Käyttäjän manipulointi tietoturvauhkana

Oulun yliopisto
Tieto- ja sähkötekniikan tiedekunta
Tietojenkäsittelytiede
LuK-tutkielma
Jasu Liedes
30.4.2019

Sisällys

Tiivistelmä

Tämän kirjallisuuskatsauksen aiheena on käyttäjän manipulointi tietoturvauhkana. Käyttäjän manipuloinnilla tarkoitetaan tekniikoita, joilla hyökkääjä pyrkii saamaan uhrin paljastamaan arkaluontoista tietoa tai toimimaan muulla hyökkääjän haluamalla tavalla. Tavoitteen saavuttamiseksi hyökkääjä ei käytä pelkästään teknisiä keinoja, vaan käyttää hyväksi uhrin psykologisia ominaisuuksia kuten tunteita. Teknisten puolustusmekanismien kehittyessä hyökkääjät ovat siirtyneet yhä enemmän käyttämään hyökkäyksissä käyttäjän manipuloinnin keinoja.

Tämän tutkielman tarkoituksena on tutkia käyttäjän manipulointia tietoturvariskinä ja löytää keinoja, joilla organisaatiot pystyisivät ehkäisemään siihen kohdistuvaa käyttäjän manipulointia. Tutkielma on kirjallisuuskatsaus aikaisempaan aiheeseen liittyvään tutkimukseen.

Avainsanat

Käyttäjän manipulointi, tietoturva

Ohjaaja

Tutkijatohtori, Mari Karjalainen

1. Johdanto

Jokaisella organisaatiolla on arkaluonteista tietoa, jota halutaan suojella. Näitä tietoja halutaan suojella, jotta niiden luottamuksellisuus (engl. *confidentiality*), eheys (engl. *integrity*) ja saatavuus (engl. *availability*) pystyttäisiin takaamaan. Edellä mainittujen ominaisuuksien prioriteetit vaihtelevat eri tietojen välillä, mutta kaikki tieto vaatii jonkinlaista suojausta. Muutoin kuka tahansa pystyisi lukemaan ja muokkaamaan tietoja tai estämään tietoja tarvitsevilta pääsyn niihin. (Schneier, 2011.)

Tietoturva on jatkuvaa kilpajuoksua hyökkääjän ja puolustajan välillä. Puolustaja haluaa suojella sille tärkeitä kohteita. Hyökkääjä pyrkii puolestaan pääsemään käsiksi niihin löytämällä suojaavista mekanismeista haavoittuvuuksia. Puolustajan työ on haastavaa, sillä sen on arvioitava kaikki tietoturvariskit. Hyökkääjälle puolestaan riittää, että se löytää ja läpäisee suojauksen heikoimmasta kohdasta.

Markkinoilla on tarjolla organisaatioille monia erilaisia ohjelmistoja ja laitteistoja, jotka mainostavat takaavansa tiedoille luottamuksellisuuden, eheyden tai saatavuuden. Tällaisia ovat esimerkiksi tietojärjestelmät ja protokollat, jotka vastaavat käyttäjän tunnistamisesta, käyttöoikeuksien hallinnasta tai tapahtumien kirjaamisesta lokeihin. Tällaiset ovatkin erittäin tärkeitä osia organisaatioiden tietoturvassa.

Kuitenkin, jotta tietojärjestelmä voisi olla hyödyllinen, on sen oltava vuorovaikutuksessa ihmisen kanssa (Peltier, 2006; Schneier, 2011). Tätä vuorovaikutusta kutsutaan ihmisen ja tietokoneen väliseksi vuorovaikutukseksi (engl. *human-computer interaction, HCI*). Schneierin (2011) mukaan tämä ihmisen ja tietokoneen välinen vuorovaikutus onkin tietojärjestelmien suurin tietoturvariksi. Teknisten suojausten parantuessa hyökkääjät ovatkin siirtyneet käyttämään yhä enemmän hyväksi ihmisen heikkouksia (Abraham & Chengalur-Smith, 2010).

Hyökkäystä, joka käyttää hyväksi ihmisen psykologisia ominaisuuksia, kuten auttamisen halua, kutsutaan käyttäjän manipuloinniksi (engl. *social engineering, SE*) (Happ, Melzer, & Steffgen, 2016; Peltier, 2006). Käyttäjän manipuloinnilla tarkoitetaan tekniikoita, joilla pyritään ohjaamaan ihmistä toimimaan halutulla tavalla tai paljastamaan luottamuksellista tietoa (Mann, 2008; Mitnick & Simon, 2011). Hyökkääjä pyrkii vetoamaan vahvasti uhrin tunteisiin. Siten häiritsemään hänen kykyään havainnoida tilannetta ja tehdä rationaalisia päätöksiä (Workman, 2008). Käyttäjän manipuloinnin hyökkäykset eivät vaadi juurikaan teknistä osaamista ja ovat halpoja toteuttaa. Onnistuessaan ne voivat ohittaa parhaimmatkin tekniset suojausmekanismit. Ihminen onkin usein syyllinen siihen, että hyökkääjä onnistuu läpäisemään järjestelmän tekniset puolustusmekanismit (Schneier, 2011).

Joulukuussa 2015 ukrainalainen voimalaitos joutui hyökkäyksen kohteeksi. Kohdistettu käyttäjän manipuloinnin hyökkäys oli osa tätä hyökkäystä, joka aiheutti sähkökatkoksia arvioiden mukaan noin 225 tuhannen ihmisen koteihin. Vaikka hyökkäys sisälsi myös hyvin paljon teknisiä osa-alueita, oli käyttäjän manipuloinnilla suuri merkitys sen onnistumisessa. Kyseisessä hyökkäyksessä osa voimalaitoksen työntekijöistä sai huijaussähköpostin, joka vaikutti tulleen luotettavalta taholta. Se sisälsi Word-dokumentin, joka avattaessa asensi haittaohjelman uhrin koneelle. Haittaohjelmalla kerätyt tiedot mahdollistivat varsinaisen hyökkäyksen onnistumisen. (Lee, Assante, & Conway, 2016.)

Käyttäjän manipuloinnilta puolustautumista ei voi lähestyä samalla tavalla kuin puolustautumista teknisempiä hyökkäyksiä vastaan. Schneierin (2011) mukaan ihmisen toiminnasta aiheutuvien riskien hallinta on huomattavasti hankalampaa kuin teknisten riskien. Monet haavoittuvuudet, joita tekniset hyökkäykset käyttävät hyväksi, voidaan paikata päivittämällä järjestelmä tai ottamalla uusi suojausmekanismi käyttöön. Suojausmekanismit toimivat käyttäjästä riippumatta. Käyttäjän manipuloinnin hyökkäys kohdistuu ihmiseen ja jokainen hyökkäyksen uhri reagoi tilanteeseen yksilöllisesti. Tämä tekee puolustautumisesta vaikeaa. Peltierin (2006) mukaan käyttäjän manipuloinnin hyökkäys onkin kaikista hyökkäystekniikoista hankalin puolustaa.

Uhka organisaation tietoturvalla ei aina tule sen ulkopuolelta. Peräti 50-75 % organisaatioiden tietoturvaan liittyvistä tapaturmista ja väärinkäytöksistä aiheutuvat organisaation jäsenten toimesta (D'Arcy, Hovav, & Galletta, 2009; Peltier, 2006). Abrahamin ja Chengalur-Smithin (2010) tekemän tutkimuksen mukaan kaikki 2000-luvun levinneimpien haittaohjelmien levittämiseen käytettiin käyttäjän manipuloinnin tekniikoita. Monien tutkimusten mukaan kuitenkin ihmiselementti on jäänyt vähälle huomiolle tietoturvaan liittyvässä tutkimuksessa ja sen toteutuksen suunnittelussa (Abraham & Chengalur-Smith, 2010; Öǀütçü, Testik, & Chouseinoglou, 2016). On siis tärkeää, että aihepiiriä tutkitaan lisää. Siten on mahdollista löytää keinoja, joilla pystytään pienentämään käyttäjän manipuloinnin riskiä organisaatioiden tietoturvalle.

Toisessa luvussa esittelen lyhyesti tässä tutkimuksessa käytettyä tutkimusmenetelmää ja tiedonhaun eri vaiheita. Kolmannessa luvussa käsittelen käyttäjän manipuloinnin hyökkäyksen osa-alueita ja esittelen tarkemmin joitakin käyttäjän manipuloinnin yleisimpiä esiintymismuotoja.

Neljännessä luvussa esittelen ja vertailen eri tutkimusten tuloksia ja pyrin tuomaan esiin keinoja, joita tutkimuksissa on pienentävän käyttäjän manipuloinnin riskiä. Käsittelen tietoturvatietoisuuden, tekniset ratkaisut, tietoturvakäytänteiden ja auditoinnin merkitystä organisaation kyvylle suojautua käyttäjän manipuloinnilta.

Viidennessä luvussa pohdin kirjallisuuskatsauksessa esiin tulleita ongelmia ja havaintoja. Kuudennessa luvussa käsittelen lyhyesti, tutkimuksen rajoituksia ja miten tutkimusta voitaisiin jatkaa aiheesta eteenpäin.

2. Tutkimusmenetelmä

Tämän tutkielman tutkimusmenetelmänä on käytetty kirjallisuuskatsausta. Tämä luku kuvaa tutkimuksessa käytetyn aineiston hakemista ja rajaamista.

Lähteenä käytettyjen tutkimusten hakemiseen on käytetty Scopus-viitetietokantaa. Käytettyjä hakusanoja ovat mm.”social engineering”, ”security awareness”, ”information security” ja “computer security”. Hakutulokset on rajattu ensin englanninkielisiin tieteellisten lehtien julkaisuihin. Näistä on tiivistelmien perusteella valittu ne julkaisut kirjallisuuskatsaukseen, joissa on toteutettu empiirinen tutkimus. Lähteiden laadun arviointiin käytin JUFO luokitusta. Hyväksyin kirjallisuuskatsaukseen ne julkaisualustat, jotka ovat saaneet jonkin JUFO luokituksen.

3. Käyttäjän manipulointi

Tässä luvussa määrittelen ja käsittelen käyttäjän manipulointiin liittyviä keskeisiä termejä, käsittelen hyökkäyksen rakennetta sekä esittelen yleisimpiä hyökkäysmuotoja.

3.1 Käyttäjän manipuloinnin teoriaa

Käyttäjän manipuloinnilla (engl. *social engineering*) tarkoitetaan tekniikoita, joilla pyritään saamaan uhri paljastamaan arkaluonteista tietoa tai toimimaan muulla hyökkääjän haluamalla tavalla (Mitnick & Simon, 2011). Tavoitteen saavuttamiseksi hyökkääjä ei käytä pelkästään teknisiä työkaluja, vaan käyttää hyväksi myös ihmisen psykologisia ominaisuuksia (Happ, Melzer, & Steffgen, 2016).

Hyökkääjä pyrkii vetoamaan vahvasti uhrin tunteisiin ja siten luomaan häiriötekijöitä uhrin kyvylle havainnoida tilannetta ja tehdä rationaalisia päätöksiä (Workman, 2008). Schneierin (2011) mukaan ihminen on luonnostaan huono arvioimaan riskejä, vaikka tietoa olisikin riittävästi käytettävissä. Esimerkiksi liikenteessä oman virheen riski arvioidaan usein matalammaksi kuin se oikeasti on. Toisaalta lentäessä lento-onnettomuuden riski arvioidaan huomattavasti korkeammaksi kuin se todellisuudessa on. Käytettävissä olevaa tietoa rajoittamalla huono arviointikyky korostuu entisestään. (Schneier, 2011.)

Jos hyökkääjä pystyy rajoittamaan käytössä olevan tiedon määrää, päätökseen käytettävissä olevaa aikaa tai muulla tavoin häiritsemään uhrin arviointikykyä, käyttäjän manipuloinnin onnistumisen todennäköisyys kasvaa. Arviointi kyvyn heikentämiseksi hyökkääjä käyttää hyväksi uhrin psykologisia ominaisuuksia, kuten ahneutta, pelkoa tai auttamisen halua (Happ, Melzer, & Steffgen, 2016). Peltier (2006) lisää omaisuuksien joukkoon ihmisten taipumuksen luottaa toisiin ihmisiin sekä laiskuuden. Workmanin (2007) mukaan ihmiset ovat myös valmiita antamaan arkaluontoista tietoa päästäkseen sosiaalisesti haluttuun ihmisryhmään tai saadessaan sillä muiden arvostusta ja hyväksyntää. Hän havaitsi myös tutkimuksessaan, että työntekijät olivat valmiita antamaan yhä arkaluontoisempaa tietoa voittaakseen tutkimukseen kuuluneessa pelissä.

Tetri ja Vuorinen (2013) jakavat käyttäjän manipuloinnin kolmeen osaan. Ensimmäinen on tunkeutuminen (engl. *act of intrusion*), jolla tarkoitetaan tapahtumaa, jossa hyökkääjä läpäisee kohdejärjestelmän (engl. *target system*) puolustusmekanismit. Toiseksi hyökkäys toteutetaan ”sosiaalisesti” eli se sisältää ei-teknisen osa-alueen. Kolmanneksi hyökkääjällä on jokin päämäärä hyökkäykselle. Se voi olla esimerkiksi jokin esine, tieto tai sisäänpääsy järjestelmään.

3.1.1 Kohdejärjestelmä

Hyökkäyksellä on aina jokin kohde, johon hyökkääjä pyrkii pääsemään käsiksi. Se voi olla mm. tietojärjestelmä, tietokanta tai laite. Useimmiten kohde on jokin verkossa oleva tietojärjestelmä, jota käyttää useita henkilöitä useiden eri rajapintojen kautta. Järjestelmään on aina jokin määrä mahdollisia sisäänkäyntejä (engl. *entry points*) päästä käsiksi. Näiden sisäänkäyntien määrä riippuu rajapintojen ja käyttäjien määrästä. Nämä voidaan jakaa teknisiin ja sosiaalisiin sisäänkäynteihin. Sosiaalisilla sisäänkäynneillä (engl. *social entry point*) tarkoitetaan yksilöitä, joilla on pääsy järjestelmään sekä järjestelmän ulkopuolisia asioita ja esineitä, jotka sisältävät tietoa kohdejärjestelmästä.

Tällaisia sosiaalisia sisäänkäyntejä ovat mm. organisaation verkkosivut, sosiaalisen median tilit sekä roska-astiat. (Tetri & Vuorinen, 2013.)

3.1.2 Järjestelmään tunkeutuminen

Toinen Tetrin ja Vuorisen (2013) määrittämä käyttäjän manipuloinnin osa-alue oli, että se sisältää ei-teknisen osa-alueen. Tällä tarkoitetaan sitä, että järjestelmään päästään tunkeutumaan hyväksikäyttäen sosiaalisia sisäänkäyntejä. Hyökkääjä pyrkii läpäisemään kohdejärjestelmän puolustusmekanismit keräämällä tietoa ja käyttämällä hyväksi näitä sisäänkäyntejä.

Analysoimalla näitä sosiaalisia sisäänkäyntejä hyökkääjän on mahdollista löytää uusia hyökkäyksen kohteita organisaatiossa tai keinoja ohittaa puolustusmenetelmiä. Yksittäinen tieto ei ole itsessään kovin vaarallinen organisaation kannalta. Hyökkääjän yhdistellessä niitä, niistä voi muodostua polku, jota pitkin hyökkääjä pystyy läpäisemään järjestelmän puolustusmekanismit. (Tetri & Vuorinen, 2013.)

3.1.3 Hyökkäyksen tavoite

Tetrin ja Vuorisen (2013) mukaan hyökkäyksellä on aina jokin tavoite, jonka hyökkääjä pyrkii saavuttamaan. Useimmiten se on jokin tieto, joka on suojattu ulkopuolisilta. Hyökkääjän tavoittelema arkaluonteinen tieto voi olla esimerkiksi käyttäjätunnuksia tai luottokorttitietoja. Käyttäjän manipuloinnin tavoitteena voi olla myös olla esimerkiksi kulunvalvonnan ohittaminen tai tiedonkeruu organisaation rakenteista tai käytössä olevista teknologioista (Mitnick & Simon, 2011).

3.2 Hyökkäyksien muodot

Käyttäjän manipuloinnin -hyökkäys voi olla täysin itsenäinen hyökkäys tai osa isompaa hyökkäystä. Itsenäisessä hyökkäyksessä hyökkääjä saavuttaa tavoitteensa suoraan käyttäjän manipuloinnilla (Tetri & Vuorinen, 2013). Esimerkiksi luottokorttitietoja tavoitteleva hyökkääjä voi saavuttaa tavoitteensa käyttämällä huijaussähköposteja verkkourkintaan ja siten saamaan uhrit luovuttamaan tietonsa.

Useimmissa hyökkäyksissä hyökkääjä pyrkii välttämään fyysistä kontaktia käyttäjän manipuloinnin uhrien kanssa. Kommunikaatio tapahtuu tällöin sähköpostitse tai puhelimitse. (Mitnick & Simon, 2011). Hyökkääjä ei välttämättä kommunikoi suoraan uhrin kanssa, vaan hyökkäys voi tapahtua myös epäsuorasti. Esimerkki tällaisesta hyökkäyksestä on esimerkiksi haittaohjelman sisältävien muistitikkujen jättäminen organisaation läheisyyteen (Mouton, Leenen, & Venter, 2016).

Kun käyttäjän manipulointi on osana isompaa hyökkäystä, sitä voidaan käyttää esimerkiksi jalansijan saamiseksi organisaation tietojärjestelmissä tai tiedonkeruussa. Leen, Assanten ja Conwayn (2016) tekemän analyysin mukaan hyökkäyksessä ukrainalaiseen voimalaitokseen käytettiin kohdennettua verkkourkintaa (engl. *spear phishing*) tietojärjestelmien käyttäjätunnusten kalastamiseen. Käyttäjätunnukset eivät olleet hyökkäyksen päämääränä, vaan niitä käytettiin työkaluna isomman päämäärän saavuttamiseksi.

Useimmiten organisaation kohdistuvissa käyttäjän manipuloinnin hyökkäyksissä riittää, että yksi organisaation työntekijä lankeaa huijaukseen. Mouton, Leenen ja Venter (2016) esittelevät tilanteen, jossa hyökkääjä esiintyy organisaation työntekijänä ja seuraa toista työntekijää organisaation lukituista ovista. Tällainen hyökkäys voi kohdistua keneen tahansa, kenellä on kulkuoikeudet organisaation tiloissa. Se voi olla työntekijä, alihankkija tai toimitusjohtaja. Abawajyn (2014) mukaan organisaation tietoturvan taso onkin yhtä korkea kuin sen heikoin lenkki.

3.2.1 Tiedonkeruu

Kaikki käyttäjän manipuloinnin hyökkäykset vaativat tiedonkeruuta (engl. i*nformation gathering*) hyökkäyksen kohteesta. Tarvittava tiedonkeruun määrä ja tapa kerätä se vaihtelevat kohteen mukaan. Tiedonkeruu tapahtuu aina ennen varsinaista hyökkäystä. Sen tarkoituksena on mahdollistaa myöhempi hyökkäys ja pienentää kiinnijäämisen riskiä. (Tetri, & Vuorinen, 2013.)

Yksi vanhimmista tiedonkeruun keinoista on roska-astioiden tutkiminen (engl. d*umpster diving*). Siinä hyökkääjä käy läpi organisaation roskia ja pyrkii löytämään tietoa, joka auttaisi hyökkäyksen myöhemmissä vaiheissa. Tieto voi olla itsessään arkaluontoista kuten asiakirjoja tai käyttäjätunnuksia, tai sellaista, jotka helpottavat hyökkäyksen myöhemmissä vaiheissa, kuten laitteiden ohjekirjoja. (Peltier, 2006.)

Kulkukoodien ja salasanojen keräämiseksi hyökkääjä voi seurata uhrin toimintaa kulkukoodin vaativilla ovilla tai hänen kirjautuessa laitteelle (Peltier, 2006). Seuraaminen voi tapahtua mm. olan yli kurkkimalla (engl. *shoulder surfing*), kameran tai näppäinpainalluksia tallentavan ohjelmalla (engl. *keylogger*) (Tetri, & Vuorinen, 2013).

On myös mahdollista, että tiedonkeruun aikana hyökkääjä löytää etsimänsä ja varsinaista tunkeutumista kohdejärjestelmään ei tarvita. Esimerkiksi, hyökkääjä voi saada haltuunsa haluamansa tiedon löytämällä sen roskakorista tai varastetusta laitteesta. Hän voi myös saada tiedon salakuuntelemalla organisaation työntekijöiden keskustelua. Kuitenkin tiedonkeruun päämääränä on valmistautuminen varsinaiseen hyökkäykseen. (Tetri, & Vuorinen, 2013.)

3.2.2 Verkkourkinta

Verkkourkinnassa (engl. *phishing*) huijari tai hyökkääjä luo juonen, jonka tarkoituksena on saada uhrilta arkaluontoista tietoa tai rahaa. Hyökkäyksen onnistuminen vaatii, että uhri lankeaa juoneen ja seuraa hyökkääjän antamia ohjeita. (Mann, 2008.)

Tyypillinen tämän kaltainen juoni voi olla esimerkiksi tekaistu sähköposti, jossa ilmoitetaan, että uhrin jonkin palvelun tili suljetaan, jos hän ei toimi viestissä tulleiden ohjeiden mukaisesti (Workman, 2008). Sähköpostissa ohjataan käyttäjä seuraamaan linkkiä, joka johtaa aidonnäköiselle sivustolle. Sivusto on ulkoasultaan ja osoitteeltaan samankaltainen kuin palvelu, jota se mimikoi. Tämä voi olla esimerkiksi kirjautumissivu pankin verkkopalveluun (Mann, 2008). Uhrin yrittäessä kirjautua palveluun hänen tunnukset otetaan talteen ja niitä voidaan käyttää myöhemmin (Mann, 2008).

Tämän jälkeen hyökkääjä voi joko ohjata uhrin oikean palvelun sivustolle tai pyytää uhria yrittämään uudelleen ja tallentaa salasanat, joita hän yrittää. Salasanoja voidaan yrittää käyttää tulevaisuudessa muissa hyökkäyksissä. Jos puolestaan uhri ohjataan

kirjautumisyrityksen jälkeen aidolle sivustolle, kirjautumisen ilmoitetaan epäonnistuneen. Uuden yrityksen jälkeen kirjautuminen aitoon palveluun onnistuu. Hyökkääjä on saanut uhrin tunnukset, eikä uhri mitä todennäköisimmin huomannut mitään. (Schneier, 2011.)

Myös suomessakin yleiset nigerialaiskirjeet ovat verkkourkintaa. Niissä uhrille ilmoitetaan, että hän on syystä tai toisesta ansainnut merkittävän summan rahaa. Kuitenkin rahojen saamiseksi kohteen on maksettava erinäisiä kustannuksia, kuten kuljetuskustannuksia, ennen kuin hän pääsisi käsiksi rahoihin. Jos uhri lankeaa huijaukseen ja maksaa rahat, syntyy uusi ”yllättävä” ja hieman edellistä suurempi kustannus, joka toimii esteenä rahojen saannille. (Poliisi.)

Verkkourkinta hyökkäykset suunnataan yleensä suurelle massalle sillä sähköpostiviestin ja huijaussivuston luomisen jälkeen se ei vaadi hyökkääjältä juurikaan toimia. Hyökkääjän ei tarvitse olla lähelläkään uhreja, vaan hän voi toimia verkon yli mistä päin maailmaa tahansa. Suuren massan ja edullisuuden vuoksi riittää, että pienikin prosenttiosuus uhreista lankaa juoneen ja se on hyökkääjälle kannattavaa. (Mann, 2008.)

Verkkourkinta voidaan toteuttaa myös kohennettuna verkkourkintana (engl. *spear phishing*). Tällöin ihmismassojen sijaan huijaus on suunnattu vain tietyn organisaation työntekijöille tai jopa yksittäiselle henkilölle. Tällaiset hyökkäykset voivat olla erittäin tehokkaita ja vaikeasti havaittavia. (Krombholz, Hobel, Huber, & Weippl, 2015.)

Flores ym. (2015) tekemän tutkimuksen mukaan lähes 10% työntekijöistä avasi kohdentamattomassa huijaussähköpostiviestissä olevan linkin ja heistä yli puolet suorittivat sen takana olevan binääritiedoston. Goel, Williams ja Dincelli (2017) totesivat tutkimuksessaan, että kohdentaminen lisäsi huomattavasti käyttäjän manipuloinnin tehokkuutta. Peräti 68,7 % Goelin ym. (2017) tutkimukseen osallistuneista opiskelijoista avasi kurssi-ilmoittautumisen epäonnistumista esittävän huijausviestin ja seurasi siinä olevaa linkkiä.

Kohdennetussa verkkourkinnassa tiedonkeruun rooli korostuu. Hyökkäys alkaa tiedonkeruulla kohdeorganisaatiosta ja sen jäsenistä. Tämän kerätyn tiedon pohjalta lähetetään kohdehenkilöille sähköposti, jolla pyritään saada uhri tai uhrit toimimaan halutulla tavalla. (Krombholz ym., 2015.)

3.2.3 Verukkeen luominen

Verukkeen luomisella (engl. *pretexting*) tarkoitetaan hyökkäystä, jossa huijari pyrkii lavastamaan tilanteen, jonka seurauksena luovuttaa arkaluontoista tietoa tai toimii muuten huijarin haluamalla tavalla. Luodun tilanteen on oltava sellainen, että se vakuuttaa uhrin tilanteen aitoudesta. Hyökkääjä esiintyy tällaisessa hyökkäyksessä toisena henkilönä ja pyrkii vakuuttamaan uhrin. Onnistuneen verukkeen luominen voi olla huomattavasti haastavampaa kuin verkkourkinnassa. Jotta tilanne vakuuttaisi uhrin, se vaatii huomattavaa tiedonkeruuta ja taitoa manipuloida uhria. (Workman, 2008.)

Mouton ym. (2016) esittelivät esimerkkitilanteen, jossa hyökkääjä esiintyy organisaation työntekijänä ja pyrkii saamaan siivoojaa avaamaan hänelle oven tilaan, johon pääsyä on rajoitettu. Tässä hyökkääjä pyrkii käyttämään hyväksi uhrin auttamisen halua. Toisessa heidän esittelemässä tilanteessa hyökkääjä esiintyy tietojärjestelmän ylläpitäjä. Hän pyytää organisaation työntekijää joko suoraan antamaan käyttäjätunnuksensa tai salasanansa tai vaihtamaan salasanan johonkin hyökkääjän haluamaan. Myös Peltier

(2006) esittelee hyvin samankaltaisen hyökkäyksen tehokkuutta. Tällaisessa hyökkäyksessä hyökkääjä käyttää hyväksi auktoriteettia sekä uhrin luontaista auttamisen halua pyrkiessään vakuuttamaan uhri siitä, että hän on ylläpitäjä ja tarvitsee uhrin tunnuksia. Jos hyökkäys onnistuu, hyökkääjällä on samat oikeudet organisaation tietojärjestelmiin kuin uhrilla.

3.2.4 Catfish-hyökkäys

Catfish-hyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkääjä yrittää muodostaa luottamussuhteen uhrin kanssa tekeytymällä toiseksi ihmiseksi tai valepersoonaksi (van Schaik ym., 2017). Tällaisessa hyökkäyksessä hyökkääjä voi esimerkiksi luoda käyttäjän sosiaalisen median palveluun ja pyrkiä muodostamaan luottamussuhteen kohteen kanssa. Hyökkääjä pyrkii tämän jälkeen käyttämään luottamussuhdetta hyväksi useimmiten taloudellisen hyödyn saamiseksi. Hyökkäyksellä voidaan myös pyrkiä hankkimaan lisää tietoa kohteesta hyökkäyksen myöhempiä vaihteita varten.

Esimerkkinä catfish-hyökkäyksestä on nettirakas, joka esiintyy toisena henkilönä. Huijari pyrkii luomaan luottamussuhteen uhriin keskustelemalla tämän kanssa. Poliisin mukaan Suomessa yleisimpiä ovat tapaukset, jossa osapuolina suomalainen mies ja ulkomaalainen nainen. Jossain vaiheessa joko mies pyytää naista luokseen tai nainen ehdottaa sitä itse. Huijari pyytää uhrilta rahaa viisumi- ja matkustuskustannuksiin. Huijari ilmoittaa aina uudesta kustannuksesta, joka estää häntä saapumasta uhrin luo. (Poliisi.)

Silicin ja Backin (2016) mukaan yritykset käyttävät paljon sosiaalisen median sivustoja yrityksen toiminnan tukena. Liian usein kuitenkin näiden palveluiden tuomia riskejä ei oteta riittävän hyvin huomioon. Tällöin sosiaalinen media avaa hyökkääjille mahdollisuuden käyttää tätä haavoittuvuutta hyväksi. Heidän mukaansa hyökkääjän on melko helppo luoda esimerkiksi valeprofiili sosiaalisen median palveluun. Sen avulla hän pystyy liittymään organisaation työntekijöiden sisäisiin sosiaalisen median ryhmiin.

3.2.5 Sisäiset uhkat

Käyttäjän manipuloinnin uhka ei tule aina organisaation ulkopuolelta, vaan se voi tulla myös sen sisältä. Sisäiset uhkat (engl. *insider threat*), kuten organisaation nykyiset tai aikaisemmat työntekijät, voivat olla hyvin vaarallisia organisaation tietoturvalle. D'Arcy, Hovav ja Galletta (2009) mukaan jopa 50-75 % organisaatioihin kohdistuvista tietoturvauhista tulevat niiden sisältä. Erityisesti nykyisillä työntekijöillä on mahdollisuus väärinkäyttää heillä olevaa tietoa ja luottamusta. Mitkään puolustusmekanismit eivät voi poistaa kokonaan organisaation sisältä tulevaa uhkaa. (Schneier, 2011.)

Sisäinen uhka ei tarkoita pelkästään järjestelmän loppukäyttäjän haitallista toimintaa. Järjestelmän asentajat, huoltajat ja ylläpitäjät voivat myös melko helposti päästä käsiksi dataan tai jättää takaportin auki järjestelmään tai verkkoon. Myös järjestelmän tai organisaation tietoturvaa auditoiva henkilö on mahdollinen sisäinen uhka. Havaitessaan ongelmia organisaation tietoturvassa hän voi olla ilmoittamatta niistä ja käyttää niitä hyväksi myöhemmin. (Schneier, 2011.)

Nykyisillä ja entisillä työntekijöillä on jo valmiiksi hyvin paljon tietoa organisaation käytänteistä, henkilöstöstä ja käytössä olevasta teknologiasta. Heillä on usein jo valmiiksi pääsy organisaation verkkoon tai tietojärjestelmiin. Työntekijän on melko helppoa saada haltuunsa kollegan käyttäjätunnukset tai käyttää laitetta, johon joku muu on jo

kirjautunut. Tällöin hän saa syyn vieritettyä muille, kun hyökkäys paljastuu. (Medlin, Cazier, & Foulk, 2008.)

4. Käyttäjän manipuloinnilta puolustautuminen

Tässä luvussa esittelen kirjallisuuskatsauksen tutkimuksissa esiin tulleita erilaisia ratkaisuja, joilla organisaatiot pystyvät pienentämään käyttäjän manipuloinnin riskiä. Tutkimukset tarjoavat erilaisia ratkaisuja käyttäjän manipuloinnin tuoman tietoturvariskin pienentämiseksi.

4.1 Tietoturvatietoisuus

Abawajy (2014) määrittelee käyttäjien tietoturvatietoisuuden (engl. *information security awareness*) ymmärryksen tasoksi, joka organisaation jäsenellä on tietoturvakäytänteiden noudattamisen tärkeydestä. Mitä paremmin hän ymmärtää tietoturvakäytänteet, niiden syyt sekä noudattamatta jättämisen seuraukset, sitä korkeampi tietoturvatietoisuus hänellä on. Schaab ym. (2017) lisäävät määritelmään käyttäjän ymmärryksen siitä, kuinka hän voi säännöstelemällä omaa toimintaansa ehkäistä mahdollisia tietoturvatapaturmia. Siposen (2000) mukaan tietoturvatietoisuuden kasvaessa käyttäjän johtuvan tietoturvatapaturmien riski pienenee.

4.1.1 Tietoturvakoulutus

Käyttäjien tietoturvakoulutuksella ja tietoturvatietoisuudella on positiivinen vaikutus heidän kykyyn havaita ja puolustautua käyttäjän manipuloinnilta (Aburrous ym., (2010); D'Arcy ym., 2010; Flores ym., 2015; Happ ym., 2016; Heartfield ym. (2016); Öğütçü ym., 2016). Myös Peltier (2006) mukaan tietoturvakäytänteiden jatkuva ja huolellinen koulutus on tehokas tapa parantaa organisaation tietoturvaa. Siten tietoturvakoulutus parantaa käyttäjien tietoturvatietoisuutta.

Kuitenkin Goelin ym. (2017) mukaan yleispätevä koulutus on ollut tehoton käyttäjien valistamisessa kohdennettua verkkourkintaa vastaan. Heidän mukaan tulevaisuudessa koulutusta pitäisi yhä enemmän kohdentaa sen mukaan, millaisia tilanteita hän kohtaa toimiessaan organisaatiossa. Heartfield ym. (2016) puolestaan havaitsivat tutkimuksissaan, että kulunut aika edellisestä itseopiskelusta on merkittävä tekijä uhrin kyvyssä havaita ja puolustautua käyttäjän manipuloinnin hyökkäyksiltä. Luentopohjaisella tietoturvakoulutuksella sen sijaan ei ollut selkeää vaikutusta uhrin alttiuteen käyttäjän manipuloinnille.

Schaab ym. (2017) mukaan konkreettiset esimerkit uhkatilanteista ja niissä toimimisesta ovat olennainen osa onnistunutta tietoturvakoulutusta. Lisäksi koulutus ei saisi olla yksisuuntaista luennointia, vaan koulutettavat olisi otettava aktiivisemmin mukaan koulutukseen. Goelin ym. (2017) mukaan myös jakaminen erilaisiin koulutuksiin esimerkiksi työnkuvan perusteella voisi parantaa tietoturvakoulutuksen tehokkuutta.

Peltierin (2006) mukaan koulutus ei kuitenkaan saa olla kertaluontoista, vaan sen on oltava jatkuvaa. Hänen mukaansa tietoturvakoulutusta tulisi järjestää vähintään kerran puolessa vuodessa. Koulutuksen on jatkuttava koko sen ajan, kun henkilö on osa organisaatiota.

Puolestaan Kearneyn ja Krugerin (2016) tekemän tutkimuksen mukaan kokemattomat työntekijät olivat alttiimpia käyttäjän manipuloinnille. He luovuttivat käyttäjätunnuksensa tai muuta henkilökohtaista tietoa kokeneempia työntekijöitä

useammin. Tästäkin syystä on tärkeää, että tietoturvakoulutus aloitetaan heti, kun henkilö liittyy organisaatioon.

Schaab ym. (2017) mukaan käyttäjän manipulointiin liittyvissä tietoturvakoulutuksissa pitäisi keskittyä entistä enemmän siihen, millaisia keinoja hyökkääjä voi käyttää yrittäessään taivutella uhria toimimaan hänen haluamallaan tavalla. Käyttäjille pitäisi antaa konkreettisia keinoja hyökkääjän suostuttelun havaitsemiseksi ja oikean reagointitavan löytämiseksi. Joihinkin hyökkäyksiin toimii perinteinen ajatus, että jos jokin kuulostaa liian hyvältä ollakseen totta, niin se ei ole. Tällaisten tarkistusten soveltaminen ei onnistu suoraan verukkeen luomiseen tai hienovaraiseen suostutteluun, jossa hyökkäyksessä uhrille ei suoraan tarjota konkreettista hyötyä.

4.2 Tekniset puolustusmekanismit

Tutkimuksissa (Dhinakaran, Nagamalai, & Lee, 2010; Aburrous ym., 2010) on yritetty löytää tehokkaita teknisiä puolustusmekanismeja käyttäjän manipuloinnilta puolustautumiseksi. Suuri osa käyttäjän manipuloinnista tapahtuu verkon yli, joten tekniset puolustusmekanismit ovat avainroolissa hyökkäyksiltä puolustautuessa (Abawajy, 2014).

Dhinakaran, Nagamalai ja Lee (2010) analysoivat miljoonia organisaation työntekijöille tulleita huijaussähköposteja. Analyysin pohjalta he kehittivät monikerroksisen järjestelmän, joka pyrki suodattamaan huijaussähköpostit pois. Sähköpostien arviointiin he käyttivät menetelmää, joka otti huomioon mm. erilaisia suodattimia ja IP-osoitteiden listaamista. Ohjelmiston lisäksi he kouluttivat myös käyttäjiä havaitsemaan epäilyttäviä sähköposteja ja ilmoittamaan niistä. He tarkkailivat järjestelmän toimintaa kaksi vuotta ja havaitsivat sen onnistuneen hyvin. Peräti 95 % huijaussähköposteista estettiin ja sähköpostien väärin liputtaminen väheni 80 %. Myös Aburrous ym. (2010) mukaan huijaussähköposteja ja -verkkosivuja voidaan koneellisesti luokitella ja siten ehkäistä verkkourkinnan yrityksiä.

Markkinoilla on ollut kuitenkin aikaisemminkin samankaltaisia ohjelmistoja, joilla on pyritty estämään verkko- ja sähköpostihuijauksia, mutta Dhinakaran ym. (2010) yksikään niistä ei estänyt hyökkäyksiä riittävän tehokkaasti, sillä hyökkääjät keksivät jatkuvasti uusia keinoja kiertää niitä vastaan asetettuja vastatoimenpiteitä. Vaikka heidän kehittämä uusi järjestelmä verkkohuijausten havaitsemiseksi kehittyy ja päivittyy säännöllisesti uusien havaintojen mukaan, uskon että hyökkääjät pystyvät jatkossa kehittämään huijaussähköposteja, joita järjestelmä ei riittävän tehokkaasti osaa suodattaa pois.

Vaikka tekniset puolustusmekanismit ovat organisaation turvallisuuden kannalta välttämättömiä, ne eivät yksin pysty suojaamaan organisaatiota käyttäjän manipuloinnin uhkilta (Abawajy, 2014).

4.3 Tietoturvakäytänteet

Tietoturvakäytänteet (engl. *security policy*) ovat organisaation laajuisia opasteita ja malleja siitä, mikä on oikea tapa toimia erilaisissa tilanteissa. D'Arcy ym. (2010) mukaan tietoturvakäytänteet ovat merkittävässä roolissa organisaation sisältä tulevien uhkien lieventämiseksi. Heidän mukaan on erityisen tärkeää, että käyttäjä ymmärtää tietoturvakäytänteitä noudattamatta jättämisestä seuraukset.

Lisäksi tietoturvakäytänteiden olisi syytä määrittää, mikä kaikki tieto on arkaluonteista sekä kuinka kunkin eri tason salaisuuksien kanssa tulisi toimia. Käyttäjän pitäisi pystyä aina olemaan käytänteiden pohjalta selvillä siitä, onko hänen käsittelemä tieto arkaluontoista vai ei. (Schaab ym., 2017.)

Goelin ym. (2017) mukaan verkkourkinnalle altistumisen riskiä voidaan hieman pienentää tiedottamalla selkeästi siitä, millaisista asioista ja mitä kautta organisaatio on yhteydessä sen jäseniin tai asiakkaisiin. Esimerkiksi pankki voi mainostaa, että ei ole koskaan asiakkaisiin yhteydessä sähköpostitse.

4.4 Auditointi

Schaab ym. (2017) mukaan tietoturva-auditoinnilla voidaan teknisten uhkien lisäksi arvioida myös organisaation kykyä vastustaa käyttäjän manipuloinnin hyökkäyksiä. Heidän mukaansa perinteiseen auditoinnissa, kuten tunkeutumistestauksessa (engl. *penetration testing*) olisi arvioitava myös alttiutta käyttäjän manipuloinnille.

D'Arcy ym. (2010) mukaan tietoturvakäytänteiden vaikutus riippuu käyttäjän kokemuksesta siitä, kuinka kova rangaistus (engl. *punishment severity*) väärin toimimisesta seuraa ja kuinka todennäköisesti rangaistus toteutuu (engl. *punishment certainty*). Heidän mukaan rangaistuksen kovuudella on hieman suurempi vaikutus organisaation sisäisen uhkan pienentämiseen kuin rangaistuksen varmuudella. (D'Arcy, Hovav, & Galletta, 2009.)

Erilaisten ohjeiden ja sääntöjen laatiminen ei yksistään riitä tietoturvan takaamiseksi, vaan kuten D'Arcyn ym. (2009) tekemän tutkimuksen mukaan tarvitaan myös selkeät seuraamukset niiden rikkomisesta sekä valvontaa. Kuten Dhinakaran ym. (2010) totesivat, että teknologian ja puolustusmekanismien kehittyessä, hyökkääjät pyrkivät jatkuvasti löytämään uusia keinoja ohittaa puolustusmekanismit. Tämän vuoksi tietoturvariskejä ja niitä pienentävien tekijöitä on myös jatkuvasti auditoitava.

5. Pohdinta

Käyttäjän manipuloinnilta puolustautuminen on hyvin hankalaa, sillä sitä esiintyy monissa eri muodoissa. Yleisimpiä hyökkäysmuotoja ovat verkkourkinta, verukkeen luominen sekä catfish-hyökkäykset. Lisäksi se voi kohdistua keneen tahansa yksilöön organisaation sisällä ja ohittaa parhaimmatkin tekniset puolustusmekanismit. Silti se on jäänyt organisaatioiden tietoturvassa hyvin pienelle huomiolle.

Muutamissa tutkimuksissa on pyritty analysoimaan erilaisia käyttäjän manipuloinnin hyökkäyksiä ja löytämään näistä yhtäläisyyksiä. Joitakin tutkimuksien havaitsemia yhtäläisyyksiä ovat hyökkäyksen motiivi, kohdejärjestelmä sekä hyökkäyksen sosiaalinen osa-alue. Kuitenkin alalta puuttuu vielä vakiintunut käyttäjän manipuloinnin malli, jota hyödyntämällä voitaisiin ymmärtää käyttäjän manipulointia paremmin ja puolustautua sitä vastaan. Mallissa käyttäjän manipuloinnin hyökkäykset olisi pystyttävä purkamaan selkeiksi palasiksi. Näitä palasia ja niiden välisiä suhteita tarkastelemalla voitaisiin arvioida ja lieventää käyttäjän manipuloinnin hyökkäyksien riskejä osa-alue kerrallaan.

Erityisesti tietoturvatietoisuudella tuntui olevan suuri vaikutus siihen, kuinka hyvin yksilö pystyy havaitsemaan ja vastustamaan käyttäjän manipuloinnin hyökkäyksiä. Tietoturvakoulutus vaikuttaa olevan paras tapa kasvattaa käyttäjien tietoturvatietoisuutta. Kuitenkin perinteinen luennointi vaikutti hyvin vähän käyttäjien kykyyn vastustaa hyökkäyksiä. Sen sijaan jatkuvampi ja kohdennettu tietoturvakoulutus lisäsi huomattavasti enemmän kykyä puolustautua käyttäjän manipuloinnilta. Myös itseopiskelulla oli suurempi vaikutus kuin perinteisellä luennoinnilla.

Parissa tutkimuksessa oli toteutettu tekninen puolustusmekanismi, joka pyrki havaitsemaan huijaussähköpostit tai -verkkosivut. Nämä ratkaisut olivat tutkimusten mukaan lyhyellä aikavälillä tehokkaita. Kuitenkin teknologian kehittyessä ja huijareiden pyrkiessä kiertämään suojausmekanismeja, teknisten puolustusmekanismien teho heikkenee.

Tietoturvan ollessa jatkuvassa liikkeessä tarvitaan myös jatkuvaa uudelleen arviointia tietoturvakäytänteiden oikeellisuudesta. Auditointia tarvitaan myös teknisten laitteiden ja järjestelmien lisäksi myös ihmisten kykyyn havaita ja reagoida oikein käyttäjän manipulointiin.

Kuten johdannossa mainittiin, että hyökkääjälle riittää, että hän läpäisee tai ohittaa kohdejärjestelmän puolustusmekanismit yhdestä kohtaa. Tämän takia käyttäjän manipulointiin tai muuhunkaan tietoturvariskiin ei ole yhtä täydellistä ratkaisua. Tietoturva vaatii jatkuvasti huomiota, eikä sitä voida toteuttaa pelkästään kertaluontoisin ratkaisuin.

6. Johtopäätökset

Käyttäjän manipuloinnilla tarkoitetaan keinoja, joiden avulla hyökkääjä pyrkii saavuttamaan tavoitteensa käyttämällä uhrin psykologisia ominaisuuksia hyväkseen. Se ei kuitenkaan poissulje hyökkäyksen teknistä osa-aluetta, vaan useimmiten toimii teknisen hyökkäyksen apuvälineenä. Teknisten puolustusmekanismien kehittyessä hyökkääjät ovat siirtyneet yhä enemmän käyttämään hyökkäyksissä käyttäjän manipuloinnin keinoja.

Organisaatioissa tarvitaan kattavia ja monipuolisia keinoja puolustautua erilaisia käyttäjän manipuloinnin hyökkäyksiä vastaan. Organisaation kyky puolustautua koostuu niin teknisistä puolustusmekanismeista, organisaation laajuisista tietoturvakäytänteistä sekä yksilöiden kyvystä havaita ja puolustautua käyttäjän manipuloinnilta.

Tämän tutkielman tarkoituksena on tutkia käyttäjän manipulointia tietoturvariskinä ja löytää mahdollisia keinoja, joilla organisaatiot pystyisivät pienentämään käyttäjän manipuloinnin riskiä. Tutkielma on kirjallisuuskatsaus aikaisempaan aiheeseen liittyvään tutkimukseen.

Kirjallisuudessa (Mann, 2008; Schneier, 2011) mainitaan kulunvalvonta yhtenä tärkeänä keinona käyttäjän manipuloinnin ehkäisemiseksi. Kulunvalvontaan ja käyttäjän manipulointiin liittyvää tutkimusta löytyi hyvin vähän. Tämä voi johtua siitä, että suurin osa käyttäjän manipuloinnin hyökkäyksistä tapahtuu verkon yli.

Tämä kirjallisuuskatsaus ei ole systemaattinen katsaus aiheeseen, joten se ei kattavasti kuvaa aiheesta tehtyä tutkimusta. Jatkotutkimuksissa voitaisiin esimerkiksi tutkia erikseen organisaation jäsenten aiheuttamia tahallisia ja tahattomia sisäisiä tietoturvariskejä.

Tahattomalla sisäisellä riskillä tarkoitetaan organisaation jäsentä, joka ei itse aktiivisesti pyri toimimaan väärin, vaan muuten toiminnallaan luo mahdollisuuden, jota jokin kolmas osapuoli voi käyttää hyväkseen (D'Arcy ym., 2009.) Esimerkki tahattomasta sisäisestä tietoturvariskistä on saman salasanan käyttö organisaation eri palveluissa ja sen ulkopuolisissa palveluissa. Tällöin henkilön motiivina ei ole tietoturvariskien aiheuttaminen organisaatiolle. Riskin aiheuttamisen taustalla voi olla esimerkiksi henkilön riittämätön tietämys oikeaoppisesta salasanojen käytöstä tai yksinkertaisesti laiskuus. Tahallisessa sisäisessä tietoturvariskissä henkilö puolestaan käyttää asemaansa väärin saavuttaakseen itselleen hyötyä tai aiheuttaakseen organisaatiolle vaikeuksia. Myös Crossler ym. (2013) tuovat esiin tarpeen näiden sisäisten uhkien erottamisen toisistaan, sillä niiden ehkäiseminen eroaa hyvin paljon toisistaan.

Muutamat tutkimukset, kuten Pouryousefi ja Frooman (2019), Tetri ja Vuorinen (2013) ja Workman (2008), ovat yrittäneet mallintaa käyttäjän manipuloinnin hyökkäystä ja sen osa-alueita, mutta vakiintunutta mallia ole vielä syntynyt. Tällaisen vakiintunen mallin luominen voisi helpottaa huomattavasti käyttäjän manipuloinnin hyökkäysten ymmärtämistä ja niiden riskitekijöiden lieventämistä.

Pouryousefi ja Frooman (2019) pyrkivät tutkimuksessaan mallintamaan kuluttajiin kohdistuneita huijauksia. Heidän mallissa huijaukset jaettiin neljään kategoriaan sen mukaan, onko uhrilla mahdollisuutta havaita (engl. *observe*) tai arvioida (engl. *judge*) huijaukseen liittyvän tietoa ja sen aitoutta.

Jos sekä huijarilla että uhrilla on käytössä sama määrä tietoa ja he molemmat pystyvät arvioimaan sen oikeellisuuden, heidän välinen tieto on symmetristä. Tällöin huijauksen onnistumisen todennäköisyys on pieni. Kun huijari pystyy rajoittamaan uhrin mahdollisuutta havaita tai arvioida jotakin tietoa, heidän tietonsa ovat epäsymmetriset. Tällöin uhri on altis huijaukselle (Pouryousefi & Frooman, 2019.)

Kun uhrilla ei ole käytettävissä huijauksen kannalta merkittävää tietoa, eikä hän ymmärrä käytössä olevan tiedon riittävyyttä tai oikeellisuutta, hän on hyvin altis huijaukselle. Uhri on puolestaan melko altis huijaukselle, jos hänellä on käytössään riittävä määrä informaatiota, mutta hän ei ymmärrä sen merkitystä tai muuten epäonnistuu sen arvioinnissa. Samoin silloin, kun uhrilla on käytössä rajattu määrä tietoa, jonka oikeellisuuden hän pystyy arvioimaan, mutta häneltä puuttuu jokin merkittävä tieto, jota huijari pystyy käyttämään hyväkseen. (Pouryousefi & Frooman, 2019.)

Esimerkiksi tämän kaltaista mallia voitaisiin jatkossa yrittää laajentaa yksilöstä organisaatioon, jolloin erilaisten käyttäjän manipuloinnin riskejä pystyttäisiin paremmin arvioimaan. Tietoturvariskit ovat organisaatiokohtaisia, mutta mallin avulla riskien suuruus voitaisiin paremmin arvioida ja niihin reagointi voisi olla systemaattisempaa. Tämä helpottaisi myös käyttäjän manipuloinnin puolustuskyvyn auditointia.

Tulevaisuudessa tutkimusta voitaisiin suunnata siihen, miten käyttäjän manipulointi voitaisiin saada osaksi perinteistä penetration-testausta. Tämän kautta olisi mahdollista, että organisaatiot havaitsisivat käyttäjän manipuloinnille altistavat riskitekijät aikaisemmin ja pystyisivät reagoimaan niihin ennen kuin hyökkääjä hyväksikäyttää niitä.

Lähteet

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology, 33*(3), 236-247.

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183-196.

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert systems with applications*, *37*(12), 7913-7921.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*, *32*, 90-101.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Dhinakaran, C., Nagamalai, D., & Lee, J. K. (2010). Multilayer approach to defend phishing attacks. *Journal of Internet Technology, 11*(3), 417-426.

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security, 23*(2), 178-199.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? internet security and human vulnerability. *Journal of the Association of Information Systems, 18*(1), 22-44.

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat–Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61*, 372-377.

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access, 4*, 6910-6928.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers and Security, 61*, 46-58.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid. *SANS Industrial Control Systems*, *23*.

Mann, I. (2008). *Hacking the Human: Social Engineering Techniques and Security Countermeasures*. Gower Publishing, Ltd.

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP), 2*(3), 71-83.

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

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*, 186-209.

Öłütçü, G., Testik, Ö M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers and Security, 56*, 83-93.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Systems Security, 15*(5), 13-21.

Poliisi. Huijauksen monet muodot. Haettu 31.3.2019 osoitteesta http://www.poliisi.fi/rikokset/huijaukset.

Pouryousefi, S., & Frooman, J. (2019). The consumer scam: an agency-theoretic approach. *Journal of Business Ethics*, *154*(1), 1-12.

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. *Information and Computer Security, 25*(2), 206-222.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior, 60*, 35-43.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014-1023.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559.

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

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.