattiseen vahvuuteen sekä henkilöstön vahvuuteen, jotta tietoturva pysyy vahvana ja murtovarmana. Teknologioiden modernisoituessa käyttäjän manipulointikeinotkin muuttuvat, mikä johtaa uudenlaisiin uhkiin tietoturvassa. Tulosten pohjalta voidaan todeta, että käyttäjän manipulointi on yhä kasvava ilmiö erityisesti yritysten tietoturvapolitiikassa ja siihen tulisi kiinnittää erityistä huomiota turvatakseen arkaluonteista tietoa.

Asiasanat: tietoturva, käyttäjän manipulointi, tietojenkalastelu

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

Casper Almén

Abstract

Social Engineering and How to Prepare for It in Businesses

Year 2022 Pages 46

This Bachelor's thesis studied the phenomenon of social engineering in the context of information security. Social engineering refers to a planned security attack against an organization or an individual, using a variety of manipulation-based attack methods. The objective of this work was to identify different ways in which companies can prepare themselves against social engineering attacks. It also examined how the threat of social engineering has changed in recent years and what it might look like in the future.

The thesis has been conducted as a narrative literature review. Previous internationally published studies and academic publications were selected as material. The material was analyzed using material-based content analysis.

The results of the thesis indicate that social engineering preparedness measures need to focus on systematic strength and personnel strength to keep the security strong and break-proof. As technologies become more modern, the means of social engineering change, leading to new threats to information security. The results show that social engineering is a growing phenomenon, especially in corporate security policies, and should be given special attention to protect sensitive information.

Keywords: information security, social engineering, phishing

Sisällys

1 Johdanto ... 7
2 Työn lähtökohdat ... 8
2.1 Tutkimustehtävä ja tutkimuskysymykset ... 8
2.2 Aiheen rajaus ... 8
2.3 Keskeiset käsitteet ... 9
3 Tietoturva ja CIA-malli ... 12
4 Käyttäjän manipulointi ja hyökkäysmetodit ... 13
4.1 Termin määrittelyä ... 13
4.2 Käyttäjän manipuloinnin hyökkäysmetodit ... 15
4.2.1 Tietojenkalastelu ... 15
4.2.2 Houkuttelu ... 17
4.2.3 Peitetarina ... 18
4.2.4 Käänteinen käyttäjän manipulointi ... 18
4.2.5 Tailgating ... 19
4.2.6 Olan yli kurkkiminen ... 20
4.2.7 Dyykkaus ... 20
5 Käyttäjän manipuloinnin vaiheet ... 21
5.1 Tiedon hankinta ... 22
5.2 Suhteen ja luottamuksen kehittäminen ... 23
5.3 Luottamuksen hyödyntäminen ... 24
5.3.1 Ystävällisyys, vastavuoroisuus ja velvollisuus ... 24
5.3.2 Myönnytys ja johdonmukaisuus/sitoutuneisuus ... 25
5.3.3 Niukkuus ... 25
5.3.4 Auktoriteetti ... 26
5.3.5 Ryhmäpaine ... 27
5.4 Saadun tiedon hyödyntäminen ... 27
6 Tutkimusmenetelmät ... 28
6.1 Narratiivinen kirjallisuuskatsaus ... 28
6.2 Aineistolähtöinen sisällönanalyysi ... 28
7 Kirjallisuuskatsauksen toteutus ... 29
7.1 Aineisto keruu ja analysointi ... 29
7.2 Validiteetti ja reliabiliteetti ... 31
8 Tutkimustulokset ... 32
8.1 Käyttäjän manipuloinnin varautumiskeinot ... 32
8.1.1 Systemaattinen vahvuus ... 33
8.1.2 Henkilöstön vahvuus ... 34

8.2 Käyttäjän manipulointi viime vuosien aikana ja tulevaisuudessa 37
9 Yhteenveto 38
10 Johtopäätökset 39
Lähteet 41
Kuviot 46
Taulukot 46

1 Johdanto

Vuonna 2022 maailmassa on yhteensä noin 5 miljardia internetin käyttäjää, mikä on noin 63,1 % maailman väkiluvusta. On lähes mahdotonta ajatella enää maailmaa ilman tietokoneita ja internetiä. Internetin ajatellaankin olevan nykyaikaisen tietoyhteiskunnan peruspilari. (Statista Research Department 2022.) Tietotekniikan yleistymisen ja kehittymisen myötä kuitenkin myös tietoturvasta on tänä päivänä tullut yksi suurimmista maailmanlaajuisista uhista ja huolista tietokoneiden käyttäjille (Soomro, Shah & Ahmed 2016, s. 216–217). Uhkien määrä myös vain lisääntyy vuosien saatossa. Esimerkiksi Suomen kansallinen Kyberturvallisuuskeskus raportoi vuonna 2019 noin 4,5 tuhatta tietoturvaloukkausta ja uhkailmoitusta, vuonna 2020 tämä vastaava luku oli noin 12 tuhatta tapausta. Tämä tarkoittaa siis yli 100 % kasvua tietoturvaloukkauksissa ja -uhissa yhden vuoden aikana. (Clausnitzer 2021.)

Tässä työssä selvitetään käyttäjän manipulointiin tutustumisen myötä, että miten käyttäjän manipuloinnin hyökkäyksiin voidaan varautua yritysten näkökulmasta. Työssä analysoidaan myös, miten käyttäjän manipuloinnin uhka on muuttunut viimeisten vuosien aikana ja miten hyökkäykset tulevat mahdollisesti muuttumaan tulevaisuudessa. Käyttäjän manipulointi tarkoittaa käytännössä sitä, että hyökkääjä yrittää saada käsiinsä arkaluontoista tietoa kohteiltaan erilaisia metodeja hyödyntäen, jotka sisältävät usein ihmisvuorovaikutusta ja kommunikointia. Tietoturvauhat ovat jatkuva päänvaiva erityisesti yritysten toiminnassa ja keskeisenä tekijänä tietoturvauhissa korostuu käyttäjän manipulointi. (Hadnagy & Wilson 2010, s. 9–10.)

Työ alkaa esittelemällä käyttäjän manipulointi -ilmiötä tarkemmin, eli mitä kyseinen käsite tarkoittaa ja minkälaisia metodeja siihen muun muassa kuuluu. Käsitteen tarkentamisen jälkeen tutkimuskysymysten myötä tutkitaan, miten käyttäjän manipuloinnilta voidaan varautua. Pitkälti kuka tahansa voi hyötyä opinnäytetyössä tehdyn kirjallisuuskatsauksen tuloksista. Tietoturvan tärkeys koskee jokaista ihmistä, sillä kuka vain voi joutua tietoturvahyökkäyksen ja käyttäjän manipuloinnin kohteeksi, joka on yksi tietoturvahyökkäyksen muodoista.

Opinnäytetyö on toteutettu narratiivisena kirjallisuuskatsauksena. Aineisto on kerätty hyödyntäen kansainvälisiä ja englanniksi julkaistuja tutkimusartikkeleita ja uutisia. Aineistossa on myös hyödynnetty asiantuntijakirjallisuutta. Aineisto on analysoitu käyttäen aineistolähtöistä sisällönanalyysiä, jossa aineistosta poimitaan tutkimuskysymysten kannalta olennaiset asiat luoden kokonaisvaltaisen katsauksen tutkittavaan ilmiöön (Tuomi & Sarajärvi 2018, s. 84).

2 Työn lähtökohdat

2.1 Tutkimustehtävä ja tutkimuskysymykset

Aiheesta käyttäjän manipulointi löytyy paljon aikaisempaa tutkimustietoa. Tavoitteena on kirjallisuuskatsauksen avulla koota luotettava, informatiivinen ja päivitetty katsaus aiheesta hyödyntäen aikaisempaa tutkimustietoa ja asiantuntijakirjallisuutta. Aihetta havainnollistetaan myös hyödyntämällä konkreettisia esimerkkejä tapahtumista liittyen käyttäjän manipulointiin.

Tutkimuskysymykseksi asetettiin sellaisten keinojen selvittäminen, joiden avulla yritykset voivat varautua käyttäjän manipuloinnilta. Tavoitteena varautumisessa on, että mitään arkaluonteista tietoa ei menetetä tai sellainen ei joudu väärien henkilöiden käsiin. Tutkimuskysymykseksi asetettiin myös sen selvittäminen, miten käyttäjän manipuloinnin uhka on vuosien saatossa muuttunut ja minkälaisena uhkana se näyttäytyy edelleen tulevaisuudessa tietotekniikan kehittyessä.

Tutkimuskysymykset ovat seuraavat:

1. Minkälaisin keinoin yritykset voivat varautua käyttäjän manipuloinnilta?
2. Miten käyttäjän manipuloinnin uhka on muuttunut kuluneiden vuosien aikana ja miltä sen tulevaisuus tällä hetkellä näyttää?

Tutkimuskysymyksiin vastaamalla tavoitteena oli saada konkreettisia käytännön esimerkkejä siitä, miten yritykset voivat varautua käyttäjän manipuloinnin uhalta, jotta ne eivät joutuisi sen uhriksi. Tavoitteena oli myös saada kokonaiskuva siitä, miten suuri ongelma käyttäjän manipulointi on ja tulee tulevaisuudessa olemaan.

2.2 Aiheen rajaus

Työn teoriaosuudessa käsitellään yleisellä tasolla käyttäjän manipulointia ja erilaisia manipulointikeinoja. Työssä ei kuitenkaan käsitellä hyökkäystekniikoiden teknistä puolta tai mennä niiden yksityiskohtiin.

Varautumista käyttäjän manipuloinnilta käsitellään yrityksien näkökulmasta. Rajaus perustuu siihen, että kaikissa tutkimuksissa ja artikkeleissa puhutaan yleensä vain yritysten ja yritysten varautumiskeinoista. Yksityishenkilöt voivat kuitenkin hyödyntää myös lähes samoja varautumiskeinoja, mutta selkeyden vuoksi työssä puhutaan vain yritysnäkökulmasta. Käyttäjän manipulointi on aiheena kuitenkin erittäin ajankohtainen (Clausnitzer 2021), mikä tuo lisää painoarvoa opinnäytetyölle.

Tarkastelu on työssä myös rajattu pahantahtoiseen manipulointiin, jolla hyökkäävällä osapuolella on tarkoitus esimerkiksi varastaa, kiristää tai vahingoittaa hyökkäyksen kohdetta. Tässä ei siis tarkastella niin kutsuttua hyväntahtoista manipulointia, joksikin esimerkiksi terapiaa voidaan mieltää (Hadnagy & Wilson 2010, s. 10–18).

2.3 Keskeiset käsitteet

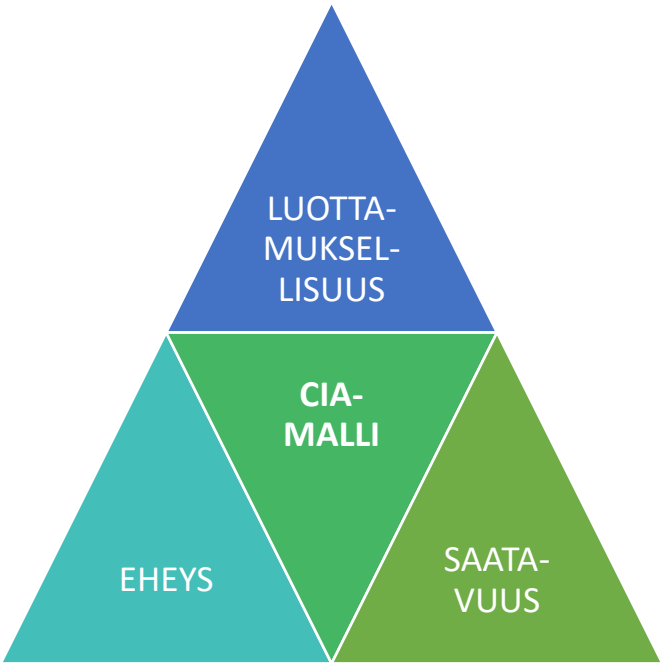
Tietoturva	Menetelmät, joilla varmistetaan suojatun tiedon luottamuksellisuus, eheys ja saatavuus, jotta tieto turvataan ja se ei pääsisi vääriin käsiin (Turvallisuuskomitea 2018, s. 15).
Käyttäjän manipulointi	Tietoturvan kontekstissa tapahtuva hyökkäys, jolla pyritään vaikuttamaan toisen ihmisen päätöksentekoon käyttämällä hyödyksi erilaisia hyökkäysmetodeja. Tämän kaltaiset vaikuttamishyökkäykset ovat usein vuorovaikutuksessa ihmisten kanssa, joissa hyväksikäytetään ihmisten inhimillisiä virheitä hyödyntämällä psykologisia vaikutteita. (Hadnagy & Wilson 2010, s. 9–10.)
Haavoittuvuuskartoitus	Toimintatapa, jolla pyritään kartoittamaan omassa toiminnassa tietoturvan heikkoudet ja vahvuudet. Haavoittuvuuskartoitusta voidaan analysoida tarkemmin kahden tekijän avulla, jotka ovat systemaattinen vahvuus ja henkilöstön vahvuus. (Mann 2008 s. 155–160.)
Systemaattinen vahvuus	Haavoittuvuuskartoituksessa analysoitava tekijä, jolla tutkitaan omassa tietoturvassa kykyä varautua käyttäjän manipuloinnin hyökkäyksiltä teknisten välineiden, järjestelmien ja fyysisen ympäristön kautta. Tässä ei oteta huomioon ihmisten vaikutusta hyökkäyksiin varautumisessa. (Mann 2008 s. 155–160.)
Henkilöstön vahvuus	Haavoittuvuuskartoituksessa analysoitava tekijä, jolla tutkitaan omassa tietoturvassa kykyä varautua käyttäjän manipuloinnin hyökkäyksiltä ihmisten kautta. Tässä ei oteta huomioon erilaisten välineiden ja ympäristön vaikutusta hyökkäysten varautumisessa. (Mann 2008 s. 155–160.)
Tietojenkalastelu	Käyttäjän manipuloinnin hyökkäysmetodi, jolla hyökkääjä pyrkii pääsemään käsiksi hyökkäyksen kohteen arkaluonteiseen tietoon tyypillisesti huijaussähköpostiviestien kautta. Hyökkääjä pyrkii esittäytymään usein luotettavana lähteenä huijatakseen

	kohdettaan. Englanniksi ilmiötä kutsutaan termillä phishing. (Hadnagy 2018, s. 229.)
Kohdennettu tietojenkalastelu	Tietojenkalastelun muoto, jota toteutetaan tietylle kohteelle, kuten tietylle yritykselle tai ihmiselle suuremman joukon sijaan. Englanniksi ilmiötä kutsutaan termillä spear-phishing. (Krombholz ym. 2015, s. 5; Salahdine & Kaabouch 2019, s. 4–5.)
Valaanpyynti	Tietojenkalastelun muoto, jota toteutetaan korkea-arvoisille henkilöille. Tyypillisesti nämä henkilöt ovat johtoasemissa esimerkiksi yrityksissä. Englanniksi ilmiötä kutsutaan termillä whaling. (Krombholz ym. 2015, s. 5; Salahdine & Kaabouch 2019, s. 4–5.)
Tekstiviestihuijaus	Tietojenkalastelun muoto, jota esiintyy tekstiviestien muodossa. Englanniksi ilmiötä kutsutaan termillä smishing, joka muodostuu sanoista short message service phishing. (Hadnagy 2018, s. 240.)
Soittopyyntöurkinta	Tietojenkalastelun muoto, jota esiintyy äänen muodossa esimerkiksi puhelimessa tai ääniviestien välityksellä. Englanniksi ilmiötä kutsutaan termillä vishing, joka muodostuu sanoista voice phishing. (Hadnagy 2018, s. 233.)
Houkuttelu	Käyttäjän manipuloinnin hyökkäysmetodi, jossa hyökkääjä käyttää tietynlaista houkutinta päästäkseen tavoitteisiinsa kohteensa kanssa. Tämä houkutin voi olla esimerkiksi lupaus palkinnosta, sisällöstä tai palveluksesta, joka houkuttelee hyökkäyksen kohdetta toimimaan hyökkääjän haluamalla tavalla. (Ozkaya 2018, s. 284.)
Peitetarina	Käyttäjän manipuloinnin hyökkäysmetodi, jossa hyökkääjä luo itselleen identiteetin, jonka taakse hän naamioituu hyökkäyksen aikana. Hyökkääjä voi keksiä kokonaan uuden identiteetin tai esittäytyä jo olemassa olevana henkilönä tai yrityksenä. (Hadnagy & Wilson 2010, s. 78–93.)

Käänteinen käyttäjän manipulointi	Käyttäjän manipuloinnin hyökkäysmetodi, jossa hyökkäyksen kohde ottaa normaalista poiketen yhteyttä hyökkääjään. Hyökkääjä luo tilanteen, jossa kohde tuntee tarvitsevansa hyökkääjää omiin tarpeisiinsa. Tätä voidaan toteuttaa esimerkiksi sosiaalisen median kautta väärennettyjen profiilien avulla. (Krombholz, Hobel, Huber, Weippl 2015, s. 3.)
Tailgating	Käyttäjän manipuloinnin hyökkäysmetodi, joka tarkoittaa suomeksi vapaasti käännettynä ”perässä roikkumista”. Tässä hyökkääjä seuraa fyysisesti tietyn yrityksen työntekijää, kunnes hän pääsee alueelle, jonne hänellä ei olisi normaalisti pääsylupaa. Tämä tapahtuu esimerkiksi tilanteissa, joissa moni ihminen menee samalla ovenavauksella sisälle suojattuihin tiloihin. (Ozkaya 2018, s. 111.)
Olan yli kurkkiminen	Käyttäjän manipuloinnin hyökkäysmetodi, jossa hyökkääjä pyrkii saamaan tietoa kohteeltaan tyypillisesti kurkkien hänen olkansa yli, jota hyökkääjän ei ole tarkoitus nähdä. Esimerkiksi salasanoja, käyttäjätunnuksia tai koodeja voidaan nähdä tätä metodia hyödyntämällä. Hyökkääjä voi myös hyödyntää erilaisia välineitä helpottaakseen näkyä halutulle tiedolle, kuten kameraa, kiikareita tai kännykkää. (Choi, Choi, Su 2016, s. 514–516.)
Dyykkaus	Toimintaa, jossa henkilö kaivaa ja kerää roska-astioista tavaraa. Yleiskäytössä tällä termillä tarkoitetaan toimintaa, jossa sitä tekevä ihminen elää köyhyydessä ja etsii ruokaa, vaatteita tai panttipulloja selviytyäkseen. Tietoturvan kontekstissa tämä on yksi käyttäjän manipuloinnin hyökkäysmetodeista, jossa hyökkääjä etsii hyödyllistä tietoa roska-astioista, jota hän voi käyttää edukseen osana suurempaa tietoturvahyökkäystä. (Ozkaya 2018, s. 110.)

3 Tietoturva ja CIA-malli

Tietoturvalla tarkoitetaan erilaisia menetelmiä, joilla suojeltua tietoa pyritään turvaamaan niin, ettei se joutuisi vääriin käsiin (Turvallisuuskomitea 2018, s. 15). Tietoturvassa korostuu niin kutsuttu CIA-malli, joka muodostuu sanoista *Confediality* (suom. luottamuksellisuus), *Integrity* (suom. eheys) ja *Availability* (suom. saatavuus). Näissä kiteytetään tietoturvan merkitys ja mitä tekniset toimet pyrkivät tehtävillään tekemään. (Varshney & Gupta 2017, s. 1–2.) Mallia kutsutaan myös CIA-kolmioksi, sillä jokainen osa-alue mallissa on riippuvainen toinen toisistaan (Kuvio 1). Tämä tarkoittaa siis sitä, että tietoturva ei olisi täydellinen ja kokonaisvaltainen ilman jokaista kolmion osa-aluetta. (Coss & Samonas 2014, s. 1–2.)



Kuvio 1. Tietoturvan CIA-malli

Luottamuksellisuudella tarkoitetaan tietoturvassa sitä, että suojattu data pysyy luottamuksellisena ja arkaluonteista dataa suojataan oikealla tavalla. Suojattuun dataan pääsee täten käsiksi vain henkilöt, joilla on siihen oikeus. (Varshney & Gupta 2017, s. 1–2.)

Eheydellä vuorostaan tarkoitetaan sitä, että vain oikeutetut henkilöt saavat muokata tietoa. Tieto täten pysyy johdonmukaisena ja täsmällisenä, kun sitä ei ulkopuolinen henkilö ilman asianmukaista todennusta pääse muokkaamaan. Eheys takaa näin turvallisen toiminnan järjestelmissä, jossa voidaan toimia huolimatta ulkoapäin tulevista tietomuutoksista. (Varshney & Gupta 2017, s. 1–2.)

Saatavuudella pyritään siihen, että tieto on aina saatavilla oikeille henkilöille, kun sitä tarvitaan. Tämä siis tarkoittaa sitä, että saatavuus on toteuduttava haluttuun tietoon ilman minkäänlaisia esteitä. (Varshney & Gupta 2017, s. 1–2.)

Tietoturvan tavoitteena on siis tiedon suojeleminen tietoturvahyökkäyksiltä, kuten esimerkiksi käyttäjän manipuloinnilta. Jos tietoturvahyökkäys onnistuu, se vahingoittaa CIA-kolmion osa-alueita, eli vähentää tiedon luottamuksellisuutta, eheyttä ja/tai saatavuutta. (Varshney & Gupta 2017, s. 1–2; Coss & Samonas 2014, s. 1–2.)

4 Käyttäjän manipulointi ja hyökkäysmetodit

Tässä luvussa tarkennetaan käsitettä käyttäjän manipulointi ja mitä se tarkoittaa. Tämän lisäksi luvussa esitellään yleisimpiä käyttäjän hyökkäysmetodeja liittyen käyttäjän manipulointiin.

4.1 Termin määrittelyä

Käyttäjän manipulointi (engl. Social engineering) tarkoittaa tietoturvan kontekstissa erilaisia manipulointikeinoja ja hyökkäysmetodeja, joiden avulla hyökkääjä pyrkii vaikuttamaan manipuloinnin kohteen päätöksentekoon. Käyttäjän manipulointi luo silloin tietoturvauhan hyökkäyksen kohteelle. Kohteina ovat tyypillisesti ihmiset, joko yksityishenkilöt tai henkilöstö yrityksissä. Hyökkäyksen kohde pyritään saamaan tekemään asioita, joita normaalisti hän ei välttämättä tekisi. Manipulointia voidaan kuvailla muun muassa valehteluna, huijaamisena, näyttelemisenä sekä valheellisten ihmissuhteiden luomisena. Valitettavan usein on myös niin, ettei kohde tajua tehneensä virheen. Hyvin yleinen manipulointikeino onkin tietojenkalastelu-viestit, joissa hyökkääjä yrittää nimensä mukaisesti houkutella saada jotain tietoa kohteeltaan hyödyntäen erilaisia psykologisia vaikutteita. (Hadnagy & Wilson 2010, s. 9–10; Krombholz ym. 2015, s. 2–3.) Erilaisia manipulointikeinoja ja hyökkäysmetodeja käydään tarkemmin läpi myöhemmissä luvuissa. Esimerkiksi toisinaan ihmiskontaktia ei tarvitse lainkaan, jotta voidaan suorittaa onnistunut hyökkäys, kuten esimerkiksi dyykkauksessa tai olan yli katsomisessa. (Hadnagy & Wilson 2010, s. 9–10.)

Käyttäjän manipuloinnin motiivina on usein saada luvaton pääsy johonkin ympäristöön, kuten yrityksen tietokantoihin, raha tai muun arkaluonteisen tiedon saanti. Toisin sanoen hyökkääjä pääsee tavoitteeseensa ja samalla kohde puolestaan kärsii menettämällä arkaluontoista dataa tai muuta, joka on ollut hyökkääjän tavoitteena. (Hadnagy & Wilson 2010, s. 9–10; Krombholz ym. 2015, s. 2–3.) Kuitenkin käyttäjän manipulointi -termin merkitys on yllättävän monimutkainen, mikä selitetään tässä luvussa myöhemmin.

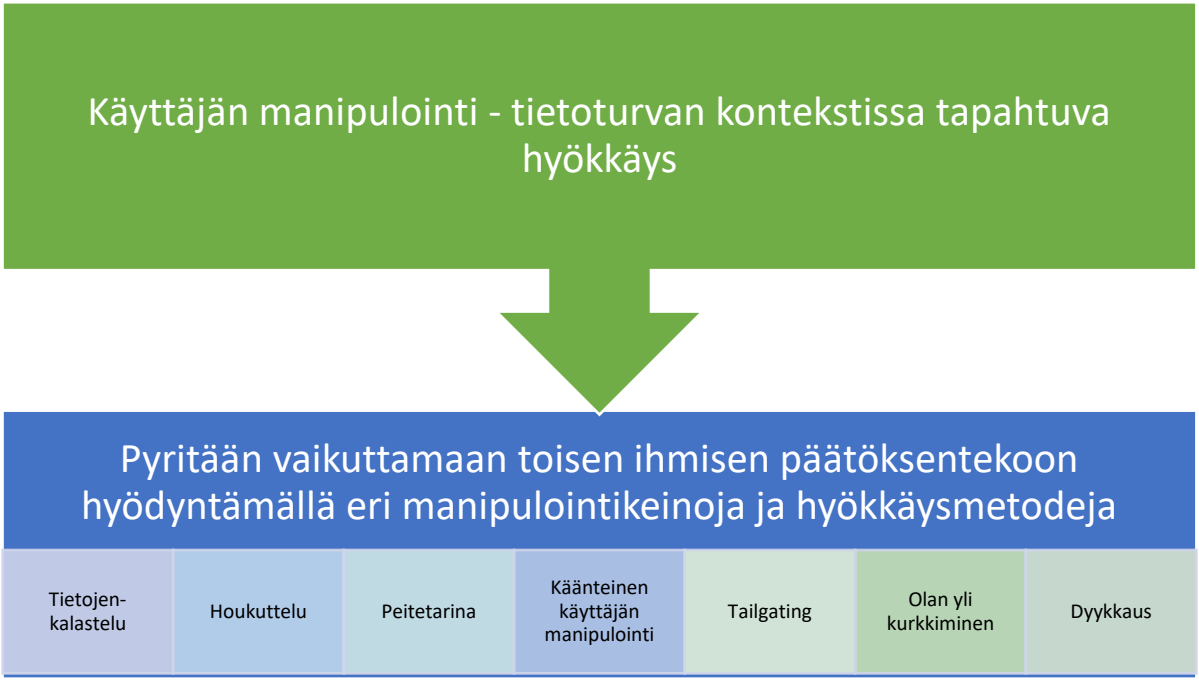
Usein ihmiset olettavat, että kyberhyökkäykset ja tietoturvauhat ovat yleisesti vain teknisiin asioihin liittyviä uhkia, joita vastaan suojaudutaan esimerkiksi palomuureilla, tietosuojapäivityksillä ja virustorjuntaohjelmilla. Kuitenkin todellisuus ei voisi olla kauempana tästä, sillä usein heikko lenkki yrityksissä on nimenomaan ihmiset, joita ei voida samaan tapaan suojata kuten ohjelmistoja. Tästä syystä teknisellä tasolla murtautuminen esimerkiksi yrityksen sisäiseen infrastruktuuriin voi olla hyvinkin työlästä vahvojen suojausten myötä. Kuitenkin käyttäjän manipuloinnin taidot osaava ihminen voi saada paljon enemmän irti paljon pienemmällä vaivalla. (Ozkaya 2018, s. 5.)

On hyvä huomioida, mitä ”käyttäjän manipulointi” -termillä tarkoitetaan. Englanniksi termi ”Social engineering” on suhteellisen yleistävä termi, joka kattaa muutakin, kuin pelkästään tietoturvaan kohdistuvia hyökkäyksiä. Esimerkiksi termillä voidaan ajaa myös positiivista asiaa. Lääkärit tai terapeutit voivat vaikuttaa ihmisten päätöksentekoon hyvässä tarkoituksessa, jolloin tavoitteena on esimerkiksi ihmisen hyvinvoinnin edistäminen. (Ozkaya 2018, s. 11; Hadnagy & Wilson 2010, s. 10–18.) Tätä esiintyy periaatteessa aivan arkielämässäkin missä vain tilanteessa, jossa halutaan vaikuttaa toisten ajatuksiin ja mielipiteisiin. Tavoitteena on silloin muuttaa vaikutuksen alaisena olevien päätöksentekoon ilman, että hän menettää jotain tai kärsii sen seurauksista. Kuitenkin tietoturvan kontekstissa tällaista ”hyväntahtoista manipulointia” ei ole olemassa, sillä se on pelkästään tietoturvan asettamista vaaran alle. (Hadnagy & Wilson 2010, s. 10–18.)

Suomeksi ”social engineering” -termille ei ole olemassa mitään vakiintunutta käännöstä. Osa käyttää pelkästään englannin kielistä termiä ilmiötä kuvaillessaan, kun taas osa käyttää erilaisia muunnelmia termistä ”käyttäjän manipulointi”, kuten esimerkiksi ”sosiaalinen vaikuttaminen” tai ”sosiaalinen manipulointi”. Tässä työssä käytetään termiä ”käyttäjän manipulointi” hämmennyksen välttämiseksi. Samaten Sanastokeskus ja Kyberturvallisuuden sanasto käyttävät tätä ilmaisua. Joka tapauksessa, suomen kielellä kaikki muunnelmat termistä ”käyttäjän manipulointi” liittyvät yksinomaan negatiiviseen tarkoitukseen tietoturvaan kohdistettuna. (Sanastokeskus 2003; Turvallisuuskomitea 2018, s. 19.)

4.2 Käyttäjän manipuloinnin hyökkäysmetodit

Tässä luvussa käsitellään erilaisia manipulointikeinoja sekä hyökkäysmetodeja, joka ovat yleisimpiä keinoja käyttäjän manipulointiin liittyen (Kuvio 2).

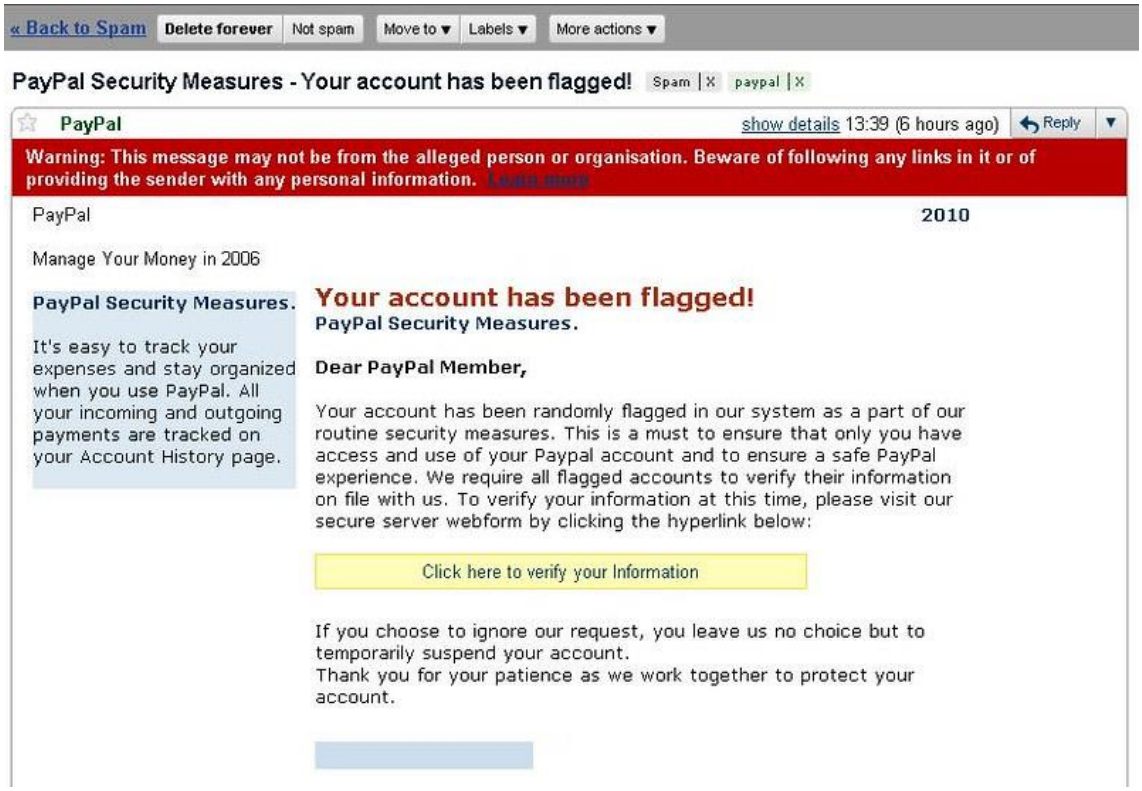


Kuvio 2. Käyttäjän manipulointi ja eri manipulointikeinot ja hyökkäysmetodit

4.2.1 Tietojenkalastelu

Tietojenkalastelu (engl. Phishing) on käyttäjän manipuloinnin manipulointikeino, jolla hyökkääjä pyrkii manipuloimaan kohdettansa paljastamaan arkaluonteista tietoa usein teeskentelemällä olevansa luotettava lähde. Teoriassa tietojenkalastelua voi tapahtua monella eri tavalla, mutta tyypillisin ja yleisin tapa tällaisille hyökkäyksille tapahtuu sähköpostin kautta. Tällä tavalla tietojenkalasteluviestejä voidaan lähettää suurissa määrin lukuisille ihmisille roskapostiviestien tavoin. Tietojenkalastelu on nykyään käyttäjän manipuloinnin käytetyimpiä menetelmiä hyökkääjien keskuudessa ja onkin tietomurtojen yksi suurimpia tekijöitä. (Krombholz ym. 2015, s. 3; Hadnagy 2018, s. 229; Sumner & Yuan 2019 s. 1.)

Sähköpostiviesti on tehokas tapa levittää haittaohjelmia tai linkkejä haitallisiin verkkosivuihin, joilla voidaan uhata ja kiristää kohdetta entistä tehokkaammin (Krombholz ym. 2015, s. 3; Hadnagy 2018, s. 229). Alla on esimerkki tyypillisestä tietojenkalasteluyrityksestä sähköpostissa (Kuvio 3).



Kuvio 3. Esimerkki tietojenkalastelusta (Lähde: Flickr)

Kuten kuviossa näkyy, lähettäjä on pyrkinyt vaikuttamaan vastaanottajaan väittämällä viestin tulleen PayPalilta. Viestissä pyydetään klikkaamaan linkkiä, joka viestin mukaan vahvistaisi vastaanottajan omat tiedot. Käyttäjää varoitellaan tilin sulkemisesta, mikäli vastaanottaja ei tee kuten pyydetään, lisäten näin painetta hyväuskoiselle lukijalle. Tämä on klassinen esimerkki kohteen manipuloimisesta, kun kiireellä pyritään painostamaan kohde reagoimaan hyökkääjän haluamalla tavalla. (Hadnagy 2018, s. 134–137.)

Tietojenkalastelua esiintyy myös monissa eri muodoissa sähköpostien lisäksi. Jos tietojenkalastelua kohdistetaan tiettyihin ihmisiin tai yrityksiin, kyseessä on *kohdennettu tietojenkalastelu* (engl. spear-phishing). Tämäntyyppiset tietojenkalastelut ovat usein hienovaraisemmin luotu, sillä näissä tapauksissa hyökkääjän on ensin täytynyt kerätä tietoa kohteestaan ennen itse hyökkäystä, jotta huijaus nähtäisiin mahdollisen uskottavana. Kun hyökkäysten kohteena on korkea-arvoisia henkilöitä, kuten yrityksen johtajia, käytetään englanniksi nimitystä *whaling*. (Krombholz ym. 2015, s. 5; Salahdine & Kaabouch 2019, s. 4–5.) Suomeksi tämä termi on nimetty valaanpyynniksi. Tässä samaan tapaan tietojenkalastelua suoritetaan huolellisemmin, sillä hyökkäyksen onnistumisen mahdollisuusprosentti on huomattavasti pienempi verrattuna tavanomaiseen tietojenkalasteluun, jossa kohteena voi olla kuka tahansa tavallinen ihminen. Yksityishenkilöillä ei välttämättä ole yhtä lailla hallussa käyttäjän manipuloinnilta suojautuminen. (Krombholz ym. 2015, s. 5.)

Toisenlaisia tietojenkalastelun muotoja ovat *vishing* (toiselta nimeltään engl. voice phishing) ja *smishing* (toiselta nimeltään engl. short message service phishing) (Hadnagy 2018, s. 233–240). Suomeksi nämä termit ovat soittopyyntöurkinta ja tekstiviestihuijaus (Sanastokeskus 2020). Soittopyyntöurkinta -metodissa tietojenkalastelua tehdään äänen muodossa, kuten puhelimessa tai ääniviestillä. Tekstiviestihuijaus -metodissa tietoja urkitaan vuorostaan tekstiviestin muodossa. Nämä metodit eivät ole yhtä suosittuja ammattilaishyökkääjien keskuudessa, sillä ne eivät ole yhtä tehokkaita kuin sähköpostin kautta tehty tietojenkalastelu. (Hadnagy 2018, s. 233–240.)

Yksi suurimmista onnistuneista tietojenkalasteluhyökkäyksistä tapahtui 2013–2015 välillä, kun liettualainen ryhmä onnistui huijaamaan Googlelta ja Facebookilta yli 100 miljoonan dollarin edestä rahaa tietojenkalasteluviestien avulla sähköpostissa. Viesteissä hyökkääjäryhmä esitteli itseään taiwanilaisyrityksenä nimeltä Quanta, jonka kanssa Facebook ja Google tekevät normaalisti kauppaa. Kyseiset viestit oli lähetetty Googlen ja Facebookin työntekijöille, jotka olivat hyökkäysten aikana vastuussa yritysten transaktioista. Tämän takia työntekijät siirsivät tietämättään mittavat summat rahaa hyökkääjille. (Huddleston 2019.)

4.2.2 Houkuttelu

Houkuttelulla (engl. baiting) tarkoitetaan hyökkäysmetodia, jolla hyökkääjä houkuttelee kohteensa toimimaan haluamallaan tavalla käyttämällä jonkinlaista houkutinta hyödyksi. Hyökkääjä voi luvata esimerkiksi jonkinlaisen palkinnon kohteelle, jos hän toimii hyökkääjän tavoitteiden mukaisesti. Sähköpostien kautta hyökkääjät voivat esimerkiksi lähettää houkuttelevia linkkejä, joissa lukee viestin saajan voittaneen esimerkiksi suuren summan rahaa. (Ozkaya 2018, s. 284; Salahdine & Kaabouch 2019, s. 4–5.) Myös laittomasti tuotettua sisältöä, eli piraattisisältöä, kuten elokuvia, pelejä ja muita mediaohjelmia, voidaan käyttää hyödyksi, kun ihmiset haluavat ladata laittomasti haluamaansa sisältöä. Hakkerit voivat houkutella käyttäjiä lataamaan linkkien kautta sisältöä, jotka oikeasti sisältävätkin haittaohjelmia. Näin hyökkääjät voivat lopulta kiristää käyttäjiä ja varastaa heidän tietojaan. (Ozkaya 2018, s. 284.)

Toinen tapa houkutella ihmisiä on jättää esimerkiksi haittaohjelman sisältävän USB-tikku organisaation parkkipaikalle siinä toivossa, että joku hyväuskoinen ihminen ottaisi sen mukaansa ja laittaisi sen kyseisen organisaation tietokoneeseensa kiinni. Siten tikussa oleva haittaohjelma voi levitä koko organisaation verkostoon tehden valtavaa tuhoa. Näin kävi vuonna 2008 Lähi-idässä, kun USA:n armeijan tietoverkkoon päästiin käsiksi yhden USB-tikun avulla. Valtavia määriä USA:n armeijan arkaluonteista dataa siirrettiin hyökkääjille kenenkään huomaamatta. Tämä on yksi suurimpia tietomurtoja Yhdysvaltain armeijan historiassa. (Stewart 2010.)

4.2.3 Peitetarina

Peitetarina (engl. pretexting) on nimensä mukaisesti tapa, jolla hyökkääjä naamioi itsensä jonkinlaisen identiteetin taakse, jolla hän esittäytyy kohteelleen. Hyökkääjä voi esimerkiksi esittäytyä pizzakuskina, IT-tukihenkilönä, yrityksen johtajana tai missä tahansa muussa roolissa ja opetella sen täydellisesti. Käytännössä peitetarinan hyödyntäminen vaatii hyökkääjältä erinomaisia näyttelijän taitoja, jotta hän kuulostaa mahdollisimman uskottavalta kohteelle. (Hadnagy & Wilson 2010, s. 78–93; Salahdine & Kaabouch 2019, s. 5.) Peitetarinan ei aina tarvitse olla kokonaan keksitty, vaan hyökkääjä voi esittää jotain oikeaa ihmistä tai yritystä, jonka identiteetin hän on opetellut itselleen riittävän tiedonhankinnan jälkeen. Peitetarinaa voi käytännössä hyödyntää niin kasvotusten, puhelimessa tai internetissä. Peitetarina yhdistettynä tietojenkalasteluun voikin olla erittäin voimakas raha, kun hyökkääjä luo uskottavan kuvan itsestään ja viestin sisällöstä. (Hadnagy & Wilson 2010, s. 78–93.)

Luultavasti tunnetuin ja yksi vanhimpia peitetarinoita on niin kutsuttu ”nigerialaiskirje”, jossa yhdistyy peitetarinan lisäksi myös edelliset mainitut metodit eli tietojenkalastelu ja houkuttelu. Tässä huijauksessa sähköpostiviestin lähettäjä tekeytyy olevansa nigerialainen prinssi, joka olisi valmis lähettämään viestin saajalle suuren summan rahaa, kunhan aluksi huijauksen kohde lähettää tietyn alkusumman huijarille jonkun ongelman ratkomiseksi. Sinisilmäinen kohde voi lähettää valtavia summia rahaa huijarille ilman, että mitään rahaa ei tulekaan toiselta puolelta. Tämä oli varsin tehokas käyttäjän manipuloinnin hyökkäys sähköpostin alkuvuosina ja monet ihmiset tulivat näin huijatuiksi. (Ozkaya 2018, s. 9.)

Peitetarinaa hyödynnettiin myös muutama vuosi sitten käyttäjän manipuloinnin vaikuttamiskeinona vuonna 2017, kun kanadalainen yliopisto joutui huijauksen kohteeksi, mikä johti yli 8 miljoonan dollarin menettämiseen. Hyökkääjä esitti yhtä koulun tukkumyyjistä ja osasi taitavasti suostutella yliopiston henkilökuntaa luovuttamaan heidän pankkitietonsa hyökkääjälle. (Pearson 2017.) Hyökkäyksessä yhdistettiin hyökkäysmetodeina peitetarina sekä tietojenkalastelu sähköpostiviestissä, joka oli tarpeeksi uskottava hyökkäyksen onnistumiseksi.

4.2.4 Käänteinen käyttäjän manipulointi

Reverse social engineering, eli vapaasti suomennettuna käänteinen käyttäjän manipulointi, tarkoittaa toimintaa, jolla hyökkääjä pyrkii saamaan kohteensa ottamaan aktiivisemman roolin manipuloinnin aikana. Toisin sanoen hyökkääjä pyrkii luomaan tilanteen, jossa hyökkäyksen kohde luulee tarvitsevansa hyökkääjän apua omiin tarpeisiinsa. Esimerkiksi hyökkääjä voi esittää olevansa IT-tukihenkilö. Hyökkääjä on voinut esimerkiksi ensin onnistua asentamaan jonkun haittaohjelman kohteen tietokoneeseen, jonka jälkeen kohde luulee tarvitsevansa hyökkääjän apua. Peitetarinaa hyödyntämällä kohteelta on paljon helpompi urkkia mitä tahansa tietoja ongelman ”korjaamiseen”. (Krombholz ym. 2015, s. 3.)

Hyökkäys voidaan toteuttaa myös sosiaalisen median kautta. Tällaisten medioiden, kuten Facebookin tai Instagramin kautta hyökkääjä voi luoda itselleen houkuttelevan profiilin ja odottaa, kunnes kohde ottaa häneen yhteyttä. Yhteyden luomista voi parantaa samat kiinnostuksen kohteet ja kuvapostaukset. Etenkin deittailusovellusten, kuten Tinderin kautta hyökkääjä voi houkutella kohdettaan viehättävällä profiililillaan, jonka ei tietenkään tarvitse olla aito. Kun yhteys on luotu, taitava hyökkääjä voi alkaa urkkimaan haluamiaan tietoja hyväuskoiselta kohteeltaan. (Irani ym. 2011, s. 3–5.) Tämäntapaisia vaikuttamishyökkäyksiä kutsutaan yleisesti rakkauspetoksiksi tai -huijauksiksi. Vuosina 2019–2020 kaksi suomalaisnaista onnistui saamaan rakkauspetosten avulla suuria määriä rahaa vanhemmilta miehiltä erilaisilla seuranhakupalstoilla. He onnistuivat huijaamaan yhteensä 170 000 € keksimällä erilaisia syitä rahan saamiseen, joihin nämä miehet lankesivat. (Tuominen 2022.)

4.2.5 Tailgating

Tailgating -termille ei löydy varsinaista termiä suomeksi, mutta sen voi vapaasti kääntää ”perässä roikkumiseksi”. Tämä metodi käytännössä tarkoittaa sitä, että hyökkääjä saa pääsyn jollekin fyysiselle alueelle, jonne hän ei normaalisti saisi mennä. Tätä toteutetaan ympäristössä tyypillisesti niin, että hyökkääjä seuraa toisen henkilön perässä, jolla vuorostaan on pääsy kyseiselle suojatulle alueelle. Hyökkääjä kävelee hänen mukanaan esimerkiksi ovesta sisään alueelle. (Ozkaya 2018, s. 111; Salahdine & Kaabouch 2019, s. 5.) Tämä metodi hyödyntää erityisesti seurattavan ihmisen kohteliaisuutta, sillä jos suojatulle alueelle pääseminen vaatii esimerkiksi läpikulkua ovesta läpi, tyypillisesti ensimmäisenä sisään menevä ihminen pitää kohteliaasti ovea auki seuraavalle sisääntulijalle. Jos kyseisen ympäristön ulko-ovet ovat myös hitaita sulkeutumaan, kuka tahansa voisi nopeasti livahtaa sisään samalla ovenavauksella, kun ovi on menossa kiinni itsestään. Jos ovi tarvitsisi sattumoisin avainkortin, hyökkääjä voi esitellä etsivänsä taskuistaan sitä, kunnes joku muu avaa oven hänen puolestaan. (Ozkaya 2018, s. 111.)

Hyökkääjä voi myös käyttää hyödykseen peitetarinaa parantaakseen mahdollisuuksiaan päästä alueelle. Jos hyökkääjä esimerkiksi esittäytyy jonkinlaisena huoltohenkilönä ja kantaa raskaita tavaroita molemmilla käsillään, on toinen ihminen yleensä ilomielin auttamassa häntä päästä sisälle. Eräs Ylen toimittaja (Peiponen 2018) testasi vuonna 2018 useiden yritysten tilaturvallisuutta tällä tavoin pukeutumalla pelkkään huomioliiviin ja kantaen tikkaita toisessa kädessään. Kokeilun aikana hän pääsi tunkeutumaan jopa kymmeneen yhdestätoista yrityskohteesta. Useat yritysten työntekijät auttoivat toimittajaa pääsemään sisätiloihin ilman minkäänlaisia turvatoimia tai kysymyksiä siitä, millä asialla kyseinen toimittaja oli. (Peiponen 2018.)

4.2.6 Olan yli kurkkiminen

Olan yli kurkkiminen (engl. shoulder surfing) tarkoittaa toimintaa, jossa hyökkääjä katsoo toisen ihmisen olan yli nähdäkseen jotain kriittistä tietoa, jota ei ole tarkoitettu hänen nähtäväkseen. Tämä voi tarkoittaa mitä tahansa arkaluonteista tietoa, kuten esimerkiksi salasanoja ja käyttäjätunnuksia. Tämä varsin yksinkertainen hyökkäys on hyvä esimerkki metodista, joka vaatii hyvinkin vähän taitoja sen hyödyntämiseen. (Choi ym. 2016, s. 514–516.) Tämä metodi on yksinkertaisuutensa vuoksi erittäin pahalaatuinen hyökkäysmetodi, sillä sitä voi käyttää melkeinpä missä tahansa ympäristössä. Etenkin ympäristöt, joissa on paljon ihmisiä samassa tilassa, ovat optimaalisia olan yli kurkkimiselle. Väkitungoksessa kohde ei yleensä tajua olevansa hyökkäyksen kohteena. Tällaisia ympäristöjä ovat muun muassa junat, lentokentät ja ylipäätään muut julkiset paikat, kuten kahvilat ja ostoskeskukset. (Ozkaya 2018, s. 112.)

Olan yli kurkkiminen voidaan suorittaa toisillakin tavoin kuin suoralla katsekontaktilla. Sitä voidaan suorittaa erilaisten välineiden avulla, jotka voivat edesauttaa hyökkääjää saamaan paremman näkökulman kohteeseensa. Esimerkiksi kännykän, kameran, kiikareiden tai muiden optisten laitteiden käyttö voi parantaa mahdollisuuksia nähdä kohteen tietoja. Hyökkääjä voi myös tallentaa videolla näkemänsä tiedon, kuten käyttäjätunnuksen ja salasanan, joita hän voi käyttää myöhempään tarkoitukseen. Välineiden avulla hyökkääjän ei tarvitse olla välttämättä edes kohteen lähellä, vaan hän voi suorittaa hyökkäyksen paljon kauempaa. Esimerkiksi, jos kohde on näppäilemässä ovikoodia yrityksen ulko-oveen, voi hyökkääjä urkkia koodia kauempaa kiikareiden avulla. (Choi ym. 2016, s. 514–516.) Tässä esimerkissä myös lämpökamera voi olla erittäin hyödyllinen väline hyökkääjälle, sillä sen avulla hän voi nähdä koodin jälkikäteen tarkastellessa lämpöpisteitä ja päätellä lämpötilan mukaan, mitä näppäintä on painettu missäkin järjestyksessä (Bekaert ym. 2022, s. 2–3).

On huomioitavaa, että olan yli kurkkiminen ei poikkeuksellisesti vastaa suoraan sitä, mitä käyttäjän manipulointi -käsitteellä tarkoitetaan, eli vaikuttamista toisen käytökseen. Kuitenkin tätä metodia käyttämällä voidaan kerätä tietoja, joita pystytään hyödyntämään erityisesti myöhemmissä vaiheissa osana suurempaa hyökkäystä. Käyttäjän manipuloinnin eri vaiheet alusta loppuun selitetään tarkemmin luvussa 5.

4.2.7 Dyykkaus

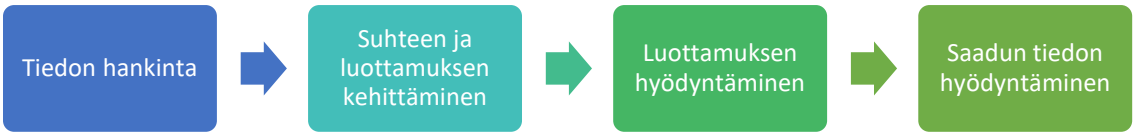
Dyykkaus (engl. dumpster diving) on nimensä mukaisesti toimintaa, jossa tekijä etsii tavaroita roska-astioista. Tämä termi tarkoittaa yleiskäytössä lähinnä ihmisiä, jotka etsivät yleisistä roska-astioista tarpeellisia tavaroita elämiseen, kuten ruokaa, pulloja tai vaatteita. Tätä toimintaa ei siksi katsota varsinaisesti pahalla, sillä sitä ei ole kielletty useissa maissa lailla, Suomi mukaanluettuna. Kuitenkin tietoturvan maailmassa dyykkauksella on toinen tarkoitus, jota hyödynnetään käyttäjän manipuloinnin vaikuttamishyökkäyksissä. (Ozkaya 2018, s 110; Luo, Brody, Seazzu & Burd 2011, s. 4–5.)

Useat yritykset eivät vaivaudu lajittelemaan roskiaan siten, että roskat, joissa on arkaluontoista materiaalia, ja normaalit roskat eroteltaisiin erikseen, vaan ne yleensä heitetään samaan roska-astiaan. Hyökkääjät voivat hyödyntää tätä tilaisuutta tonkimalla muiden roskia esimerkiksi yrityksen tilojen ulkopuolella sijaitsevasta roska-astiasta. Jos heillä käy tuuri, he voivat löytää arkaluonteista tietoa esimerkiksi yksittäisistä henkilöistä, salasanoista, haavoittuvuusraporteista ja melkeinpä mistä vain muusta. Näitä tietoja voidaan hyödyntää siten erityisesti myöhemmissä hyökkäysvaiheissa. Dyykkaus on tästä syystä myös olan yli kurkkimisen kanssa poikkeava käyttäjän manipuloinnin hyökkäysmetodi, jota hyödynnetään pääasiassa tiedonhankinnassa, eikä niinkään vaikuttamisyrityksissä. Dyykkaus on jälleen hyvä esimerkki siitä, että käyttäjän manipuloinnin hyökkäykset eivät vaadi välttämättä mitään aikaisempia taitoja. Tiettyjä hyökkäyskeinoja voi kuka tahansa osata hyödyntää niiden yksinkertaisuuden ja helppouden takia. (Ozkaya 2018, s 110; Luo, Brody, Seazzu & Burd 2011, s. 4-5.)

Vuonna 2010 Boston Globe-lehden kuvaaja Yhdysvalloissa osoitti, mitä roskien huono hävittäminen voi saada aikaan. Hän huomasi roska-astiassa lojuvan lukuisia määriä asiakirjoja, joissa oli listattuna sairaalassa käyneiden ihmisten nimiä, osoitteita, sosiaaliturvatunnuksia ja testituloksia. Selvisi, että lääkärilaskutusyhtiö yhdessä asianomaisten lääkäreiden kanssa olivat heittäneet vastuuttomasti asiakirjoja roskiin ilman oikeanlaista hävittämistä. Yhdysvaltain lain mukaan nämä asiakirjat olisi kuullut hävittää esimerkiksi polttamalla tai silppuamalla. Vastuussa olevat joutuivat maksamaan 140 000 dollaria sakkoa tapahtuneesta. Jos nämä tiedot olisivat joutuneet vääriin käsiin, hyökkääjät olisivat voineet suorittaa lukuisia identiteettivarkauksia ja vaarantaneet useat potilaat muiden tietoturvahyökkäyksen kohteiksi. (Conaboy 2013.)

5 Käyttäjän manipuloinnin vaiheet

Käyttäjän manipulointi voidaan tiivistää Moutonin, Malanin, Leenenin ja Venterin (2014) mukaan neljään eri vaiheeseen, jotka ovat tiedon hankinta, suhteen ja luottamuksen kehittäminen, luottamuksen hyödyntäminen sekä saadun tiedon hyödyntäminen (Kuvio 4).



Kuvio 4. Käyttäjän manipuloinnin vaiheet

Onnistunut käyttäjän manipulointi alkaa kuvion (4) vasemmasta reunasta eli tiedon hankinnasta ja päättyy lopulta saadun tiedon hyödyntämiseen, jossa hyökkääjä käyttää hyödykseen kohteeltaan saamaansa tietoa (Mouton ym. s. 2). Nämä neljä eri vaihetta käydään läpi tarkemmin seuraavissa alaluvuissa.

5.1 Tiedon hankinta

Käyttäjän manipuloinnin ensimmäinen vaihe on tiedon hankinta. Tässä vaiheessa hyökkääjä on asettanut tavoitteensa, eli mitä hän haluaa hyökkäyksellään saavuttaa ja mikä tai kuka tulee olemaan hyökkäyksen kohteena. Tiedon hankintavaiheessa hyökkääjä käyttää aikaa etsimällä mahdollisimman paljon tietoa kohteestaan, jotta seuraavat hyökkäyksen vaiheet ovat mahdollisimman ennalta tarkoin suunniteltuja. Aikaisemmin kuvailtiin luvussa 4.2 erilaisia hyökkäysmetodeja, joita hyökkääjä voi käyttää hyödykseen. Tiedon hankintavaiheessa erityisesti dyykkaus voi osoittautua hyödylliseksi tavaksi saada tietoa kohteesta, jos hyökkääjällä käy hyvä tuuri. Jos hyökkääjän kohteena on yritys, hän voi kerätä tietoa esimerkiksi utelemalla fyysisesti yrityksen henkilöstöltä kysymällä erilaisia kysymyksiä. Hyökkääjän pitää kuitenkin pitää huoli siitä, että hän ei herätä epäilyksiä. (Ozkaya 2018, s. 14–15.) Kuvatuissa hyökkäysmetodeissa esimerkiksi peitetarinan rakentaminen, perässä roikkuminen (engl. tailgating) ja olan yli kurkkiminen voivat osoittautua erittäin hyödyllisiksi tiedonhankinnassa tarvitsematta teknisempiä taitoja.

Tietoa voidaan hankkia myös teknisemmillä keinoilla, mikä voi olla tehokkaampaa. Kaikki yleisesti saatavilla oleva tieto, kuten kohteen nettisivuilta, sosiaalisesta mediasta ja verkostosta voi löytyä paljon kaikenlaista hyödyllistä tietoa, jota hyökkääjä voi käyttää hyödykseen. Näitä ovat esimerkiksi yrityksessä työskentelevän työntekijän nimi, työnimike, läheiset ystävät ja kiinnostuksen kohteet. Hyökkääjä voi käyttää hyödykseen hakukoneita ja erilaisia sivustoja, joihin kerätään dataa ihmisistä ja muista kohteista. Myös perinteisesti soittamalla puhelimella, tekstiviestillä tai sähköpostiviestillä voidaan toteuttaa samankaltaista tiedonhankintaa. (Ozkaya 2018, s. 14–20.)

Tiedon hankinta on erittäin tärkeä osa käyttäjän manipulointia, sillä sen avulla hyökkääjä voi luoda persoonallisemman hyökkäystavan, jolla hän pyrkii vaikuttamaan kohteeseen. Onnistuneet hyökkäykset ovatkin hyödyntäneet saatua tietoa mahdollisimman paljon, jotta hyökkäyksen onnistumisen todennäköisyys kasvaa. (Mouton ym. 2014, s. 4.) Tärkeää on kuitenkin muistaa, ettei kaikkea tietoa yleensä kerätä yhtä aikaa, vaan tiedonkeruu on hyvin pitkä ja aikaa vievä prosessi. Tietoa voi tilanteen mukaan löytyä eri lähteistä vain vähän ja harvemmin vain yhtä tekniikkaa hyödyntämällä. Kuitenkin jokainen tiedonpalanen voi olla erittäin hyödyllistä hyökkääjälle, sillä ne auttavat yhdessä saamaan hyvän yleiskuvan kohteesta. (Ozkaya 2018, s. 14–20.)

5.2 Suhteen ja luottamuksen kehittäminen

Käyttäjän manipuloinnin seuraavassa vaiheessa, eli suhteen ja luottamuksen kehittämisessä, hyökkääjä aikoo hyödyntää saamaansa tietoa aiemmasta vaiheesta luodakseen suhdetta ja luottamusta hänen ja kohteensa välille. Taitava hyökkääjä osaa hyödyntää jokaista tiedonpalasta, joita hän on saanut käsiinsä tiedon hankintavaiheessa, jonka perusteella hän voi parantaa ja kohdentaa omaa lähestymistapaansa hyökkäyksen kohteeseensa. Ennen suhteen ja luottamuksen kehittämistä hyökkääjä voi luoda itselleen esimerkiksi peitetarinan, joka vahvistaa lähestymisen ”legitiimiyttä”. (Mouton ym. 2014, s. 5.)

Kun hyökkääjä on vuorovaikutuksessa hyökkäyksen kohteensa kanssa, voidaan sanoa, että hyökkäys on virallisesti alkanut. Jotta suhde luodaan onnistuneesti kohteen kanssa, täytyy hyökkääjällä olla tiedossa jo etukäteen, mitä hän haluaa kohteeltaan, kehen itse hyökkäys kohdistetaan ja mihin suuntaan hän aikoo viedä keskustelua. Tämäkään ei ole mitenkään nopea prosessi, vaan se vaatii paljon kärsivällisyyttä ja hyviä kommunikointitaitoja, jotta lopulta kohde tuntee luottavansa häneen. Kun yhteys on luotu kohteeseen, hyökkääjä voi alkaa enemmän ja paremmin manipuloimaan kohdettaan haluamallaan tavalla. (Mouton ym. 2014, s. 5.)

Tapa, jolla hyökkäys toteutetaan, vaikuttaa suhteen luomisen prosessiin. Jos kommunikointi hyökkääjän ja kohteen välillä on fyysistä, eli he puhuvat esimerkiksi kasvotusten, hyökkääjä pyrkii olemaan mahdollisimman ystävällinen ja jopa imarteleva kohteensa kanssa. Tavoitteena on, että kohde tuntee olonsa turvalliseksi ja hyväksi hänen kanssaan. Positiiviset interaktiot kohteen kanssa voivat vaikuttaa häneen psykologisesti positiivisella tavalla, jolloin seuraavilla keskustelukerroilla kohde tuntee olonsa entistä rennommaksi hyökkääjän kanssa. Nämä ovat toki myös hyökkääjän kannalta tärkeitä piirteitä, jos keskustelua käydään ilman fyysistä vuorovaikutusta, eli esimerkiksi sähköpostin kautta. Kuitenkin nämä korostuvat erityisesti fyysisessä ympäristössä, sillä siinä keskustelua käydään tiiviimmin, eli hyödynnetään ”small talk” tyyppistä kommunikointia. (Ozkaya 2014, s. 132–137.)

Taitava käyttäjän manipuloinnin hallitsija tietää, miten keskustelu tulee etenemään ja miten hänen kannattaa reagoida keskustellessaan kohteensa kanssa. Ensimmäisessä kohtaamisessa ei kuitenkaan välttämättä aina synny saman tien kahdenkeskistä yhteisymmärrystä ja luottamusta, vaan käyttäjän manipuloinnin ensimmäisen vaiheen tapaan tämäkin voi olla hyvinkin pitkä ja vaativa prosessi hyökkääjän kannalta. Tämä vaikuttaa erityisesti silloin, jos kommunikointi tapahtuu vain viestittelyn kautta eikä kasvotusten. (Ozkaya 2014, s. 132–137.)

5.3 Luottamuksen hyödyntäminen

Kolmannessa vaiheessa osana käyttäjän manipulointia, eli luottamuksen hyödyntämisessä, hyökkääjä on onnistunut rakentamaan yhteyden kohteensa kanssa, joka puolestaan luottaa hyväuskoisesti häneen. Tämä vaihe on itse manipulointihyökkäyksen kulminoituminen, sillä tässä vaiheessa hyökkääjä voi alkaa vaikuttamaan kohteensa käytökseen haluamallaan tavalla. Hyökkäyksen ensisijainen tavoite onkin saada kohde haluamaan itse toimia hyökkääjän haluamalla tavalla, jolloin kohde olisi todennäköisemmin täydellä luottamuksella ja sitoumuksella mukana. (Mouton ym. 2014, s. 5.)

On olemassa paljon erilaisia keinoja, joilla voidaan vaikuttaa toisen henkilön käyttäytymiseen, kun suhde kohteen kanssa on luotu. Hyökkääjä voi esimerkiksi alkaa urkkimaan haluamiaan tietoja kohteeltaan, tai kuten käänteisessä taivuttelumetodissa, kohde voidaan saada pyytämään hyökkääjän apua. Samalla tavalla myös houkuttelu ja tietojenkalastelu -hyökkäysmetodeissa kohde voidaan saada toimimaan hyökkääjän toivomalla tavalla. (Mouton ym. 2014, s. 5.) Vaikuttaminen voidaan myös jakaa tarkemmin kahdeksaan eri periaatteeseen, jotka käydään seuraavissa luvuissa läpi.

5.3.1 Ystävällisyys, vastavuoroisuus ja velvollisuus

Ystävällisyys on keskeinen osa yhteyden luomisessa ja sitä voidaan myös hyödyntää osana manipulointia. Jos hyökkääjä on aidosti ystävällinen ja puhuu kohteelleen jostain asiasta, joka kiinnostaa tätä toista henkilöä, on kohde siten myös paljon avoimempi ja ystävällisempi myös takaisin. Tässä siis korostuu esimerkiksi samat kiinnostuksen kohteet, puhetapa, kehonkieli ja yleinen olemus, kun hyökkääjä on vuorovaikutuksessa kohteensa kanssa. Tämä tapahtuu etenkin fyysisessä ympäristössä, kun hyökkääjä puhuu kasvotusten kohteensa kanssa, mutta sitä voi tapahtua myös esimerkiksi puhelimen kautta keskustellessa. (Hadnagy 2018, s.110, 144–146.)

Ystävällisyyteen kuuluu olennaisesti myös *vastavuoroisuuden* tunteen luominen. Hyökkääjä voi esimerkiksi tarjota apuaan jossain, missä kohde tarvitsisi apua ja siten hän voi vuorostaan pyytää takaisinmaksuna jotain. (Hadnagy 2018, s. 125.) Tällainen ”jotain jotakin vastaan” ajattelutapa on itsessäänkin käyttäjän manipuloinnin hyökkäysmetodi, joka tunnetaan paremmin nimellä *quid pro quo*. Siinä hyökkääjä toimii juuri näin, että hän tarjoaa jotain kohteellensa, jos hän saisi vastineeksi myös haluamansa asian kohteeltaan. (Salahdine & Kaabouch 2019, s. 8.)

Ystävällisyyttä voidaan osoittaa myös *velvoitteena*, joka käytännössä pakottaisi ihmisen toimimaan tietyllä tavalla. Tätä tapahtuu erityisesti tilanteissa, jossa sosiaaliset normit ja hyvät käytöstavat pakottavat ihmiset käyttäytymään kohteliaasti. (Hadnagy 2018, s. 128.) Aikaisemmin mainittu Ylen tietoturvakokeilu (Peiponen 2018) osoittaa juuri tämän osana käyttäjän

manipulointia, kun toimittaja kantoi tikkaita käsissään ja osoitti kuuluvansa päästä yritysten sisätiloihin. Tällöin monille yritysten työntekijöille tuli halu olla ystävällisiä ja auttaa toimittajaa pääsemään ovien ja esteiden läpi, jotta läpikulku olisi sujuvaa. (Peiponen 2018.)

5.3.2 Myönnytys ja johdonmukaisuus/sitoutuneisuus

Myönnytys on myös tapa saada hyökkääjän oma tahto läpi kommunikoidessa kohteen kanssa. Tämä tarkoittaa tilannetta, jossa kohde saadaan suostumaan pyyntöön, josta hän aluksi kieltäytyy. Toisin sanoen henkilö pyytää toiselta henkilöltä jotain, josta hän tietää toisen kieltäytyvän. Tämän jälkeen kysyjä pienentää pyynnön vaatimuksia, jolloin siihen suostuminen kuulostaakin paremmalta ja houkuttelevalta. (Hadnagy 2018, s. 131–132.) Klassinen esimerkki tämän käytöstä on automyyjien keskuudessa, jossa myyjä ehdottaa hintaa myymästään autosta. Aluksi myyjä pyytää suurempaa summaa, joka olisi vaikea hyväksyä asiakkaan näkökulmasta. Tämän jälkeen myyjä päättää ”poikkeuksellisesti” pienentää pyydettyä summaa autosta. Tämä vaikuttaa heti paremmalta vaihtoehdolta asiakkaan näkökulmasta, joka joko hyväksyy ehdotetun hinnan tai tekee vuorostaan oman vastatarjouksen, jossa hän nostaa pyytämäänsä hintaa hieman ylöspäin. Tämä jatkuu, kunnes molemmat osapuolet löytävät yhteisymmärryksen hinnasta. (Hill 2009.)

Myönnytystä voidaan toisin sanoen tulkita tinkimisenä. Käyttäjän manipuloinnin vaikuttamishyökkäyksissä myönnytystä voidaan myös toteuttaa tinkimisen tavoin. Hyökkääjä voi pyytää henkilökohtaisia tietoja kohteeltaan, jotta hän voisi korjata esimerkiksi kohteen ”tietokoneongelman”. Jos hyökkääjä kuitenkin utelee liikaa tietoja lyhyellä aikavälillä, voi kohde suhtautua niihin epäillen ja vastahakoisesti. Mutta jos hyökkääjä kysyykin yhden asian kerrallaan, voi kohteesta saada paljon enemmän irti ja kohde suhtautuu paljon myönteisemmin kysymyksiin. (Hadnagy 2018, s. 131–134.)

Johdonmukaisuus ja *sitoutuneisuus* ovat myös tärkeitä ominaisuuksia onnistuneessa käyttäjän manipuloinnissa. Kun hyökkääjä on kärsivällinen ja ei poikkea peitetarinastaan, vaikuttaa hän siten uskottavammalta kohteelleen. Johdonmukaisuus luo tällä tavoin aidomman kuvan peitetarinaa hyödyntävästä ihmisestä ja hän on näin luotettavampi ja lähestyttävämpi. Näillä ominaisuuksilla hyökkääjän on myönnytyksen tavoin helpompi pyytää ensin pienempiä pyyntöjä, jotka ovat kohteen näkökulmasta hyväksyttäviä. Ajan kuluessa hyökkääjän on helpompi pyytää suurempiä pyyntöjä, kun hän on sitoutunut rooliinsa ja ollut johdonmukainen kohteellensa. (Hadnagy 2018, s. 142–144.)

5.3.3 Niukkuus

Niukkuus on tapa saada jostain asiasta houkuttelevampi ihmisille harvinaisuuden ja poikkeavuuden avulla. Toisin sanoen asioiden arvo nousee, mitä harvinaisempia ja eksklusiivisempia ne ovat. Tätä esiintyy arkipäiväisesti myydyissä kaikenlaisissa tavaroissa ja palveluissa.

Yrityksillä on myös tyypillistä mainostaa myytäviä tuotteita ja palveluja hyödyntämällä niiden rajallisuutta ja kiireellisyyttä. Mainoksissa käytetään esimerkiksi erilaisia lausahduksia, kuten ”Alekampanja voimassa xx asti” tai ”Vain xx jäljellä”. (Hadnagy 2018, s. 134–135.)

Käyttäjän manipuloinnin vaikuttamishyökkäyksissä niukkuutta voidaan hyödyntää saman kaltaisesti tilanteissa, joissa hyökkääjä tarjoaa jonkinlaisia palveluitaan tietyin ehdoin. Tällä luodaan painetta ja lisätään tarjotun palveluksen arvoa ja tärkeyttä, jolloin kynnys niihin suostumiseen voi laskea. (Hadnagy 2018, s. 134–137.) Aikaisemmin luvussa 4.2.1 käsiteltiin tietojenkalastelua hyökkäysmetodina ja näytettiin kuvio (Kuvio 3) tyypillisestä tietojenkalasteluyrityksestä. Siinäkin viestin lähettäjä on yrittänyt luoda kiireyttä käsiteltävälle asialle, jotta viestin saaja kokisi hädän tunnetta ja halua korjata asia pikimmiten, sillä muuten hänen tilinsä suljettaisiin.

5.3.4 Auktoriteetti

Auktoriteetilla tarkoitetaan henkilöä, jolla on virallista valtaa muiden ylitse päätöksenteossa, kontrollissa ja hän voi vaikuttaa muiden toimintatapaan. Sillä tarkoitetaan myös henkilöä, joka on ekspertti tietyssä asiassa, minkä avulla hänellä on vaikutusvaltaa muihin ihmisiin. Tämä on merkki siis ihmisestä, jolla on piirteitä johtajuudesta, itsevarmuudesta ja päättäväisyydestä. Tästä syystä ihmiset, joilla on auktoriteettivaltaa, mielletään yleensä sellaisiksi, joihin voidaan luottaa. (Cambridge Dictionary, n.d.)

Auktoriteettia voidaan näyttää fyysisesti omalla kehonkielellä. Vastaavasti jos tämä henkilö seisoo rinta edessäpäin, leuka ylhäällä ja varma ilme kasvoillaan, antaa hän tutkitusti itsevarman ja päättäväisen kuvan muille. Myös vaatetuksella on merkitystä, sillä se antaa samalla tavalla jonkinlaisen kuvan ihmisten mielissä, minkälainen henkilö on kyseessä ja mitä hän tekee työkseen. Esimerkkinä olisi valkoinen laboratoriotakki, jota käytetään tieteilijöiden ja lääkäreiden keskuudessa. Tämä antaa välittömästi kuvan ihmisestä, joka olisi jonkinlainen ekspertti tietyssä aihealueessa ja jolta siten löytyy myös auktoriteettia. (Hadnagy 2018, s. 137–142.)

Käyttäjän manipuloinnissa voidaan myös hyödyntää auktoriteetin antamaa kuvaa. Hyökkääjä voi siis tietoisesti käyttää tietynlaisia vaatteita ja varmaa elekieltä hyökkäyksen kohteen edessä, jotka viestivät auktoriteetista. Tällaista metodia käytetään monesti peitetarinan yhteydessä, jossa hyökkääjä väittää olevansa johtoasemassa ja saisi tällä tavoin kohteensa toimimaan haluamansa mukaan. Hyvillä näyttelijän taidoilla hyökkääjä voi jopa käyttää hyödykseen uhkailua tai muita aggressiivisia toimia, jos hyökkäyksen kohde ei halua ensin toimia, kuten on pyydetty. Onnistunut peitetarina ja auktoriteetin esittäminen vaativat kuitenkin myös sen, että hyökkääjällä olisi kaikki tarvittava tieto, jotta onnistuneesti voitaisiin esittää johtoasemassa olevaa henkilöä. (Hadnagy 2018, s. 140–142.)

5.3.5 Ryhmäpaine

Ryhmäpaine voi olla voimakas työkalu, kun halutaan vaikuttaa toisen käytökseen. Ihmisillä on tapana matkia muita, jos joku ryhmäläisistä toimii tietyllä tavalla. Matkiminen ja toisista mallin ottaminen on monesti alitajuinen reaktio, joka saa ihmisen tekemään samoin, ettei hän erottuisi joukosta. Paine kasvaa sen mukaan, mitä suurempi ryhmä on toteuttamassa tiettyä toimintaa. Tästä syystä moni ei välttämättä toimisi tietyllä tavalla, jos he olisivat yksin tai heidän pitäisi olla ensimmäisenä toimimassa. Perässä seuraaminen on huomattavasti luontevampaa ja helpompaa. (Hadnagy 2018, s. 149–151.)

Käyttäjän manipuloinnissa ryhmäpainetta voidaan luoda tilanteessa, jossa hyökkääjä esimerkiksi uskottelee ja perustelee toimintaansa siten, että muut ihmiset tai yritykset ovat hyväksyneet hänen toimintansa. Se myös kertoo siitä, että hyökkääjä on ollut tekemisissä muiden kanssa ja heidän kanssaan vuorovaikutus on ollut ”moitteetonta”. Koska hyökkääjä todennäköisesti valehtelee, niin tämä ei ole totta, mutta tämän sanominen luo painetta ja arvoa hyökkääjän viestiin. Silloin kohde olisi todennäköisemmin paljon suostuvaisempi hyökkääjän pyyntöihin, kun hän ei haluaisi erottua enemmistöjoukosta. (Hadnagy 2018, s. 149–151.)

5.4 Saadun tiedon hyödyntäminen

Kun hyökkääjä on onnistunut saamaan kohteen toimimaan tietyllä tavalla tai jakamaan haluamaansa tietoa, hän voi sitten hyödyntää sitä vapaasti omaksi hyväkseen. Tämä ei teknisesti ole enää osana itse hyökkäystä, sillä hyökkäys on jo toteutunut, kun hyökkääjä on saanut kaiken tarvitsemansa kohteeltaan. Kuitenkin hyökkääjä voi suunnitella, jos hän aikoo hyväksikäyttää kohdettaan uudelleen onnistuneen hyökkäyksen jälkeenkin ja mahdollisesti pyrkiä saamaan lisää tietoa tekemällä uusia hyökkäyksiä. (Mouton ym. 2014, s. 4–5.)

Hyökkääjä voi myös hyödyntää suhdettaan kohteen kanssa niin, että onnistuneen hyökkäyksen jälkeen hän manipuloi kohdettaan tuntemaan halutulla tavalla. Esimerkiksi hyökkääjä voi vakuutella kohteelle, ettei hän tehnyt mitään väärää ja saada kohde ymmärtämään hänen motiivejansa tai uskomaan, että mitään hyökkäystä ei edes tapahtunut. Tällä tavoin hyökkääjä voi pahimmassa tapauksessa välttää hyökkäyksen aikaansaamat seuraukset osittain tai jopa kokonaan. (Mouton ym. 2014, s. 4–5.)

6 Tutkimusmenetelmät

Tässä luvussa avataan tutkimuksessa hyödynnettyjä tutkimusmenetelmiä, eli minkälaisin menetelmin tutkimuksen aineisto on kerätty ja analysoitu.

6.1 Narratiivinen kirjallisuuskatsaus

Tämä opinnäytetyö toteutetaan kirjallisuuskatsauksena. Työssä tutustutaan tarkemmin käsiteltävään aiheeseen aikaisempien tutkimusten ja kirjallisuuden kautta sekä analysoidaan aihetta niitä vertaillen ja tietoa yhdistellen. Tarkemmin sanottuna työ toteutetaan narratiivisena kirjallisuuskatsauksena, joka on yksi kirjallisuuskatsauksen muodoista (Salminen 2011, s. 6).

Narratiivisessa kirjallisuuskatsauksessa luodaan yleiskatsaus tutkittavaan ilmiöön. Narratiivinen kirjallisuuskatsaus eroaa esimerkiksi systemaattisesta kirjallisuuskatsauksesta niin, että aineiston valinta ei noudata tiukkoja tai tarkkoja metodisia sääntöjä. Yleiskatsauksessa pyritään kuitenkin valitsemaan tutkimuskysymysten kannalta olennaisia, ajankohtaisia ja luotettavia tutkimuksia sekä asiantuntijakirjallisuutta aineistoon. Aikaisempien tutkimusten ja kirjallisuuden perusteella pyritään saamaan selkeä ja ajankohtainen kuva kyseisestä ilmiöstä. Työn tavoitteena on vastata selkeästi ja kokoavasti tutkimuskysymyksiin ja muodostamaan niistä johtopäätöksiä. (Salminen 2011, s. 6–7.)

6.2 Aineistolähtöinen sisällönanalyysi

Aineiston analysointi toteutetaan aineistolähteisenä sisällönanalyysinä. Sisällönanalyysi on laadullisen tutkimuksen yksi eniten käytetyimmistä analysointimenetelmistä. Aineistolähtöisessä sisällönanalyysissä aineistosta nostetaan esille olennaiset lähteet tutkimuskysymysten perusteella. Aineistolähteinen sisällönanalyysi on paljon hyödynnetty apuväline aineiston järjestämiseen etenkin silloin, kun kyseessä on kirjallisuuskatsaus. (Tuomi & Sarajärvi 2018, s. 78–84, 102.)

Aineistoa analysoitaessa tulee niiden sisältöä verrata keskenään, jotta voidaan löytää yhteenkuuluvia merkityskokonaisuuksia tutkittavan ilmiön kannalta. Merkityskokonaisuudet tarkoittavat aineistossa ilmeneviä samankaltaisuuksia, jotka esitellään kirjallisuuskatsauksen tuloksissa. Samankaltaisuudet yhdistetään kokonaisuuksiksi, joiden avulla vastataan tutkimuskysymyksiin. Kirjallisuuskatsauksissa riittää yleensä, että aineistosta tekee yksinkertaisia luokitteluja. Täten tutkittavasta ilmiöstä luodaan kattava kuva, kun sisältökokonaisuudet ja tutkimuksen tulokset ovat tiivistetty yhteen pohjaten tutkimuskysymyksiin. Näin saadaan lopulta kattava ja johdonmukainen käsitys tutkittavasta ilmiöstä. (Tuomi & Sarajärvi, 2018, s. 84, 102.)

7 Kirjallisuuskatsauksen toteutus

Tässä luvussa kerrotaan tarkemmin, miten valittuja tutkimusmenetelmiä on käytännössä hyödynnetty aineiston keruu- sekä analysointivaiheessa

7.1 Aineisto keruu ja analysointi

Kirjallisuuskatsauksen aineisto on kerätty tiedonhaun aikana käyttämällä seuraavia hakusanoja englanniksi: *social engineering*, *social engineering countermeasures, social engineering report, new social engineering threats, social engineering statistics* ja *deepfake in social engineering*. Aineisto kerättiin hyödyntämällä Google Scholaria ja Finna-hakupalvelua. Myös jo aineistoon valittujen tutkimusten lähdeluetteloa hyödynnettiin etsiessä muita tutkimuksia samasta aiheesta.

Aineiston hakeminen tehtiin kokonaan englanniksi, koska englannin kielellä opinnäytetyöhön sopivaa aineistoa oli enemmän saatavilla. Aineistoon pyrittiin valitsemaan mahdollisimman tuoreita tutkimuksia, jotta saataisiin ajankohtaista tietoa tutkittavasta ilmiöstä. Aineiston sisäänottokriteereiksi asetettiin myös, että tutkimukset ovat vertaisarvioituja ja ne käsittelevät käyttäjän manipuloinnin varautumiskeinoja sekä käyttäjän manipuloinnin uhkaa menneiden vuosien aikana että tulevaisuudessa.

Aineistoa valittaessa mahdollisista tutkimuksista luettiin ensin tiivistelmä, johdanto ja pohdinta. Näin saatiin kokonaiskuva siitä, mitä tutkimuksessa on tutkittu ja soveltuuko se opinnäytetyön aineistoon, eli vastaako se ainakin jompaankumpaan tutkimuskysymykseen. Lopulliseksi aikaväliksi rajautui 2008–2022 ja aineiston kooksi yhteensä 17 tutkimusta (Taulukko 1). Aineisto luokiteltiin sisällönanalyysiä hyödyntäen koskevaksi joko ensimmäistä tai toista tutkimuskysymystä. Tutkimukset painottuvat viime vuosina julkaistuihin, sillä yhteensä 8 tutkimusta on julkaistu vuosina 2020–2022. Erityisesti toisen tutkimuskysymyksen kohdalla oli tärkeää huomioida, että hyödynnetyt aineistot ovat viime vuosina julkaistu, sillä siinä analysoidaan käyttäjän manipuloinnin uhan muutosta viime vuosina ja sen tulevaisuutta.

Aineiston nimi	Tekijä(t)	Julkaisuvuosi	Tutkimuskysymys (1. tai 2.)
Hacking the Human: Social Engineering Techniques and Security Countermeasures	Mann, I.	2008	1. Käyttäjän manipuloinnin varautumiskeinot
An overview of social engineering malware: Trends, tactics, and implications	Abraham, S. & Chengalur-Smith, I.	2010	1. Käyttäjän manipuloinnin varautumiskeinot

Social Engineering in Social Networking Sites: Affect-Based Model	Algarni, A., Xu, Y., Chan, T., & Tian, Y.	2013	1. Käyttäjän manipuloinnin varautumiskeinot
Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks	Conteh, N. & Schmick, P.	2016	1. Käyttäjän manipuloinnin varautumiskeinot
Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques	Moses, S. & Rowe, D.	2016	1. Käyttäjän manipuloinnin varautumiskeinot
Incognito: Shoulder-surfing resistant selection method	Still, J. & Bell, J.	2018	1. Käyttäjän manipuloinnin varautumiskeinot
Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues	Aldawood, H. & Skinner, G.	2019	1. Käyttäjän manipuloinnin varautumiskeinot
Identification and prevention of social engineering attacks on an enterprise	Parthy, P. & Rajendran, G.	2019	1. Käyttäjän manipuloinnin varautumiskeinot
The Emergence of Deepfake Technology: A Review	Westerlund, M.	2019	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
Artificial Intelligence Technologies Using in Social Engineering Attacks	Ryabchuk, N., Grishko, N., Grishko, V., Rudenko, A., Petryk, V., Bapiyev, I. & Fedushko, S.	2020	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
The deepfake threat to face biometrics	Wojewidka, J.	2020	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
Social engineering in 2021	Kaspersky	2021	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
The Human Hacking Report	SlashNext	2021	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus

Social engineering: Concepts, Techniques and Security Counter-measures	Syed, A.	2021	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
Social Engineering Attacks During the COVID-19 Pandemic	Venkatesha, S., Reddy KR. & Chandavarkar, B. R.	2021	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
Forrester: These 5 threats could hobble pandemic recovery	Vigliarolo, B.	2021	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus
Data Breach Investigations Report	Verizon	2022	2. Käyttäjän manipuloinnin uhan muutos ja tulevaisuus

Taulukko 1. Opinnäytetyön aineisto

7.2 Validiteetti ja reliabiliteetti

Opinnäytetyö on pyritty toteuttamaan mahdollisimman objektiivisesti alusta loppuun ja kuvailemaan kaikki sen toteutusvaiheet läpinäkyvästi ja selkeästi, mikä lisää opinnäytetyön validiteettia eli luotettavuutta sekä reliabiliteettia eli kirjallisuuskatsauksen johdonmukaisuutta ja toistettavuutta (Saaranen-Kauppinen & Puusniekka 2006). Validiteetin lisäämiseksi olen tietoisesti pyrkinyt myös välttämään sitä, että esimerkiksi omat mielipiteeni eivät ole vaikuttaneet aineiston valinnassa, analysoinnissa ja tulosten raportoinnissa.

Koska opinnäytetyö on toteutettu narratiivisena kirjallisuuskatsauksena, on kuitenkin mahdollista, että jotain oleellista tietoa on voinut jäädä pois. Esimerkiksi systemaattiseen kirjallisuuskatsaukseen olisi kuulunut systemaattinen tutkimuksien läpikäynti tietyltä ajanjaksolta, jolloin kaikki saatavilla oleva tieto olisi pyritty käymään läpi. Aineiston valinnassa on kuitenkin pyritty ensin tekemään laaja yleiskatsaus tutkittavaan ilmiöön käymällä läpi eri sitä koskevia tutkimuksia ja asiantuntijakirjallisuutta. Katsauksen jälkeen aineistoksi on valittu mielestäni parhaiten sopivat lähteet, joilla asetettuihin tutkimuskysymyksiin voitaisiin kattavasti vastata. Aineiston luotettavuutta lisää myös se, että aineisto koostuu täysin kansainvälisesti julkaistuista ja vertaisarvioiduista lähteistä.

Opinnäytetyön luotettavuutta voi kuitenkin vähentää se, että aineisto koostuu kokonaan englanninkielisistä tutkimuksista ja kirjallisuudesta. Vaikka omaan hyvät englannin kielen taidot, tiedon tulkitsemiseen ja kääntämiseen suomeksi liittyy aina omat haasteensa, jotta lähteiden alkuperäinen tieto pysyisi mahdollisimman samanlaisena.

8 Tutkimustulokset

Tässä luvussa vastataan tutkimuskysymyksiin. Tutkimuskysymyksiksi esitettiin työn alussa seuraavat:

1. Minkälaisin keinoin yritykset voivat varautua käyttäjän manipuloinnilta?
2. Miten käyttäjän manipuloinnin uhka on muuttunut kuluneiden vuosien aikana ja miltä sen tulevaisuus tällä hetkellä näyttää?

Luku jakautuu pääasiassa kahteen alalukuun eli käyttäjän manipuloinnin varautumiskeinoihin sekä käyttäjän manipulointiuhkaan kuluneiden vuosien aikana sekä tulevaisuudessa.

8.1 Käyttäjän manipuloinnin varautumiskeinot

Tarkastellessa varautumiskeinoja käyttäjän manipuloinnille, on hyvä asettaa itselleen selkeä kuva siitä, mikä on oman tietoturvan asema tällä hetkellä. Tämä voidaan toteuttaa haavoittuvuuskartoituksella, jolla selkeytetään kuvaa siitä, millä alueilla omat vahvuudet ja heikkoudet tietoturvassa sijaitsevat. Haavoittuvuuskartoitusta voidaan toteuttaa muun muassa tarkastustyökalujen, automaattisten asennusten ja manuaalisen testauksen kautta. Nykyään on myös yleistä, että yritykset ulkoistavat kolmansia osapuolia analysoimaan ja testaamaan heidän tietoturvansa hallintaa ja yleistä tilannetta. (Mann 2008, s. 155.)

Tietoturvan testausta voidaan esimerkiksi toteuttaa siten, että yrityksen sisäpiiriläinen ottaa yhteyttä ulkoiseen osapuoleen, joka suorittaa kokeilumielessä käyttäjän manipuloinnin vaikuttamishyökkäyksiä kyseiseen yritykseen. Tässä testauksessa voi olla myös osallisena yrityksen sisältä henkilöstöä, jolloin hyökkäyksen olosuhteet ja tiedonsaanti muuttuvat. Jokainen vaihe hyökkäyksen edetessä raportoidaan huolellisesti, jotta testauksen jälkeen yrityksen sisäpiirissä voidaan analysoida hyökkäyksen vaikutuksia ja miten testauksesta tietämättömät ovat reagoineet hyökkäykseen. (Mann 2008, s. 211–213.)

Tietoturvan testauksella voidaan määritellä, mihin osa-alueisiin pitää panostaa enemmän vahvistaakseen yrityksen omaa tietoturvaa. Tällä tavoin voidaan myös paremmin analysoida mahdollisia uhkia, joita voi kohdistua niin henkilöitä kuin yrityksiä kohtaan. Lopullisen haavoittuvuuskartoituksen jälkeen voidaan suorittaa muun muassa jälkitestausta ja parannuksia, joilla vahvistetaan omaa tietoturvaa entisestään. (Mann 2008, s. 155–160.)

Haavoittuvuuskartoituksessa voidaan tutkia yrityksen tietoturvaa kahden tekijän kautta. Tähän kuuluu teknisiä ja ei-teknisiä käytäntöjä, joilla määritellään yrityksen valmius varautua käyttäjän manipuloinnin vaikuttamishyökkäyksiin. Tekniseksi käytännöksi kutsutaan systemaattista vahvuutta (engl. systemic strength) ja ei-tekniseksi käytännöksi henkilöstön vahvuutta (engl. personnel strength). Tietyissä tapauksissa voi olla mahdollista, että osa käyttäjän manipuloinnin hyökkäyksistä voidaan estää vain toisella näistä tekijöistä. Vähintään

toinen näistä tekijöistä on tällöin haavoittuvuuskartoituksen mukaan vahvuutena. On kuitenkin tärkeää maksimoida molempien tekijöiden vahvuus, jotta mahdollisuudet käyttäjän manipuloinnin hyökkäyksien onnistumiselle ovat mahdollisimman pienet. Jos jompaakumpaa näistä tekijöistä, tai pahimmassa tapauksessa kumpaakaan ei pidetä tärkeänä ja ne jätetään huomioimatta, ovat yritykset tai yksityishenkilöt alttiimpia kohteita onnistuneille käyttäjän manipuloinnin hyökkäyksille. (Mann 2008, s. 155–160.) Systemaattista vahvuutta ja henkilöstön vahvuutta käydään tarkemmin läpi seuraavissa luvuissa.

8.1.1 Systemaattinen vahvuus

Analysoidessa käyttäjän manipuloinnin vahvuuksia ja heikkouksia, *systemaattinen vahvuus* tarkoittaa kykyä vastustaa käyttäjän manipuloinnin vaikuttamisyrityksiä tavoilla, jotka eivät vaadi ihmisen vuorovaikutusta, vaan se tapahtuu itsenäisesti. Tähän voidaan luokitella esimerkiksi fyysinen ympäristö, ihmisten käytössä olevat eri työvälineet, systeemit tai mekanismit, joita käytetään joka päivä työnteossa ja/tai arkielämässä. Yleinen virhe käyttäjän manipuloinnin varautumiskeinoja pohtiessa on se, että ne koskevat ainoastaan yleistä ihmisen tietoisuutta ja ymmärrystä käyttäjän manipuloinnista ilmiönä. Vaikkakin monet käyttäjän manipuloinnin vaikuttamishyökkäyksistä ovat sellaisia, jotka rajoittuvat ainoastaan ihmiskontaktiin, voidaan systemaattisella vahvuudella vähentää tai poistaa näitä uhkia yhtä merkittävästi. (Mann 2008, s. 155–158, 167.)

Jos systemaattiset tekijät ovat tietoturvan kannalta vahvuuksina, voidaan päätellä, että ne edesauttavat pysäyttämään henkilöstöön kohdistuvaa vaikuttamista ja manipulointia. Esimerkki systemaattisesta vahvuudesta on sähköpostin automaattinen suodatus viesteille, joka tulkitsee, mitkä viestit ovat roskapostia ja mitkä eivät. Muita tyypillisiä vahvuuksia systemaattisissa tekijöissä ovat vahva todennus, tehtävien erottelu sekä toimintojen tehokas vertaisarviointi. (Mann 2008, s. 155–158, 167.)

Etenkin yksinkertaiset askeleet laitteiden suojaamiseen ovat elintärkeitä systemaattisen vahvuuden saavuttamisessa. Vahvojen salasanojen käyttö, erilaisten virustorjuntaohjelmistojen hyödyntäminen sekä laitteiden päivitysten ajan tasalla pitäminen antavat huomattavasti vahvemman suojan hyökkäyksiä vastaan. (Syed 2021, s. 3.) Tämä korostuu etenkin ihmisten henkilökohtaisissa elektronisissa välineissä, joissa usein on heikompi suoja hyökkäyksiä vastaan. Jos yrityksen resurssit ovat riittävät, on mahdollista laajentaa suojausta myös henkilökohtaisiin välineisiin, joilla turvataan niin ihmisten henkilökohtaiset tiedot kuin myös itse yrityksen. (Abraham & Chengalur-Smith 2010, 10.) Suojauksella turvataan tiedon eheyttä, joka on yksi CIA-mallin osa-alueista. Toisin sanoen suojauksella voidaan rajoittaa mahdollisuutta tiedon muokkaamiseen ulkopuolisen tahon toimesta.

Vahvistamalla systemaattisia tekijöitä, voidaan löytää suoria tai osittaisia ratkaisuja luvussa 4.2 mainittuihin käyttäjän manipuloinnin hyökkäysmetodeihin. Äsken mainittu

sähköpostiviestien suodatus on tehokas tapa välttää tietojenkalastelua, jolloin haitalliset viestit menevät suoraan roskapostiin. Sama pätee myös tietojenkalastelun muihin muotoihin, kuten tekstiviestien välityksellä tapahtuvaa urkintaa (engl. smishing). Sähköpostissa on myös mahdollista estää viestejä, jos niitä on lähetetty ulkopuoliselle taholle ja niihin on sisälletty luottamuksellista tietoa. On myös hyvä täsmentää ja merkata tietoa sen mukaan, mikä on erittäin luottamuksellista, mikä vapaata tietoa ja mikä jotain siltä väliltä. Siten eri järjestelmät osaavat myös tulkita, mitä tietoa voidaan jakaa kenelle ja kuinka avoimesti. (Mann 2008, s. 156, 182–184; Parthy & Rajendran 2019, s. 4.) CIA-mallin osa-alueet luottamuksellisuus ja saatavuus korostuvat tässä, kun haluttu tieto on aina saatavilla oikeille henkilöille.

Fyysiset hyökkäykset, kuten dyykkaus, perässä roikkuminen (engl. tailgating) ja olan yli katsominen, voidaan estää fyysisillä turvatoimilla (Parthy & Rajendran 2019, s. 4). Tällaisiin turvatoimiin kuuluu muun muassa valvontakameroiden lisääminen ja pääsyn rajaaminen työympäristöön useilla pääsyovilla. On myös hyvä harkita monivaiheisen ja biometrisen tunnistautumisen käyttöönottoa. (Conteh & Schmick 2016, s. 5.) Biometrista tunnistautumista voidaan toteuttaa esimerkiksi sormi-, ääni-, silmä- tai kasvojentunnistuksella, jotka auttavat fyysisen ympäristön turvallisuuden maksimoinnissa (Moses & Rowe 2016, s. 6–7). Erityisesti silmätunnistus on hyvä ratkaisu lämpökameraa vastaan, jolloin näppäinkoodia ei hyödynnetä ovien, laitteiden ja muiden järjestelmien avaamiseen (Still & Bell 2018, s. 2). Monivaiheinen todennus auttaa myös erityisesti suojaamaan tiedon saatavuutta CIA-mallin mukaisesti, eli sen varmistamista, että vain oikeilla henkilöillä on pääsy tietoon.

8.1.2 Henkilöstön vahvuus

Käyttäjän manipulointiin varautumisessa *henkilöstön vahvuudella* tarkoitetaan tapoja estää ja ehkäistä käyttäjän manipuloinnin hyökkäyksiltä suoraan ihmisten kautta ja avulla. Tässä ei siis oteta huomioon edellisessä luvussa mainittuja teknisiä apuvälineitä, vaan analysoidaan ja hyödynnetään yksittäisten ihmisten omia taitoja, tietoisuutta ja valmiutta. (Mann 2008, s. 155–156.) Jos yksittäinen henkilö tai yrityksen henkilöstö osaa tunnistaa käyttäjän manipuloinnin hyökkäykset niiden tapahtuessa ja tietää miten niihin tulee reagoida, voidaan sanoa heidän olevan tietoisesti varautuneita tällaisiin tapauksiin. (Mann 2008, s. 155–156; Syed 2021, s. 3.)

Koska ihmisvuorovaikutus on hyvin keskeisessä osassa käyttäjän manipuloinnin hyökkäyksissä, liittyen esimerkiksi hyökkääjän peitetarinan tai tietojenkalastelun hyödyntämiseen, tärkein ja konkreettisin tapa suojautua hyökkäyksiltä on kasvattaa henkilöstön tietoisuutta. (Conteh & Schmick 2016, s. 34.) Esimerkiksi tietojenkalasteluviestien yhteydessä aiheesta tietoinen oleva hyökkäyksen kohde osaa tunnistaa haitalliset viestit ja tietää niiden olevan epäluotettavia. Perässä roikkuminen (engl. tailgating) voidaan estää siten, että yritysten henkilöstöt eivät päästä kohteliaisuuden vuoksi tuntemattomia sisätiloihin, vaikka hyvät käytöstavat

voisivat painostaa käyttäytymään toisin. Olan yli katsominen voidaan välttää niin, että mahdollisen hyökkäyksen kohde ymmärtää olla katsomatta mahdollisesti arkaluonteista tietoa yleisissä paikoissa, kuten kahviloissa tai julkisessa liikenteessä. Myös mahdollisten näppäinkoodien suojaaminen kädellä tai keholla estää suoran katsekontaktin ja tekee siten urkinnasta haastavampaa. (Moses & Rowe 2016, s. 9; Parthy & Rajendran 2019, s. 4.)

Hyvä keino tietoisuuden lisäämisessä on henkilöstön yhteiseen kouluttamiseen panostaminen. Yksinkertaiset säännöt henkilöstölle, kuten ”Älä avaa epäilyttäviä linkkejä tai liitteitä sähköpostissa” tai ”Älä jaa henkilökohtaista tietoa tuntemattomille” auttavat suojaamaan arkaluonteista tietoa tehokkaasti (Parthy & Rajendran 2019, s. 4; Syed 2021, s. 3). Asiasta voidaan viestiä ja kouluttaa monella eri tavoin, kuten esimerkiksi muistiolapuilla, julisteilla, tai kasvotusten keskustellen. Fyysisten keinojen lisäksi interaktiiviset harjoitteluohjelmat tai muut omaperäiset ja mielenkiintoiset tavat auttavat, jolloin aiheen oppiminen ja muistaminen jää mieleen parhaiten. Yrityksen on syytä ylläpitää jatkuvaa kehitystä, testausta ja tietoisuutta, sillä ihmiset eivät välttämättä tule muistamaan kaikkea pitkällä aikavälillä. (Mann 2008, s. 196–199; Aldawood & Skinner 2019, s. 4.)

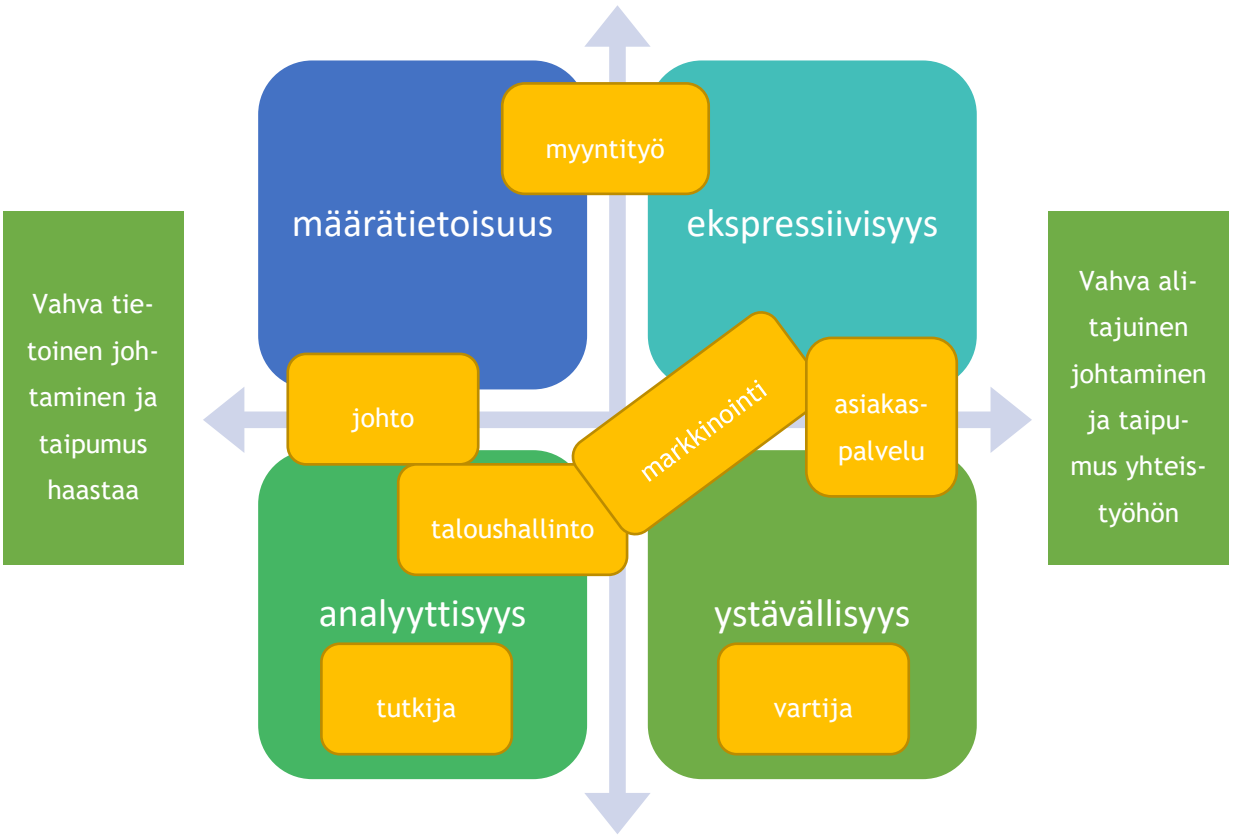
Kun kyseessä on yritys tai muu organisaatio, täytyy huomioida pitkälti kaikki yrityksen edustajat ja työntekijät. Tämä johtuu siitä, että käyttäjän manipuloinnin hyökkäykset voivat kohdistua mihin ja kehen vain. Jos tietoisuus käyttäjän manipuloinnista on joillakin henkilöillä heikkoa, on organisaatiossa tietoturvaheikkous, jota ulkopuoliset hyökkääjät voivat hyväksikäyttää. (Aldawood & Skinner 2019, s. 5–6.) Erityisesti on tärkeää painottaa tietoisuuden lisäämistä uusille työntekijöille. Tällä tavoin minimoidaan hyökkäysten onnistumisen todennäköisyyttä, kun jokainen henkilö on riittävän tietoinen ajankohtaisista uhista. Yritysten johtohenkilöillä ja pitkäaikaisilla työntekijöillä on todennäköisemmin parempi tietoturvaymmärrys kuin uudemmilla työntekijöillä. (Mann 2008, s. 195–196, 201–202.)

Motivaation ja käytäntöjen ylläpito ja noudattaminen ovat olennainen osa varautumista käyttäjään kohdistuvia manipulointihyökkäyksiä vastaan. Työelämän lisäksi ihmisten pitäisi noudattaa näitä käytäntöjä myös vapaa-ajalla henkilökohtaisilla elektronisilla välineillä. Tämä on ollut usein yksi suurimpia kipukohteita yritysten tietoturvapolitiikassa, sillä ihmisiä ei välttämättä kiinnosta seurata tiukasti sääntöjä omalla ajallaan. Tämän lisäksi liiallinen valvominen ja sääntöjen tiukentaminen voi koitua pikemminkin haitaksi yrityksille, jolloin henkilöstö voi kokea työympäristön ankeana. Tietoturvakulttuurin pitäminen positiivisena ja kannustavana auttaa ihmisiä pitämään paremmin huolta kaikista käyttämistään laitteista, sekä työ- että vapaa-ajalla. (Abraham & Chengalur-Smith 2010, 10–11; Aldawood & Skinner 2019, s. 5–6.)

Sosiaalisen median eri alustat voivat olla erittäin hyödyllisiä paikkoja hyökkääjän näkökulmasta kerätä lisää tietoa ja mahdollisesti tehdä hyökkäyksiä yksityishenkilöitä ja yrityksiä vastaan. Siksi ihmisten on tärkeää ymmärtää, mitä kannattaa jakaa omalla profiililillaan ja mitä

ei, sillä hyökkääjät ottavat huomioon kaiken mahdollisen tiedon, jota he löytävät kohteestaan. Yritysten näkökulmasta täytyy huomioida, mitä tietoa työntekijät saavat jakaa yritykseen liittyen omassa sosiaalisessa mediassaan. (Algarni, Xu, Chan & Tian 2013, s. 7.)

On myös hyvä ottaa huomioon ”tyypilliset” persoonallisuuspiirteet, joita tiettyjen alojen työntekijöiltä löytyy yritysmaailmassa (Kuvio 5). Tällä pyritään kartoittamaan, ketkä työntekijät ovat tyypillisesti luonteenpiirteiltään analyyttisempia ja ketkä avoimempia ja ystävällisempiä. Näillä saadaan selville, ketkä olisivat mahdollisen manipulointihyökkäyksen aikana haavoittuvaisempia ja ketkä haastavampia kohteita. (Mann 2008, s. 162–166, 201–202.)



Kuvio 5. Tyypilliset persoonallisuuspiirteet työtehtävissä, mukailtu Mannin (2008) mukaan

Kuten yllä olevasta kuviosta näkyy, Mannin (2008) mukaan erityisesti ihmiset, jotka ovat muiden ihmisten kanssa paljon tekemisissä ja vuorovaikutuksessa, ovat huomattavasti alttiimpia manipulointihyökkäyksiin. Tähän kuuluu muun muassa henkilöt, jotka ovat asiakaspalvelun, vartijan tai markkinoinnin työtehtävissä. Johdon, tutkimuksen ja taloushallinnan työtehtävissä työskentelevät ihmiset ovat puolestaan luonteeltaan analyyttisempia ja ovat siten haastavampia kohteita käyttäjän manipuloinnin hyökkäyksille. (Mann 2008, s. 162–166, 201–202.)

On hyvä kuitenkin muistaa, että Kuvio 5 ei kerro täydellä varmuudella kaikkien ihmisten luonteenpiirteitä, sillä eroavaisuuksia löytyy aina. Se on kuitenkin suuntaa antava esimerkki

tyypillisistä persoonallisuuspiirteistä liittyen erilaisiin työtehtäviin. Yrityksen johdon tai tietoturvan parantamisesta vastaavan kannattaa aina ottaa huomioon analysoidessa yrityksen kaikkia mahdollisia tietoturvaheikkouksia. (Mann 2008, s. 162–166, 201–202; Aldawood & Skinner 2019, s. 5–6.) Riippuen työtehtävistä, joillekin henkilöille on kriittisempää tietää enemmän ja saada laajempi pääsyoikeus yrityksen eri järjestelmiin. Eri rooleissa työskenteleville työntekijöille voidaan antaa roolipainotettuja ohjeita ja oikeuksia päästä käsiksi arkaluonteiseen tietoon ja järjestelmiin. (Mann 2008, s. 195–196, 201–202.) CIA-mallin mukaan tietoturva on siten vahvempi, kun tiedon saatavuutta rajataan tietyille henkilöille, jolloin luottamuksellisuus myös vahvistuu.

8.2 Käyttäjän manipulointi viime vuosien aikana ja tulevaisuudessa

Käyttäjän manipulointi on yhä keskeisempi aihe yritysten tietoturvapolitiikassa, sillä tämänkaltaiset hyökkäykset ovat olleet viime vuosina jyrkässä nousussa. Tämä trendi jatkuu näillä näkymin tulevaisuudessakin. SlashNext:n Human Hacking -raportin (2021) mukaan käyttäjän manipuloinnin hyökkäykset aikavälillä 2020–2021 olivat nousseet 270 %. (SlashNext 2021, s. 8.) Verizonin vuoden 2022 tietomurtoraportin mukaan jopa 82 % kaikista vuosina 2020–2021 onnistuneista tietomurroista hyödynsivät ihmiselementtiä osana hyökkäystä. Edellisen vuoden raportissa vastaava luku oli 85 %. Tämä on hyvin suuri osuus, kun otetaan huomioon kaikki maailmalla tapahtuneet ja raportoidut tietomurrot. Pääasiallinen motiivi näille murroille on ollut taloudellinen (89 %) eli raha, mutta kuitenkin pieni osa tietomurroista pohjautuu vakoiluun (11 %). (Verizon 2022, s 33, 98.)

Käyttäjän manipuloinnissa otetaan yhä enemmän hyötyä irti maailman tapahtumista. Esimerkiksi koronapandemian aikana vuonna 2021 useat rikolliset käyttivät hyödykseen vallitsevaa tilannetta ja naamioituivat COVID-19-kampanjoinnin taakse ja näin huijasivat useita ihmisiä tietojenkalastelusähköposteilla saadakseen käyttäjätunnuksia. Samankaltaisia hyökkäyksiä on hyödynnetty erityisesti tartuntasovellusten ja koronapassin myötä, kun niistä tuli suuri puheenaihe uutisissa. Hyökkääjät käyttivät peitetarinanaan muun muassa Maailman terveysjärjestöä ja näin uskottelivat kohteilleen hyökkäysviestien olevan legitiimejä. (Kaspersky 2021; Venkatesha, Reddy & Chandavarkar 2021, s. 2.)

Jatkuva teknologian kehitys vaikuttaa käyttäjän manipulointiin merkittävästi. Hyökkäykset muokkautuvat yhä hienostuneimmiksi, ja siksi ne ovat yhä suurempi uhka niin yksittäisille ihmisille kuin yrityksille. Nykyään käyttäjän manipuloinnin hyökkäyksiä voidaan automatisoida tehokkaasti bottien avulla, joka vuorostaan lisää hyökkäysten määrää ja säästää enemmän aikaa hyökkääjien näkökulmasta. Bottien avulla voidaan esimerkiksi tehokkaammin kerätä tietoa hyökkäyskohteista ja olla vuorovaikutuksessa heidän kanssaan. (Vigliarolo 2021; Venkatesha ym. 2021, s. 2.)

Suhteellisen uudet teknologiat, kuten esimerkiksi Deepfake-teknologia, voivat muodostaa uuden uhan käyttäjän manipuloinnissa. Deepfake koostuu sanoista *deep learning* ja *fake*, mikä tarkoittaa suomeksi *syvää oppimista* ja *valheellista*. Se on tapa muokata ja manipuloida kuvia tai videoita ihmisten kasvoista. Tämä luo mahdollisuuden muokata ihmisen kasvojen päälle toisen ihmisen kasvot hyödyntäen tekoälyä. Näin voidaan luoda hyperrealistinen kuva ihmisestä, joka ei oikeasti ole totta, vaan tekoälyn luoma illuusio. Teknologian nimitys Deepfake kuvastaa siis tekoälyn luomaa valheellista kuvaa. (Westerlund 2019, s. 2; Ryabchuk ym. 2020, s. 4–5.) Deepfake-väärennökset voidaan tehdä myös äänimuodossa, jossa tekoäly rakentaa jonkun halutun ihmisen äänen, jonka avulla voidaan rakentaa kokonaisia lauseita tätä ääntä käyttämällä. Näin voidaan luoda jälleen illuusio siitä, että joku ihminen on puhunut jotain, mitä hän ei oikeasti ole sanonut. (Westerlund 2019, s. 3).

Deepfake on teknologiana saanut suurta huomiota viime vuosina viihdetyökaluna, mutta se on myös herättänyt huolta sen väärinkäytöstä. Käyttäjän manipuloinnissa tätä teknologiaa voidaan hyödyntää erityisesti biometristen tunnistusten haastamisessa. On mahdollista, että hyökkääjä voi ohittaa tätä tunnistautumistapaa käyttävät teknologiat, jotka tarvitsevat tunnistautumiseen ihmisen fyysisiä ominaisuuksia, kuten ääntä, kasvoja tai muita kehonosia. (Wojewidka 2020.)

9 Yhteenveto

Käyttäjän manipulointi on käsitteenä hyvin laaja ja sillä voidaan erityisesti englanniksi (social engineering) tarkoittaa monta asiaa. Tietoturvan kontekstissa ja suomeksi tällä kuitenkin tarkoitetaan aina toimintaa, jossa pyritään vaikuttamaan muiden päätöksentekoon eri hyökkäysmetodeja hyödyntäen. Hyökkääjä pyrkii manipuloimalla usein saamaan kohteeltaan arkaluontoista tietoa, kuten käyttäjätunnuksia, salasanoja tai muita henkilökohtaisia tietoja.

Tämän kirjallisuuskatsauksen tarkoituksena oli selvittää, miten käyttäjän manipulointiin voidaan varautua ja miten käyttäjän manipuloinnin uhka on muuttunut viime vuosien aikana ja tulee muuttumaan tulevaisuudessa. Manipulointiin varautumisessa on tärkeää ymmärtää omassa työympäristössä olevat tietoturvan vahvuudet ja heikkoudet. Niitä voidaan tarkastella kahden tekijän kautta, jotka ovat systemaattinen vahvuus ja henkilöstön vahvuus (Kuvio 6). Systemaattisella vahvuudella tarkoitetaan varautuneisuutta käyttäjän manipuloinnin hyökkäyksiin tasolla, joka ei tarvitse ihmisten vuorovaikutusta. Käytännössä systemaattista vahvuutta voidaan parantaa vahvistamalla elektronisten laitteiden suojausta esimerkiksi vahvemmilla salasanoilla ja virustorjuntaohjelmistoilla. Fyysisen ympäristön turvallisuutta voidaan vuorostaan parantaa esimerkiksi turvakameroilla ja sisäänpääsyjärjestelmillä, jotka rajoittavat helppoa sisäänpääsyä työtiloihin.

Henkilöstön vahvuudella tarkoitetaan ihmisten kykyä varautua käyttäjän manipuloinnin hyökkäyksiin. Henkilöstön vahvuutta voidaan parantaa lisäämällä työntekijöiden tietoisuutta käyttäjän manipuloinnista. Muun muassa itsenäinen harjoittelu ja yritysten luomat koulutukset, harjoitusohjelmat ja ohjeistukset auttavat jokaista työntekijää ymmärtämään tämän aihealueen tärkeyden. Tarpeen tullen henkilöstö osaa tunnistaa, jos hyökkäys on toteutumassa ja tietävät, miten sellaisessa tilanteessa tulisi toimia ja reagoida.

Systemaattinen vahvuus	Henkilöstön vahvuus

• Työvälineiden ja -järjestelmien suojaus
  • Vahvat salasanat
  • Vahva todennus
  • Päivitysten ylläpito
  • Virustorjuntaohjelmistot
  • Tiedonjakamisen rajoittaminen
  • Jatkuva kehitys ja testaus
• Fyysiset turvatoimipiteet
  • Valvontakamerat
  • Pääsyn rajoittaminen työalueelle
  • Biometrinen tunnistautuminen
	• Tietoisuuden kasvattaminen
	  • Koulutus
	  • Harjoitteluohjelmat
	• Motivaation ylläpito
	  • Käytäntöjen noudattaminen vapaa-ajalla
	• Tiedonjakamisen rajoittaminen
	• Jatkuva kehitys ja testaus

Kuvio 6. Varautumiskeinot käyttäjän manipuloinnin hyökkäyksiin

Käyttäjän manipuloinnin vaikutus on ollut koko maailmassa suuri. Suurin motiivi tämänkaltaisille hyökkäyksille on ollut taloudellinen, mikä ei tulevaisuudessakaan tule todennäköisesti muuttumaan. Tämä tarkoittaa sitä, että suurin osa hyökkääjistä pyrkii saamaan onnistuneesta hyökkäyksestä jotain, jolla on rahallista arvoa. Käyttäjän manipuloinnin hyökkäykset pyrkivät ottamaan hyödyn maailman tapahtumista, jotka edesauttavat hyökkäysten aitoudentuntoa. Teknologia myös kehittyy lujaa vauhtia ja niin myös käyttäjän manipuloinnin hyökkäykset kehittyvät sen mukana. Hyökkäyksissä hyödynnetään yhä enemmän teknologiaa, mitä ei ole ennen ollut saatavilla. Tällaisia teknologioita on muun muassa Deepfake-teknologia ja kehittynyt automatisointi bottien avulla.

10 Johtopäätökset

Kirjallisuuskatsaus vahvisti näkemystäni siitä, miksi käyttäjän manipulointia ilmiönä on tärkeää tutkia ja erityisesti siihen liittyen erilaisia tapoja, miten manipuloinnilta voidaan varautua. Teknologian kehitys vaikuttaa myös yhtä lailla käyttäjän manipulointiin, sillä kehitystä

voidaan käyttää myös pahaan tarkoitukseen. Käyttäjän manipuloinnilta varautumisessa onkin siksi tärkeää, että systemaattinen vahvuus pysyy jatkuvasti vahvana, jotta uusia hyökkäysmetodeja voidaan haastaa aina jollain tavalla. Mielestäni yhtä tärkeää on muistaa henkilöstön vahvuus, joka on ehkä tärkeämmässä osassa käyttäjän manipuloinnin varautumisessa. Huomattava määrä näistä hyökkäyksistä kohdistuu yksinomaan ihmisiin, jolloin teknistä osaamista ei välttämättä tarvitsisi lainkaan.

Kyberturvallisuuden ekspertin Dobrean (2018) mukaan, jota Ozkaya (2018) esittelee kirjassaan, pohjoismaat ovat parhaiten valmistautuneet kyberhyökkäyksiin. Tämä tarkoittaa siis sitä, että systemaattinen vahvuus näissä maissa on erittäin vahvaa, sillä haittaohjelmatartuntojen määrä on hyvin alhainen. Kuitenkin huomioidaan, että näiden maiden kansalaisten luottamus toisia ihmisiä kohtaan on myös todella korkea. Myös luottamus valtioiden eri instituutioihin on samalla tavalla korkealla tasolla. Tämä voi osoittautua uhaksi henkilöstön vahvuutta analysoitaessa, sillä korkea luottamus esimerkiksi muihin ihmisiin voi johtaa helposti käyttäjän manipuloinnin hyökkäyksiin. (Ozkaya 2018, s. 408.) Tämä on mielestäni asia, johon Suomessa tulee kiinnittää erityisesti huomiota tietoturvan saralla liittyen henkilöstön kouluttamiseen, tietoisuuden parantamiseen sekä varautumiskeinojen kehittämiseen käyttäjän manipulointia vastaan.

Lähteet

Sähköiset

Abraham, S., & Chengalur-Smith, I. 2010. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society, 32(3), s. 183-196. https://doi.org/10.1016/j.techsoc.2010.07.001

Aldawood, H., & Skinner, G. 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet, 11(3), s. 73. https://doi.org/10.3390/fi11030073

Algarni, A., Xu, Y., Chan, T., & Tian, Y. C. 2013. Social engineering in social networking sites: Affect-based model. 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), s. 508-515. IEEE. DOI: 10.1109/ICITST.2013.6750253

Bekaert, P., Alotaibi, N., Mathis, F., Gerber, N., Rafferty, A. C., Khamis, M., & Marky, K. 2022. Are Thermal Attacks a Realistic Threat? Investigating the Preconditions of Thermal Attacks in Users' Daily Lives. Nordic Human-Computer Interaction Conference, s. 1-9. https://doi.org/10.1145/3546155.3546706

Cambridge Dictionary. 2022. Viitattu 5.11.2022. https://dictionary.cambridge.org/dictionary/english/authority

Choi, D., Choi, C., & Su, X. 2016. Invisible secure keypad solution resilient against shoulder surfing attacks. 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS) s. 514-517. IEEE. DOI: 10.1109/IMIS.2016.77

Clausnitzer, J. 2021. Number of information security violations and threat cases reported in Finland in 2020. https://www.statista.com/statistics/1224712/number-of-reported-information-security-violations-and-threats-finland/

Conaboy, C. 2013. Doctors, billing company pay $140,000 penalty for records tossed in public dump. Viitattu 17.11.2022. https://www.boston.com/uncategorized/noprimarytag-match/2013/01/07/doctors-billing-company-pay-140000-penalty-for-records-tossed-in-public-dump/

Conteh, N. Y., & Schmick, P. J. 2016. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), s. 31. http://dx.doi.org/%2010.19101/IJACR.2016.623006

Hadnagy, C. & Wilson, P. 2010. Social Engineering: The Art of Human Hacking. E-kirja. John Wiley & Sons, Incorporated, New York.

Hadnagy, C. 2018. Social Engineering: The Science of Human Hacking. E-kirja. John Wiley & Sons, Incorporated, Newark.

Hill, D. 2009. How to Negotiate the Salary Using the Power of the Norm of Reciprocity. Viitattu 5.11.2022. https://ezinearticles.com/?How-to-Negotiate-the-Salary-Using-the-Power-of-the-Norm-of-Reciprocity&id=2449465

Huddleston, T. 2019. How this scammer used phishing emails to steal over $100 million from Google and Facebook. Viitattu 10.11.2022. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

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

Kaspersky. 2021. Social Engineering in 2021. https://go.kaspersky.com/rs/802-IJN-240/images/NJ_Social_Engineering_KFP.pdf

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

Luo, X., Brody, R., Seazzu, A., & Burd, S. 2011. Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), s. 1-8. https://doi.org/10.4018/irmj.2011070101

Mann, I. 2008. Hacking the Human: Social Engineering Techniques and Security Countermeasures. E-kirja. Taylor & Francis Group.

Moses, S., & Rowe, D. C. 2016. Physical security and cybersecurity: Reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. International Journal for Information Security Research (IJISR), 6(2), s. 667-676. https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/Physical-Security-and-Cybersecurity-Reducing-Risk-by-Enhancing-Physical-Security.pdf

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. 2014. Social engineering attack framework. 2014 Information Security for South Africa, s. 1-9. IEEE. DOI: 10.1109/ISSA.2014.6950510

Ozkaya, E. 2018. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert. E-kirja. Packt Publishing, Limited, Birmingham.

Parthy, P. P., & Rajendran, G. 2019. Identification and prevention of social engineering attacks on an enterprise. 2019 International Carnahan Conference on Security Technology (ICCST) s. 1-5. IEEE. 10.1109/CCST.2019.8888441

Pearson, J. 2017. A Canadian University Gave $11 Million to a Scammer. Viitattu 19.10.2022. https://www.vice.com/en/article/yww4xy/a-canadian-university-gave-dollar11-million-to-a-scammer

Peiponen, P. 2018. Katso paljastava piilokameravideo – Ylen toimittaja testasi tärkeiden yritysten ja laitosten tilaturvallisuutta: Lähes kaikilla puutteita kulunvalvonnassa. Viitattu 1.11.2022. https://yle.fi/uutiset/3-10320853

Ryabchuk, N., Grishko, N., Grishko, V., Rudenko, A., Petryk, V., Bapiyev, I., & Fedushko, S. 2019. Artificial Intelligence Technologies Using in Social Engineering Attacks. CybHyg s. 546-555. http://star.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-2654/paper43.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV – Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Viitattu 23.11.2022. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/

Salahdine, F., & Kaabouch, N. 2019. Social engineering attacks: A survey. Future Internet, 11(4), s. 89. https://doi.org/10.3390/fi11040089

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopiston julkaisuja, Opetusjulkaisuja 62, Julkisjohtaminen 4. https://www.univaasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Samonas, S., & Coss, D. 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3). https://www.proso.com/dl/Samonas.pdf

Sanastokeskus. 2020. Viitattu 8.11.2022. https://sanastokeskus.fi/tsk/fi/termitalkoot/haku-266.html?page=get_id&id=ID122&vocabulary_code=TSKTT

SlashNext. 2021. The Human Hacking Report. https://www.slashnext.com/wp-content/uploads/2021/10/SlashNext-Human-Hacking-Report.pdf

Soomro, Z. A., Shah, M. H., & Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), s. 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Statista. 2022. Number of internet and social media users worldwide as of July 2022. https://www.statista.com/statistics/617136/digital-population-worldwide/

Stewart, P. 2010. Spies behind 2008 cyber attack, U.S. official says. Reuters. Viitattu 19.10.2022. https://www.reuters.com/article/us-usa-cyber-attack-idUSTRE67P00X20100826

Still, J. D., & Bell, J. 2018. Incognito: Shoulder-surfing resistant selection method. Journal of information security and applications, 40, s. 1-8. https://doi.org/10.1016/j.jisa.2018.02.006

Sumner, A., & Yuan, X. 2019. Mitigating phishing attacks: an overview. Proceedings of the 2019 ACM Southeast Conference, s. 72-77. https://doi.org/10.1145/3299815.3314437

Syed, A. M. 2021. Social engineering: Concepts, Techniques and Security Countermeasures. arXiv preprint arXiv:2107.14082. https://doi.org/10.48550/arXiv.2107.14082

Tuomi, J., & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi. E-kirja.

Tuominen, A. 2022. Oululainen nainen tehtaili rakkauspetoksilla jopa 170 000 euroa – uhreina vanhemmat miehet. Viitattu 8.11.2022. https://www.iltalehti.fi/kotimaa/a/330d6df5-01ec-4d9a-a744-ea4a4897dbff

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Viitattu 8.11.2022. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Varshney, G., & Gupta, H. 2017. A security framework for IoT devices against wireless threats. 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) s. 1-6. IEEE. DOI: 10.1109/TEL-NET.2017.8343548

Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. 2021. Social engineering attacks during the COVID-19 pandemic. SN computer science, 2(2), s. 1–9. https://doi.org/10.1007/s42979-020-00443-1

Verizon. 2022. 2022 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

Vigliarolo, B. 2021. Forrester: These 5 threats could hobble pandemic recovery. Viitattu 10.11.2022. https://www.techrepublic.com/article/forrester-these-5-threats-could-hobble-pandemic-recovery/

Westerlund, M. 2019. The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11). http://doi.org/10.22215/timreview/1282

Wojewidka, J. 2020. The deepfake threat to face biometrics. Biometric Technology Today, 2020(2), s. 5-7. https://doi.org/10.1016/S0969-4765(20)30023-0

Kuviot

Kuvio 1. Tietoturvan CIA-malli 12
Kuvio 2. Käyttäjän manipulointi ja eri manipulointikeinot ja hyökkäysmetodit 15
Kuvio 3. Esimerkki tietojenkalastelusta (Lähde: Flickr) 16
Kuvio 4. Käyttäjän manipuloinnin vaiheet 21
Kuvio 5. Tyypilliset persoonallisuuspiirteet työtehtävissä, mukailtu Mannin (2008) mukaan .. 36
Kuvio 6. Varautumiskeinot käyttäjän manipuloinnin hyökkäyksiin 39

Taulukot

Taulukko 1. Opinnäytetyön aineisto 31