Deniz Anttila

# KÄYTTÄJÄN MANIPULOINTI ORGANISAATION TIETOTURVAUHKANA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

# TIIVISTELMÄ

Anttila, Deniz
Käyttäjän Manipulointi Organisaation Tietoturvauhkana
Jyväskylä: Jyväskylän yliopisto, 2016, 31 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Seppänen, Ville; Moilanen, Panu

Tämän tutkielman aiheena on käyttäjän manipulointi organisaation tietoturvauhkana. Käyttäjän manipulointi (engl. *social engineering*) viittaa organisaation henkilöstön inhimillisiin piirteisiin tietoturvariskin tekijänä. Vahva tekninen tietoturvantaso suojaa organisaatiota verkon välityksellä yritetyiltä tietomurroilta, mutta järjestelmien käyttäjien inhimilliset heikkoudet jäävät usein huomiotta. Tutkielmassa kuvaillaan, kuinka käyttäjän manipulointi toimii tietoturvaa uhkaavana tekijänä, sekä kuinka organisaatio voi varautua manipulointia hyödyntäviä hyökkäyksiä vastaan.

Tutkielman tavoitteena on tunnistaa tekijät, jotka mahdollistavat käyttäjään kohdistuvan manipuloinnin, sekä keinot, joilla organisaatio voi varautua käyttäjän manipuloinnin varalta. Tutkielmassa kuvaillaan myös, kuinka organisaation tulee huomioida kolme lähestymistapaa torjuakseen käyttäjän manipulointia hyödyntäviä hyökkäyksiä. Lähestymistavat ovat organisaationlaajuinen lähestymistapa, käyttäjäkohtainen lähestymistapa, sekä tekninen lähestymistapa.

Tutkielmassa tutustutaan lähestymistapojen ratkaisuina esitettyihin organisaationlaajuiseen toimintamalliin, käyttäjäkohtaiseen hyökkäyksen tunnistusmalliin, sekä biometriseen teknologiaan. Nämä esitetään organisaation puolustautumiskeinoina käyttäjän manipulointia hyödyntäviä hyökkäyksiä vastaan.

Tutkielman tuloksina ovat kuvaukset käyttäjän manipuloinnin käsitteestä, käyttäjän manipuloinnin yleisistä metodeista, sekä lähestymistavoista hyökkäysten tunnistamiseksi ja torjumiseksi. Tutkielma suoritetaan kirjallisuuskatsauksena.

Asiasanat: tietoturva, käyttäjän manipulointi, tieto- ja viestintärikokset, tietoturvapolitiikka, verkkohyökkäykset.

# ABSTRACT

Anttila, Deniz
Social Engineering as an Information Security Threat for an Organization
Jyväskylä: University of Jyväskylä, 2016, 31 p.
Information systems science, Bachelor's Thesis
Supervisor: Seppänen, Ville; Moilanen, Panu

The topic of this thesis is Social Engineering as an Information Security Threat for an Organization. Social Engineering (SE) refers to the information security aspect of the humane weaknesses in the personnel working within an organization. A strong technical level of information security provides protection towards hacking, but the humane weaknesses of system users are usually left unnoticed. This thesis describes how social engineering is an information security threat and how can an organization be able to prepare for these attacks.

The goal of this thesis is to identify the factors, which enable social engineering and the methods to prevent it. This thesis describes how an organization should consider three different approaches to prevent social engineering attacks. The approaches are an organization-wide approach, user-specific approach and a technical approach.

Through the different approaches the thesis will familiarize with an organization-wide model, a user-specific attack identification model, and a biometric technical solution. These are shown as the means of defense against social engineering for an organization.

The results of this thesis are the description of social engineering, it's methods, and the approaches to consider to prevent social engineering attacks. The thesis is conducted as a literary review.

Keywords: information security, social engineering, customer information security, information security policy.

# KUVIOT

# SISÄLLYS

# 1 JOHDANTO

Yksityisten, sekä julkisten organisaatioiden tietojärjestelmillä on useita käyttäjiä organisaation eri tasoilla. Tietojärjestelmät voivat pitää tietokannoissaan organisaatiolle hyvinkin arkaluontoista tietoa, kuten yritysten asiakastietoja, henkilötietoja tai muuta tärkeää liiketoimintaa koskevaa tietoa. Tietoturvan taso tulee olla teknisesti luotettava ja läpäisemätön perinteisimmille kyberhyökkäyksille. Tietojärjestelmän tietoturva voi olla kuitenkin uhattuna teknisestä läpäisemättömyydestään huolimatta. Organisaatioiden kohtaamat tietoturvallisuuden ongelmat sisältävät myös henkilöstön käyttäytymiseen liittyvän näkökulman. Varotoimien epäonnistuminen tietoturvallisuuden uhkia kohtaan on osin jäänyt huomiotta, varsinkin koskien käyttäjän manipuloinnin uhkia (Workman, 2007.) Itse tietojärjestelmän käyttäjä voi toimia uhkana tietoturvalle, sillä käyttäjää voi sosiaalisten metodien avulla manipuloida ja siten saada hänet jakamaan informaatiota tai toimimaan hyökkääjän avuksi. Tätä informaatioturvan näkökulmaa käsittelee käyttäjän manipulointi (engl. *social engineering*).

Phillipsin (2007) mukaan vuonna 2007 Yhdysvaltojen IRS:lle (Internal Revenue Service, verovirasto) tehtiin organisaation henkilökunnan ja tietojärjestelmien käyttäjien manipulointia testaava auditointi, jonka tavoitteena oli selvittää henkilökunnan taipumusta altistua käyttäjien manipulaatiota hyödyntäville hyökkäyksille. IRS:llä oli auditointia suorittaessa lähes 100 000 ihmisen henkilökunta, joilla on myös pääsy veronmaksajien verotietoihin. Veronmaksajien verotietoja prosessoitiin 240:ssä tietojärjestelmässä sekä 1500:ssa tietokannassa. Auditoinnissa käytettiin manipuloinnin taktiikkaa, jossa puhelinsoittaja teeskenteli olevansa organisaation teknologiaosaston ohjelmistopäivitystä suorittava henkilö, sekä pyysi kohdettaan avustamaan häntä järjestelmäongelman kanssa. Soittaja pyysi työntekijää auttamaan häntä antamalla käyttäjänimensä ja väliaikaisesti vaihtamaan salasanansa soittajan ehdottamaan salasanaan.

95,858:sta IRS:n työntekijästä valittiin kokeeseen 102 henkilöä, joihin lukeutui työntekijöitä, esimiehiä ja yksi urakoitsija. 102:sta soiton kohteeksi valitusta työntekijästä 61, eli noin 60 %, noudatti soittajan ohjeita ja vaihtoi salasanansa soittajan ehdottamaan salasanaan. Kokeen tavoitteena oli lisäksi selvittää, kuinka suuri osa manipuloinnin yrityksistä huomattaisiin, sekä ilmoitettaisiin

organisaatiossa ylemmälle tasolle, jotta organisaatio voisi minimoida mahdolliset vahingot varoittamalla muuta henkilökuntaa. Vain 8 henkilöä 102:sta soiton kohteesta raportoi urkintaa suorittavasta puhelinsoitosta eteenpäin (Phillips, 2007.)

Phillipsin (2007) kuvaileman auditoinnin tuloksiin perustuen oli riski, että IRS toimittaisi luvattomille henkilöille pääsyn veronmaksajien dataan. Tätä veronmaksajien dataa luvaton henkilö voisi mahdollisesti käyttää identiteettivarkauksiin tai muihin vilpillisiin tarkoituksiin. Enemmistö henkilökunnasta ei joko ymmärtänyt täysin käyttäjätunnusten turvallisuusvaatimuksia, tai he eivät pitäneet veronmaksajien tietojen turvaamista riittävän korkeana prioriteettina heidän jokapäiväisessä työssään. Auditoinnin tuloksissa oli huolestuttavinta se, että samankaltaisia auditointeja oli pidetty jo aikaisemmin vuosina 2001 sekä 2004. Reaktiona aikaisemmin suoritettuihin käyttäjien manipulointia testaaviin auditointeihin IRS suoritti korjaavia toimia nostattaakseen tietoisuutta järjestelmien tunnusten suojelemisen vaatimuksista sekä käyttäjien manipuloinnin yrityksistä (Phillips, 2007.)

Jotta IRS:n kaltaisista tapauksista vältyttäisiin, tulee organisaation jokaisen toimijan tiedostaa manipulointia hyödyntävän hyökkäyksen mahdollisuus ja keinot miten hyökkäykset voidaan havaita. Tämä tutkielma käsittelee käyttäjien manipulointia organisaation tietoturvallisuusuhan näkökulmasta. Tutkielmassa kuvaillaan inhimillisiä piirteitä, jotka saattavat altistaa manipuloinnin uhriksi joutumista. Tutkielman tarkoituksena on myös selvittää käyttäjien manipuloinnin yleisiä metodeja ja työkaluja, sekä keinoja joilla organisaatio voi toimia uhkien minimoimiseksi. Tutkielmassa käsiteltävät käyttäjän manipuloinnin metodit ovat nousseet useasti esille aihetta koskevassa kirjallisuudessa.

Käyttäjien manipulointia hyödyntävän hyökkäyksen avustavina ohjelmistotyökaluina esitetään organisaation tietoturvallisuuden auditointia varten suunniteltuja ohjelmistoja, jotka ovat kehitetty käyttäjien manipulointia testaaville auditoijille. Ohjelmistotyökalut kuitenkin kuvastavat ominaisuuksiltaan ohjelmistoja, joita organisaation käyttäjiä kohti hyökkäävät tahotkin voisivat käyttää.

Lopuksi tutkielmassa käsitellään keinoja ja teknologiaa, joilla voidaan ehkäistä käyttäjän manipuloinnin onnistuminen organisaatiossa. Motivaationa tutkielmalle on tahto tuottaa organisaatioiden tietoturvasta vastaaville henkilöille, sekä muille organisaation jäsenille, informaatiota käyttäjien manipuloinnin uhkista ja keskeisistä keinoista niiden välttämiseksi.

Tutkielman tutkimusmenetelmänä käytettiin kirjallisuuskatsausta, jonka lähdeaineisto koostuu aiheeseen liittyvistä tieteellisistä julkaisuista, raporteista ja kirjallisuudesta. Tutkielman lähdekirjallisuutta on kerätty Jyväskylän Yliopiston Kirjaston NELLI-portaalia (http://www.nelliportaali.fi/) käyttämällä. Google Scholar-verkkopalvelua (http://scholar.google.fi/) käytettiin tukena lähdekirjallisuuden tunnettuuden arvioimiseen. Lähdekirjallisuuden valinnassa huomioitiin kirjoittajan tunnettuus ja

arvostettuus, sekä lähdetiedon alkuperä. Tutkielmassa tutkimusongelmaa lähestytään vastaamalla kysymykseen:

- Miten organisaatio voi puolustautua käyttäjän manipulointia hyödyntävän hyökkäyksen varalta?

Tutkielman tutkimustuloksena on kolmen lähestymistavan periaate organisaatiolle käyttäjän manipuloinnin uhkaa kohtaan. Lähestymistavat ovat organisaationlaajuinen, käyttäjäkohtainen ja tekninen lähestymistapa. Lähestymistavat sisältävät toimintamallin organisaation tietoisuuden kasvattamiseksi, keinon käyttäjän manipuloinnin tunnistamiseksi käytännön tilanteessa, sekä ehdotuksen vaihtoehtoisen teknologian soveltamiseksi. Tutkielmassa identifioitiin, että tärkeänä riskien minimoimisen välineenä on manipuloinnin riskien ja metodien tietoisuuden lisääminen organisaatiossa. Toiseksi, valmiiksi käsikirjoitettujen dialogien käyttäminen erikoistilanteita varten auttavat organisaation henkilökunnan jäseniä sivuuttamaan heidän inhimillisiä piirteitään, jotka saattavat toimia manipulaatiota käyttävän hyökkääjän avuksi. Kolmanneksi, biometriikkaa hyödyntävien teknisten sovellusten avulla organisaatio voi minimoida muistettavien tunnistetietojen määrää.

Seuraavassa luvussa käsitellään käyttäjän manipuloinnin termiä ja sitä, kuinka manipulointia voidaan katsoa eri näkökulmista. Lisäksi seuraavan luvun alaluvuissa perehdytään yksittäisiin tekijöihin, jotka edesauttavat käyttäjän manipulointia hyödyntävää hyökkääjää onnistumaan. Kolmannessa luvussa tarkastellaan käyttäjän manipuloinnin metodeja, eli kuinka erilaisia keinoja käyttämällä hyökkääjä voi kerätä arkaluonteista tietoa kohdeorganisaatiosta tai yksittäiseltä henkilöltä. Luku käsittelee myös käyttäjän manipulointiin hyödynnettäviä tietoteknisiä työkaluja. Neljännessä luvussa kuvataan kolmen lähestymistavan periaatetta, sekä kirjallisuudessa ehdotettuja ehkäisykeinoja käyttäjän manipulointia hyödyntävää hyökkäystä vastaan. Viimeisessä luvussa luodaan yhteenveto tutkimuksessa käsitellystä aiheesta.

# 2 KÄYTTÄJÄN MANIPULOINTI

Tässä luvussa käsitellään käyttäjän manipulointia, sen eri näkökulmia, sekä tekijöitä, jotka edesauttavat käyttäjän manipulointia hyödyntävää hyökkääjää onnistumaan. Luvussa tarkastellaan käyttäjän manipulointia käyttäjäkohtaisesta näkökulmasta. Tekijät, jotka edesauttavat käyttäjän manipulointia onnistumaan, ovat jaoteltu tässä luvussa omiin alalukuihinsa.

## 2.1 Mitä käyttäjän manipulointi on?

Manipulointi on laaja käsite, jolla voidaan viitata useaan eri aiheeseen poliittisista käytäntötavoista ihmisten mentaalisiin parannuskeinoihin. Manipulointia ilmenee ihmisten välisessä kanssakäymisessä, jota tapahtuu päivittäin eri tilanteissa, sekä eri kommunikointivälineiden välityksellä. Ihmisen manipulaation metodeja käytetään esimerkiksi lainvalvonnassa, kun epäiltyä henkilöä kuulustellaan. Opettaja saattaa käyttää manipulointia oppilaidensa välisessä kanssakäymisessä. Lapset taas saattavat käyttää manipulointia halutessaan saada tahtonsa läpi vanhemmilleen. Psykologit, lääkärit ja asianajajat voivat käyttää manipuloinniksi kuvailtavia metodeja saadakseen työhönsä liittyvää informaatiota asiakkaaltaan. Tämä tutkielma keskittyy manipuloinnin käsitteeseen organisaation tietoturvan näkökulmasta, kun manipuloinnin kohteena ovat organisaation tietojärjestelmien käyttäjät.

Organisaation tietojärjestelmien parissa työskentelevien henkilöiden tulisi olla tietoinen käyttäjän manipuloinnin tuomasta tietoturvauhkasta, sillä se on tehokas hyökkäysmetodi organisaation tietojärjestelmiä ja arkaluonteista tietoa kohtaan. Pavkovicin sekä Perkovin (2011) mukaan tietoturva on yksi tärkeä kriteeri tietojärjestelmän laadun arvioinnissa, mutta se riippuu niin teknisistä kuin ei-teknisistä tekijöistä. Lisäksi, Kotenkon, Stepashkin ja Doynikovan (2011) mukaan onnistuneen käyttäjän manipulointia hyödyntävän hyökkäyksen toteutus tekee myös teknisen hyökkäyksen mahdolliseksi ja usein johtaa suurempiin

vahinkoihin verraten pelkästään tekniseen hyökkäykseen. Samankaltaiseen johtopäätökseen päätyivät tutkimuksessaan myös Sun, Yan sekä Feng (2012).

Parhaimmankin tietojärjestelmän tietoturva ei kata sen heikointa elementtiä; tietojärjestelmän käyttäjää. Kehittynyt tekninen tietoturva on hyödytön, jos järjestelmän käyttäjä on taipuvainen manipulointiin. Täten organisaation tietoturvan tasoa voidaan parantaa henkilökunnan koulutuksen avulla ja lisäämällä tietoisuutta manipuloinnista. Osana organisaation henkilökunnan koulutusta ja informaatioturvallisuuden arviointia toimii tietoturvan läpäistyvyyden testaaminen käyttäjän manipulointia hyödyntäviä metodeja käyttäen (Pavkovic & Perkov, 2011.)

Käyttäjään kohdistuvan manipulointihyökkäyksen toimivuutta edesauttaa ihmisen halu auttaa toista ihmistä. Myös muut inhimilliset tunteet kuten materialistinen ahneus ja pelko toimivat hyökkääjän työtä edesauttavina tekijöinä. Kevin Mitnick, arvostettu yhdysvaltalainen käyttäjän manipulaation asiantuntija, on maininnut, että on huomattavasti helpompaa keinotella käyttäjä luovuttamaan salasana järjestelmään, kuin nähdä vaivaa järjestelmään murtautumiseen teknisesti (Mitnick & Simon, 2011.)

Käyttäjän manipuloinnin termiä kuvaili tarkemmin Christopher Hadnagy kirjassaan "*Social Engineering: The Art of Human Hacking*" seuraavasti: "Käyttäjän manipulointi on keino manipuloida ihminen ryhtymään toimiin, jotka voivat olla myöten tai vastoin kohteen omaa etua. Tämä voi sisältää informaation saantia, sisäänpääsyn saavuttamista tai kohteen saaminen toimimaan tietynlaisella tavalla." (Hadnagy, 2010, 10). Workman (2007) sen sijaan kuvaili käyttäjän manipulointia hyödyntävän hyökkäyksen arkkitehtuurin pyrkivän saamaan kohteen huomion, ylläpitämään hänen mielenkiintoaan, herättämään kohteessa tunteita, kuten pelkoa tai himoa, ja lopuksi saamaan kohde tekemään jokin toivottu toimenpide. Hadnagyn ja Workmanin määritykset eroavat hieman toisistaan, mutta niiden lopullinen tarkoitus on sama; saada kohde toimimaan jollakin manipuloijan haluamalla tavalla. Organisaation tietoturvan näkökulmasta manipuloijan toivoma toimenpide uhriltaan voi olla käyttäjätunnusten luovuttaminen organisaation tietojärjestelmään.

Kotenko ym. (2011) luokittelivat käyttäjän manipuloinnin hyökkäystavat kahteen luokkaan, joista ensimmäinen oli digitaalinen. Digitaalisessa hyökkäystavassa käytetään hyväksi informaatioteknologiaa eri keinoin petkuttamaan oikeutettuja järjestelmän käyttäjiä saadakseen heiltä tarvittavaa tietoa (esim. sähköpostin välityksellä). Digitaalista hyökkäystapaa käsitellään lisää seuraavassa luvussa. Toinen hyökkäystavan luokka on sosiaalinen, jossa käytetään ihmisten välistä kanssakäymistä (esim. pelottelu tai kiristys) informaation saantiin tai tiloihin sisäänpääsyä varten. (Kotenko ym., 2011.)

Sosiaalista käyttäjän manipulointia hyödyntävä hyökkäys tukeutuu siis vahvasti ihmisten mentaalisiin heikkouksiin ja piirteisiin. Cialdini (2009) tunnisti kirjassaan kuusi tekijää, jotka toimivat osana ihmisten suostuttelutaktiikoita: vastavuoroisuus, velvollisuudentunto, sosiaalinen osoitus, miellyttävyys, auktoriteetti, sekä niukkuus. Nämä suostuttelutaktiikat ovat tekijöitä, jotka ovat käytössä myös menestyvissä kaupallisten tuotteiden markkinointikampanjoissa

(Workman, 2007). Mitnick ja Simon (2011) vahvistivat Workmanin havaintoa ilmaisemalla, että vaikka käyttäjän manipuloimisen tarkoituksena ei ole tässä tapauksessa välttämättä myydä tuotetta tai palvelua, sen pyrkimys on suostutella ihmisiä luovuttamaan arkaluonteista tietoa samoilla keinoilla. Käyttäjän manipulointia hyödyntävä hyökkäys soveltaa siis myös markkinoinnissa hyväksi todettuja keinoja. Tämä on ymmärrettävää, sillä esimerkiksi jonkin tuotteen markkinoinnin tarkoitus on vaikuttaa ihmisten ostopäätöksiin ja kulutuskäyttäytymiseen.

Käyttäjän manipulointia voi myös ilmetä monin erilaisin tavoin. Esimerkiksi, kun maailmalla tapahtuu jokin suurempi katastrofi tai luonnonmullistus. Katastrofin sattuessa on myös ihmisiä huijaavia tahoja liikkeellä ottaakseen hyödyn irti sivusta seuraavien ihmisten inhimillisistä tunteista. 2001 vuoden WTC-iskut sekä Haitin maanjäristykset aiheuttivat ihmisissä myötätuntoa katastrofin uhreille ja heidän perheenjäsenilleen. Haitin maanjäristyksen jälkeen oli oikeutettua, että oli perustettu rahastoja, jotka ilmoittivat keräävänsä varoja uhrien avuksi.

Yhdysvaltain liittovaltion keskusrikospoliisi, eli FBI, (2010) kuitenkin varoitti lehdistötiedotteessaan vilpillisistä varainkeruurahastoista, jotka väittivät keräävänsä rahallista tukea 12.1.2010 tapahtuneen Haitin maanjäristyksen uhreille. Varoituksessa kehotettiin netin käyttäjiä toimimaan kriittisesti heihin kohdistuvia vetoamuksia kohtaan, jotka pyytävät viestin vastaanottajaa lahjoittamaan rahaa erilaisiin varainkeruurahastoihin. Viestien vastaanottajia kehotettiin varmistamaan varainkeruuorganisaation aitous ensin muiden nettiresurssien kautta ja tekemään lahjoituksia vain tunnettuihin varainkeruurahastoihin. Ihmisiä myös kehotettiin olemaan skeptisiä maanjäristyksen uhreiksi esittäytyviä henkilöitä kohtaan, jotka ottavat yhteyttä sähköpostitse tai sosiaalisessa mediassa. FBI kehotti myös jättää vastaamatta pyytämättömiin sähköposteihin, sekä klikkaamatta viestien sisältämiä linkkejä. Viestien sisältämien valokuvien klikkaamista pyydettiin välttämään, sillä ne saattoivat sisältää haittaohjelmia. Ohjeistus kehotti myös olemaan luovuttamatta henkilökohtaista tai taloudellista tietoa lahjoituksen pyytäjälle, sillä niitä on mahdollista käyttää henkilön identiteetin vaarantamiseen tai identiteettivarkauteen (FBI National Press Office, 2010.) FBI julkaisi varoituksensa 13.1.2010 eli heti seuraavana päivänä, kun maanjäristys oli tapahtunut Haitissa. FBI:n väestölle antamien ohjeistusten ja varoittavien esimerkkien piirteistä voi olettaa vilpillisellä taholla olevan käytössä käyttäjien manipuloinnin keinot.

FBI:n varoitukset olivat suunnattu yksittäisille henkilöille, mutta organisaatioita kohtaan kohdistetut manipuloinnin varoitukset ovat harvassa. Syy voi johtua siitä, että harvoja tutkimuksia on julkaistu käyttäjän manipulointia hyödyntävistä hyökkäyksistä organisaatioita kohtaan. Tämä taas johtuu mahdollisesti syystä, että organisaatiokohtaisen tiedon julkaiseminen voi tahria organisaation mainetta, ja uhreiksi joutuneet organisaatiot eivät todennäköisesti halua paljastaa uhriksi joutumistaan. Eräs tutkimus kuitenkin vihjaa, että organisaation tietojärjestelmän käyttäjä saattaa turvautua toimimaan avuliaasti, kun häntä

pyydetään toimimaan tai antamaan informaatiota tilanteessa, jossa häneltä puuttuu ohjeistus tai valmiina oleva yleisohje tilanteen varalta (Hadnagy, Aharoni & O'Gorman, 2010). Samassa tutkimuksessa myös vihjattiin sitä, että henkilökunta vähittäiskauppa-ympäristössä on epätodennäköisemmin huiputettavissa, kuin henkilökunta puhelinkeskuksessa tai asiakastukisivustolla (Hadnagy ym., 2010).

Kuten aikaisemmin kappaleessa mainittiin, käyttäjän manipulointihyökkäyksessä hyödynnetään järjestelmän käyttäjän inhimillisiä heikkouksia. Hyökkäys voi kohdistua keneen tahansa toimijaan työntekijästä toimitusjohtajaan. Seuraavissa alikappaleissa käsitellään ihmisten heikkouksia ja luonteenpiirteitä, jotka manipulointihyökkäyksessä toimivat hyökkääjän eduksi. Näitä piirteitä ovat välinpitämättömyys, vastavuoroisuus ja myönnytys, johdonmukaisuus, sosiaalinen osoitus, miellyttävyys ja luottamus, auktoriteetti ja pelko, sekä käyttäytyminen niukkuuden vallitessa. Esitetyt piirteet on tuotu useasti ilmi käyttäjän manipulointia käsittelevässä kirjallisuudessa.

## 2.2 Välinpitämättömyys

Välinpitämättömyys on ihmisen luonteenpiirre, jolla voi olla suuria merkityksiä organisaation tietoturvaa kohtaan. Siposen, Pahnilan ja Mahmoodin (2010) mukaan suurin uhka tietoturvallisuudelle nousee piittaamattomista työntekijöistä, jotka epäonnistuvat noudattamaan organisaation tietoturvakäytäntöjä sekä menettelytapoja. Vaikka ihmiset väittävät olevansa huolissaan informaatioturvallisuudesta, tietojensa yksityisyydestä, sekä ovat jopa valmiita maksamaan palveluista heidän henkilökohtaisten tietojensa turvaamiseksi, monessa tapauksessa he ovat valmiita luopumaan yksityisyydestään helppokäyttöisyyden nimissä. Suhteellisen pienikin palkkio saattaa motivoida hyvinkin arkaluontoisen tiedon luovuttamisen (Acquisti & Grossklags, 2003; Workman, 2008.) Käyttäjien välinpitämättömyys tietoturvan mahdollisia uhkia kohtaan edesauttaa siten metodeja hyödyntävää hyökkääjää, koska käyttäjä ei välttämättä koe tarpeelliseksi noudattaa organisaation laatimia tietoturvakäytäntöjä.

## 2.3 Myönnytys ja vastavuoroisuus

Vastavuoroisuus on ihmisten välistä kanssakäymistä, jossa osapuolet kohtelevat toisiansa samalla tavoin. Ihmiset voivat kokea vastenmielisiä tunteita sellaisia ihmisiä kohtaan, jotka ottavat, mutta eivät anna mitään vastineeksi, jolloin vastavuoroinen kanssakäyminen ei toteudu. Toisin sanoen, ihmiset pyrkivät välttämään leimautumista kitsastelijaksi (Cialdini, 2009.) Vastavuoroisuus on siis piirre, joka saattaa johtaa tilanteeseen jossa ihminen ajautuu tuntemaan olevansa kiitollisuudenvelassa, jolloin on todennäköisempää saada henkilö toimimaan manipuloivan hyökkääjän avuksi.

Myönnytyksen ilmaiseminen (engl. *concession)* on vastavuoroisen kanssakäymisen kaltainen suostuttelukeino. Myönnytys liittyy vastavuoroisuuteen tavalla, jossa myönnytyksen saanut henkilö kokee velvollisuudekseen tuottaa itsekin myönnytys, jolloin jälleen vastavuoroinen kanssakäyminen toteutuu (Cialdini & Goldstein, 2004.) Cialdini ja Goldstein (2004) selittävät myös ”ovi-päin-kasvoja”-tekniikan (engl. *door-in-the-face technique*) toimivan ihmisten myönnytyksen ja vastavuoroisuuden ansiosta. Kyseisessä ”ovi-päin-kasvoja” -tekniikassa manipuloiva henkilö käyttää strategiaa, jossa hän esittää ensin äärimmäisen pyynnön toiminnasta, joka todennäköisesti tulee vastaanottajan hylkäämäksi, ennen kuin hän esittää todellisesti haluamansa, lievemmän toiminnan (Cialdini & Goldstein, 2004).

Cialdini (2009) kuvaa kirjassaan koetta, jossa pyydettiin opiskelijoita myöntymään kaitsemaan nuorisorikollisten ryhmää päiväretkelle eläintarhaan. 83 % tehtävään pyydetyistä opiskelijoista kieltäytyi ja 17 % myöntyi. Samankaltaiselta kohderyhmältä opiskelijoita kysyttiin samaa asiaa, mutta ensin pyytämällä reilusti enemmän ponnistusta vaativaa palvelusta. Ensin heitä pyydettiin viettämään kaksi tuntia viikossa ohjaajana nuorisorikollisille vähintään kahden vuoden ajan. Vasta kohteen hylättyä paljon enemmän vaativan ensimmäisen pyynnön, tarjottiin kohteelle eläintarharetkeä. Eläintarharetken ehdottaminen oli myönnytys aikaisemman ehdotuksen hylkäämiseen. 50 % vastasi tarjoukseen vastavuoroisesti myönnytyksellä, jossa ensin pyydettiin osallistumaan paljon vaativampaan tehtävään. Myönnytystä käyttämällä suostuttelukeinona tehtävään suostuteltiin kolminkertainen määrä opiskelijoita (Cialdini, 2009.)

Cialdinin kuvailema koe osoittaa vastavuoroisuuden kanssakäymisen ja myönnytyksen esittämisen yhteisen vaikuttavuuden ihmisen päätöksentekoon. Vastavuoroisuus ja myönnytys ovat siten piirteitä, joita hyökkääjä voi hyödyntää manipuloidessaan käyttäjää toimimaan haluamallaan tavalla.

## 2.4 Johdonmukaisuus ja sitoutuminen

Johdonmukaisuus nähdään yleisesti positiivisena piirteenä ihmisessä ja epäjohdonmukaisuus siten negatiivisena piirteenä. Johdonmukainen käyttäytyminen kasvattaa luottamusta ihmisissä, kun taas epäjohdonmukaisuus herättää epäilystä ja arvaamattomuuden tunnetta. Kognitiivisen dissonanssin johdonmukaisuuden teoria (engl. *theory of cognitive dissonance*) ehdottaa, että ihmiset ovat motivoituneita ylläpitämään yhtenevyyttä asenteissa, sosiaalisissa normeissa, sekä käytöksissä, jotta he säilyttävät yhdenmukaisuuden tunteen (Festinger & Carlsmith, 1959). Ihmiset siten haluavat esittäytyä johdonmukaisina käyttäytymisessään. Itse-oikeutus teoria (engl. *self-justification theory*) lisäksi väittää, että ihmisillä on taipumusta kohottaa heidän sitoutumista valitsemaansa toimintatapaan (ja joutua negatiivisten seurauksien lisääntymisen riskiin) oikeuttaakseen itsellensä aikaisempaa käyttäytymistään (Staw & Fox, 1977). Tästä johtuen, johdonmukainen käyttäytyminen voi toimia hyökkäyksen kohdehenkilöä vas-

taan, jos manipuloija kykenee esittämään johdattelevia kysymyksiä oikeuttaakseen varsinaista pyyntöään.

Johdonmukaista käyttäytymistä hyödyntävät hyökkäykset ovat suunniteltu niin, että vaivannäön taso, jonka kohteen tulisi investoida, tulisi olemaan alhaisempi kuin saatavat edut. Siten päätös olla välittämättä varotoimenpiteistä voidaan koeta perusteltuna, kun kulut ja riskit kumoutuvat väitetyillä eduilla. Riskinä voidaan määritellä olevan epätietoisuus toimenpiteen lopputuloksista tai seurauksista ja etuna rahallinen tai ei rahallinen palkinto, jolla on jotakin todellista arvoa vastaanottajalle (Charbaji & Jannoun, 2005.) Myös Hsu & Kuo (2003) selittivät että kun ihmiset kokevat, että edut kumoavat varotoimenpiteiden ottamisen kulut, he esittävät johdonmukaisuutta, jonka aikana he ovat todennäköisemmin taipuvaisia manipulointiin saadakseen väitetyt edut.

## 2.5 Sosiaalinen osoitus

Sosiaalinen osoitus (engl. *social proof*) viittaa ihmisten taipumukseen sopeuttaa uskomuksensa ja käyttäytymisensä ympäröivien ihmisten uskomusten ja käyttäytymisen mukaiseksi tullakseen sosiaalisesti hyväksytyksi. Esimerkiksi, viitaten aikaisemmin esitettyyn IRS:n tapaukseen, jos käyttäjätunnusta kyselevän puhelun saaneen henkilön kollegat olisivat jo totelleet puhelimen välityksellä saatuja käskyjä, niin kyseisen henkilön olisi ollut helppoa sopeutua käyttäytymään samoin. Lisäksi sosiaalinen osoitus viittaa korkeampaan luottamuksen osoitukseen ihmisiä kohtaan, jotka jakavat samankaltaisia mielipiteitä keskenään varsinkin epäselvissä tilanteissa (Uebelacker & Quiel, 2014.) Sosiaalisen osoituksen vaikutus ihmisten päätöksentekoon on siten huomioitava käyttäjään kohdistuvassa manipulointihyökkäyksessä, koska se toimii keinona hyökkääjälle uhrinsa luottamuksen saavuttamiseen, sekä pyyntönsä oikeutukseen esim. vedoten muiden ihmisten päätöksiin tai tekoihin.

## 2.6 Miellyttävyys ja luottamus

Sosiaalisen osoituksen lisäksi ihmisten kokemaa miellyttävyyttä toista ihmistä kohtaan voidaan käyttää luottamuksen luomiseen. Workmanin (2008) mukaan ihminen ilmaisee luottamusta henkilöä kohtaan sekä noudattaa hänen pyyntöjä, jos hänen mielestään henkilö on viehättävä tai koettu uskottavaksi, tai omaa erikoisosaamista. Usein käyttäjän manipulointia hyväksikäyttävä hyökkäys suoritetaan käyttäen sähköpostia, postikorttia, verkkosivua, tai puhelinsoittoa, jossa on hankalaa kommunikoida henkilökohtaista miellyttävyyttä. Tästä johtuen hyökkääjä pyrkii saamaan kohteen tykkäämään hänestä ja luottamaan häneen luomalla ystävällisen viestittelysuhteen kohteen kanssa (Workman, 2008.) Mitnick & Simon (2011) tarkentavat väittämällä, että ystävällinen luottamussuhde luodaan yleensä vetoamalla ihmisten yksinäisyyteen, tai jonkin henkilön

ystävän kaipuuseen, luomalla tunne samankaltaisuudesta kohteen kanssa, tai jopa tekaisten olemalla jokin tunnettu ja pidetty henkilö.

## 2.7 Auktoriteetti ja pelko

Workman (2007) väittää, että ihmiset toisinaan paljastavat arkaa tai yksityistä tietoa henkilöille joille he tuntevat olevan velvollisia tämän tiedon antamiseksi. Käyttäjän kokema toisen henkilön auktoriteetti voi siten luoda velvollisuuden tunteen luovuttamaan arkaa tai henkilökohtaista tietoa. Myös Mouton, Malan, Leenen ja Venter (2014) kuvailivat, että ihmiset noudattavat helposti pyyntöä, jonka esittää henkilö, joka omaa enemmän auktoriteettia. Auktoriteettia voidaan myös käyttää pelon tunteen luomiseen. Workmanin (2008) mukaan käyttäjään kohdistuvan manipuloinnin uhri saattaa totella hyökkääjän antamia komentoja välttääkseen negatiiviset seuraamukset, kuten jonkin etuoikeuden tai muun arvokkaan asian menettämisen, rangaistuksen, nöyryytyksen, tai tuomitsemisen. Organisaatiot perustuvat hierarkioihin, jolloin hyökkääjän on mahdollista tekeytyä korkeampiarvoiseksi henkilöksi lisäämään kohteessaan auktoriteetin tunnetta.

## 2.8 Niukkuus

Niukkuutta voi eri tekijöiden puutteen muodossa ilmetä monella eri tavalla hyökkääjän manipuloitaessa käyttäjää. MacCrimmonin ja Wehrungin (1986) mukaan jokaisessa riskialttiissa tilanteessa on luontaista olla kolme tunnistettavaa tekijää: kontrollin puute, informaation puute, sekä ajan puute. Moutonin ym. (2014) mukaan ihmiset ovat halukkaampia myöntymään pyyntöihin, kun ne ovat harvinaisia tai niiden saatavuus on vähentyvä. Niukkuuden toimivuus perustuu Workmanin (2007) mukaan reaktanssin periaatteeseen (engl. *reactance theory*), jossa ihmiset vastaavat koettuun vajaukseen asettamalla suurempaa arvoa asioihin, joita on vähän tai niukasti.

Ajan niukkuutta käytetään käyttäjän manipulointia hyödyntävissä hyökkäyksissä yleensä kiireellisyyden tunteen luomiseen päätöksentekotilanteessa. Kiireellisyys voi mahdollistaa päätöksentekoprosessin manipuloinnin hyökkääjän saadessa tilaisuuden kontrolloida kohteelle suunnattua saatavilla olevaa informaatiota. Hyökkääjän kontrolli perustuu siihen, että kohde tuntee niukkuutta ajassa kerätä lisää informaatiota. Hyökkääjän kohteelle suunnattu saatavilla oleva informaatio voi johtaa kohdetta harhaan ja saada tämä tekemään päätös hyökkääjän hyväksi. Lisäksi, käyttäjän manipulointia hyödyntävä hyökkääjä yleensä käyttää auktoriteetin toimintaperiaatetta yhdistettynä niukkuuden tilan tunteeseen (Hadnagy, 2010.)

# 3 KÄYTTÄJÄN MANIPULOINNIN METODIT

Käyttäjän manipulointia käsittelevässä kirjallisuudessa usein ilmeneviä metodeja ovat verukkeen luominen, verkkourkinnan eri muodot, sekä paperinkeräysastian tutkiminen. Organisaatiolle nämä metodit ovat tietoturvariskejä, joita organisaation tulisi ottaa huomioon kokonaisvaltaisen tietoturvallisuuden takaamiseksi. Järjestelmien käyttäjiä manipuloivia verkkourkinnan metodeja käytetään hyökkäyksissä saamaan arkaluonteista informaatiota (kuten käyttäjätunnuksia tai salasanoja järjestelmiin), ohjaamaan henkilö lataamaan haitallinen tiedosto tai siirtymään verkkosivuille, joissa saattaa olla haittaohjelmallista sisältöä sivuston osaelementeissä. Kaikkia metodeja kuitenkin edeltää hyökkääjän informaation keruu kohteesta. Yritysten ja organisaatioiden verkkosivustoista on usein vaivatonta hakea tietoa organisaation henkilökunnasta, kuten jopa heidän sähköpostiosoitteita.

Mouton ym. (2014) ehdottivat täydennettyä käyttäjän manipuloinnin viitekehystä perustuen Mitnickin ja Simonin (2011) yksinkertaisempaan neljän vaiheen käyttäjän manipuloinnin viitekehykseen. Ehdotettu viitekehys koostuu kuudesta vaiheesta, jotka ovat *hyökkäyksen muotoilu*, *informaation keruu*, *valmistautuminen*, *suhteen luominen kohteen kanssa*, *suhteen hyödyntäminen*, sekä *kuulustelu* (Mouton ym., 2014). Viitekehyksen toinen vaihe, eli informaation keruu, on tärkeä osa käyttäjän manipulointia hyödyntävää hyökkäystä, koska hyökkäyksen kohteen kanssa luotavan luottamuksellisen suhteen kehittämisen todennäköisyys kasvaa riippuen kohdetta koskevan informaation laadusta (Mouton ym., 2014). Hyökkääjä voi suunnitella hyökkäyksensä taustatietoihin perustuvalla verukkeella, jotta se voisi onnistua suuremmalla todennäköisyydellä. Laadukas taustatieto mahdollistaa myös hyökkääjälle mutkattoman kanssakäymisen keskusteltaessa organisaation työntekijöiden kanssa kasvokkain tai puhelimessa. Hyökkääjän tulee osata organisaation sisäinen kielenkäyttö sekä ammattitermit organisaation työntekijöiden välisen kanssakäymisen onnistumisen varmistamiseksi. Muita tärkeitä taustatietoja voivat olla esimerkiksi se, että onko organisaatiolla sisäistä IT-tukea vai onko se ulkoistettua, tietokoneiden merkki, malli ja käyttöjärjestelmä, verkkoselain ja sen versio, PDF-lukijan

versio, tai onko käytössä etäkäyttö mahdollisuus, sekä mikä on etäkäytön tuottamiseen käytetty ohjelmisto (Hadnagy, Aharoni & O'Gorman, 2010.)

Seuraavissa alaluvuissa kuvaillaan tarkemmin manipuloinnin ja tiedon keräämisen metodeja. Metodeja ovat verukkeen luominen, verkkourkinta, pharming-huijaus, paperinkeräysastian tutkiminen, sekä käyttäjän manipuloinnin työkalut. Viimeisessä alaluvussa käsitellään teknisiä työkaluja, joiden avulla on mahdollista luoda haittaohjelmia, tai kerätä tietoa organisaatiosta.

## 3.1 Verukkeen luominen

Verukkeen luominen (engl. *pretexting*) viittaa hyökkääjän luomaan skenaarioon tai kuviteltuun toimintasuunnitelmaan, jolla on tarkoitus saada hyökkäyksen kohde uskomaan skenaarion mukaiseen tilanteeseen ja siten oikeuttaa hyökkääjän pyyntö. Verukkeen luominen nojaa vahvasti hyökkääjän kykyyn kerätä tietoa hyökkäyksen kohteesta, jotta hän voi luoda uskottavan skenaarion. Hyökkääjä luo siis puitteet, jotka ovat suunniteltu vaikuttamaan aiottuun uhriin, jotta hän luovuttaa arkaluontoista informaatiota tai suorittaa toimintoja, jotka vaarantavat informaation luottamuksellisuutta (Workman, 2008.)

Verukkeen luominen on enemmän kuin pelkkä valhe. Joissakin tapauksissa petkuttaja voi luoda kokonaisen identiteetin manipuloidakseen informaation vastaanottajaa. Petkuttaja voi käyttää verukkeen luomista imitoidakseen henkilöitä erinäisissä työtehtävissä, joita hän ei ikinä ole itse tehnyt, tai rooleissa, joita hän ei ole ikinä ollut (Hadnagy, 2010; Fujikawa & Nishigaki, 2011). Verukkeen luominen myös kuuluu Moutonin ym. (2014) ehdottaman viitekehyksen kolmanteen vaiheeseen, eli valmistautumisen vaiheeseen. Itse verukkeen käyttäminen taas kuuluu uhrin kanssa luotavan suhteen luomisen vaiheeseen (Mouton ym., 2014). Verukkeen käyttö on jokaisessa manipulointia hyödyntävässä hyökkäyksessä käytössä. Käyttäjän manipulointia hyödyntävän hyökkäyksen yhtenä kulmakivenä on uskottava tarina, joka oikeuttaa kohteen mielessä hyökkääjän pyynnön.

## 3.2 Verkkourkinta

Verkkourkinta (engl. *phishing*) on juoni, joka on suunniteltu saavuttamaan arkaluonteista informaatiota aiotulta uhrilta. Näitä keinoja voivat olla yhteydenotot sähköpostin, verkkosivujen tai kirjeiden välityksellä, jotka vaikuttavat saapuvan vilpittömiltä yrityksiltä tai lähettäjiltä. Yhteydenotot voivat esimerkiksi määrätä uhria luovuttamaan informaatiota välttääkseen jonkin organisaation omistaman tilin sulkeutumisen. Vaihtoehtoisesti yhteydenotto voi pyytää organisaatiota tai vastaanottajaa olemaan osana kilpailua tai lahjoitusta.

Tyypillinen verkkourkinnan juoni on sähköposti, joka vaikuttaa päällisin puolin tulevan joltakin viralliselta taholta, sekä sitä on kuvitettu kyseisen tahon aidoilla logoilla (Workman, 2008.) Viralliselta vaikuttavassa viestissä pyritään saamaan kohde luovuttamaan arkaluonteista tietoa, joko viestin sisältämän lomakkeen kautta, tai ohjaamalla linkin kautta lukija viralliselta vaikuttaviin, mutta vilpillisiin verkkosivuihin (Aslam, Wu & Zou, 2010). Arkaluontoista tietoa, kuten salasanoja ja luottokorttitietoja voidaan myöhemmin käyttää esimerkiksi sähköpostitilin sisään pääsyyn, tai verkkokauppaostosten tekoon uhrin tietämättä. Verkkourkinnan kaltainen hyökkäys suunnataan yleensä suurelle ihmismäärälle, sillä se on kohtalaisen helppo toteuttaa, jos hyökkääjällä on tiedossa suuri määrä sähköpostiosoitteita.

Organisaation tietoturvan uhkana voidaan laaja-alaisen verkkourkinnan lisäksi pitää kohdennettua verkkourkintaa (engl. *spear phishing*). Kohdennettu verkkourkinta on saman metodologian omaava sähköpostiviesti, mutta on suunnattu vain tiettyä henkilöä kohtaan. Kohdennetun verkkourkinnan vaarallisuutta korostaa se, että se on suunnattu vain tietylle henkilölle, ja viesti on muodostettu mukailemaan uhrin mielenkiinnon kohteita, tai muita henkilökohtaisia asioita. Taitava hyökkääjä voi onnistua luomaan viestistä mielenkiintoisen ja uskottavan kohteensa taustatietoja selvittämällä. Kohteena voi olla kuka tahansa henkilö organisaation toimistotyöntekijästä toimitusjohtajaan (Stembert, Padmos, Bargh, Choenni & Jansen, 2015.)

## 3.3 Pharming-huijaus

Pharming-huijaus (engl. *pharming*) on prosessi, jossa hyökkääjä saa kohteensa ohjattua tekaistuun verkkosivustoon, joka saattaa näyttää ulkoasultaan identtiseltä kuin mitä kohteen oli tarkoitus selata. Prosessi suoritetaan käyttäjän tiedostamatta tilannetta esimerkiksi, internetin tietoliikenne heikkouksia hyväksikäyttäen (Aslam ym., 2010). Hyökkäyksen kohde johdatellaan sivustoon linkin kautta, joka on sijoitettu kohdennetun verkkourkinnan uhrille lähetetyn sähköpostin sisälle. Pharming-huijaus voi siten toimia kohdennetun verkkourkinnan ohella osana kokonaisvaltaisempaa käyttäjän manipulointihyökkäystä. Pharming-huijauksen päämääränä on saada käyttäjä syöttämään arkaluontoista tietoa sivustoon, joka tallentaa syötetyn tiedon sivuston tietokantaan myöhempää vilpillistä käyttöä varten (Mathew, Hajj & Ruqeishi, 2010.) Onnistuneen huijauksen tuloksena saatu arkaluonteinen tieto voi olla hyökkäyksen lopullinen tavoite, tai vain alustavaa tiedonkeruuta esim. identiteettivarkauden valmistelua varten. Organisaation tietoturva on siten uhattuna, jos huijauksella saatu tieto on salaista, tai sisältää käyttäjän kirjautumistunnuksia.

Aslam ym. (2010) esittivät tutkimuksessaan ehdotuksen pharming-huijauksen estämiseksi. Heidän ratkaisunsa oli verkkoselaimeen asennettava ja itsenäisestikin toimiva sovellus, joka varmentaa serverin IP-osoitteen. Aslamin ym. (2010) mukaan heidän sovelluksensa toimi myös palvelunestohyökkäystä vastaan.

## 3.4 Paperinkeräysastian tutkiminen

Paperinkeräysastian tutkiminen (engl. *dumpster diving*) liittyy hyökkääjän informaation keruuseen organisaatiosta, sekä osaltaan organisaation paperijätteiden hallinnan piittaamattomuuteen. Paperinkeräysastian tutkiminen on toimintaa, jossa hyökkääjä käy organisaation rakennuksen paperijätesäiliöitä läpi löytääkseen fyysisten jätteiden seasta dokumentteja tai muita asioita, jotka voivat paljastaa arkaluonteista tietoa (Beckers, Krautsevich & Yautsiukhin, 2015).

Jätteiden seasta hyökkääjä voi onnistua poimimaan organisaatiokartoituksia, henkilöstön kalentereita, yrityksen toimintatapoja, tulostettuja sähköposteja, hylättyjä ulkoisia muistilaitteita, puhelulistoja tai muuta yrityksen dataa, joista hyökkääjä voi koota informaatiota organisaation verkkoon sisäänpääsyyn (VanStean, 2004). Paperijätteitä tutkimalla hyökkääjä voi löytää myös henkilökohtaista informaatiota, kuten yksityisiä osoitteita henkilöille suunnatuissa kirjeissä (Mouton ym, 2014). Hyökkääjän kerätessä alustavaa informaatiota kohteena olevasta organisaatiosta paperinkeräysastian tutkiminen on verkosta kerättävän materiaalin ohella hyökkääjälle tehokas ei-tekninen keino oppia organisaatiosta.

## 3.5 Käyttäjän manipuloinnin työkalut

Käyttäjän manipuloinnin hyökkäyksessä tärkeänä elementtinä toimivat hyökkääjän käytettävissä olevat työkalut, jotka voivat varioida hyökkääjän käyttämästä vaatetuksesta (Fujikawa & Nishigaki, 2011) yksinkertaiseen haittaohjelmaan USB-muistitikussa. Vaatteet jonkin organisaation yhteistyökumppanin logolla varustettuna edistävät uskottavuutta ja luottamusta hyökkääjän pyrkiessä fyysisesti organisaation toimitiloihin. Esimerkiksi, jos organisaatio käyttää ulkoista IT-tukipalvelua, hyökkääjä voi tekeytyä IT-tukihenkilön rooliin teettämällä vaatetuksen itselleen IT-tukipalvelua tuottavan yrityksen logolla. IT-tukihenkilöksi pukeutuneena hyökkääjä voi pyytää henkilöstöltä pääsyä serverihuoneeseen.

Hyökkääjän käyttämä viralliselta vaikuttava ulkoasu on kuitenkin vain yksi keinoista jolla voi onnistua organisaation henkilöstön manipuloinnissa. Käyttäjän manipulointiin tähtäävän hyökkäyksen avuksi on myös teknisiä työkaluja. Shah ja Mehtre (2013) esittivät tutkimuksessaan taulukon, joka esitti kaksi ilmaista ja avoimella lähdekoodilla tuotettua käyttäjän manipuloinnin läpäisytestaukseen käytettävää työkalua. Heidän esittämät työkalut olivat verkosta kerättävän datan visualisointiin tarkoitettu Maltego, sekä hyökkäyksen simulointiin tarkoitettu Social Engineering Toolkit (SET). Näitä työkaluja käytetään analysoimaan hyökkääjän vaikeustasoa saada (tai louhia) luottamuksellista tietoa ollessaan vuorovaikutuksessa kohde-organisaation

henkilöstön kanssa, tai tarkkailemalla heidän kommunikointia (Shah & Mehtre, 2013). Vastaavanlaisia ohjelmistoja on useampia, mutta tutkielman pituuden rajaamiseksi tässä tutkielmassa käsitellään lyhyesti vain informaation keruuta varten suunniteltu Maltego, sekä hyökkäyksen avustamista varten suunniteltu SET.

### 3.5.1 Informaation keruu Maltego:lla

Kattavan tiedonkeruun, sekä kerätyn tiedon avulla hyökkäykseen valmistautuminen ovat hyökkääjän keinoja, joilla käyttäjän manipuloinnin onnistumisen todennäköisyys kasvaa. Informaation lähteenä voi toimia kohteena olevan organisaation verkkosivut, fyysinen tarkkailu tai puhelimen välityksellä suoritetut johdattelevat kysymykset. Verkon kautta suoritettavaan informaation keruuseen on ohjelmistoyritys Paterva luonut graafisen käyttöliittymän omaavan ohjelmistotyökalun nimeltään Maltego.

Maltego antaa graafisen kuvauksen ihmisten, ryhmien, verkkosivujen ja yritysten välisistä yhteyksistä, sekä esittää jopa luottamuksellisia yhteyksiä (Shah & Mehtre, 2013). Maltego sisältää ominaisuuksia tiedonlouhintaan, linkkien analysointiin, sekä tiedon visualisointiin. Se antaa käyttäjälleen mahdollisuuden poimia suuren määrän tietoa eri lähteistä ja analysoida sitä ymmärtääkseen kytkökset ja suhteet informaatiossa. Tutkimuksessaan ohjelmistoa käytti tiedon keruun avustuksena myös hyväksi Kwok, Lai ja Yeung (2009).

### 3.5.2 Hyökkäyksen simulointi SET:illä

Tiedonkeruun lisäksi hyökkääjä saattaa käyttää teknisiä työvälineitä hyökkäyksessään, kuten haittaohjelmia. Social Engineering Toolkit (SET) on ilmainen verkosta ladattava avoimen lähdekoodin ohjelmistopaketti, joka sisältää toimintoja, joilla voidaan tuottaa yleisimmät haittaohjelmat, tai haittaohjelmia sisältävät tiedostot. Se toimii yksinkertaisen komentorivikäyttöliittymän avulla. SET on kehittynein ja ehkä ainoa avoimen lähdekoodin työkalusarja, joka on suunnattu käyttäjän manipulointia hyödyntävän hyökkäysten tueksi (Pavkovic & Perkov, 2011).

Tätä tutkielmaa kirjoittaessa SET on valmiiksi asennettuna Kali Linux-käyttöjärjestelmässä (Patel, 2013). Kali Linux on ilmainen Linux-pohjainen tietokoneen käyttöjärjestelmä, jonka voi ladata verkosta ja asentaa tietokoneelle. SET on luotu työkaluksi yritysten tietoturvaa auditoiville konsulteille helpottaakseen heitä luomaan haittaohjelmia työnsä tueksi, jotta he voisivat haittaohjelmien valmistamisen sijaan keskittyä hyökkäyksen sosiaaliseen puoleen ja suunnitteluun (Hadnagy, 2010.) Tässä tutkielmassa Kali Linux (ja siten SET) esitellään esimerkkinä työkalusta, jota käyttäjän manipulaatiota hyödyntävä hyökkääjä voisi mahdollisesti käyttää.

# 4 EHKÄISYKEINOT

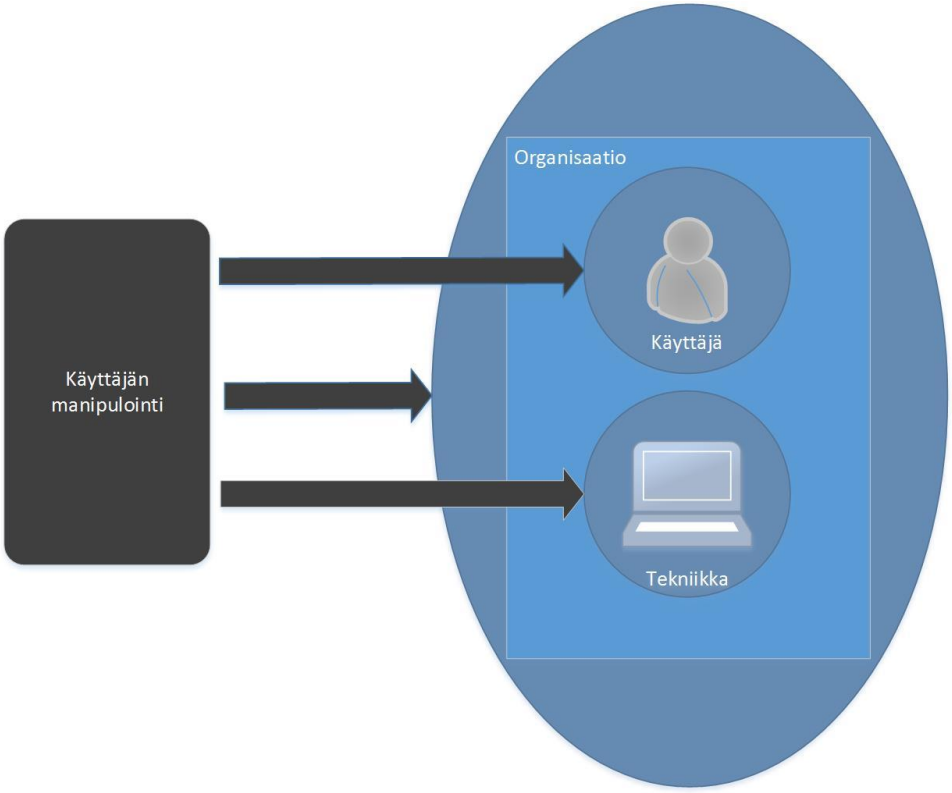
Vaikka kirjallisuutta ja menetelmiä informaation turvallisuuteen on riittoisa määrä, ihmiset usein epäonnistuvat seuraamaan edes olennaisimmat varotoimenpiteet, josta voi seurata henkilötason tai organisaation varallisuuden menetyksiä. Tässä tapauksessa ”tietäen paremmasta, mutta ei tehden paremmin” on keskeinen kohta, jota tulisi käsitellä (Workman, 2008.) Tässä luvussa esitellään varotoimenpiteitä, jotka toimivat hyökkäysten ehkäisykeinoina organisaation tasolla, henkilötasolla ja myös teknisellä tasolla, jos ihmiset onnistuvat niitä seuraamaan.

Luvuissa 1, 2 ja 3 esiteltyihin tietoihin perustuen ehdotetaan kolmen lähestymistavan periaatetta käyttäjän manipuloinnin uhkaa vastaan (Kuvio 1). Lähestymistavat ovat organisaationlaajuinen lähestymistapa, käyttäjäkohtainen lähestymistapa, sekä tekninen lähestymistapa. Lähestymistavat ovat jaoteltu näihin kohtiin, koska kirjallisuuteen perustuen voidaan väittää seuraavasti:

- hyökkäys kohdistuu organisaatioon
- hyökkäyksen väylänä toimii tietojärjestelmän käyttäjä
- hyökkäyksen päämääränä on tietojärjestelmään pääsy.

Organisaationlaajuisessa lähestymistavassa tulee selvittää, kuinka organisaation tulee toimia käyttäjän manipuloinnin uhan minimoimiseksi. Käyttäjäkohtaisessa lähestymistavassa manipuloinnin uhkaa torjutaan tietojärjestelmän käyttäjän tasolla. Lopuksi, teknisessä lähestymistavassa pyritään minimoida käyttäjän manipuloinnin mahdollisuus teknisin keinoin.

Seuraavissa alaluvuissa käsitellään näitä kolmea lähestymistapaa, sekä annetaan jokaisen lähestymistavan ongelman ratkaisusta esimerkki. Ratkaisut ovat yksinkertaisia toimintamalleja ja keinoja, joita soveltamalla, sekä organisaatio, että organisaatiossa työskentelevä yksilö voivat toimia käyttäjän manipuloinnin estämiseksi.




Kuvio 1 Kolme lähestymistapaa käyttäjän manipulointiin

## 4.1 Organisaationlaajuinen lähestymistapa

Organisaationlaajuisen lähestymistavan ratkaisuna voidaan pitää Hadnagyn (2010) kuusi askelta, jotka ovat luotu organisaatiolle toteutettavaksi käyttäjän manipuloinnin estämiseksi. Listaa on havainnollistettu kuvassa 2. Ensimmäisenä askeleena toimii organisaation kouluttaminen tunnistamaan käyttäjän manipulointia käytännössä. Hadnagyn mukaan on tärkeätä, että henkilöstö kykenee tunnistamaan organisaatioon kohdistuvan manipulointihyökkäyksen viimeistään siinä tilanteessa, kun esimerkiksi henkilö avaa tietokoneellaan tiedoston, joka herättää epäilyksiä. Jotta hyökkäyksen seuraukset voidaan minimoida, tulee mahdollisen manipulointihyökkäyksen tunnistamisen jälkeen ottaa yhteyttä esimieheen tai organisaation tietoturvallisuudesta vastaavaan henkilöön.

Seuraava askel on luoda henkilökohtaista tietoturvaa tiedostava kulttuuri organisaatiossa. Organisaation data tulee ymmärtää organisaatiossa työskentelevien henkilöiden yhteisenä datana. Jokaisen organisaatiossa toimivan henkilön tulee kuulua siten organisaatiokulttuuriin, joka panostaa sen tietoturvallisuuteen.

Kolmannessa askeleessa organisaation työntekijöiden tulee ymmärtää hyökkääjän havitteleman informaation arvo. Jos informaation ei käsitetä omaavan lainkaan, tai vain vähän arvoa, sen suojelemiseksi nähdään vähän vaivaa.

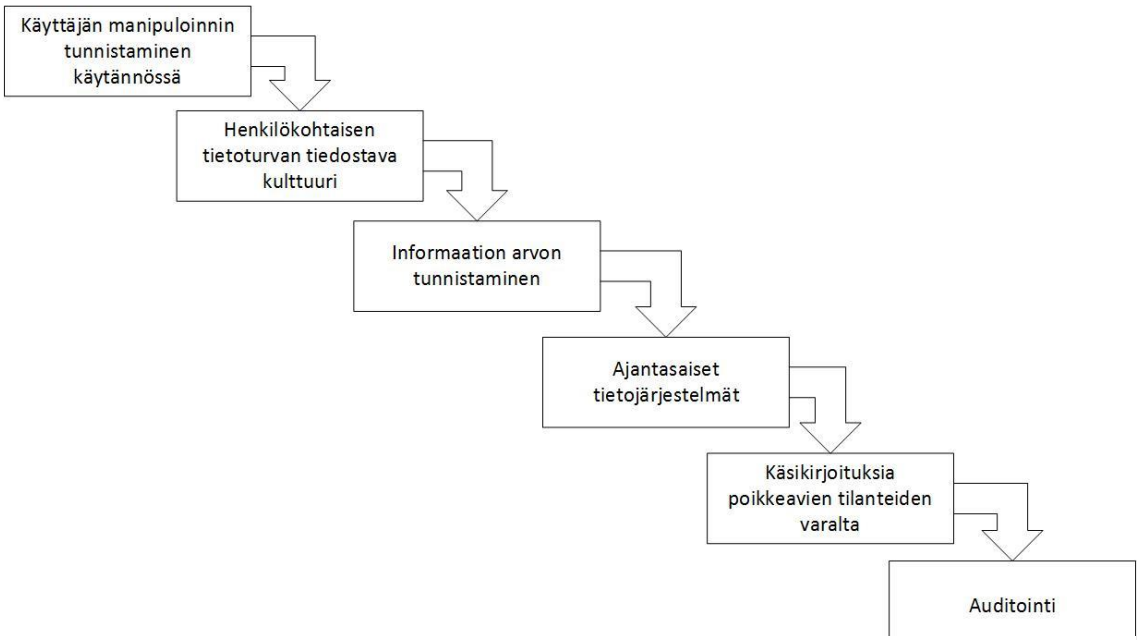
Neljäntenä organisaation tulee pitää käyttämänsä ohjelmistot päivitettynä. Askel voi toimia myös siirtymäkohtana tekniseen lähestymistapaan. Varoittavana esimerkkinä Defcon-messuilla Yhdysvalloissa järjestetyssä käyttäjän manipulointia käsittelevässä kisassa selvisi, että 60 % kohteena toimivista organisaatioista käytti ohjelmistosovelluksia, joissa oli kymmeniä julkisessa tiedossa olevia haavoittuvuuksia (Hadnagy ym., 2010). Kisan aikana organisaatioista urkittiin informaatiota puhelimitse.

Viides askel suosittelee ennalta luomaan käsikirjoituksia tilanteisiin, jotka poikkeavat normaalista käytännöstä. Normaalista poikkeava tilanne saattaa olla hyökkääjän kehittämä verukkeellinen tarina. Hadnagy (2010) ehdottaa, että käsikirjoitus voi olla seuraavanlainen:

1. Kysy henkilön työtunnusnumero sekä nimi. Älä vastaa muihin kysymyksiin, kunnes saat nämä tiedot.
2. Tunnistus informaation saamisen jälkeen kysy projektin tunnusnumeroa, joka liittyy informaatiota vaativaan projektiin.
3. Jos saat onnistuneesti kohdan 1 ja 2 informaation, ryhdy yhteistyöhön. Jos et saa informaatiota henkilöltä, vaadi henkilöä pyytämään esimiestään lähettämään sähköpostilla lupakysely sinun esimiehellesi pyytäen lupaa informaation jakamiseen.

Viides askel on myös oiva siirtymäkohta käyttäjäkohtaiseen lähestymistapaan.

Viimeisenä askeleena Hadnagy:n (2010) ehdotuksen mukaan on käyttäjän manipulointiauditointien pitäminen, sekä niistä oppiminen. Ennen käyttäjän manipulointiauditoinnin aloittamista tulee asettaa tavoitteet auditoinnille, sekä määrittää mikä kuuluu auditointiin ja mikä ei.




Kuvio 2 Organisaationlaajuinen toimintamalli (Hadnagy, 2010)

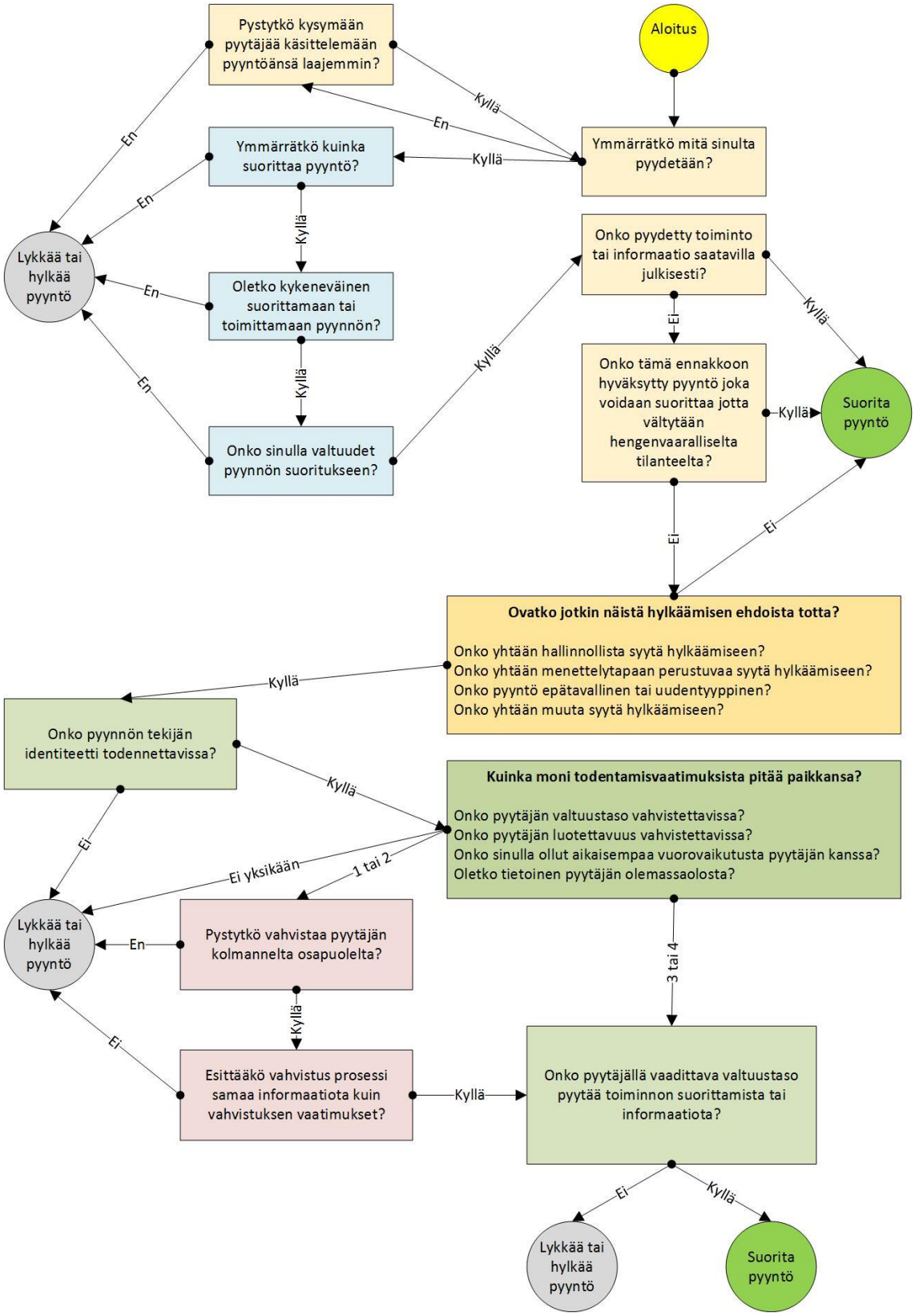
## 4.2 Käyttäjäkohtainen lähestymistapa

Kuten organisaationlaajuisen toimintamallin viidennessä askeleessa mainittiin, yksittäisille käyttäjille tulee luoda ennalta laadittuja käsikirjoituksia poikkeavien tilanteiden varalta. Ratkaisuna käyttäjäkohtaiseen lähestymistapaan esitetään Bezuidenhoutin, Moutonin, sekä Venterin (2010) tutkimuksessa ehdottama kattava manipulointihyökkäyksen tunnistamismalli (engl. *Social Engineering Attack Detection Model: SEADM*). Malli on luotu toimintamalliksi yksittäisille järjestelmien käyttäjille kohdatessaan normaalista poikkeavia tilanteita. Viisi vuotta myöhemmin Mouton, Leenen ja Venter (2015) kehittivät tunnistamismallia vielä kattavammaksi (SEADMv2). Kuvio 2 esittää suomennettua Moutonin ym. (2015) ehdottamaa käyttäjän manipulointia hyödyntävän hyökkäyksen tunnistamismallia.

Malli sisältää neljä tekijää, jotka ovat pyyntö, pyynnön tekijä, vastaanottaja (järjestelmän käyttäjä), sekä kolmas osapuoli. Keltaisella pohjalla kuvatut kohdat käsittelevät suoraan pyynnön informaatiota. Sinisellä pohjalla esitetyt kohdat käsittelevät suoraan pyynnön vastaanottavaa henkilöä riippumatta siitä ymmärtääkö vastaanottaja pyyntöä, tai onko hänellä valtuudet suorittaa pyyntö. Vihreät kohdat käsittelevät pyynnön tekijää sekä sitä, että voiko informaatiota pyynnön tekijästä vahvistaa. Kohdat, jotka ovat esitetty punaisella pohjalla, kuvaavat kolmannen osapuolen suhdetta tunnistamismalliin ja sitä, että voiko pyynnön tekijän informaatiota ulkoisesti vahvistaa (Mouton ym., 2015.)

Kuvion 2 malli antaa selkeät ohjeet toimimiseen käyttäjän vastaanottaessa normaalista poikkeavan pyynnön. Pyynnön vastaanottaja selviää tilanteesta vastaamalla mallin esittämiin kysymyksiin ja toimimalla ohjeistuksen mukaan. Mallin mukaan käyttäjä vastaa pyyntöön esittämällä pyytäjältä lisäkysymyksiä, lykkäämällä tai hylkäämällä pyyntö, tai suorittamalla esitetty pyyntö.

Jos tunnistusmalli olisi ollut käytössä johdannossa esitellyn IRS:n tapauksessa, olisi käyttäjätunnusten vuotamiselta voitu osin välttyä. IRS:n tapauksessa käyttäjää pyydettiin puhelinsoiton välityksellä kertomaan käyttäjänimensä ja vaihtamaan salasana soittajan ehdottamaan salasanaan. Näin soittaja sai käyttäjältä toimivan käyttäjänimen sekä salasanan. Tunnistusmallia seurattaessa soittajan pyyntö olisi kyseenalaistettu identiteettiänsä todennettaessa.




Kuvio 3 Käyttäjän manipulointia hyödyntävän hyökkäyksen tunnistusmalli (Mouton ym., 2015, 217)

## 4.3 Tekninen lähestymistapa

Teknisessä lähestymistavassa pyritään ratkoa ongelma; kuinka hyökkääjältä voidaan evätä pääsy järjestelmään? Yleisesti käytössä on kolme erilaista turvatoimea henkilöiden tunnistamiseen tai todentamiseen tietojärjestelmään sisäänpääsyyn. Turvatoimet perustuvat ihmisen muistiin, ihmisen mukana kannettavaan esineeseen, tai ihmisen omaan biologiaan. Ensimmäisenä ovat ihmisen muistamat salasanat, tunnusnumerot, tai avainsanat. Nämä ovat käyttäjää manipuloivalle hyökkääjälle mahdollista saada manipuloimalla kohdettaan esim. verukkeen keinoin. Seuraavana ovat tunnistamiseen tarkoitetut kannettavat laitteet kuten älykortit, korttiavaimet ja kulkukortit. Kolmantena henkilön tunnistamiseen voi käyttää biometriikkaa, eli henkilöä itseään (Mathew ym., 2010.)

Mathew ym. (2010) toteavat tutkimuksessaan, että biometrinen tunnistaminen toimii vaihtoehtona muihin tunnistuskeinoihin, sillä sitä hyökkääjän on vaikeampi kopioida tai huijata. Biometriseen tunnistamiseen käytetään ihmisen biologisia osia kuten sormenjälkiä, kasvoja, silmän iiristä tai puheääntä. Esimerkiksi silmän iiris voidaan nykyteknologialla skannata yksinkertaisella kameralla, jonka ei tarvitse olla aivan silmän läheisyydessä, vaan skannattava henkilö voi seistä kameran edessä ilman nojautumista kameraan. Iiriksen skannauksen luotettavuutta lisää se, että iiris ei muutu ihmisen vanhetessa, toisin kuten esimerkiksi silmän verkkokalvo. Biometriikkaan perustuvia tunnistimia on käytössä muutamilla lentokentillä maailmalla (Mathew ym., 2010.)

Biometriikan käytössä on tunnistettavissa vahvuuksia, joita ihmisten muistiin perustuvilla tunnisteilla, sekä mukana kannettavilla esineillä on vaikea saavuttaa. Biometrisen tunnistamisen vahvuus on esimerkiksi se, että biometriikkaa on haasteellisempaa kopioida, kuin digitaalista tietoa. Myös käyttäjän manipuloinnin yritykset ovat voimattomampia biometrisiä turvatoimia vastaan, kuin esimerkiksi muistettavia salasanoja kohtaan.

Biometriikkaan perustuvalla tunnistamisella on myös haasteensa, sillä vanheneminen ja sairaudet voivat vaikuttaa tunnistamisen toimivuuteen. Kowtkon (2014) mukaan sairaudet, jotka vaikuttavat sydämeen, keuhkoihin, sekä verenkiertoon, voivat vaarantaa helppopääsyisyyttä ja käytettävyyttä biometrisissa tunnistusjärjestelmissä. Muutokset ihmisen kehossa iän tai sairauden takia voi vaikeuttaa tunnistamista. Esimerkiksi Mathewn ym. (2010) mainitsema silmän iirikseen perustuva tunnistaminen voi kokea ongelmia tunnistaa henkilö uudestaan kaihileikkauksen jälkeen. Biometristen tunnistamislaitteiden korkea hinta on myös yleisemmän käyttöönoton kohtaama haaste (Kowtko, 2014.)

Biometriikkaan perustuva tunnistaminen on ongelmistaan huolimatta kelvollinen keino evätä hyökkääjältä pääsy tietojärjestelmään. Ihmisen biometrisia ominaisuuksia on mahdotonta manipuloiden urkkia esim. puhelimen tai verkkourkinnan välityksellä. Mutta kuten salasanoja tulee vaihtaa väliajoin, tulee biometristen ominaisuuksien rekisteriä mahdollisesti päivittää käyttäjän ikääntyessä.

# 5 YHTEENVETO JA POHDINTA

Käyttäjän manipulointi on tietoturvallisuuden näkökulma, jossa hyökkääjän menetelmänä on saada haluamansa tieto itse tietojärjestelmän käyttäjältä. Menetelmä ei sulje pois hyökkäyksen tietoteknistä puolta, vaan tukee sitä ja tekee siitä jopa vaarallisemman. Käyttäjän manipuloinnin mahdollisuuden tiedostaminen ei tulisi kuitenkaan rajata organisaation toimivuutta, vaan sen tulisi kannustaa tietoturvallisten käytänteiden harjoittamista organisaatiossa. Organisaation henkilöstön tulee kyetä tunnistamaan organisaation arkaluonteista informaatiota ja huolehtia sen suojelemisesta.

Tutkielmassa tutkittiin käyttäjän manipulointia organisaation tietoturvallisuuden näkökulmasta. Tutkimusmenetelmänä tutkimuksessa käytettiin kirjallisuuskatsausta. Tutkielman tavoitteena oli tunnistaa tekijät, jotka mahdollistavat käyttäjään kohdistuvan manipuloinnin, sekä keinot, joilla organisaatio voi varautua käyttäjän manipuloinnin varalta. Tutkimuskysymyksenä oli *miten organisaatio voi puolustautua käyttäjän manipulointia hyödyntävän hyökkäyksen varalta?* Tutkielman tuloksena oli katsaus käyttäjän manipuloinnista, sekä kirjallisuudessa havaituista ohjeista ja neuvoista hyökkäysten ennaltaehkäisyyn ja torjuntaan.

Ensimmäisessä ja toisessa luvussa kuvailtiin, kuinka käyttäjän manipulointi on toimiva hyökkäyskeino organisaation tietopääomaa kohtaan johtuen pääasiallisesti järjestelmän käyttäjän inhimillisistä piirteistä. Kirjallisuudessa kuvailtiin tilanteita, jossa hyökkääjä luo tilanteen johon käyttäjä reagoi avuliaasti. Inhimilliset piirteet, jotka edesauttavat käyttäjän manipuloijaa kohteensa manipuloinnissa olivat välinpitämättömyys, myönnytys ja vastavuoroisuus, johdonmukaisuus ja sitoutuminen, sosiaalinen osoitus, miellyttävyys ja luottamus, auktoriteetti ja pelko, sekä käyttäytyminen niukkuuden vallitessa. Inhimilliset piirteet, sekä tilanteiden mukaiset käyttäytymistavat, ovat asioita, joita käyttäjän manipulointia hyödyntävät hyökkääjät käyttävät saadakseen kohteensa luottamuksen ja myönnytyksen, sekä siten haluamansa informaation.

Tutkielman kolmannessa luvussa tutustuttiin yleisimpiin metodeihin, joita käyttäjän manipulointia hyödyntävä hyökkääjä voi käyttää pyrkiessään saamaan organisaation arkaluonteista informaatiota. Metodeja olivat verukkeen

luominen, verkkourkinta, pharming-huijaus, paperinkeräysastian tutkiminen, sekä tietotekniset työkalut. Käyttäjän manipulointia koskevassa kirjallisuudessa lisäksi kuvailtiin hyökkääjän informaatiokeruun tärkeyttä hyökkäyksen onnistumisen mahdollistamiseksi. Oheiset metodit ovat sitä vaarallisempia, mitä enemmän informaatiota hyökkääjä onnistuu saamaan organisaatiosta tai henkilökohteista. Tiedonkeruun työkaluna tutkielmassa esiteltiin informaatiokeruuta varten suunniteltu Maltego-ohjelmisto. Esimerkkinä haittaohjelmien luomiseen kehitetyistä ohjelmistoista tutkielmassa esiteltiin Social Engineering Toolkit. SET on luotu organisaatioiden auditoinnin tarpeita varten, mutta toimii myös esimerkkinä ohjelmistosta, jota käyttäjän manipulointia hyödyntävä hyökkääjä voi käyttää.

Neljännessä luvussa käyttäjän manipuloinnin uhkaa ehdotettiin ratkaistavaksi kolmen lähestymistavan kautta. Lähestymistavat olivat organisaationlaajuinen lähestymistapa, käyttäjäkohtainen lähestymistapa, sekä tekninen lähestymistapa. Käyttäjän manipulointia hyödyntävän hyökkäyksen torjuntaan ehdotettiin kuuden askeleen toimintamallia, jossa askeleina on hyökkäyksen tunnistamisen kyvyn luominen, henkilökohtaisen tietoturvallisuuden kulttuurin luominen, informaation arvon tunnistaminen läpi organisaation, ohjelmistojen päivittäminen, käsikirjoitusten käyttö, sekä käyttäjien manipuloinnin auditointien pitäminen organisaatiossa. Käyttäjäkohtaisen lähestymistavan ratkaisuksi ehdotettiin käyttäjän manipulointia hyödyntävän hyökkäyksen tunnistamismalli, joka sopii yksittäisen tietojärjestelmän käyttäjän toimintamalliksi kohdatessaan normaalista poikkeavia tilanteita. Lopuksi suositeltiin biometriikkaan perustuvaa tunnistusteknologian käyttöä tekniseksi ratkaisuksi. Biometrinen tunnistaminen ehdotettiin, koska siinä käytetään ihmistä itseään tunnistamisen keinona käyttäjätunnuksen ja salasanan sijaan.

Käyttäjän manipulointia koskevassa kirjallisuudesta voidaan havaita, että käyttäjän manipulointia hyödyntävät hyökkäykset toimivat todennäköisimmin suurissa organisaatioissa, joissa on henkilökunnalle normaalista poikkeamatonta saada yhteydenottoja ihmisiltä, jotka ovat heille entuudestaan tuntemattomia. Lisäksi on pääteltävää, että hyökkäykset voivat toimia organisaatioissa, joissa henkilökunta on kokoluokaltaan niin suuri, että he eivät kaikki tunne toisiaan. Tulevaisuuden tutkimuksen kohteena tulisi olla käyttäjän manipulointia hyödyntävien hyökkäysten toimivuus pieni- ja keskikokoisissa organisaatioissa. Lisäksi lisätutkimusta tulisi suorittaa käyttäjän manipuloinnin uhan tiedostamisesta suurissa organisaatioissa. Aiheen tutkimista saattaa vaikeuttaa isojen organisaatioiden halu pitää turvallisuuskäytäntöjään ja auditointituloksiaan salassa julkisuudelta oman julkisen käsityksen ylläpitämiseksi.

# LÄHTEET


Acquisti, A. & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *2nd Annual Workshop on Economics and Information Security-WEIS,* (1-27). Citeseer.

Aslam, B., Wu, L. & Zou, C. C. (2010). PwdIP-hash: A lightweight solution to phishing and pharming attacks. *Network Computing and Applications (NCA), 2010 9th IEEE International Symposium on,* (198-203). IEEE.

Beckers, K., Krautsevich, L., & Yautsiukhin, A. (2015). Analysis of social engineering threats with attack graphs. In Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance (pp. 216-232). Springer International Publishing.

Bezuidenhout, M., Mouton, F. & Venter, H. S. (2010). Social engineering attack detection model: SEADM. *Information Security for South Africa (ISSA), 2010,* (1-8). IEEE.

Charbaji, A. & Jannoun, S. E. (2005). Individuality, willingness to take risk, and use of a personal e-card: A lebanese study. *Journal of Managerial Psychology, 20*(1), 51-58.

Cialdini, R. B. (2009). *Influence: Science and practice* Pearson Education Boston.

Cialdini, R. B. & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu.Rev.Psychol., 55*, 591-621.

FBI National Press Office. (2010, 13.1.2010). Haitian earthquake relief fraud alert. Haettu 2/1010.2.2016 osoitteesta https://www.fbi.gov/news/pressrel/press-releases/haitian-earthquake-relief-fraud-alert

Festinger, L., & Carlsmith, J. M. (1959). Cognitive consequences of forced compliance. *The Journal of Abnormal and Social Psychology*, *58*(2), 203.

Fujikawa, M. & Nishigaki, M. (2011). A study of prevention for social engineering attacks using Real/Fake organization's uniforms: Application of radio and intra-body communication technologies. *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on,* (597-602). IEEE.

Hadnagy, C. (2010). Social engineering: The art of human hacking John Wiley & Sons.

Hadnagy, C. J., Aharoni, M. & O'Gorman, J. (2010). Social engineering capture the flag results defcon 18. *Retrieved October, 30*, 2010.

Hsu, M. & Kuo, F. (2003). The effect of organization-based self-esteem and deindividuation in protecting personal information privacy. *Journal of Business Ethics, 42*(4), 305-320.

Kotenko, I., Stepashkin, M., & Doynikova, E. (2011, February). Security analysis of information systems taking into account social engineering attacks. In *Parallel, Distributed and Network-Based Processing (PDP), 2011 19th Euromicro International Conference on* (pp. 611-618). IEEE.

Kowtko, M. A. (2014). Biometric authentication for older adults. Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, (1-6). IEEE.

Kwok, S., Lai, A. C. & Yeung, J. C. (2009). A study of online service and information exposure of public companies. *Proceedings of the ACM SIGKDD Workshop on CyberSecurity and Intelligence Informatics,* (85-90). ACM.

MacCrimmon, K. R. & Wehrung, D. A. (1986). Assessing risk propensity. *Recent developments in the foundations of utility and risk theory* (s. 291-309) Springer.

Mathew, A. R., Hajj, A. A. & Ruqeishi, K. A. (2010). Cyber crimes: Threats and protection. *Networking and Information Technology (ICNIT), 2010 International Conference on,* (16-18). IEEE.

Mitnick, K. D. & Simon, W. L. (2011). The art of deception: Controlling the human element of security John Wiley & Sons.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, August). Social engineering attack framework. In Information Security for South Africa (ISSA), 2014 (pp. 1-9). IEEE.

Mouton, F., Leenen, L., & Venter, H. S. (2015). Social engineering attack detection model: SEADMv2. 2015 International Conference on Cyberworlds (CW), , 216-223.

Patel, R. S. (2013). Kali Linux Social Engineering. Packt Publishing Ltd.

Pavković, N. & Perkov, L. (2011). Social engineering Toolkit—A systematic approach to social engineering. *MIPRO, 2011 Proceedings of the 34th International Convention,*(1485-1489). IEEE.

Phillips, M. R. (2007). *Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers*. Tech. Rep. 2007-20-107, US Treasury Inspector General for Tax Administration, Washington, DC 20220.

Shah, S., & Mehtre, B. M. (2013, December). A reliable strategy for proactive self-defence in cyber space using VAPT tools and techniques. In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on (pp. 1-6). IEEE.

Siponen, M., Pahnila, S. & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Staw, B. M., & Fox, F. V. (1977). Escalation: The determinants of commitment to a chosen course of action. Human Relations, 30(5), 431-450.

Stembert, N., Padmos, A., Bargh, M. S., Choenni, S., & Jansen, F. (2015, September). A Study of Preventing Email (Spear) Phishing by Enabling Human Intelligence. In Intelligence and Security Informatics Conference (EISIC), 2015 European (pp. 113-120). IEEE.

Sun, S., Yan, C., & Feng, J. (2012, March). Analysis of influence for social engineering in information security grade test. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 2, pp. 282-284). IEEE.

Uebelacker, S. (2014). The social engineering personality framework. *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on,* , 24-30.

VanStean, J. (2004). Dumpster diving. *Inside NetWare, 13*(9), 12.

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security, 16*(5), 463-483.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security, 16*(6), 315-331.