Kanditutkielma

Tietojenkäsittelytieteen kandiohjelma

Käyttäjän manipulointi

Tuomas Aaltonen

16.12.2021

Matemaattis-luonnontieteellinen tiedekunta

Helsingin yliopisto

Yhteystiedot

PL 68 (Pietari Kalmin katu 5)
00014 Helsingin yliopisto

Sähkopostiosoite: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Study programme
Matemaattis-luonnontieteellinen tiedekunta	Tietojenkäsittelytieteen kandiohjelma

Tekijä — Författare — Author

Tuomas Aaltonen

Työn nimi — Arbetets titel — Title

Käyttäjän manipulointi

Ohjaajat — Handledare — Supervisors

FT Tommi Meskanen

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kanditutkielma	16.12.2021	24 sivua

Tiivistelmä — Referat — Abstract

Käyttäjän manipulointi (social engineering) on tietoturvahyökkäyksen muoto, jossa järjestelmän tietoturva ohitetaan käyttäjän inhimillisiä heikkouksia hyväksikäyttämällä. Se on kasvava ongelma niin Suomessa kuin maailmanlaajuisestikin. Suurin osa käyttäjän manipuloinnin hyökkäysmuodoista perustuu sosiaaliseen lähestymistapaan (social approach). Sosiaalisessa lähestymistavassa uhria suostutellaan tai ohjataan psykologisten menetelmien avulla toimimaan hyökkääjän toivomalla tavalla.

Käyttäjän manipulointi -hyökkäykseen liittyy usein myös teknisen haavoittuvuuden hyödyntäminen, mutta aina sellaista ei tarvita. Käyttäjän koulutus ja muut ihmislähtöiset tavat ovatkin avainasemassa käyttäjän manipulointia torjuttaessa. Tekniset apuvälineet ja ratkaisut kuitenkin tukevat käyttäjää. Tässä tutkielmassa pyritään kirjallisuuskatsauksen pohjalta kuvailemaan, mihin käyttäjän manipulointi pohjautuu, miten se käytännössä ilmenee ja miten siihen voidaan varautua.

ACM Computing Classification System (CCS)
Security and privacy → Human and societal aspects of security and privacy → Social aspects of security and privacy
Social and professional topics → Computing / technology policy → Computer crime → Social engineering attacks → Phishing
Security and privacy → Software and application security → Social network security and privacy

Avainsanat — Nyckelord — Keywords

tietoturva, käyttäjän manipulointi, tietojenkalastelu

Säilytyspaikka — Förvaringsställe — Where deposited

Helsingin yliopiston kirjasto

Muita tietoja — övriga uppgifter — Additional information

Sisällys

1 Johdanto

Rikoksen uhriksi joutuminen lienee jo nyt todennäköisempää verkossa kuin fyysisessä maailmassa ja kyberrikollisuus on edelleen nopeiten kasvava rikollisuuden ala. Koronaviruspandemia on kiihdyttänyt digitalisaatiota ja tehnyt ihmiset entistä riippuvaisemmaksi digitaalisista järjestelmistä. FBI:n mukaan viranomaisten tietoon tullut kyberrikollisuus aiheutti USA:ssa vuonna 2020 ennätykselliset 4,2 miljardin dollarin vahingot (”FBI: Internet Crime Report 2020”, 2021). Maailmanlaajuisesti kyberrikollisuuden arvioidaan aiheuttavan vuonna 2021 kuuden biljoonan ja vuonna 2025 jo 10,5 biljoonan dollarin vahingot*.

Kyberrikollisuus on kasvava ja merkittävä uhka sekä yksilölle että yhteiskunnalle myös Suomessa. Julkisuudessa nostetaan lähes päivittäin esille uusia digitaalisilla alustoilla tapahtuvia huijausyrityksiä ja psykoterapiakeskus Vastaamon tietomurto vuonna 2020 sai kansainvälistäkin huomiota. Kaikkiaan Suomen poliisi kirjasi vuonna 2020 noin 20 600 nettipetosta, yli 4 400 identiteettivarkautta ja noin 1030 tietomurtoa koskevaa rikosilmoitusta**. Vuonna 2021 rikoksien määrä on ollut edelleen kasvussa ja vuoden suurimpien nettipetosten kokonaisuuksissa, kuten pankkien nimissä tehdyissä tietojenkalastelu-hyökkäyksissä, rikoshyödyt lasketaan kymmenissä miljoonissa euroissa.

Kyberrikollisuuden suosioon on monia syitä. Internetissä tapahtuva kyberrikollisuus ei tunne alueellisia rajoja ja hyökkääjät voivat toimia globaalisti. Tietoturvarikoksen houkuttelevuutta lisää myös etäisyys uhriin ja huomattavan pieni kiinnijäämisriski (Conteh ja Schmick, 2016). Oikeudessa pitävien todisteiden hankkiminen on hankalaa ja kansainvälinen yhteistyö kyberrikollisten kiinni saamiseksi ei ainakaan vielä ole täysin saumatonta. Kyberrikollisten joukko koostuu lisäksi poikkeuksellisen moninaisesta joukosta toimijoita täysin erilaisine motivaatioineen. Rikoksen tekijä voi olla yksittäinen henkilö, rikollisjärjestö tai jopa valtio.

Tietoturvarikokseen liittyy usein *käyttäjän manipulointi* tai *sosiaalinen manipulointi* (social engineering). Tietojenkalastelu (phishing) – yksi käyttäjän manipulaation alle luokitelluista hyökkäysmuodoista – on tietoturvarikoksista yleisin uhrimäärällä mitattuna. Esimerkiksi USA:ssa raportoitiin vuonna 2020 241 342 tietojenkalasteluhyökkäyksen uh-

*https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ Haettu 16.12.2021

**https://poliisi.fi/blogi/-/blogs/tietoverkkorikollisuus-poliisin-silmin-2020-2021 Haettu 16.12.2021

ria (”FBI: Internet Crime Report 2020”, 2021). Luku on yli kaksi kertaa suurempi kuin seuraavaksi yleisimmän tietoturvarikoksen uhrimäärä. Käyttäjän manipulointi, kuten tietojenkalastelu, perustuu tavallisesti sosiaalisen lähestymistapaan (social approach). Hyökkäyksen suorittamiseen ei välttämättä tarvita teknisen haavoittuvuuden hyödyntämistä, eikä hyökkäystä vastaan toisaalta voi puolustautua pelkästään teknisin keinoin. Tämä erottaa käyttäjän manipuloinnin muista tietoturvahyökkäyksistä.

Tässä tutkielmassa käyttäjän manipulointia tarkastellaan ajankohtaisen kirjallisuuskatsauksen pohjalta. Käyttäjän manipulointi on monitieteellinen kokonaisuus, mutta tutkielmassa ilmiötä lähestytään erityisesti tietoturvan näkökulmasta ja psykologinen puoli jätetään suppeammaksi. Tutkielmassa pyritään kuvailemaan, mihin käyttäjän manipulaatio pohjautuu, miten se käytännössä ilmenee ja miten siihen voidaan varautua.

Toisessa luvussa käydään läpi käyttäjän manipulaation käsitettä ja sen erityispiirteitä tietoturvahyökkäyksenä. Luvussa esitellään myös eräs suosittu tapa luokitella käyttäjän manipulaatiota. Kolmannessa luvussa tarkastellaan tärkeimpiä yksittäisiä käyttäjän manipulaation hyökkäysmuotoja, kuten jo edellä mainittua tietojenkalastelu-hyökkäysmuotoa ja sen eri variaatioita. Neljännessä luvussa käsitellään menetelmiä, joiden avulla käyttäjän manipulaatiota on mahdollista ehkäistä. Luvussa viisi pohditaan lyhyesti, miten käyttäjän manipulaation hyökkäys- ja torjuntamuodot kehittyvät.

2 Käyttäjän manipulointi

Sosiaalinen manipulointi (social engineering) on vanha termi, englanninkielisenä sitä on käytetty jo 1800-luvun lopussa (Pisani, 1983). Ilmiönä se lienee yhtä vanha kuin ihminenkin. Sosiaalinen manipulointi on psykologista manipulointia, jonka tarkoitus on saada manipuloinnin kohde tekemään tai päättämään jotain manipuloinnin suorittajan toivomalla tavalla. Tietoturvakirjailija ja -konsultti Christopher Hadnagy määrittelee sosiaalisen manipuloinnin ”kaikiksi teoiksi, jotka saavat henkilön ryhtymään toimiin, jotka ovat tai eivät ole hänen etunsa mukaisia” (Hadnagy, 2011).

Ihmiset käyttävät sosiaalista manipulointia jatkuvasti elämässään – tietoisesti tai vähemmän tietoisesti. Sosiaalisessa manipuloinnissa pyritään käyttämään hyväksi perustunteita ja muita inhimillisiä ominaisuuksia, kuten ahneutta, pelkoa tai uteliaisuutta. Monet ammattikunnat, kuten poliitikot, psykologit, lakimiehet, lääkärit ja myyjät hyödyntävät sosiaalista manipulointia työssään (Hadnagy, 2011). Vanhemmat käyttävät usein sosiaalisen manipuloinnin keinoja hyödykseen lastensa kanssa kommunikoidessaan. Toisaalta myös lapset osaavat jo varhain hyödyntää sosiaalista manipulointia saadakseen vanhemmat toimimaan haluamallaan tavalla. Esimerkkejä löytyy kaikkialta. Tämä luku avaa käsitettä tietoturvan näkökulmasta.

2.1 Tietoturvauhka digitaalisessa ympäristössä

Tietoturvan kontekstissa social engineering suomennetaan yleensä ”käyttäjän manipuloinniksi”. Käyttäjä on tietoturvarikollisen hyökkäyksen ja manipuloinnin uhri. Tietoturvahyökkäyksessä tapahtuva käyttäjän manipulointi pohjautuu samojen ominaisuuksien ja käyttäytymismallien hyödyntämiseen kuin kaikki muukin sosiaalinen manipulointi. Kuitenkin, toisin kuin useilla muilla elämän osa-alueilla, tietoturvan yhteydessä onnistuneen manipuloinnin kohteeksi joutuminen on lähes aina vahingollista (Hadnagy, 2011). Manipuloinnin suorittajalla eli hyökkääjällä on taustalla motiivi, joka on usein ristiriidassa uhrin edun kanssa. Joskus hyökkääjä voi yrittää saada uhrin lähettämään itselleen esimerkiksi rahaa. Yleensä käyttäjää kuitenkin manipuloidaan luovuttamaan hyökkääjälle yksityistä, arkaluontoista tai muuten luottamuksellista informaatiota.

Digitaalinen ympäristö on luonut hyökkääjille erityisen otolliset olosuhteet käyttäjän ma-

nipuloinnille 2000-luvun aikana. Ihmisten välinen kommunikaatio ja tietojen jakaminen tapahtuu yhä enemmän verkon välityksellä lukuisten eri sovellusten ja alustojen kautta. Internetin hyvin heterogeeninen ja jatkuvasti päivittyvä dynaaminen ympäristö takaa sen, että uusia tietoturva-aukkoja syntyy jatkuvasti lisää. Erityisesti nollapäivähaavoittuvuuksia yhdistetään menestyksekkäästi käyttäjän manipulointiin (Krombholz et al., 2015). Hyökkääjien mieleen ovat myös sosiaaliset mediat, joiden käyttö on osa useimpien ihmisten päivittäistä rutiinia. Niissä jaetaan tyypillisesti paljon henkilökohtaista tietoa ilman, että asiaa ajateltaisiin tietoturvan näkökulmasta.

Myös työpaikat ovat mukautuneet digitalisaation myötä. Koronaviruspandemia on vain kiihdyttänyt muutosta. Työtä tehdään paljon etänä ja usein työntekijän omalla laitteella, erityisesti tietotyöntekijöiden (knowledge worker) keskuudessa (Krombholz et al., 2015). Perinteinen kasvotusten tapahtuva kommunikaatio on vähentynyt. Pienenkin yrityksen työntekijät saattavat työskennellä eri mantereilla tapaamatta koskaan toisiaan fyysisesti. Tietoa jaetaan ja hallitaan kolmansien osapuolien palveluiden kautta. Työntekijä saattaa jakaa luottamuksellista tietoa, vaikka toisen osapuolen tunnistaminen olisikin pelkän virtuaalisen profiilin tai sähköpostiosoitteen varassa.

Kuten useimpia muitakin tietoturvahyökkäyksiä, myös käyttäjän manipulaatiota kohdistetaan kaikkialle yhteiskuntaan: yksityishenkilöihin, pieniin ja suuriin yrityksiin, valtioiden hallintoihin, julkisiin toimijoihin ja muihin organisaatioihin. Onnistuneen manipulointihyökkäyksen uhreiksi ovat 2010-luvulla joutuneet mm. sosiaalisen median jättiläiset Facebook ja Twitter, johtavat teknologiayritykset Apple ja Google sekä yhdysvaltaisen RSA-tietoturvatalo (Krombholz et al., 2015).

2.2 Poikkeuksellinen tietoturvahyökkäyksen muoto

Käyttäjän manipulointi eroaa muista tietoturvahyökkäyksistä oleellisesti siinä, että hyökkäys kohdistuu suoraan käyttäjään ja hänen inhimillisiin heikkouksiinsa. Usein käyttäjän manipulaatioon liittyy myös tekninen haavoittuvuus, mutta aina sellaista ei tarvita. Ilmiön asiantuntijat (mm. Hadnagy, 2011; Krombholz et al., 2015; Conteh ja Schmick, 2016) ovat yhtä mieltä siitä, että käyttäjän manipulaatiota on mahdotonta estää vain teknisillä suojautumiskeinoilla. Käyttäjän manipulointi on siksi ylivertainen tapa päästä käsiksi suojattuihin tietoihin. Se mahdollistaa järjestelmän suojauksen ohittamisen riippumatta tietoturvan teknisen tasosta.

Käyttäjät myös tyypillisesti yliarvioivat kykynsä tunnistaa manipulaatioyritykset (Qin

ja Burgoon, 2007). Lisäksi hyökkäykset kehittyvät ja saavat uusia piirteitä jatkuvasti. Sähköposti on perinteisin ja yleisin kanava käyttäjän manipulaatioon ja sähköpostitse tapahtuvat hyökkäykset tunnistetaankin verrattain hyvin. Sen sijaan esimerkiksi verkon pilvi- ja yhteisöpalveluiden kautta tapahtuvat manipulaatioyritykset yllättävät käyttäjät helpommin (Krombholz et al., 2015).

2.3 Taksonomia ilmiön luokitteluun

Käyttäjän manipulaatio on laaja ja monitahoinen kokonaisuus, jota voidaan purkaa ja luokitella monella tapaa. Krombholz ja muut rakentavat artikkelissaan (Krombholz et al., 2015) taksonomian (taxonomy), jossa eri hyökkäysmuotoja luokitellaan hyökkäyksissä käytettyjen lähestymistapojen, kanavien sekä hyökkäyksen suorittajan perusteella (Taulukko 2.1).

Käyttäjän manipulaatiosta puhuttaessa tärkein lähestymistapa on sosiaalinen lähestymistapa (social approach). Sosiaalisessa lähestymistavassa uhria suostutellaan tai ohjataan toimimaan hyökkääjän toivomalla tavalla psykologista manipulaatiota hyödyntäen. Käyttäjän manipuloinnissa käytettäviä psykologisia menetelmiä käydään läpi seuraavassa aliluvussa 2.4. Hyökkääjä rakentaa sosiaalisessa lähestymistavassa suhdetta uhriin tyypillisesti pitkän aikaa, jolloin onnistuneen hyökkäyksen mahdollisuus kasvaa merkittävästi. Ainakin vielä 2000-luvun taitteessa sosiaalisen lähestymistavan vallitseva yhteydenpitoväline oli puhelin (Granger, 2001). Vuonna 2021 käyttäjän manipulointia tapahtuu edelleen puhelimitse matkapuhelinten ja VoIP:n (IP-puhe) välityksellä, mutta sähköpostin, tekstiviestien ja muun kirjallisen verkkoviestinnän osuus sosiaalisessa lähestymistavassa lienee kasvanut huomattavasti.

Fyysisellä lähestymistavalla (physical approach) tarkoitetaan sananmukaisesti toimintatapaa, johon liittyy jokin reaalimaailman fyysinen toiminto. Perinteinen fyysinen lähestymistapa on ollut organisaatioiden roskasäiliöiden penkominen (dumpster diving), jossa hyökkääjä voi etsiä roskien joukosta esimerkiksi henkilö- tai kirjautumistietoja. Digitalisaation myötä dokumentit liikkuvat kuitenkin yhä useammin vain sähköisessä muodossa.

Teknisessä lähestymistavassa hyödynnetään jotain teknistä alustaa, pääsääntöisesti internetiä. Useimmat ihmiset käyttävät samaa salasanaa kaikissa verkkopalveluissa (Granger, 2001). Tämä on yksi merkittävä tekijä, joka tekee internetistä erityisen houkuttelevan ympäristön käyttäjän manipulaatiolle. Salasanoja ja muita tietoja voidaan yrittää kerätä uhreilta esimerkiksi hyökkääjän luomien valeverkkosivujen kautta. Lisäksi hyökkääjä voi

Hyökkäysmuotojen taksonomia							
	Tietojen-kalastelu	Olan yli kurkki-minen	Roskien penko-minen	Käänteinen manipu-lointi	Tauko-paikka	Edistynyt jatkuva uhka	Houkut-telu
Kanava							
Sähköposti	✓			✓		✓	
Pikaviestimet	✓			✓			
Puhelin, VoIP	✓			✓			
Sosiaalinen media	✓			✓			
Pilvi	✓						
Verkkosivusto	✓				✓	✓	
Fyysinen	✓	✓	✓	✓			✓
Toimija							
Ihminen	✓	✓	✓	✓			✓
Ohjelmisto	✓		✓	✓	✓	✓	
Tyyppi							
Fyysinen		✓	✓				✓
Tekninen					✓	✓	
Sosiaalinen				✓			
Sosio-tekninen	✓			✓	✓	✓	✓

Taulukko 2.1: Taksonomia käyttäjän manipulaation hyökkäysmuotojen luokitteluun suomeksi käännettynä (Krombholz et al., 2015).

hyötyä verkosta suuresti jo ennen varsinaista kontaktia uhriin. Internet on erinomainen paikka kerätä informaatiota potentiaalisesta kohteesta. Varsinkin sosiaalisissa medioissa ja yhteisöissä tietoja jaetaan hyvin varomattomasti. Yrityksistä ja henkilöistä löytyy huomattavan paljon yksityiskohtaista tietoa tavallisella hakukoneen käytöllä. On myös olemassa teknisiä apuvälineitä, joiden avulla tietoja voidaan kerätä entistäkin tehokkaammin. Yksi suosituimmista työkaluista tähän tarkoitukseen on ohjelmisto nimeltään Maltego. Maltego on linkkien analysointityökalu, joka tarjoaa reaaliaikaisen tiedon louhinnan ja tiedonkeruun sekä näiden tietojen esittämisen solmupohjaisessa kaaviossa *.

Onnistuneet hyökkäykset käyttävät eri vaiheissa monia tai jopa kaikkia edellä läpi käytyjä lähestymistapoja. Erityisen tehokasta on yhdistää tekninen ja sosiaalinen lähestymistapa, jolloin puhutaan sosio-teknisestä lähestymistavasta (social-technical approach). Sosio-teknistä lähestymistapaa hyödynnetään esimerkiksi tietojenkalastelu- ja houkutteluhyökkäyksissä, joita käsitellään tarkemmin aliluvuissa 3.1 ja 3.2.

Hyökkäys voidaan suorittaa joko ihmisen toimesta tai automatisoidusti ohjelmiston avulla. Ihmisen rajallinen kapasiteetti voi joskus olla esteenä laajamittaisen hyökkäyksen toteuttamiselle, mutta ohjelmistojen avulla hyökkäystä voidaan skaalata lähes loputtomasti. Ohjelmistoja hyödynnetään useimmissa hyökkäysmuodoissa.

Suosituin kanava käyttäjän manipuloinnin toteuttamiselle on sähköposti, mutta pikaviestintäpalvelujen suosio hyökkääjien keskuudessa on kasvussa. Myös puhelimitse ja VoIP:n kautta tapahtuva manipulaatio on edelleen yleistä. Hyökkääjän luomat tai hakkeroimat verkkosivut toimivat hyökkäysväylänä usein tietojenkalastelu- ja taukopaikkahyökkäyksien (waterholing) yhteydessä. Muita taksonomiaan sisällytettyjä hyökkäysväyliä ovat sosiaalinen media sekä pilvipalvelut.

2.4 Psykologiset menetelmät

Kyberrikollisuuden käyttäjän manipuloinnissa hyödynnetään samoja psykologisia vaikuttamisen ja suostuttelun keinoja kuin kaikessa muussakin sosiaalisessa tai psykologisessa manipuloinnissa. Keinoja ja tekniikoita lienee tuhansia, mutta suurimman osan niistä voi luokitella kuuden perusperiaatteen alle (Cialdini, 2009). Nämä periaatteet ovat vastavuoroisuus (reciprocity), johdonmukaisuus (consistency), auktoriteetti (authority), niukkuus (scarcity), pidettävyys (liking) ja sosiaalinen validointi (social proof). Periaatteet käydään

*https://www.maltego.com/ Haettu 16.12.2021

seuraavaksi läpi erityisesti Cialdinin kuvauksiin nojaten (Cialdini, 2009), mutta samat käsitteet esiintyvät muussakin kirjallisuudessa (mm. Hadnagy, 2011 ja Ghafir et al., 2016).

Vastavuoroisuudessa on kyse kiitollisuudenvelasta. Kun henkilö vastaanottaa lahjan, palveluksen tai kohteliaisuuden, tuntee hän velvollisuudekseen antaa jotain takaisin. Tarjoilijat saavat tutkitusti suurempia tippejä antaessaan laskun yhteydessä asiakkailleen makeisen – ja selvästi suurempia tippejä antaessaan vielä toisen ylimääräisen makeisen kertoen samalla asiakkaiden olleen erityisen mukavia (Strohmetz et al., 2002). Lobbaajat pyrkivät samaan vastavuoroisuuteen tarjotessaan poliitikoille illallisia tai vaalikampanjatukea. Käyttäjän manipulaatiossa hyökkääjä voi esimerkiksi lahjan antamisen yhteydessä kohteliaasti pyytää, että lahjan vastaanottaja lataisi ”tuotekatalogin” hyökkääjän ylläpitämältä verkkosivustolta (Hadnagy, 2011).

Ihmiset noudattavat todennäköisemmin ohjeita tai suosituksia, jos ne tulevat henkilöltä, jota he pitävät *auktoriteettina*. Auktoriteetti voi rakentua mm. lain, organisaation hierarkian, pukeutumisen tai tutkintonimikkeen ja muiden tittelien kautta (Hadnagy, 2011). Käyttäjän manipulaatiossa auktoriteetin hyödyntäminen osana hyökkäystä on varsin tyypillistä. Hyökkääjät voivat tekeytyä mm. viranomaisiksi, pankin edustajaksi, uhrin esimieheksi tai teknisen tuen asiantuntijaksi.

Mitä vähemmän jotain asiaa on olemassa, sitä enemmän ihmiset haluavat sitä. Kuluttajille suunnattu markkinointi on tyypillinen esimerkki *niukkuutta* hyödyntävästä sosiaalisesta manipuloinnista. Tarjoukset ovat voimassa rajoitetun ajan tai tuotetta on saatavilla rajoitettu määrä. Niukkuuteen liittyy tavallisesti siis ihmisen ahneus. Käyttäjän manipulointi -hyökkäyksissä uhria voidaan houkutella hyökkääjän sivustolle ”voitetun” palkinnon perässä. Käyttäjän manipuloinnissa pyritään rajoittamaan myös aikaa, jota hyökkäyksen kohteelle annetaan päätöksentekoon (Hadnagy, 2011). Kun uhrille luodaan kiireen tunne, on uhri alttiimpi manipuloinnille. Edellisen esimerkin palkinnon lunastamiseen voidaan antaa rajattu aika. Ajan niukkuuteen yhdistetään tavallisesti myös auktoriteetti (Hadnagy, 2011). Hyökkääjä voi esimerkiksi esimiehen nimissä vaatia tilisiirron tekemistä mahdollisimman nopeasti.

Ihmiset haluavat toimia elämässään *johdonmukaisesti*. Johdonmukaisuuteen liittyy sitoutuminen. Kun ihminen on panostanut resurssejaan – esimerkiksi aikaa tai rahaa – johonkin asiaan, on hän sitoutunut viemään projektin loppuun. Käyttäjän manipulaatiossa hyökkääjä voi aluksi suostutella uhria johonkin vähäpätöiseltä tuntuvaan tekoon (Hadnagy, 2011). Tämä pienen palveluksen tai myönnytyksen saaminen ei ole hyökkääjän todellinen päämäärä. Kuitenkin sitouttamisen kautta uhri luovuttaa hyökkääjälle jatkossa todennä-

köisemmin tiedon tai muun hyödykkeen, jota hyökkääjä lopulta tavoittelee.

Ihminen on taipuvaisempi suostumaan pyyntöön, jos pyyntö tulee henkilöltä, josta ihminen pitää. *Pidettävyys* rakentuu muutaman keskeisen tekijän perusteella. Näitä tekijöitä ovat henkilön ulkonäkö, samankaltaisuus ja mahdollisesti jopa tärkeimpänä se, että henkilö vaikuttaa pitävän meistä itsestämme. Pitämisen voi osoittaa esimerkiksi kehumalla ja hymyilemällä. Toisaalta ihmiset vaistoavat teeskentelyn helposti, ja pidettävyyden rakentaminen voi olla vaikeampaa kuin se aluksi kuulostaa (Hadnagy, 2011).

Sosiaalisella validoinnilla tarkoitetaan ihmisen luontaista tarvetta toimia samalla tavalla kuin muut ihmiset. Puhutaan myös laumakäyttäytymisestä. Esimerkiksi verkkokaupat hyödyntävät ilmiötä näyttämällä, mitä muut asiakkaat ovat ostaneet, tai mitkä tuotteet ovat suosituimpia. Sosiaalinen validointi on erityisen vahva työkalu, kun ihminen on epävarma ja tilanne on epäselvä (Hadnagy, 2011). Tällaiset olosuhteet ovat tyypillisiä käyttäjän manipulaatiossa. Väärennettyjen palautteiden tai kommenttien kirjoittaminen, mahdollisesti sosiaalisessa mediassa luotujen valeprofiilien kautta, on eräs hyökkääjien käyttämä sosiaalista validointia hyödyntävä tekniikka. Ihminen voi epäröidä esimerkiksi jonkin tiedoston lataamista, mutta latauslinkin alla olevat positiiviset kommentit saattavat olla ratkaiseva tekijä päätöksenteossa.

Näiden kuuden Cialdinin periaatteen lisäksi on syytä mainita *uteliaisuus*, jota ei voi helposti luokitella minkään muun periaatteen alle, mutta jota hyödynnetään käyttäjän manipulointi -hyökkäyksissä jatkuvasti. Uhrin uteliaisuutta käytetään hyväksi esimerkiksi houkuttelu- ja tietojenkalasteluhyökkäyksissä (Krombholz et al., 2015). Linkkejä ja tiedostoja pyritään nimeämään mahdollisimman houkuttelevasti, jotta uhrin mielenkiinto heräisi. Apuna voidaan käyttää esimerkiksi ajankohtaisia tapahtumia tai julkisuuden henkilöitä (Abraham ja Chengalur-Smith, 2010).

Käyttäjän manipulaation hyökkäysmuodot ja niissä käytettävät teknologiat kehittyvät kaiken aikaa, mutta psykologiset menetelmät eivät pohjimmiltaan juurikaan muutu. Manipulointi pohjautuu aina samoihin inhimillisiin ominaisuuksiin. Hyökkäysmuodosta ja hyökkäyksen taustatarinasta riippuen menetelmiä voidaan hyödyntää eri tavoin. Käyttäjän manipulaation tapahtuessa verkossa kirjallisen viestinnän kautta, ovat sosiaalisen kanssakäymisen vaikuttamismahdollisuudet hieman rajatummat. Hyökkääjän on vaikeaa tai mahdotonta vaikuttaa uhriin esimerkiksi ulkonäöllä, (mikro)ilmeillä tai äänenpainoilla. Verkossa hyökkääjän on toisaalta helpompi hyödyntää esimerkiksi tekaistua auktoriteettia. Hyökkääjä ei juuri koskaan esiinny omana itsenään käyttäjän manipulointi -hyökkäyksessä (Hadnagy, 2011).

3 Hyökkäysmuodot

Tässä luvussa käydään läpi taksonomiassa esiteltyjä hyökkäysmuotoja (Taulukko 2.1). Ne ovat yleisestikin käyttäjän manipuloinnin tunnetuimpia ja tärkeimpiä hyökkäysmuotoja. Luvun lopussa käsitellään lisäksi joitakin merkittäviä hyökkäysmuotoja taksonomian ulkopuolelta.

3.1 Tietojenkalastelu

Tietojenkalastelu (phishing) on sosio-tekniseen lähestymistapaan perustuva, suosittu hyökkäysmuoto. Hyökkäys suoritetaan sähköpostin, tekstiviestin tai pikaviestipalvelun kautta. Samaa kalasteluviestiä lähetetään suurelle joukolle käyttäjiä roskapostin tapaan. Tämä eroaa tyypillisestä käyttäjän manipulaatiosta, joka on tavallisesti suunnattu yksittäiselle käyttäjälle tai rajatulle käyttäjäryhmälle (Krombholz et al., 2015). Perinteisen tietojenkalasteluhyökkäyksen tekijät luottavat kuitenkin enemmän määrään kuin laatuun. Hyökkäyksen toivotaan onnistuvan tarpeeksi monen käyttäjän kohdalla niin, että toiminta on kannattavaa.

Käyttäjän vastaanottamassa viestissä on tavallisesti linkki, joka johtaa hyökkääjän ylläpitämälle sivustolle(Krombholz et al., 2015). Sivuston kautta kalastellaan käyttäjän tietoja, esimerkiksi henkilötietoja, kirjautumistietoja tai luottokortin numeroa. Sivusto voi näyttää jonkin tunnetun organisaation tai palvelun sivustolta, kuten pankin tai sosiaalisen median kirjautumissivulta. Kirjautumisen jälkeen käyttäjä voidaan uudelleen ohjata oikealle sivustolle niin, ettei käyttäjä huomaa mitään erikoista.

Toinen yleinen tapa on asettaa viestin liitteeksi tiedosto, joka sisältää haittaohjelman (Krombholz et al., 2015). Jos käyttäjä avaa tiedoston, voi haittaohjelma antaa hyökkääjälle etäkäyttöoikeuden laitteeseen. Haittaohjelma hyödyntää tyypillisesti nollapäivähaavoittuvuutta. Tätä tapaa käytetään erityisesti yrityksiin kohdistuvissa kalasteluhyökkäyksissä. Menetelmä mahdollistaa murtautumisen myös yrityksien hyvin suojattuihin sisäverkkoihin.

Massoittain tapahtuvat tietojenkalasteluhyökkäykset eivät kuitenkaan aina tuota hyökkääjälle toivottua tulosta. Sen rinnalle onkin syntynyt kohdennettua tietojenkalastelua

(spear phishing). Tällaisessa hienostuneemmassa kalasteluyrityksessä kohderyhmä on huomattavasti rajatumpi ja hyökkäyksen eteen nähdään enemmän vaivaa (Krombholz et al., 2015). Potentiaalisista uhreista kerätään tietoja – usein ohjelmallisesti – mm. sosiaalisesta mediasta ja organisaatioiden kotisivuilta. Uhrin lisäksi tietoja kaivetaan myös uhrin lähipiiristä ja kalasteluviesti voidaan yrittää naamioida esimerkiksi ystävän tai kollegan lähettämäksi. Hyökkääjä voi tutkia organisaation ajankohtaisia tapahtumia tai mistä ja millaisella kieliasulla uhri keskustelee ystäviensä kanssa. Viesti laaditaan niin, että se vaikuttaa aidosti uhrin ystävän tai kollegan lähettämältä.

Kohdennettujen tietojenkalasteluhyökkäyksien onnistumisprosentti on huomattavasti perinteistä tapaa suurempi ja sen suosio hyökkääjien keskuudessa on kasvussa. Eräs tutkimus osoitti, että hyökkäyksen onnistumisprosentti nousi 16:sta 72:een, kun kalasteluviesti näytti tulleen tuntemattoman henkilön sijaan käyttäjän ystävältä (Jagatic et al., 2007).

Googlea ja Facebookia vastaan vuosina 2013-2015 kohdistettu hyökkäys on tiettävästi rikoshyödyltään suurin yksittäinen käyttäjän manipulaatio -hyökkäys*. Se toteutettiin kohdennetun tietojenkalastelun avulla. Hyökkäyksen takana ollut liettualaismies esiintyi Googlen ja Facebookin suurimman tavarantoimittajan, tietokonevalmistaja Quanta Computerin edustajana (”Social engineering scams ensnare Google, Facebook and their users”, 2017). Tavarantoimittajan nimissä hän onnistui laskuttamaan väärennetyillä asiakirjoilla yli 100 miljoonan dollarin edestä tuotteita ja palveluja hyökkäystä varten luomille tileilleen ennen kiinnijäämistään.

Kalasteluhyökkäyksen kohteena oli rajattu joukko yrityksien Google Docs -palvelua käyttäviä työntekijöitä. Mies lähetti heille sähköpostin, joka kertoi jonkun jakaneen dokumentin Google Docs -palvelussa sähköpostin vastaanottajan kanssa. Kun käyttäjä klikkasi viestissä ollutta aidon näköistä avaa-painiketta, ilmestyi näytölle viesti, jossa pyydettiin Google Docsille lupaa hallita yhteystietoja sekä lukea, lähettää, poistaa ja hallita sähköposteja. Kyseessä ei kuitenkaan ollut oikea Google Docs -palvelu vaan Googlen alustalla toimiva – ilmeisesti hyökkääjän luoma – samanniminen sovellus.

Tietojenkalastelusta voidaan eriyttää omiksi alakategorioikseen myös muita variaatioita. Valaanpyynnistä (whaling) puhutaan, kun hyökkäys kohdistetaan organisaation korkean profiilin henkilöihin, kuten toimitusjohtajaan (Salahdine ja Kaabouch, 2019). Vhishing-hyökkäyksellä viitataan VoIP:n kautta ja SMiShing- tai SMSishing-hyökkäyksellä tekstiviestitse tapahtuvaan tietojenkalasteluun (Yeboah-Boateng ja Amanor, 2014).

*https://www.tessian.com/blog/examples-of-social-engineering-attacks/ Haettu 16.12.2021

Suomessa tekstiviestitse tapahtuvaa tietojenkalastelua on tehty viime vuosina esimerkiksi Postin nimissä**. Uhreille lähetetyissä tekstiviesteissä oli tekaistu paketin saapumisilmoitus. Viestin vastaanottaja joutui identiteettivarkauden uhriksi tunnistautuessaan pankkitunnuksillaan tekstiviestissä olleen linkin kautta. Hyökkääjät hakivat varastettujen henkilötietojen avulla lainoja rahoitusyhtiöiltä. Rikoshyötyä hyökkääjät saivat yhteensä noin 375 000 euroa.

3.2 Houkuttelu

Houkutteluhyökkäys (baiting) on esimerkki hyökkäysmuodosta, joka voi yhdistää kaikki aliluvussa 2.3 kuvatut lähestymistavat. Teknistä lähestymistapaa hyödynnetään ainakin hyökkäyksen valmisteluvaiheessa, jolloin tallennusvälineeseen, kuten USB-muistitikkuun, asennetaan haittaohjelma. Lisäksi uhria on mahdollisesti profiloitu verkossa. Samalla on saatettu etsiä vihjettä siitä, minne tallennusväline kannattaisi ”unohtaa”.

Fyysinen lähestymistapa otetaan käyttöön, kun tallennusväline viedään syötiksi jonnekin, josta hyökkäyksen kohde sen todennäköisesti löytää. Organisaatioon kohdistuvassa hyökkäyksessä tallennusväline voidaan yrittää ujuttaa organisaation tiloihin, mutta myös julkiset paikat, kuten kahvilat tai parkkipaikat, ovat hyökkääjien suosiossa (Krombholz et al., 2015).

Sosiaalinen lähestymistapa pohjautuu houkutteluhyökkäyksessä ihmisen uteliaisuuden hyödyntämiseen. Uhrin toivotaan olevan tarpeeksi utelias poimiakseen tallennusvälineen mukaansa ja yhdistääksensä sen omaan laitteeseensa. Ihmisen uteliaisuutta hyödynnetään lisäksi nimeämällä tallennusvälineen tiedostot houkuttelevasti, kuten ”henkilöstön irtisanomissuunnitelma 2021” (Krombholz et al., 2015).

Houkutteluhyökkäykseen ei aina tarvita fyysistä lähestymistapaa (Conteh ja Schmick, 2016). Se voidaan suorittaa myös verkossa, jossa uhri houkutellaan esimerkiksi mainoksien avulla painamaan linkkiä, joka johtaa rikollisen luomalle valesivustolle. Valesivustolla uhri yritetään saada luovuttamaan tietoja tai lataamaan haittaohjelma.

**https://poliisi.fi/-/poliisi-tutkii-viime-vuonna-tapahtunutta-mittavaa-petosaaltojen-kokonaisuutta Haettu 16.12.2021

3.3 Käänteinen manipulointi

Käänteinen käyttäjän manipulaatio (reverse social engineering) on epäsuorasti toteutettu hyökkäys, jossa aloitteen uhrin ja hyökkääjän väliselle kommunikaatiolle tekee uhri. Uhri uskoo hyökkääjän olevan jokin luotettava taho, esimerkiksi teknisen tuen edustaja. Hyökkäys voidaan tyypillisesti jakaa kolmeen eri vaiheeseen, jotka ovat *sabotointi* (sabotage), *mainostaminen* (marketing) ja *tuki* (support) (Granger, 2001). Hyökkääjä luo uhrille aluksi ongelmatilanteen, kuten teknisen vian tai illuusion sellaisesta. Tämän jälkeen uhrille vihjataan esimerkiksi mainonnan muodossa, että luotettavana tahona esiintyvällä hyökkääjällä olisi ratkaisu ongelmaan. Kun hyökkääjä saa yhteydenoton uhrilta, hyökkääjä tarjoaa uhrille ratkaisumallia, mutta pyrkii samalla pääsemään käsiksi tavoittelemiinsa tietoihin. Hyökkääjä voi ilmoittaa tarvitsevansa esimerkiksi käyttäjän salasanan ongelman ratkaisemiseksi.

3.4 Taukopaikka

Taukopaikkahyökkäyksen (waterholing) englanninkielinen termi viittaa eläinten juomapaikkaan, jossa saalistaja vaanii uhrejaan. Tietoturvarikollisuuden kontekstissa juomapaikalla viitataan sivustoon, jossa potentiaaliset uhrit säännöllisesti vierailevat. Hyökkääjä ei siis kohdista hyökkäystään suoraan uhriin, vaan uhrin todennäköisesti vierailemaan sivustoon. Hyökkääjä murtautuu sivustolle ja saastuttaa sen haittaohjelmalla, joka latautuu uhrin laitteelle.

Vuonna 2013 tapahtuneen taukopaikkahyökkäyksen uhreiksi joutui suuri joukko maailman johtavien teknologiayrityksien IT-ammattilaisia (Krombholz et al., 2015). Hyökkääjä murtautui ensiksi iOS:n parissa työskentelevien ohjelmistokehittäjien suosimalle keskustelufoorumille nimeltään *IPhoneDevSDK*. Hyökkääjä asensi verkkosivustolle Javan nollapäivähaavoittuvuutta hyödyntäneen haittaohjelman, jonka avulla hyökkääjä pääsi edelleen murtautumaan sivustolla vierailleiden käyttäjien laitteisiin. Hyökkäyksen seurauksena ainakin Applen ja Facebookin, väitetysti myös Twitterin, sisäisiin verkkoihin murtauduttiin.

3.5 Edistynyt jatkuva uhka

Edistynyt jatkuva uhka (APT, advanced persistent threat) ei ole yksittäinen hyökkäystekniikka vaan laveampi termi pitkäkestoiselle, kohdennetulle hyökkäysmuodolle. APT-hyökkäys saattaa kestää kuukausia tai jopa vuosia ja hyökkäykset kohdennetaan isoihin toimijoihin (Krombholz et al., 2015). Hyökkäys vaatii paljon resursseja ja sen takana onkin usein voimakas taho, kuten valtio. Hyökkäys hyödyntää tavallisesti kohdennettua tietojenkalastelu- ja/tai taukopaikkahyökkäystä.

3.6 Muita muotoja

Edellisten lisäksi taksonomiassa nostetaan esille jo edellisessä luvussa mainittu organisaatioiden roskasäiliöiden penkominen sekä olkapään yli kurkkiminen (shoulder surfing). Ne ovat kumpikin tavanomaisia fyysiseen lähestymistapaan nojaavia hyökkäysmuotoja.

Taksonomian ulkopuolelta on syytä mainita suosittu sosio-tekniseen lähestymistapaan perustuva ponnahdusikkunahyökkäys (pop-up windows). Ponnahdusikkunahyökkäyksessä käyttäjää yritetään manipuloida painamaan linkkiä, joka johtaa hyökkääjän ylläpitämälle sivustolle (Salahdine ja Kaabouch, 2019). Ponnahdusikkunassa voidaan esimerkiksi ilmoittaa laitteelta löytyneestä viruksesta, jonka voisi väitetysti poistaa linkin kautta löytyvien ohjeiden avulla. Sivustolla uhrilta voidaan yrittää kalastella tietoja tai uhrin konetta voidaan yrittää saastuttaa haittaohjelmalla.

Muita merkittäviä käyttäjän manipuloinniksi luokiteltavia hyökkäysmuotoja ovat mm. hieman tietojenkalastelun kaltainen tekniikka nimeltään sivustoharhautus (pharming) sekä perässä roikkumis -hyökkäys (tailgating), jossa hyökkääjä livahtaa esimerkiksi yrityksen suljettuihin tiloihin talon työntekijän perässä. Vähemmän hienovaraisia fyysiseen lähestymistapaan perustuvia hyökkäyksiä ovat informaation fyysinen varastaminen tai sen kiristäminen.

4 Torjunta

Käyttäjän manipuloinnin tärkeimpänä torjuntakeinona nähdään koulutus ja tiedotus aiheesta (mm. Hadnagy, 2011; Krombholz et al., 2015; Conteh ja Schmick, 2016). Vaikka nämä ihmislähtöiset tavat ovatkin tärkeimmässä asemassa taistelussa käyttäjän manipulaatiota vastaan, myös teknisillä torjuntakeinoilla on oma merkittävä roolinsa. Koulutus on tehokas tapa torjua esimerkiksi tietojenkalasteluhyökkäyksiä, mutta riittämätön keino taukopaikkahyökkäyksiä vastaan suojautumisessa (Krombholz et al., 2015).

4.1 Ihmislähtöiset tavat

Käyttäjän manipulaation paras torjuntakeino on koulutettu käyttäjä. Siksi tietoisuuden levittäminen – erilainen koulutus ja tiedotus aiheesta – on tehokkain työkalu käyttäjän manipulaatiota ehkäistessä. Käytännössä tämä näkyy siten, että organisaatiot kouluttavat henkilöstöään ja palveluntarjoajat valistavat asiakkaitaan. Viranomaiset voivat varoittaa ajankohtaisista hyökkäysmuodoista omilla kanavillaan tai median kautta. Media luo tietoisuutta myös oman uutisointinsa kautta.

Koulutus ja tiedotus voi olla esimerkiksi käyttäjän manipulaation yleisimpiin ja uusimpiin hyökkäysmuotoihin perehtymistä tai yleistä turvallisten toimintamallien läpikäyntiä. Yrityksissä ja organisaatioissa koulutus räätälöidään luonnollisesti tarpeen mukaan, esimerkiksi henkilötietoja käsiteltäessä laki määrää tietyt velvoitteet. Organisaatiosta riippumatta koulutuksen ei kuitenkaan pitäisi olla vain kertaluontoinen tai edes säännöllisesti toistuva tapahtuma, vaan kiinteämpi osa organisaation kulttuuria (Hadnagy, 2011). Jokaisen organisaation tulisi sisällyttää tietoturva operatiivisiin tavoitteisiinsa (Conteh ja Schmick, 2016).

Vuonna 2011 julkaistu tutkimus osoittaa toistuvan koulutuksen tai ohjeistamisen tehokkuuden käyttäjän manipuloinnin torjunnassa (Bowen et al., 2011). Tutkimus suoritettiin kahden erillisen otoksen avulla (Taulukko 4.1). Kumpaankin otokseen kuului 2000 Columbian yliopiston opiskelijaa ja henkilökunnan jäsentä. Käyttäjille lähetettiin tietojenkalasteluhyökkäystä jäljittelevä yhteydenotto. Jos käyttäjä vastasi yhteydenottoon, lähettivät tutkijat hänelle myöhemmin sähköpostiviestin. Viestin vastaanottajalle kerrottiin, että henkilön toimintamalli asettaa henkilön alttiiksi tietojenkalasteluhyökkäyksille. Joitakin

viikkoja myöhemmin informoiduille käyttäjille lähetettiin uusi variaatio hyökkäyksestä. Otoksien tulokset olivat yhteneväisiä. Kahden ohjeistuksen jälkeen vain muutama yksittäinen käyttäjä harhautui, kolmannen ohjeistuksen jälkeen uhreja ei ollut enää yhtään. Näyttäisi siis siltä, että myös hitaammat oppijat sisäistävät turvallisen käyttäytymismallin muutaman muistutuksen jälkeen.

Koulutus on tehokkaampaa, kun erot käyttäjäryhmien välillä huomioidaan. Yrityksissä uudet työntekijät ovat muita työntekijöitä alttiimpia käyttäjän manipulaatiolle (Conteh ja Schmick, 2016). FBI:n mukaan riski joutua kyberrikoksen uhriksi kasvaa iän myötä ja FBI keskittääkin yhdessä IC3:n (Internet Crime Complaint Center) kanssa resurssejaan erityisesti yli 60-vuotiaiden ikäryhmän koulutukseen ("FBI: Internet Crime Report 2020", 2021). Koulutuksessa on myös syytä huomioida se, että ihmisryhmät ovat haavoittuvaisempia eri käyttäjän manipuloinnin muodoille. Naiset ovat miehiä alttiimpia aukaisemaan hyökkääjien lähettämiä sähköpostiviestejä jos ne näyttävät tulleen sosiaalisen median kautta (Conteh ja Schmick, 2016). Miehet sen sijaan lankeavat helpommin viesteihin, joissa vaikuttimena käytetään valtaa, rahaa tai seksiä. Yli 60-vuotiaat ihmiset joutuvat erityisesti mm. romanssihuijauksen (romance scam) uhriksi ("FBI: Internet Crime Report 2020", 2021).

Organisaatioissa on koulutuksen lisäksi tärkeää kiinnittää huomiota organisaation sisäisesti laatimaan tietoturvaohjeistukseen tai -politiikkaan (security policy) (Conteh ja Schmick, 2016). Käyttäjän manipuloinnin torjumiseksi tietoturvaohjeistuksen on hyvä sisältää ohjeita esimerkiksi salasanojen sekä fyysisen ja digitaalisen tiedon hallintaan (Ghafir et al., 2016). Salasanojen pitää olla riittävän monimutkaisia, ja niitä olisi hyvä vaihtaa säännöllisen tiheästi. Sekä fyysisessä että digitaalisessa muodossa oleva tieto pitää hävittää asianmukaisesti roskien penkomis -hyökkäysmuodon torjumiseksi. Muita organisaation tietoturvaohjeistukseen sisällytettäviä merkityksellisiä asioita ovat mm. fyysinen kulunvalvonta, digitaalinen pääsynhallinta sekä ohjeistus sille, minkälaisia tietoja organisaatiosta voi julkisesti kertoa (Ghafir et al., 2016). Ohjeistusta on lisäksi päivitettävä säännöllisesti.

Organisaation on tärkeää valvoa, että organisaation laatimaa tietoturvaohjeistusta myös noudatetaan (Conteh ja Schmick, 2016). Organisaatio voi käyttää apunaan esimerkiksi sisäisiä tai ulkopuoliselta taholta tilattua auditointeja. Auditoinneissa selvitetään, kuinka hyvin organisaation tietoturvaohjeistus toimii käytännössä. Muita keinoja tarkkailuun ovat verkkolokien, työntekijöiden käyttöoikeuksien sekä laitteiden konfiguraatioiden säännöllinen tarkastaminen (Conteh ja Schmick, 2016). Myös työntekijän oma vastuunkanto on tarpeellista (Ghafir et al., 2016). Kollegan tietoturvarikkomukset tai ohjeistuksen vas-

Tietojenkalasteluhyökkäyksillä saatujen vastauksien lukumäärä: 1. tutkimus				
Tyyppi	**1. kierros**	**2. kierros**	**3. kierros**	**4. kierros**
Sähköposti sisäisellä URL:lla	52	2	0	-
Sähköposti ulkoisella URL:lla	177	15	1	0
Kirjautumistieto-lomakkeet	39/20	4/1	0	-
PDF-liitetiedosto	45	0	-	-

Tietojenkalasteluhyökkäyksillä saatujen vastauksien lukumäärä: 2. tutkimus				
Tyyppi	**1. kierros**	**2. kierros**	**3. kierros**	**4. kierros**
Sähköposti sisäisellä URL:lla	69	7	1	0
Sähköposti ulkoisella URL:lla	176	10	3	0
Kirjautumistieto-lomakkeet	69/50	10/9	0	-
PDF-liitetiedosto	71	2	0	-

Taulukko 4.1: Taulukoidut tutkimustulokset suomeksi käännettynä (Bowen et al., 2011). Taulukon kolmannen rivin vinoviivan vasemmanpuoleinen luku ilmaisee niiden käyttäjien lukumäärän, jotka avasivat linkin kautta kirjautumistietoja pyytävän lomakkeen ja oikeanpuoleinen luku niiden käyttäjien lukumäärän, jotka myös täyttivät kirjautumistiedot lomakkeen avattuaan.

tainen toiminta tulisi aina raportoida organisaation johdolle.

Käyttäjän manipulaatiota torjuttaessa on tärkeää, että koulutus ja tietoturvaohjeistus suunnataan organisaation kaikille työntekijöille – eikä vain tietotyöläisille tai IT-osaston henkilökunnalle (Ghafir et al., 2016). Useimmat IT-osaston ulkopuoliset työntekijät uskovat, että tietoturva on vain IT-ammattilaisten huolenaihe. Tämä saattaa olla totta joidenkin tietoturvauhkien kohdalla, mutta käyttäjän manipulointia kohdistetaan kaikkialle. Siksi esimerkiksi siivoojien tai vastaanottovirkailijoiden jättäminen käyttäjän manipulaation torjuntaa käsittelevän koulutuksen tai tietoturvaohjeistuksen ulkopuolelle on hyvin huono käytäntö.

4.2 Tekniset tavat

Teknisillä tavoilla pyritään pääasiallisesti turvaamaan verkkoliikennettä. Organisaation jokaiseen laitteeseen tulisi asentaa perinteisen palomuurin lisäksi tunkeilijan havaitsemisjärjestelmä (Intrusion Detection System, IDS) ja murron estojärjestelmä (Intrusion Prevention System, IPS) (Conteh ja Schmick, 2016). Laitteissa, joita käytetään organisaation ulkoisessa tilassa, pitäisi käyttää demilitarisoituja alueita (demilitarized zone, DMZ) ja virtuaalista erillisverkkoa (Virtual Private Network, VPN). Organisaatio voi rajoittaa ulkoisen verkon käyttöä sallimalla pääsyn vain tietyille sivustoille verkkosuodattimen (web filter) avulla. Lisäksi kaikki käyttämättömät portit ja ohjelmat tulisi sulkea. Yhdessä nämä tekniikat ja ohjelmistot rakentavat kerroksittaisen suojan, jolloin yhden suojakerroksen pettäminen ei vielä vaaranna järjestelmän turvallisuutta (Conteh ja Schmick, 2016). Yksityishenkilönkin on mahdollista hyödyntää edellä mainituista ohjelmistoista ja tekniikoista suurinta osaa, usein myös kuluttajille suunnattuina versioina.

Käyttäjän manipulaation hyökkäysmuodoista esimerkiksi taukopaikkahyökkäyksiä on huomattavan vaikea torjua pelkällä käyttäjän koulutuksella. Jos hyökkäys livahtaa tietoturvaohjelmiston ohitse, ei käyttäjällä ole juurikaan mahdollisuuksia huomata hyökkäystä. Kohdennettu verkkosivujen valvonta on eräs mahdollinen tapa torjua taukopaikkahyökkäyksiä (Krombholz et al., 2015). Käytännössä tämä toteutetaan niin, että yritys selvittää suosituimmat sivustot työntekijöiden keskuudessa ja tarkkailee näitä sivustoja erityisen huolellisesti.

Yleinen tietoturvan tekninen kehitys edesauttaa osaltaan myös käyttäjän manipulaatiolta suojautumisessa. Käyttäjän manipulointi -hyökkäyksien tavoitteena on usein identiteettivarkaus, eli käytännössä jonkin verkkopalvelun, yhden tai useamman henkilön kirjautumistietojen haltuun saaminen. Hyökkääjälle riitti pitkään käyttäjätunnuksen ja salasanan anastaminen. Nykyisin monet palveluntarjoajat ja organisaatiot ovat kuitenkin ottaneet käyttöön monivaiheisen tunnistautumisen (multi-factor authentication, MFA), jolloin kirjautuminen ei enää onnistu pelkän salasanan avulla. Monivaiheinen tunnistautuminen voidaan suorittaa kolmen menetelmän avulla (Ometov et al., 2018). Käyttäjän tunnistamisessa käytetään:

- jotain, jota käyttäjä tietää, esimerkiksi salasana
- jotain, jota käyttäjä omistaa, esimerkiksi älypuhelin
- jotain, jota käyttäjä on, esimerkiksi biometrinen tieto

Tunnistautuminen tapahtuu vähintään kahdella näistä menetelmistä, tyypillisesti salasanan ja älypuhelimen avulla. Tunnistautumisessa tullaan tulevaisuudessa hyödyntämään aiempaa enemmän biometriikkaa (Ometov et al., 2018), joka tehnee identiteettivarkaudet entistä vaikeammaksi.

5 Pohdinta

Käyttäjän manipulaatio kehittyy jatkuvasti. Jos hyökkäysmuoto tai sen mahdollinen taustatarina on uhrille ennestään tuttu, on hyökkääjän vaikeampi manipuloida uhriaan. Nigerialaiskirjeiden onnistumisprosentti on nykyisin tuskin kovin suuri. Useimmat ihmiset eivät myöskään todennäköisesti luovuta luottokorttitietojaan tai verkkopankin tunnuksiaan kovin helposti jos niitä sähköpostitse kysellään. Moni osaa suhtautua epäluuloisesti oudosta numerosta puhelimeen saapuneeseen viestiin, joka kertoo odottamattomasta tavaralähetyksestä. Moni saattaa kuitenkin antaa sovellukselle luvan hallita esimerkiksi laitteen yhteystietoja tai kuvagalleriaa asiaa sen enempää pohtimatta. Ei ole myöskään niin yksinkertaista hahmottaa, miten ensimmäisen lemmikkieläimen julkinen muistelu sosiaalisessa mediassa voisi olla tietoturvariski tai miksi sosiaalisessa mediassa kiertävään keveämieliseen kyselyyn ei kannattaisi antaa äidin tyttönimeä.

Hyökkäysmuodot jalostuvat myös uuden tekniikan myötä. Paperiarkistojen siirtyessä digitaaliseen muotoon on roskien penkomisesta hiljalleen tulossa vähemmän merkittävä hyökkäysmuoto. Edistynyt syväväärennös (deep fake) on vastaavasti esimerkki teknologiasta, joka on mahdollistamassa aivan uudenlaisen hyökkäysmuodon synnyn. Näyttää siltä, että pian tulee aika, jolloin syväväärennöksiä on mahdotonta erottaa aidoista tallenteista ihmisaistein. Vuonna 2019 erään brittiläisen energiayhtiön toimitusjohtaja luuli saaneensa puhelun esimieheltään, saksalaisen emoyhtiön johtajalta (Stupp, 2019). Esimies vaati kiireellistä maksua unkarilaiselle tavarantoimittajalle. Todellisuudessa puhelimessa ei ollut esimies vaan tekoälyn avulla rakennettu imitaatio esimiehen äänestä. Ääni oli kuitenkin niin vakuuttava saksalaisine korostuksineen, että toimitusjohtaja tuli huijatuksi. Hän teki 243 000 dollarin tilisiirron hyökkääjän luomalle tilille. Tapaus on tiettävästi ensimmäinen raportoitu käyttäjän manipulaatio -hyökkäys, jonka onnistumisen mahdollisti edistyneen syväväärennöksen käyttö.

Uusi tekniikka antaa työkaluja paitsi hyökkääjälle myös tietoturvan kehittäjille. Kuten edellä käsitelty tapauskin osoittaa, tulevaisuudessa on tarve tekoälylle, joka voi ainakin kohtalaisen suurella todennäköisyydellä havaita eron aidon ja väärennetyn median välillä. Tällaiseen tekoälyyn pohjautuvia työkaluja on jo kehitteillä (Maksutov et al., 2020). Sähköpostien ohjelmallinen suodatus on ollut jo pitkään arkipäivää ja ilmeisimmät huijausyritykset päätyvät roskapostiksi tai poistetuiksi. On mahdollista, että mediatallenteita

suodatetaan joidenkin vuosien kuluttua yhtä rutiininomaisesti. Tekoälyn kehitys antanee muitakin uusia puolustuskeinoja käyttäjän manipulaatiota vastaan ja tehostaa jo käytössä olevia tapoja.

6 Yhteenveto

Käyttäjän manipulointi on tietoturvahyökkäyksen muoto, jossa tietoturva ohitetaan käyttäjän inhimillisiä heikkouksia hyväksikäyttämällä. Se on kasvava ongelma niin Suomessa kuin maailmanlaajuisestikin. Kyberrikolliset pyrkivät käyttäjän manipuloinnin avulla pääsemään käsiksi henkilön tai organisaation suojattuihin tai salaisiin tietoihin. Toisinaan käyttäjää voidaan manipuloida tekemään muutakin, esimerkiksi lähettämään hyökkääjälle rahaa.

Onnistuneen käyttäjä manipulointi -hyökkäyksen suorittamiseen ei aina tarvita teknisen haavoittuvuuden hyödyntämistä. Hyökkäystä ei voida myöskään torjua tehokkaasti vain teknisin keinoin. Nämä ominaisuudet erottavat käyttäjän manipuloinnin muista tietoturvahyökkäyksistä.

Useimmat käyttäjän manipuloinnin hyökkäysmuodot pohjautuvat sosiaaliseen lähestymistapaan. Sosiaalisessa lähestymistavassa uhria suostutellaan tai ohjataan toimimaan hyökkääjän toivomalla tavalla psykologisia keinoja hyödyntäen. Nämä psykologiset menetelmät eivät pohjimmiltaan juurikaan muutu – manipulointi perustuu lopulta aina samoihin inhimillisiin heikkouksiin ja ominaisuuksiin. Psykologisiin menetelmiin liittyvä koulutus tai tieto ei siis myöskään vanhene kovin nopeasti.

Käyttäjän manipuloinnin hyökkäysmuodot ja niissä käytettävät teknologiat sen sijaan kehittyvät jatkuvasti. Teknologian kehittyessä myös tekniset tavat torjua käyttäjän manipulaatiota tehostuvat tai muuttuvat. Asiantuntijoiden mukaan organisaation sisäisesti laatima tietoturvaohjeistus ja sitä tunnollisesti noudattava, koulutettu käyttäjä ovat parhaat aseet taistelussa käyttäjän manipulaatiota vastaan. Tekniset apuvälineet ja ratkaisut kuitenkin tukevat käyttäjiä, ja niiden merkitys voi tulevaisuudessa kasvaa.

.

Lähteet

Abraham, S. ja Chengalur-Smith, I. (2010). ”An overview of social engineering malware: Trends, tactics, and implications”. *Technology in Society* 32.3, s. 183–196.

Bowen, B. M., Devarajan, R. ja Stolfo, S. (2011). ”Measuring the human factor of cyber security”. Teoksessa: *2011 IEEE International Conference on Technologies for Homeland Security (HST)*, s. 230–235. DOI: 10.1109/THS.2011.6107876.

Cialdini, R. B. (2009). *Influence : science and practice*. eng. 5th ed., Pearson international ed. Boston, MA: Pearson Education. ISBN: 0-205-60999-6.

Conteh, N. ja Schmick, P. (helmikuu 2016). ”Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks”. *International Journal of Advanced Computer Research* 6, s. 31–38. DOI: 10.19101/IJACR.2016.623006.

”FBI: Internet Crime Report 2020” (2021). eng. *Computer fraud & security* 2021.4, s. 4–4. ISSN: 1361-3723.

Ghafir, I., Prenosil, V., Alhejailan, A. ja Hammoudeh, M. (2016). ”Social Engineering Attack Strategies and Defence Approaches”. Teoksessa: *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, s. 145–149. DOI: 10.1109/FiCloud.2016.28.

Granger, S. (joulukuu 2001). *Social Engineering Fundam entals, Part I : Hacker Tactics*. URL: https://www.social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html.

Hadnagy, C. (2011). *Social engineering : the art of human hacking*. eng. Hoboken, NJ: Wiley. ISBN: 0470639539.

Jagatic, T., Johnson, N., Jakobsson, M. ja Menczer, F. (lokakuu 2007). ”Social phishing”. *Commun. ACM* 50, s. 94–100. DOI: 10.1145/1290958.1290968.

Krombholz, K., Hobel, H., Huber, M. ja Weippl, E. (2015). ”Advanced social engineering attacks”. *Journal of Information Security and Applications* 22. Special Issue on Security of Information and Networks, s. 113–122. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2014.09.005. URL: https://www.sciencedirect.com/science/article/pii/S2214212614001343.

Maksutov, A. A., Morozov, V. O., Lavrenov, A. A. ja Smirnov, A. S. (2020). ”Methods of Deepfake Detection Based on Machine Learning”. Teoksessa: *2020 IEEE Conference*

of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), s. 408–411. DOI: 10.1109/EIConRus49466.2020.9039057.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. ja Koucheryavy, Y. (2018). "Multi-Factor Authentication: A Survey". *Cryptography* 2.1. ISSN: 2410-387X. DOI: 10.3390/cryptography2010001. URL: https://www.mdpi.com/2410-387X/2/1/1.

Pisani, D. J. (1983). "Reclamation and Social Engineering in the Progressive Era". *Agricultural History* 57.1, s. 46–63. ISSN: 00021482, 15338290. URL: http://www.jstor.org/stable/3742658.

Qin, T. ja Burgoon, J. K. (2007). "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering". Teoksessa: *2007 IEEE Intelligence and Security Informatics*, s. 152–159. DOI: 10.1109/ISI.2007.379548.

Salahdine, F. ja Kaabouch, N. (2019). "Social Engineering Attacks: A Survey". *Future Internet* 11.4. ISSN: 1999-5903. DOI: 10.3390/fi11040089. URL: https://www.mdpi.com/1999-5903/11/4/89.

"Social engineering scams ensnare Google, Facebook and their users" (2017). *Network Security* 2017.5, s. 1–2. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(17)30043-0. URL: https://www.sciencedirect.com/science/article/pii/S1353485817300430.

Strohmetz, D. B., Rind, B., Fisher, R. ja Lynn, M. (2002). "Sweetening the till: the use of candy to increase restaurant tipping 1". *Journal of Applied Social Psychology* 32.2, s. 300–309.

Stupp, C. (2019). "Fraudsters used AI to mimic CEO's voice in unusual cybercrime case". *The Wall Street Journal* 30.08.

Yeboah-Boateng, E. O. ja Amanor, P. M. (2014). "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices". *Journal of Emerging Trends in Computing and Information Sciences* 5.4, s. 297–307.