Haaga-Helia
ammattikorkeakoulu Oy

Sosiaalisen manipuloinnin keinot ja niiltä suojautuminen

Elisa Parolo

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2020

Tiivistelmä

Haaga-Helia
ammattikorkeakoulu Oy

Tekijä(t)
Elisa Parolo

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Sosiaalisen manipuloinnin keinot ja niiltä suojautuminen

Sivu- ja liitesivumäärä
37 + 0

Tämän opinnäytetyön tarkoituksena on tutkia sosiaalista manipulointia tietoturvailmiönä. Tutkimus toteutettiin sisällöntutkimuksena laadullisin menetelmin. Työn tavoitteena on kerätä eri lähteistä kattava katsaus ilmiön toteutustapoihin sekä hyväksi havaittuihin suojausmenetelmiin. Työ on rajattu siten, että sisällössä analysoidaan vain sosiaaliset manipulointihyökkäykset, jotka toteutetaan tietomurron toteuttamista tai tämän helpottamista varten.

Verkkohyökkääjät osaavat taitavasti suostutella meidät luovuttamaan henkilökohtaista tietoa, jota he myöhemmin hyödyntävät tietomurroissa tai tietomurtojen suunnittelussa. Hyökkääjä voi lähestyä uhria sähköpostitse, puhelimitse tai jopa kasvotusten: täysin turvallista kommunikointikanavaa, jossa kyseisiä hyökkäyksiä ei tapahtuisi, ei ole olemassa. Hyökkäyksen olennaisena osana on luottamussuhteen rakentaminen uhriin, jonka seurauksena hyökkääjän on helpompi suostutella häntä luovuttamaan arkaluontoista tietoa. Tähän hyökkääjällä on käytössä lukuisia keinoja, joiden avulla hän pystyy manipuloimaan uhrinsa käytöstä ja tunneskaalaa. Hyökkääjä ei myöskään tavoittele pelkästään salasanoja ja luottokorttinumeroita, vaan myös muuta arkaluontoista tietoa voidaan hyödyntää tietomurtojen suunnittelussa.

Tämän kaltaisilta hyökkäyksiltä on hankalaa suojautua. Sosiaaliset manipulointihyökkäykset kohdistuvat suoraan käyttäjiin, jotka eivät hyökkääjien käyttämien tekniikoiden ansiosta aina edes ymmärrä joutuneensa hyökkäyksen uhriksi. Organisaatioiden kuuluisi panostaa käyttäjien koulutukseen sekä tietoturvakulttuurin luomiseen organisaation sisäisesti niin, että hyvät käytännöt ovat osa työskentelytapoja. On myös olemassa useita teknisiä ratkaisuja, jotka voivat tukea käyttäjiä havaitsemaan ja suojautumaan näiltä hyökkäyksiltä sekä niiden seurauksilta. Niillä ei yksin kuitenkaan ole mahdollista saavuttaa tarvittavaa tietoturvatasoa.

Työ toteutettiin keväällä 2020.

Asiasanat
kyberturvallisuus, verkkohyökkäykset, tietomurto, tietoturvapolitiikka, henkilöstökoulutus

Sisällys

1. Johdanto

Ihmisten välistä kanssakäymistä ohjaa moni kirjoittamaton sääntö. Me emme näihin juurikaan kiinnitä huomiota, mutta kyseisillä säännöillä on meille alitajuisesti valtavasti merkitystä, sillä näiden perusteella päättelemme kehen voimme luottaa. Luottamukseen sekä suostutteluun perustuvia vuorovaikutustekniikoita osataan taitavasti hyödyntää myös rikoksissa, kuten tietomurtojen suunnittelussa.

Tämän projektin tarkoituksena oli tutkia verkkorikollisten käyttämää tekniikkaa, jonka tavoitteena on saada meidät paljastamaan heille henkilökohtaisia tietojamme: ilmiö nimeltään sosiaalinen manipulointi.

Tässä työssä tutkittiin, miten sosiaalista manipulointia toteutetaan, jotta siitä johtuvia tietoturvavahinkoja ja tietomurtoja olisi mahdollista ennaltaehkäistä ja lieventää. Opinnäytetyön tavoite oli tuottaa mahdollisimman laaja katsaus ilmiöön: mitä sosiaalinen manipulointi on? Miten sitä hyödynnetään ja mitä sillä tavoitellaan? Miten sen voi tunnistaa ja miten siltä voi suojautua? Miksi se on tehokas? Lisäksi työ sisältää erilaisia suojautumiskeinoja käyttäjille ja organisaatioille, joita on suunniteltu olemaan tehokkaita juuri tämän kaltaisien hyökkäyksiä vastaan. Tässä tekstissä esitettyjen tuloksien tarkoitus on auttaa tunnistamaan vaaratilanteet sekä auttaa hahmottamaan parempia suojautumiskeinoja niin käyttäjille kuin organisaatioille.

Sosiaalinen manipulointi on vain yksi tietoturvan osa-alue, mutta se on mielestäni ainoa, johon meistä jokainen voi vaikuttaa omalla käytöksellään riippumatta teknisestä taustasta. Tämän työn lopputuloksena syntyneitä tuloksia voi hyödyntää organisaation tietoturvakäytäntöjen suunnittelussa, niiden parantamisessa, koulutustilaisuuksissa sekä muissa kehityshankkeissa. Toivoisin myös, että jokainen työn lukija pohtisi omaa käyttäytymistä verkossa sekä mahdollisuuksiensa mukaan parantaisi omia tottumuksiaan.

Tämä on tutkimustyyppinen opinnäytetyö ja tutkimusongelman lähestymistavaksi valikoitui laadullinen sisällöntutkimus. Aineistona käytettiin erilaisia aiheeseen liittyviä julkaisuja: kirjoja, tutkimuksia, esseitä, tutkielmia, artikkeleita ja verkkojulkaisuja. Aineisto on peräisin Haaga-Helian kirjaston tarjoamista tietokannoista sekä ilmiötä käsittelevistä kirjoista, pienimmässä määrin ainestoa löytyi julkisesta verkosta. Tämä rajaaminen oli tietoinen päätös, jotta aineiston laatu sekä sen perusteella syntyvien tuloksien luotettavuus olisi mahdollisimman korkea.

Projekti rajattiin siten, että työssä analysoidaan ainoastaan sosiaaliset manipulointihyökkäykset, joiden lopullinen kohde on jokin tietojärjestelmä. Suojautumiskeinoissa vastaavasti esiteltiin erilaisia suojausrakenteita ja -käytäntöjä, joita on todettu toimivaksi juuri tämän kaltaisia manipulointihyökkäyksiä vastaan. Projektin ei ollut tarkoitus toteuttaa aiheeseen liittyvää kyselyä käyttäjien kesken tai muutenkaan sisällyttää tai analysoida käyttäjien mielipiteitä tai kokemuksia aiheeseen liittyen.

Alla oleva taulukko sisältää opinnäytetyössä olevia termejä sekä niiden määritelmän.

Termi	Määritelmä
Phishing	Verkon kautta saapuva yhteydenotto, jossa yritetään kalastella viestin saajalta arkaluontoista tietoa.
Spear phishing	Phishing-yritys, joka on kohdistettu tiettyyn henkilöön, osastoon tai organisaatioon.
Whaling	Phishing-yritys, joka on kohdistettu toimitusjohtajiin ja muihin johtoryhmän henkilöihin.
Vishing	Puhelimen kautta toteutettu tietojenkalasteluyritys.
Smishing	Tekstiviestin kautta toteutettu tietojenkalasteluyritys.
Shodan	Hakukone, jolla pystyy hakemaan verkossa olevia laitteita sekä näiden konfigurointeja.

2. Sosiaalinen manipulointi

2.1. Määritelmä

Sosiaalista manipulointia on käytetty ihmisten välisessä vuorovaikutuksessa kautta aikojen. Kyseistä toimintaa voisi kuvailla tilanteeseen räätälöitynä, ovelana ja hienovaraisena ihmisten taivutteluna, jonka tavoitteena on saada toista ihmistä käyttäytymään tietyllä tavalla, toisen keskusteluosapuolen suunnitelmien mukaisesti. Ihmisten välinen kanssakäyminen on jatkuvaa sosiaalista manipulointia – olemme päivittäin tilanteissa, joissa tekojamme yritetään eri keinoin ohjata tai me yritämme vaikuttaa toisen ihmisen käytökseen. Keinoja toteuttaa sosiaalista manipulointia on monenlaisia, ja sosiaalista manipulointia on toki mahdollista käyttää myös hyvään tarkoitukseen. Tietoturvailmiönä, tosin, sosiaalinen manipulointi on keskustelun toiselle osapuolelle poikkeuksetta haitallista: hyökkääjän yhteydenoton tavoite on oman edun edistäminen, ja tämä saavutetaan manipuloimalla uhria käyttäytymään hyökkääjän toivomalla tavalla. Tavoitteena voi esimerkiksi olla uhrin suostuttelu paljastamaan hyökkääjää kiinnostavia tietoja, kuten sisäänkirjautumistietoja, luottokorttitietoja tai muuta manipuloinnin uhrin tiedossa olevaa dataa. (Hadnagy & Wilson 2010, 10–11.)

Kaikki tieto, mikä paljastuu onnistuneen sosiaalisen manipuloinnin hyökkäyksen yhteydessä, ei suinkaan ole arkaluonteista, tai hyökkäyksen kohde ei mielestään luokittelisi paljastettua informaatiota sellaiseksi. Hyökkääjän tavoittelema lopputulos voi myös olla muuta kuin tiedonsaanti: sosiaalisen manipuloinnin avulla voidaan myös esimerkiksi yrittää päästää tiloihin, joihin ei muuten olisi pääsyä. (Mann 2008, 2.)

Sosiaalista manipulointia voidaan toteuttaa kahdella tavalla: hyökkääjä voi kommunikoida uhrin kanssa suoraan tai hyökkäys voidaan toteuttaa tietokoneen välityksellä. Esimerkkejä suorasta vuorovaikutuksesta ovat:

- valtuutetun työntekijän seuraaminen ulkopuolisista kiellettyyn alueeseen
- tekeytyminen organisaation työntekijäksi tai ihmiseksi, jolla on pääsy organisaation sisäiseen dataan
- auktoriteettihahmoksi tai valtuutetuksi työntekijäksi tekeytyminen.

Tietokoneen välityksellä tapahtuvissa hyökkäyksissä hyödynnetään erilaisia ohjelmistoja. Esimerkkejä tämäntyyppisistä hyökkäyksistä ovat:

- erilaiset pop-up ikkunat, jotka ilmestyvät uhrin näytölle hänen vieraillessa saastuneella verkkosivulla,
- sähköpostitse tai tekstiviestitse lähetetyt kalasteluviestit (mm. phishing),
- ”nigerialaisprinssi” ja muut vastaavat huijauskirjeet. (Singh 2013, 23–25.)

Kalasteluviesteiksi voidaan määritellä myös whaling, spear phishing, vishing ja smishing.

Sosiaalisen manipuloinnin tarkoitus on edesauttaa tietomurtoja ja muita järjestelmiin tunkeutumista keräämällä kohteesta tietoa erilaisten tiedonkeruumenetelmien avulla. Hyökkääjän päämäärä on selvittää keinoja, joiden avulla hän pääsee onnistuneesti haluttuun kohteeseen, joko fyysisesti tai tietokoneen välityksellä, ja pääsee hyödyntämään kohteessa olevaa dataa omiin tarkoituksiin. Vaikka sosiaalinen manipulointi on vakava tietoturvauhka, sitä ei kuitenkaan voida tämän perustella luokitella hakkeroinniksi, vaikka tosin on tilanteita, joissa sosiaalinen manipulointihyökkäyksen toteuttaja on myös tietomurron suorittaja. (Thornburgh, 2.)

Edellä kerrotun perusteella sosiaalisessa manipulointihyökkäyksessä voidaan identifioida kaksi keskeistä ominaispiirrettä: hyökkäyksen kohteena on ihminen sekä hyökkäyksen tavoitteena on tieto. Virheellisesti sosiaalisten manipulointihyökkäyksien tavoitteeksi usein ajatellaan olevan pelkästään salasanat ja luottokorttitiedot, mutta tosiasiassa kyseisien hyökkäyksien tavoitteena voi olla myös tieto tiedosta, esimerkiksi arkaluontoisen datan fyysinen sijainti tai tiedon haltijan nimi. Hyökkäyksen ytimenä toimii ajatus, että oikeilla keinoilla ja toimivilla työkaluilla hyökkääjä saavuttaa tavoitteensa vain uhrilta kysymällä, usein jopa niin, ettei uhri itse edes ymmärrä joutuneensa huijauksen uhriksi. Mielestäni, tietyissä tapauksissa, ero viattoman keskustelun ja sosiaalisen manipulointihyökkäyksen välillä saattaa olla ainoastaan keskustelun toisen osapuolen tarkoitus hyötyä keskustelutilanteesta jollain tavalla. Tämä tekee sosiaalisesta manipuloinnista erittäin vaarallisen tietoturvauhkan, sillä normaalin kanssakäymisen seurauksena saatamme keskustella myös henkilökohtaisista asioista, jotka eivät ole julkisesti saatavilla olevaa tietoa. Keskustelun toinen osapuoli voi päättää olla hyödyntämättä tietoa tai käyttää tätä tavoittaakseen omia etuja.

Sosiaalisen manipuloinnin hyökkäyksiä voidaan kategorisoida kolmella tavalla: ensimmäinen tapa on kategorisointi hyökkäyksessä käytetyn kanavan mukaan, toinen tapa perustuu hyökkäyksen toteuttajaan ja kolmas perustuu hyökkäystapaan. Käytetyin kanava sosiaalisen manipuloinnin hyökkäyksissä on sähköposti, mutta myös pikaviestimet, sosiaalisen median sivut, verkkosivut ja puhelinsoitot ovat tehokkaita yhteydenottokanavia. Toteuttaja voi olla joko henkilö tai ohjelmisto, joista toinen on huomattavasti nopeampi ja tehokkaampi saavuttamaan suuren määrän uhreja: jokainen yksittäinen suora yhteydenotto on aina yksittäisen ihmisen tekemä, kun taas tietokoneen välityksellä tapahtuva hyökkäys voidaan tietyissä tapauksissa jopa automatisoida erilaisten ohjelmistojen avulla. Se tekee näin huijausviestin jakelusta huomattavasti laajemman kuin suoran yhteydenoton välityksellä tapahtuvassa hyökkäysyrityksessä. Sosiaalisen manipuloinnin hyökkäystapa voi olla

fyysinen, tekninen, sosiaalinen tai sosiotekninen. Fyysisellä hyökkäystavalla viitataan tarvittavan tiedon etsimiseen fyysisistä tiloista, tekninen toteutustapa hyödyntää teknologian antamia mahdollisuuksia tavoittaa uhria ja tarvittavaa tietoa, sosiaalinen hyökkäystapa tapahtuu kasvotusten ja perustuu voimakkaasti uhrin suostutteluun. Viimeinen, eli sosiotekninen toteutustapa, on yhdistelmä teknistä ja sosiaalista toteutustapaa. Esimerkki tästä ovat esimerkiksi haittaohjelmia sisältävät USB-tikut, joita tarkoituksella jätetään uhrien löydettäväksi. Uhrin uteliaisuus tarkastaa USB-tikun sisältöä usein ajaa hänet liittämään tikun tietokoneeseensa, minkä seurauksena sen sisältämä haittaohjelma pääsee leviämään uhrin tietokoneeseen ja mahdollisesti myös muihin verkossa oleviin koneisiin. (Krombholz, Hobel, Huber & Weippl 2014, 4–5.)

Yhteydenottokanavasta riippumatta kaikki sosiaaliset manipulointihyökkäykset rakentuvat kolmen sosiaalipsykologian avainkonseptien ympärille: ihmisen suostutteluun käytetyt menetelmät, vaikuttamiseen ja vakuuttamiseen käytetyt menetelmät sekä vuorovaikutuksen perusteena olevat asenteet ja uskomukset. Näiden taitavalla hyödyntämisellä hyökkääjä voi luoda uhriin uskottavan, aidolta vaikuttavan suhteen, jota hän voi omien etujen mukaisesti, sopivan hetken tullessa, käyttää hyväksi. Vaihtoehtoisesti näitä voidaan myös soveltaa herättämään uhrissa vahvoja tunteita, kuten iloa tai pelkoa, jotta tunnekuohun yhteydessä uhri olisi heikommassa asemassa ja siten alttiimpi paljastamaan hyökkääjän tavoittelemaa tietoa. On tärkeää muistaa, että normaali ihmisten välinen kanssakäyminen perustuu luottamukseen siihen, että toinen osapuoli on juuri se henkilö, joka hän kertoo olevansa. Sosiaalisessa manipuloinnissa näin ei tosin ole. (Peltier 2006, 2–3.)

Näiden edellisissä kappaleissa esitettyjen väitteiden perusteella voidaan tulla johtopäätökseen, että sosiaaliset manipulointihyökkäykset eivät ole impulsiivisesti toteutettuja interaktioita eikä niiden tehokkuus perustu pelkästään hyvään onneen tai sattumaan. Sosiaalinen manipulointihyökkäys on tarkkaan mietitty prosessi, jossa uhrin lähestymiseen käytetyt tavat pohjautuvat vahvasti ihmisten välisen luontevan kanssakäymisen rakenteisiin. Tämän tarkoitus on edesauttaa hyökkäyksen naamioitumista normaaliksi, viattomaksi vuorovaikutukseksi. Tehokkuutta lisää se, että hyökkäykset suunnitellaan olemaan alitajuisesti vaikuttavia sekä vaistomaisia reaktioita herättäviä, mutta kuitenkin nostattamatta uhrin epäilyksiä huijauksen uhriksi joutumisesta; lisäksi ei ole olemassa kommunikointikanavia, joissa sosiaalista manipulointia ei toteutettaisi. Se vaikeuttaa hyökkäyksiin varautumista ja käyttäjien suojautumista.

Sosiaaliset manipulointihyökkäyksien tapaukset ovat tiettyjen tilastojen mukaan nousussa. Yhdysvaltojen liittovaltiopoliisi FBI:n vuosittaisessa Internet Crime Report -julkaisussa kä-

sitellään ja tilastoidaan FBI:n ilmiantosivulle ilmoitettuja tapauksia verkkorikoksista. Vuoden 2015 raportin tilastossa, jossa raportointivuoden toteutuneen kyberrikokset järjestetään uhrien määrän perusteella, sosiaaliseksi manipulointihyökkäykseksi luokitellut phishing, vishing ja smishing löytyvät sijalla 10. Vuonna 2017 kyseinen ryhmittymä nousi sijalle 3, ja vuoden 2019 raportissa nämä olivat nousseet ykkössijalle yli 100 000 uhriluvun määrällä. FBI arvioi, että vain noin 15 % kyberrikoksista tulee viranomaisten tietoon, joten uhrien todellinen määrä on todennäköisesti huomattavasti raportoitua korkeampi. (FBI 2015, 17; FBI 2017, 20; FBI 2019, 19.)

FBI:n tilastoista voidaan havaita, miten sosiaalisten manipulointihyökkäyksien suosion trendi on nouseva ja sosiaaliset manipulointihyökkäykset ovat nykypäivänä edelleen laajasti rikollisten hyödyntämiä. Mielestäni yksi syy kyseiselle havainnolle voisi olla järjestelmien sekä yleisesti organisaatioiden tietoturvakäytäntöjen monimutkaistuminen ja kovettuminen. Ohjelmistojen ja verkkojen tietoturvataso on noussut viime vuosina teknologisen kehityksen ansiosta, ja tehnyt näin suojauksen murtamisesta hankalamman. On mielestäni loogista päätellä, että sosiaalisen manipuloinnin suosio kasvaa teknologian kehittyessä turvallisemmaksi, sillä se onnistuessaan manipulointihyökkäys nopeuttaa rikollisen työtä huomattavasti. Rikollisen mahdolliset vaihtoehdot nykytilanteessa järjestelmän murtamiseksi ovat joko hankala, hidas ja työläs prosessi, jossa hän ohjelmistojen avulla yrittää saada pääsyn kohteeseen herättämättä epäilyksiä ja aiheuttamatta hälytyksiä, tai vaihtoehtoisesti hän voi ottaa yhteyttä henkilöön, jolla on jo myönnetty pääsy järjestelmään, ja anastaa häneltä kirjautumistiedot itselleen taitavasti toteutetulla manipulointihuijauksella.

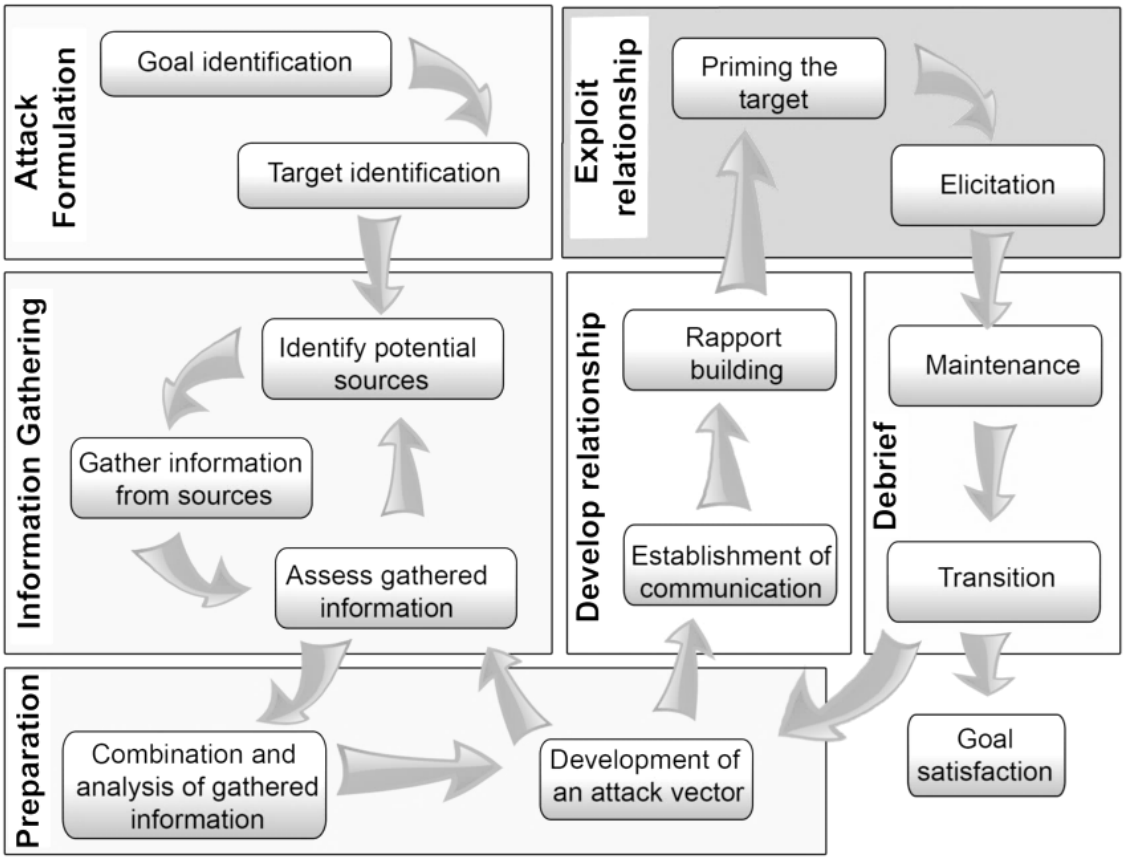
2.2. Kohteen valinta ja hyökkäyksen eteneminen

Sosiaalisen manipulointihyökkäyksen etenemissyklistä on esitetty erilaisia rakenteita. Kirjassaan Wozniak, Simon ja Mitnick (2003) tunnistavat hyökkäyksessä neljä päävaihetta: tiedonkeruu, luottamussuhteen muodostaminen, luottamussuhteen hyödyntäminen ja saadun tiedon käyttäminen.

Nämä vaiheet voivat saman hyökkäyksen aikana toistua useita kertoja niin, että seuraava iteraatio hyödyntää edellisen syklin aikana paljastunutta tietoa, kunnes hyökkääjä lopulta pääsee tavoitteeseensa. (Thornburgh, 2.)

Wozniakin ym. esittämä sosiaalisen manipuloinnin hyökkäyksen etenemisen neljän vaiheen kaava on esitetty olevan kuitenkin liian rajallinen. Siinä tuodaan erinomaisesti esiin

hyökkäyksen päävaiheet sekä päärunko, mutta ymmärrettävästi neljän vaiheen rakenteessa jää moni välivaihe mainitsematta. Konferenssitutkielmassaan Mouton, Leenen, Maian ja Venter (2014, 4) esittävät laajennetun kuvan 1 mukaisen hyökkäysrakenteen, jossa sosiaalisen hyökkäyksen eteneminen kuvataan yksityiskohtaisemmin:



Kuva 1. Sosiaalisen manipulointihyökkäyksen etenemissykli (mukaillen Mouton, Leenen, Maian & Venter 2014)

Mielestäni kuvassa 1 esitetään myös yksityiskohtaisemmin vaiheiden riippuvuudet toisistaan. Wozniakin ym. esittämät hyökkäyksen pääpiirteet säilyvät tässäkin tunnistettavissa. Mouton ym. kuitenkin lisäävät oman rakenteensa ensimmäiseksi vaiheeksi tavoitteen ja kohteen valitseminen. Mielestäni lisäys on olennainen ja perusteltu, sillä se on todellisuudessa sosiaalisen manipulointihyökkäyksen alkusysäys ja koko tapahtumaketjun käynnistäjä. Oletettavasti Wozniakin ym. manipulointihyökkäysrakenteessa tämä on sivuutettu itsestään selvänä vaiheena. Mouton ym. lisäävät syklin rakenteeseen myös tiedonkeruun ja luottamussuhteen muodostamisen väliin vaiheen, jonka tarkoitus on analysoida tiedonkeruuvaiheessa kerätty tieto yhteydenottoa varten, sekä loppuun vaiheen, jonka aikana hyökkääjä tarkkailee uhrin mielialaa syyllisyydentunteiden tai ahdistuneisuuden varalle. Mouton ym. analysoivat mielestäni sosiaalisen manipuloinnin hyökkäyssykliä perusteelli-

semmin kuin Wozniak ym. Lähteet eivät tästä huolimatta ole ristiriidassa. Niissä on havaittavissa huomattava määrä yhtäläisyyksiä sekä ne tukevat toisiaan hyökkäyssyklin pääpiirteiden identifioimisessa.

Kun kohde on hyökkääjän tiedossa, ensimmäinen tehtävä on tiedonkeruu hyökkäystä varten. Tämän vaiheen aikana tarkoitus on kerätä mahdollisimman paljon erilaista taustatietoa kohteesta, niin organisaatiosta ja organisaation vastuuhenkilöistä kuin hyökkäyksen kohteeksi valikoidusta järjestelmästä ja sen ominaisuuksista. Turhaa tietoa ei ole sosiaalisessa manipuloinnissa olemassa, vaikka kerätty informaatio voi alussa vaikuttaa itsestään selvältä. (Wozniak, Simon & Mitnick 2003.)

Verkkosivut ovat erinomainen paikka aloittaa tiedonhakua, sillä myös monella yksityishenkilöllä on myös omat kotisivut, jonne he julkaisevat tietoa niin työ- kuin yksityiselämästä. Googlen tarjoamaa tarkennettua hakua voi hyödyntää paljastamaan julkisesti saatavilla olevia yrityksen sisäisiä dokumentteja ja tiedostoja. Shodan-nimisen hakukoneen avulla voidaan hakea tietoa palvelinten erilaisista käyttöjärjestelmistä, reitittimistä ja harvinaisista palvelinohjelmistoista. Sosiaalisen median avulla on mahdollista saada valtavasti tietoa kohteesta, riippumatta siitä onko hyökkäyskohteeksi valikoitunut organisaatio tai yksityishenkilö. Sosiaalista mediaa voi hyödyntää monella tavalla: mielenkiintoista tietoa voi saada myös analysoimalla kuvien metadataa tai sijaintitietoja. Roskakoreista tai paperinkeräyksestä voi löytyä sisäisiä, salaisia dokumentteja. (Hadnagy & Wilson 2010, 34–43.)

Vaihtoehtoisesti hyökkääjän ei tarvitse aktiivisesti etsiä tietoa uhreista, vaan hän voi myös julkaista päivityksen esimerkiksi sosiaalisessa mediassa tai muualla verkossa ja odottaa, että uhri itse päättää paljastaa hyökkääjälle hyödyllistä tietoa. Sosiaalisen median avulla kerätty tieto ei tosiaan aina tule uhrin käyttäjäprofiilista, vaan tietoja voi myös saada kuvan 2 kaltaisella päivityksellä:

Kuva 2. Esimerkki somen tiedonkalastelupäivityksestä (mukaillen Marsden s.a.)

Kuvan 2 tapaisia päivityksiä on sosiaalisessa mediassa useita, ja lähes poikkeuksetta kyseiset päivitykset saavat paljon huomiota. Käyttäjät eri puolilta maailmaa jakavat päivityksen kommenttikentässä kuvan kaavan mukaisesti luodun “kuninkaallisen nimensä”. Käyttäjät näkevät tämän viattomana pelinä, jonka tarkoitus on viihdyttää ja hauskuuttaa saman päivityksen lukijoita, ja moni kuvan 2 kaltainen päivitys sosiaalisessa mediassa onkin luotu ainoastaan viihdemielessä. “Kuninkaallisesta nimestä” taitava sosiaalinen manipuloija voi kuitenkin saada paljon hyödyllistä tietoa: kuten kuvassa 2 näkyy, käyttäjiä pyydetään paljastamaan isovanhempien nimen ja ensimmäisen lemmikin nimen. Nämä ovat monessa palvelussa vastauksia turvakysymyksiin, joihin kohdejärjestelmä pyytää vastaamaan, mikäli käyttäjä ilmoittaa salasanan unohtuneen ja pyytää salasanan itseresetointia. Hyökkääjä voi mahdollisesti johtaa sosiaalisen median tilin nimestä esimerkiksi käyttäjätunnuksen tiettyyn palveluun tai sähköpostiosoitteen paikallisosan: manipuloija siirtyy palveluun, kirjoittaa tarvittavaan kenttään käyttäjätunnuksen ja painaa tämän jälkeen salasanan resetointilinkkiä. Mikäli palvelun turvakysymyksien vastaukset vastaavat noita sosiaalisen median päivityksen yhteydessä paljastuneita tietoja, hyökkääjä pääsee resetoimaan käyttäjän salasanan ja onnistuu kirjautumaan palveluun toisena käyttäjänä. Vaikka hyökkääjä ei pääsisi hyödyntämään tällä tavalla paljastunutta tietoa heti, tieto voidaan myös varastoida

tulevia käyttötarkoituksia varten. Sosiaalisessa manipuloinnissa turhaa tietoa ei tosiaan ole: jopa sosiaalisen median viattoman oloisista päivityksistä voi saada arvokasta tietoa hyökkäyksen kannalta ja hyökkäyksen lopputavoitteen saavuttamisen kannalta.

Helsingin Sanomat julkaisi opinnäytetyöprojektin ajankohdan aikana artikkelin, jossa käyttäjiä varoitettiin jakamasta henkilökohtaista tietoa edellisessä kappaleessa esitetyn “pelin” kaltaisiin päivityksiin. Artikkelissa kerrotaan, miten kyseisten päivityksien avulla paljastuneita tietoja voidaan hyödyntää esimerkiksi salasanamurroissa. Artikkelissa haastateltu kyberturvallisuuskeskuksen johtaja myös muistuttaa, että yksittäinen paljastus ei välttämättä vaaranna käyttäjän tietoturvaa. Verkossa jaetuista useampien knoppitietojen keräämisen avulla on tosin mahdollista luoda yksityiskohtaisen kuvan uhrin elämästä, harrastuksista ja työpaikoista. Tiedonkeruu voi jatkua joissain tapauksissa jopa vuosien ajan. (Kangasniemi 2020.)

Artikkelissa olevan kyberturvallisuuskeskuksen johtajan näkemykset siitä, että sosiaalisessa mediassa paljastettua tietoa voi käyttää hyödyksi salasanojen murtamisessa tukevat saamani lopputulosta, johon päädyin analysoidessa kuvan 2 sisältöä. Lisäksi artikkelissa mainittu verkossa olevan tiedon kerääminen ja yhdistäminen samaan henkilöön on juuri se syy, minkä takia Wozniak ym. myös varoittavat käyttäjiä siitä, että hyödytöntä tietoa ei sosiaalisessa manipuloinnissa ole. Mitä enemmän uhrista tiedetään, sitä uskottavampi sosiaalinen manipulointihyökkäys voidaan häneen kohdistaa.

Kun hyökkääjä kokee keränneensä ja analysoineensa riittävästi tietoa kohteesta, seuraavana vuorossa on yhteydenotto uhriin. Ensimmäinen yhteydenotto toimii myös perustana luottamussuhteen luomiselle, sillä mielestäni tietyissä tapauksissa huijari voi ottaa yhteyttä uhriin vain kerran. Ensivaikutelmasta uhrin ei pitäisi alkaa epäilemään hyökkääjään motiiveja tai epäilemään hyökkääjän identiteetin aitoutta, sillä mielestäni pahimmassa tapauksessa epäonnistunut tai epäluotettavalta kuulostava yhteydenotto voi nostaa koko organisaation valmiustasoja, vaikeuttaen tai jopa hetkellisesti kokonaan estäen tulevia manipulointiyrityksiä.

Yhteydenotto uhriin voi tapahtua esimerkiksi kasvotusten, puhelimitse tai sähköpostitse. Yhteydenoton sävyllä on kuitenkin huomattavasti merkittävämpi painoarvo kuin yhteydenottotavalla. Erilaisia uhria suostuttelevia ja vakuuttavia keinoja voivat esimerkiksi olla merkittävässä asemassa organisaatiossa olevan henkilön esittäminen, avun pyytäminen esittäen uutta työntekijää tai avun tarjoaminen uhrille jonkun ongelman ratkaisemiseksi. (Wozniak, Simon & Mitnick 2003.)

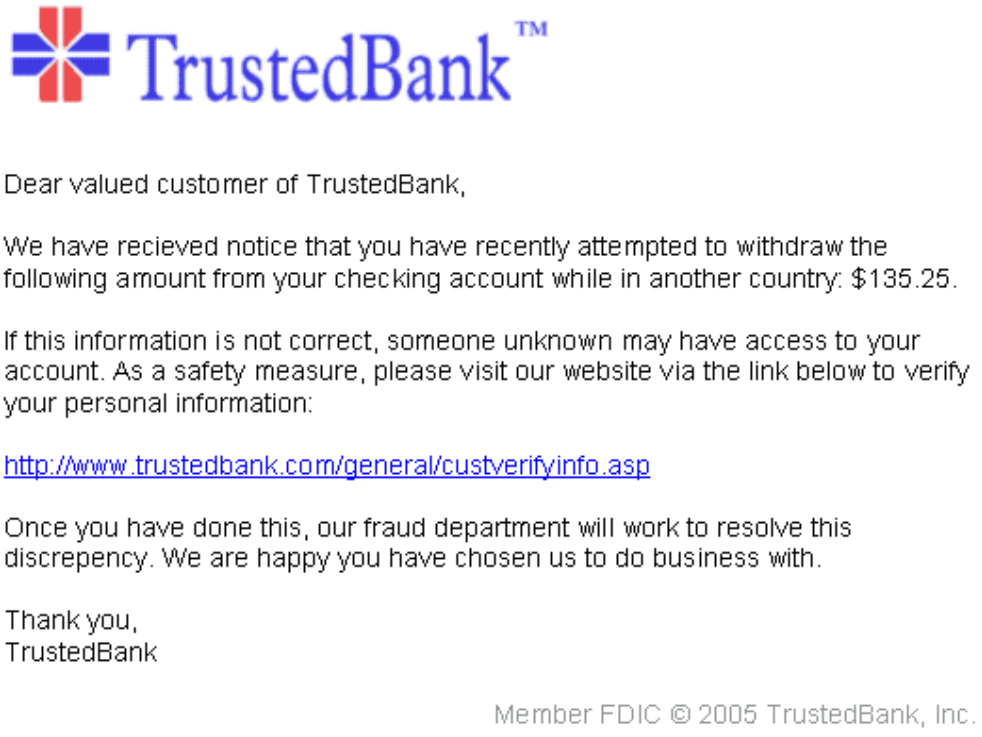
Näiden keinojen lisäksi hyökkääjä voi suostutella uhriaan muilla keinoilla: keinotekoinen tai valheellinen niukkuus herättää uhrissa kiireellisyyden tunteita, joka edesauttaa uhrin tunteiden ja käytöksen manipulointia. Myös vastavuoroisuutta on helppoa hyväksikäyttää, mikäli hyökkääjä aloitti hyökkäyksensä tekemällä uhrille palveluksen tai auttamalla häntä jonkin ongelman ratkaisemisessa. Pelkästään toisesta ihmisestä pitäminen tai pyrkimys toteuttaa annettu lupaus voivat ohjata uhria paljastamaan hyökkääjälle tietoa: monessa kulttuurissa nähdään kohteliaisuutena auttaa pulassa olevaa henkilöä. Uhri voi ymmärrettävästi ajatella, että annetun lupauksen rikkominen saattaa antaa hänestä epäluotettavan kuvan. (Rusch 1999.)

Uhrin suostuttelu toimimaan hyökkääjän toivotulla tavalla on tärkeässä osassa sosiaalista manipulointia, ja hyökkääjällä on monta tapaa yrittää suostutella uhriaan. Menetelmästä riippumatta, suostuttelun ydin on kohdehenkilön oman tahdon taivuttamista niin, että uhri itse nimenomaan haluaa ajatella, reagoida tai toimia hyökkääjän edun mukaisesti. Tehokkaasti toteutettu sosiaalisen manipuloinnin uhrin suostuttelu rakentuu viiden perusperiaatteen avulla: ihmissuhteen rakentaminen ja vaaliminen, tarkan päämäärän asettaminen, ympäristön tarkkailu, joustavuus ja itsetutkiskelu. Suhdetta uhriin kuuluisi alusta asti hoitaa erityisen tarkasti: hyökkääjän kuuluu toimia empaattisesti ja tarkkailla uhrin mielialaa ja tunteita. Nämä ovat kriittisen tärkeitä juuri suostuttelun onnistumisen kannalta, sillä ilman aidolta vaikuttavaa suhdetta hyökkääjän on hyvin vaikeaa, ellei mahdotonta, suostutella uhriaan toimimaan halutulla tavalla. Päämäärän asettaminen auttaa hyökkääjää fokusoimaan energiansa toivottuun lopputulokseen, sillä päämäärän asettamisella välivaiheineen on myös vaikutusta hyökkääjän omaan käytökseen. Tämän seurauksena hän alkaa toimia myös alitajuisesti huomattavasti vakuuttavammalla tavalla manipulointiyrityksessään. Ympäristön tarkkailulla tarkoitetaan uhrin elekielen ja ilmeiden tarkkaa tulkintaa, mikäli hyökkäykseen valkoitu toteutustapa antaa tähän mahdollisuuden. Tämä tarkoittaa jatkuvaa arviointia oman suostutteluyrityksen toimivuudesta: tämä on vahvasti yhteydessä kolmanteen peruspilariin eli joustavuuteen. Mikäli havaitaan, että valittu tekniikka ei tuota toivottuja tuloksia, osaava hyökkääjä osaa tarvittaessa joustaa omista asetetuista tavoitteista ja vaihtaa omaa käytöstään, manipulointitekniikkaa tai tavoitettavia kohteita, jotta hänen käytöksensä säilyisi mahdollisimman luontevana ja uhrin epäilyksiä herättämättä. Itsetutkiskelulla viitataan hyökkääjän omiin tunteisiin, joita myös kuuluu jatkuvasti tarkkailla suostuttelun aikana. Hyökkääjän omat mielipiteet, ajatukset ja tuntemukset tulisi kontrolloida ja tarvittaessa muokata manipulointihyökkäystä silmällä pitäen. (Hadnagy & Wilson 2010, 182–187.)

Hyökkääjä hyödyntää yhteydenotossansa nimiä, titteleitä, järjestelmien nimiä ja muita tietoja, mitä hän on tiedonhakuvaiheessa onnistunut löytämään kohteestaan. Tämä auttaa

häntä luomaan itsestään kuvan, että hän on luotettava henkilö. Tämä taas on edellytys luottamussuhteen synnylle, joka taas puolestaan johtaa uhrin suhtautumiseen auttavaisesti viestinnän toiseen osapuoleen. Viestin ulkonäkö saattaa olla tarkka jäljitelmä organisaation tai organisaation asiakkaan käyttämästä viestipohjasta, jossa rikollinen hyödyntää yrityksen sisäistä termistöä. Viesti voi herättää uhrissa tiettyjä voimakkaita tunteita, kuten iloa, pelkoa tai ahneutta: tämä on tahallista ja tämän tarkoitus on saada uhri poikkeamaan normaaleista käytännöistä ja ohjeistuksista. Uhri voi jopa olla täysin tietoinen siitä, että hänen käytöksensä ei ole virallisen ohjeistuksen mukaisesti hyväksyttävää, mutta hyökkääjän herättämät vahvat tunteet toimivat kiireellisyyden luomisen lisäksi myös perusteluksi virallisesta ohjeistuksesta poikkeamiseen. (Thornburgh, 2.)

Nämä edellä kerrotut manipulointihyökkäyksen elementit ovat mahdollisesti helpommin havaittavissa tilanteissa, joissa hyökkääjä ja uhri kommunikoivat suoraan kasvotusten. Nämä samat suostuttelukeinot ovat tosin tunnistettavissa myös teknologisissa hyökkäystavoissa. Esimerkiksi voisi käyttää kuvakaappauksen huijausviestistä, jossa yritetään pankin nimessä kalastella uhrin tietoja.



Kuva 3. Esimerkki huijausviestistä (mukaillen Levine s.a.)

Kuten kuvasta 3 voi huomata, tiedonhakuvaiheessa hyökkääjä on kerännyt tietoa, että uhri on kyseisen pankin asiakas: uhri on mahdollisesti itse voinut kertoa olevansa pankin

asiakas omalla sosiaalisen median käyttäjätilillä ymmärtämättä tämän paljastuksen seurauksia, sillä kyseinen tieto ei ole arkaluonteista eikä monikaan näkisi paljastusta kovinkaan vakavana tietoturvauhkana. Luottamussuhdetta uhriin luodaan esittämällä luotettavaa instituutiota, pankkia. Esiintyminen pankin toimihenkilönä luo automaattisesti myös auktoriteettiin perustuvan suhteen uhriin, sillä pankki nähdään arvokkaana ja tärkeänä instituutiona, johon kuuluisi suhtautua vakavasti ja kunnioittavasti. Viestin tyylittely yrittää jäljitellä pankin viestien ulkoasua, viestin alussa on näkyvä pankin logo ja viestin sävy on ammattimainen. Viestin sisältö pyrkii herättämään voimakkaita tunteita uhrissa, sillä suurehko ulkomailla nostettu summa aiheuttaa hänessä hämmennystä ja pelkoa pankkitietojen joutumisesta vääriin käsiin. Tähän ongelmaan kuuluisi myös kiireellisesti puuttua, jotta uusia käteisnostoja ei enää tehtäisi. Uhrille ei anneta tarkoituksellisesti aikaa tai mahdollisuutta rauhallisesti ja järkevästi suhtautua tilanteeseen ja tästä huolehtii viestin lopussa oleva linkki. “Pankki” tarjoaa mahdollisuuden nopeasti selvittää hankalaa tilannetta, jossa uhrin talous on uhattuna. Linkki on ovelasti naamioitu niin, että se näyttää johtavan suoraan pankin sivuille. Linkkiä klikkaamalla uhri todennäköisesti päätyy hyökkääjän omille sivuille, jossa pahimmassa tapauksessa uhri syöttää oikeat verkkopankkitietonsa suoraan hyökkääjälle. Näin hyökkääjä saa juuri tavoittelemansa tiedon ja pääsee kirjautumaan kohteeseen. Tämä viesti on tehokas meidän omien psykologisten puutteidemme vuoksi: viestin sisältö on mietitty ja rakenteellisesti luotu olemaan mahdollisimman tehokas sosiaalisen manipuloinnin hyökkäysväline.

Luvussa 2.2 käytettyjen tutkimuksien ja kirjojen tekijät ovat yksimielisiä siitä, että hyvin toteutetun sosiaalisen manipulointihyökkäyksen tärkein kulmakivi on uskottavan ja luotettavan suhteen luominen uhriin. Tämän tärkeyttä perustellaan sillä, että uhrin täytyy luottaa hyökkääjään, ennen kuin hänet voidaan suostutella paljastamaan henkilökohtaista tai arkaluonteista tietoa. Tapoja luoda tämän kaltaista luottamussuhdetta on lukuisia, jokainen riippuvainen mm. sosiaalisen manipulointihyökkäyksen ominaisuuksista sekä käytetyistä yhteydenottotavoista.

Kun hyökkääjä on onnistuneesti saanut uhrin paljastamaan haluamansa tiedon, hän lopettaa hyökkäyksensä tarkkailemalla uhrinsa mielialaa, mikäli hyökkäykseen valittu kommunikointikanava ja –tapa antaa tähän mahdollisuuden. Tämän vaiheen tarkoitus on varmistaa, että uhrin mieliala on palautunut normaaliksi eikä uhrilla ole huono omatunto tai syyllisyyden tunteita paljastuneen tiedon johdosta. (Mouton, Leenen, Maian & Venter 2014, 6–7.)

Kun sosiaalinen manipulointihyökkäys on saatu päätökseen, hyökkääjä arvioi paljastuneen tiedon hyödyntämismahdollisuutta. Tarvittaessa aikaisemmin tekstissä esitetty hyökkäyssykli aloitetaan alusta, hyödyntäen edellisessä syklissä paljastunutta tietoa. Mikäli taas paljastunut tieto voidaan suoraan käyttää tietomurrossa, kuten pankkitunnusten tai kirjautumistietojen tapauksessa, sosiaalinen manipulointihyökkäys voidaan todeta päättyneeksi. Hyökkääjä voi itse hyödyntää näitä tietoja tai hän voi myydä nämä eteenpäin muille verkossa toimiville rikollisille.

Edellisten kappaleiden perusteella voidaan päätellä, että menestyksekäs sosiaalinen manipulointihyökkäys vaatii huomattavan määrän valmisteluja mutta myös taitavan toteuttajan, joka osaa käyttäytyä tilanteesta huolimatta luontevasti ja rennosti. Tämä korostuu varsinkin tilanteissa, joissa sosiaalinen manipuloija kohtaa uhrinsa kasvotusten. Kyvykäs sosiaalinen manipuloija on empaattinen, karismaattinen, sosiaalinen sekä vaikuttaa vaarattomalta. Tämä tukee myös luvun 2.1 lopussa olevaa johtopäätöstä, jossa esitettiin, miten sosiaalinen manipulointihyökkäys on hyvin suunniteltu ja strukturoitu yhteydenotto, jonka toteutuksessa hyvin vähän on jätetty sattuman varalle. Hyökkääjän luonne nousee siis myös tärkeään asemaan hyökkäyksen onnistumisen kannalta.

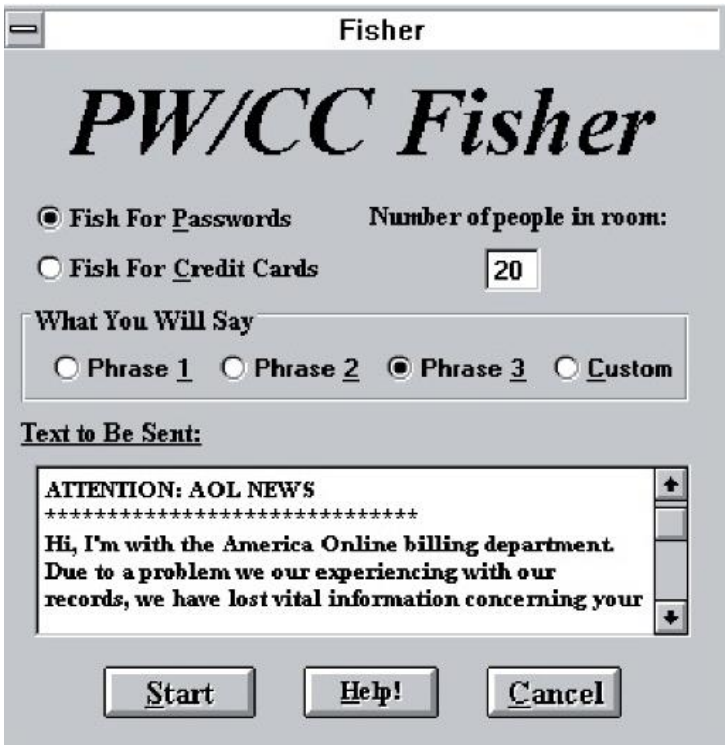
2.3. Mainittavia tapauksia

Yksi tunnetuimpia ja vanhimpia sosiaalisista manipulointihyökkäysmenetelmistä on niin sanottu “nigerialaiskirjehuijaus”, jonka virallisempi nimi “419 huijaus” viittaa nigerialaiseen lakipykälään 419, joka tekee tämän kaltaisista hyökkäyksistä laittomia sekä asettaa rangaistusvaatimukset kyseiseen rikokseen syyllistyneille. Hyökkääjä lähestyi uhria sähköpostitse ja tyypillisesti viestissä hyökkääjä paljasti uhrille tietävänsä suuresta summasta rahaa, jonka saamiseksi hän kuitenkin tarvitsisi uhrin apua. Viestissä hyökkääjä pyysi uhria antamaan pankkitilinsä tietoja suuren rahasumman “pesua” varten. 419 huijauksen takia moni henkilö on menettänyt suuria summia rahaa ja tämän huijauksen seurauksena on jopa kidnapattu henkilöitä. (Gillaerts & Gotti 2008, 261.)

Ensimmäiset sosiaalisen manipuloinnin automatisoidut ratkaisut kehitettiin pian Internetin luonnin jälkeen. Vuonna 1994 AOL eli America Online -palvelu kukoisti: kyseessä oli webportaali, jossa käyttäjien oli mahdollista luoda sähköpostitili, keskustella muiden käyttäjien kanssa pikaviestimen avulla sekä käyttää selainta verkon surffailuun (Computer Gaming World 1994, 118). Verkon tietoturva oli tuolloin lähinnä suurien organisaatioiden ja hallintoelinten ongelma, eivätkä tavalliset käyttäjät osanneet vielä varoa verkossa liikkuvia huijareita tai epäillä heidän huijausyrityksiänsä sellaisiksi.

AOL-portaalin käyttäjä “Da Chronic” kehitti 90-luvun puolivälissä ohjelman, jonka tarkoitus oli huijata käyttäjiä luovuttamaan luottokortti- tai kirjautumistietoja sekä häiritä AOL:n normaalia toimintaa. Nimeksi ohjelma sai AOHell. Hyökkääjien alkuperäinen päämäärä oli huijata itselleen ilmaisen pääsyn web-portaaliin, maksamatta noin 20 dollarin kuukausimaksua, hyödyntämällä käyttäjien antamia salasanoja ja luottokortteja, joita siihen asti kalasteltiin yksittäisiltä käyttäjiltä yksittäisen hyökkääjän toimesta. Hyökkääjien suosimat paikat toteuttaa kyseisiä huijauksia olivat ymmärrettävästä syystä uusien käyttäjien chattihuoneet. AOHell-ohjelman yksi käyttötapauksista oli seuraavanlainen:

- hyökkääjä sai itselleen käyttöön AOL-tilin joko varastamalla salasanan tai maksamalla kuukausimaksu varastetulla luottokortilla tai pankkitiedoilla
- hyökkääjä keksii tililleen uskottavan kuuloisen käyttäjänimen, kuten ”Laskutusosasto” tai ”Admin”
- hyökkääjä kirjotti AOHell-ohjelman kenttään haluamansa huijausviestin, jossa hän pyysi haluamansa tiedon kuten salasanoja tai luottokorttitietoja
- hyökkääjä paikansi yhden uusien käyttäjien chattihuoneista
- Hyökkääjä käynnisti ohjelman, joka lähetti jokaiselle käyttäjälle yksityisviestinä hyökkääjän ennalta määrätyn viestin.



Kuva 4. AOHellin käyttöliittymän näkymä (mukaillen Rekouche 2011)

Kuten kuvasta 4 voi havaita, ohjelma lähetti halutun viestin valitun chattihuoneen käyttäjille. Lisäksi se myös automaattisesti tallensi saapuneet vastaukset myöhempää käyttöä varten. Ohjelma oli helppokäyttöinen eikä sen hyödyntämiseen tarvittu teknistä osaamista, joten sen käyttäjämäärä oli huomattava. Onnistumisprosentti oli korkea monesta syystä: hyökkäys kohdistettiin uusiin käyttäjiin, jotka eivät tunteneet palvelua tai siihen aikaan

edes Internetiä, automatisointi mahdollisti hyökkäyksen kohdistamisen monen chattihuoneeseen samanaikaisesti, hyökkäykseen hyödynnettiin varastettuja käyttäjätilejä, jotka eivät olleet yhdistettynä hyökkääjän identiteettiin sekä AOL-palvelun käyttämä verkkoinfrastruktuuri ei mahdollistanut hyökkääjän jäljittämistä puhelinnumeron perusteella. (Rekouche 2011, 1–9.)

Vuonna 2002 PayPalin käyttäjiin kohdistui lyhyen ajan sisällä kaksi hyökkäystä. Yrityksen nimissä lähetettiin kalastelusähköposteja, joissa käyttäjiä kehotettiin kirjautumaan palveluun klikkaamalla sähköpostista löytyvää linkkiä, jotta palvelun tuottajat tietäisivät tilin olevan vielä aktiivinen. Pian sen jälkeen toinen sähköposti saavutti käyttäjiä ja jälleen kerran käyttäjiä pyydettiin kirjautumaan palveluun pyydetyn linkin kautta, jotta käyttäjä voisi tarkistaa oman tiedon oikeellisuuden “tapahtuneen tietomurron jälkeen”. (Rosencrance 2002.)

Vuonna 2009 FBI:n “Operation Phish Phry” jäljitti kymmeniä yhdysvaltalaisia ja egyptiläisiä talousrikollisia, jotka olivat vuodesta 2007 siirtäneet pankin asiakkailta rahaa omiin pankkitileihinsä varastettujen pankkitunnusten avulla. Rikoksen mahdollistivat uhreille lähetetyt kalastelusähköpostit, joiden avulla rikolliset onnistuivat kalastelemaan uhrien pankkitietoja ja salasanoja pankin kirjautumissivuston näköisen verkkosivun kautta. (Singer 2012.)

Vuonna 2014 Sony joutui valtavan tietomurron kohteeksi: hyökkääjät julkaisivat suuren määrän organisaation salaisia dokumentteja, palkkatietoja ja työntekijöiden sähköposteja. Viranomaisten rikostutkinnan edetessä esiin tuli vahvoja viitteitä siitä, että hyökkäyksen alkuperä olisi Pohjois-Korea. Valtion hallintamuoto herätti epäilyksiä siitä, että hyökkäyksen alkuperä olisi yksittäisen kansalaisen tai hakkeriryhmän tekoja, vaan hyökkäystä olisi edesauttanut, ainakin jossain muodossa, Pohjois-Korean valtio. Hyökkääjät todennäköisesti onnistuivat pääsemään organisaation verkkoon kohdennetuilla kalasteluviesteillä organisaation johdolle, verkon ylläpitäjille ja muille tärkeille avainhenkilöille, joissa heitä pyydettiin vahvistamaan AppleID:n käyttäjätunnuksia ja salasanoja. Organisaation vuodetuissa sähköpostiviesteissä oli useita viitteitä AppleID:stä sekä pyyntöjä varmistaa viestin saajan sisäänkirjautumistietoja. (Van Der Werff & Lee, 2015; Keizer 2015.)

Maailmaa säännöllisesti ravistelevat kriisitilanteet herättävät ihmisissä stressin, pelon ja epätietoisuuden tunteita, joita verkon rikolliset, sosiaaliset manipuloijat mukaan lukien, alkavat välittömästi hyödyntää omien rikollisten tavoitteiden saavuttamiseksi. Normaalissa tapauksessa sosiaalinen manipuloija pyrkisi yhteydenotollaan herättämään uhrissaan voi-

makkaita tunteita. Näissä kriisitilanteissa, tosin, sosiaalisen manipuloijan on vain hyödynnettävä yhteiskunnassa sillä hetkellä vallitsevaa huolta. Tuorein tämän kaltainen tapaus on maailmaa tällä hetkellä ravisteleva koronaviruskriisi, jota on jo osattu laajasti hyödyntää sosiaalisten manipulointihyökkäyksien toteuttamisessa. Sähköpostit vaikuttavat olevan luotettavilta lähettäjiltä, kuten esimerkiksi Maailman Terveysjärjestöltä, vakuutusyhtiöiltä tai saman organisaation työntekijältä. Viesteissä kehotetaan vastaanottajaa klikkaamaan erilaisia linkkejä tai lataamaan sähköpostissa olevia liitteitä tietokoneelle. Jotkut viesteissä olevat linkit avaavat huijaussivun, jossa käyttäjää kehotetaan syöttämään kirjautumistietojaan aidon näköiseen sisäänkirjautumissivulle. Sivustot ovat rakennettu lähettämään tällä tavalla syötetyt kirjautumistiedot suoraan hyökkääjän sähköpostiin. Viestien otsakkeita analysoimalla sähköpostit tulivat Venäjältä, Alankomailta, Saksasta ja Afrikasta. (Baggett & Alibe 2020.)

Myös Suomessa on havaittu huijausviestejä, jotka yrittävät käyttää hyödyksi koronakriisin aiheuttamaa epävarmuutta. Maaliskuussa Kyberturvallisuuskeskuksen julkaisemassa uutisessa käyttäjiä varoitettiin liikkeellä olevista huijaussähköposteista, joissa käyttäjiä pyydettiin lataamaan erilaisia koronavirukseen liittyviä ohjeistuksia tai työpaikan nimissä lähetettyjä tärkeitä tiedostoja. (Kyberturvallisuuskeskus 2020.)

Esimerkkejä riittäisi listattavaksi tähän kappaleeseen, sillä sosiaalisia manipulointihyökkäyksiä on toteutettu onnistuneesti useita Internetin historian saatossa. Mielenkiintoista on tosin analysoida sosiaalisten manipulointihyökkäysten historiaa ja evoluutiota vertaamalla näitä muihin kyberrikoksissa havaittuihin muutoksiin vuosien saatossa.

Esseessään professori Grabosky tutkii kyberrikollisuuden evoluutiota ja tunnistaa kolme merkittävää muutostrendiä: kyberrikosten toteutustavat ovat kehittyneempiä, kyberrikolliset tavoittelevat hyökkäyksillään taloudellista voittoa sekä uusina toimijoina ovat nousseet kansainvälisen järjestäytyneen rikollisuuden lisäksi myös valtiolliset toimijat (Grabosky 2017, 15–36). Tässä kappaleessa esitettyjen esimerkkien perusteella voidaan tulla johtopäätökseen, että myös sosiaaliset manipulointihyökkäykset ovat kehittyneet muiden kyberrikosten lailla. Siinä missä Internetin ensimmäisinä vuosina sosiaalista manipulointia harjoittivat nuoret harrastajat tavoitteena huijata itselleen lisää käyttöaikaa AOL-portaalissa yksittäisiltä käyttäjiltä, vuosien saatossa rinnalle on noussut valtiollisia toimijoita, jotka kohdistavat hyökkäyksen suuriin kansainvälisiin yhtiöihin tai joiden koko hyökkäyksen tavoite on rahallisen voiton maksimoiminen. Osittain sosiaalisten manipulointihyökkäysten muutos johtuu myös lisääntyneistä internetin tarjoamista mahdollisuuksista, jotka tarjoavat huomattavasti suuremman kirjon mahdollisuuksia käyttää tai myydä eteenpäin käyttäjiltä anastettua tietoa.

3. Suojautuminen

Tietoturva kokonaisuudessaan on mielestäni laaja, monimutkainen ja vaikeasti ymmärrettävä osa-alue tavalliselle käyttäjälle. Tämä on hyvin ymmärrettävä tunne, sillä sellainen tietoturva todellisuudessa on: sitä ei voida nähdä yksittäisenä komponenttina, ohjelmistona tai toimintatapana, vaan käyttäjien ja organisaatioiden tietoturva on aina osiensa summa ja yhtä vahva kuin sen heikoin lenkki. Vaikka yksittäisen osa-alueen tehokkuus olisikin helposti mitattavissa ja näyttäisi erinomaisen tehokkaalta päältä puolin, pienikin haavoittuvuus muualla verkossa voi avata ovet hyökkääjille ja haittaohjelmille järjestelmiin, joita luultiin mahdottomiksi murtaa. Tehokkuutta ja toimivuutta on myös helppo mitata, kun kyse on ohjelmistoista ja muista teknisistä ratkaisuista: ohjelmistojen lokit auditoidaan, löydetyt haavoittuvuudet paikataan päivityksellä ja yhteensopivuuksia testataan. Miten mitataan käyttäjien osaamistaso ja kiinnostus ylläpitämään omaa ja organisaation tietoturvaa sosiaalisia manipulointihyökkäyksiä vastaan? Miten voidaan tilastoida, kuka on alttiimpi manipulointiyritykselle ja kuka taas paljastaa liikaa tietoa kahvipöydässä? Tietoturvan ihmisaspektin laiminlyöminen voi johtaa vakaviin seurauksiin organisaatioissa. Täydellistä ratkaisua kaikkien manipulointitilanteiden torjumiseen ei ole, mutta on monta toimintatapaa, joita on todettu hyväksi ja toimivaksi suojauskeinoiksi.

3.1. Koulutus ja tietoisuuden lisääminen

Kuten aikaisemmassa luvussa esitettiin, sosiaalisten manipulointihyökkäyksien kohteena on aina ihminen. Tämän perusteella voidaan päätellä, että myös näiden ehkäisyssä kuuluisi vahvasti keskittyä käyttäjiin ja heidän osaamiseensa. Hyökkääjät suunnittelevat hyökkäyksiään hyvin tarkasti ja meidän psykologisia heikkouksiamme hyödyntäen. Heidän yhteydenottonsa ovat hienovaraisia ja vaikuttavat vaarattomilta, käyttäjässä herätetään voimakkaita tunteita ja hyökkäys on suunniteltu saamaan meidät käyttäytymään vaistomaisesti. Tehokkaan koulutuksen suunnittelussa nämä hyökkäyksien ominaisuudet kuuluisivat olla vahvasti esillä, jotta käyttäjät osaisivat tunnistaa vaaran kohdatessaan sosiaalista manipulointia ja pysähtyisivät analysoimaan edessä oleva tilanne kriittisin silmin.

Organisaation hyvää tietoturvatasoa ei saavuteta satunnaisilla tunnin pituisilla koulutuksilla, vaan organisaation kuuluisi luoda ilmapiiri, jossa tietoturvatietoisuus on luonnollisesti osa hyviä toimintatapoja sekä käyttäjät näkevät tietoturvakäytäntöjä yhtenä osana päivittäisiä rutiineja. (Hadnagy & Wilson 2009, 339–340.)

Yleisesti tietoturvakoulutuksien tuloksia analysoidessa voidaan identifioida kaksi suurta epäonnistumista: käyttäjät eivät koulutuksesta huolimatta ymmärrä tai havaitse riskien todellista suuruutta eivätkä he tunne tai välitä virallisista toimintaohjeista. Käyttäjiä pitää kannustaa olemaan aktiivisia toimijoita organisaation tietoturvan ylläpitämisessä eivätkä pelkästään passiivisia käyttäjiä, jotka siirtävät vastuun tietoturvan ylläpitämisestä organisaation johdolle tai tietylle ohjelmistolle. Erityisesti pelotteluviestit, uhkailut ja muut varoitukset eivät yleensä tuota toivottua lopputulosta, vaan ne lisäävät käyttäjien stressiä ja pahimmillaan saavat käyttäjän toimimaan aivan kuin riskejä ei olisi lainkaan. Huomattavia poikkeamia organisaation ohjeistuksen ja päivittäisen käytännön toiminnan välillä ei pitäisi olla; lisäksi organisaation tehtävä on luoda helposti seurattavia rutiineja, jotka tukevat käyttäjien ohjeistuksen mukaista käyttäytymistä. (Bada, Sasse & Nurse 2019, 1–3.)

Käyttäjien koulutus ja tietoisuuden lisääminen nousevat hyvin tärkeään asemaan sosiaalisten manipulointihyökkäysten ehkäisyssä myös siksi, koska tämän tyyppisissä hyökkäyksissä korostuu voimakkaasti yksittäisen käyttäjän rooli osana koko organisaation tietoturvaa hyökkäyksen kohdistuessa organisaatioon. Mielestäni edellisissä kappaleissa esitetyt näkemykset tukevat hyvin toisiaan, sillä ne puhuvat samasta asiasta eri näkökulmasta: mikä olisi organisaation tietoturvatason ideaalitilanne ja miten tätä voitaisiin lähteä saavuttamaan välttämällä yleisimmät virheet. Hyvän tietoturvakulttuurin luominen organisaation sisäisesti on myös mielestäni tärkein työkalu oman ja organisaation suojaamista varten.

Sosiaalisen manipulointihyökkäyksien yhdeksi suojauskeinoksi on ehdotettu luonnetestien käyttöönottoa, joiden tarkoitus olisi käyttäjien koulutustarpeiden selvittäminen sekä koulutusresurssien kohdistaminen työntekijöiden luonteen perusteella perinteisen metodien sijasta. Kyselykaavakkeen kysymyksiin kuuluisi vastata vaistomaisesti ja ajattelematta vastausta liikaa, jotta saataisiin mahdollisimman totuudenmukainen näkemys käyttäjän luonteesta. Saatujen tulosten perusteella työntekijät jaetaan eri ryhmiin ja jokaisen ryhmän koulutusmateriaalit suunnitellaan ryhmien jäsenten yhteisten luonteenpiirteiden perusteella. Tällä tavalla toteutettu koulutus mahdollistaisi perusteellisemman paneutumisen käyttäjien kohtaamiin haasteisiin heidän luonteensa perusteella sekä tarjoaa räätälöityjä työkaluja käyttäjille oman suojaustason ylläpitämiseen. (Mann 2010, 162–167.)

Edellisessä kappaleessa esitetty kirjailijan idea kuulostaa paperilla hyvältä keinolta arvioida henkilöiden koulutustarpeita ja kohdistaa organisaation koulutusresursseja työntekijöiden tarpeiden perusteella, mutta itselläni tosin herää kyseiseen koulutustapaan liittyen muutama epäilys. Ensimmäisenä kyseenalaistaisin toimintatavan laillisuuden, sillä kyseinen työntekijöiden “erotteleminen” luonteenpiirteiden voitaisiin tulkita jopa Suomen lain-

säädännön vastaiseksi. Tämä voidaan mahdollisesti myös nähdä työntekijöiden asettamisena eriarvoisiin asemiin, ”huonoihin” ja ”parempiin”, jonka seurauksena työmoraali sekä kiinnostus tietoturvaa kohti saattaa laskea. Lisäksi luonnetestin ideoijan pätevyys ja ammattitaidon mittaaminen saattaa osoittautua haastavaksi, ellei mahdottomaksi. Mihin tieteellisiin tutkimuksiin tai konsepteihin kyseisellä tavalla toteutettu koulutus perustuisi? Valitettavasti kirjailija ei paljasta, onko kyseisistä luonnetesteistä syntynyt mitattavia tuloksia, jotka tukevat hänen teoriaansa luonnetestien perusteella toteutetuista koulutuksista. Väittäisin, että työntekijöiden luonteen huomioimisella osana koulutusta ei ole vaikutusta koulutuksen onnistumisen kannalta. Päinvastoin tämä voi olla jopa haitallista, mikäli tämän seurauksena työntekijä kokee voivansa soveltaa virallisia toimintatapoja luonteensa perusteella. Luonteesta huolimatta säännöt, käytännöt ja toimintatavat kuuluisi organisaatiossa olla samat.

Tehokkaan tietoturvatason saavuttamiseksi erityisesti sosiaalisia manipulointihyökkäyksiä silmällä pitäen, yksi ehdotetuista ratkaisuista on rakentaa organisaation suojaustasoa “sipulimaisesti”. Ytimessä, tärkeämpänä suojauskeinona, on organisaation tietoturvakäytännöt. Näissä kuuluisi määritellä verkon tietoturvatason minimivaatimuksien lisäksi myös selkeän ohjeen organisaation arkaluontoisesta tiedosta, jota työntekijät eivät saa missään tapauksessa paljastaa kysyjästä riippumatta. Tämä selkeyttää rajan arkaluontoisen ja ei-arkaluontoisen tiedon välillä. Seuraavana suojauskerroksena kuuluisi olla tietoisuuden lisääminen käyttäjien kouluttamisen avulla. Koulutuksessa pitäisi käsitellä sosiaalisten manipulointihyökkäyksessä käytetyt psykologiset tekniikat, tietoa luottamussuhteen hyväksikäytöstä sekä muista metodit, joilla hyökkääjät saavat itselleen tavoittelemansa tiedon. Suojauspolitiikkarakenteen seuraava kerros on erityisesti suunnattu niille työntekijöille, jotka asemansa vuoksi ovat usein tekemisissä muiden työntekijöiden ja ulkopuolisten kanssa. Tällaisia ovat esimerkiksi aulatyöntekijät, sihteerit ja tukipalveluhenkilöstö. On erittäin tärkeää nostaa näiden työntekijöiden tietoisuutta hyökkääjien käyttämistä suostuttelukeinoista sekä miten niiltä tehokkaasti voidaan suojautua. Seuraava “suojauskerros” on tietoturvakäytäntöjen toistaminen ja valmiustason jatkuva varmistaminen. Käyttäjiä pitää ajoittain muistuttaa vaaroista ja käytössä olevista suojauskeinoista esimerkiksi säännöllisellä palaverilla, jossa läpikäydään organisaatioon kohdistuneet uhat sekä kerrataan käytännöissä määriteltyjä suojauskeinoja. Suojauspolitiikan toiseksi viimeinen kerros käsittelee “sosiaalisen manipuloinnin miinojen” implementointia organisaatiossa. Nämä “miinat” ovat käytäntöjä, joiden tarkoitus on hidastaa tai pysäyttää hyökkäystä erilaisin keinoin ja varoittaa käyttäjiä verkossa olevasta vaarasta. Esimerkiksi organisaatio voi implementoida käytännön, jossa puhelimitse pyydetyn salasanan resetoinnin yhteydessä tukipalveluiden työntekijä kysyy käyttäjältä kolme ennalta sovittua kysymystä, joiden vastaus on myös tu-

kipalvelun työntekijän tiedossa. “Sipulimaisen” tietoturvakäytäntöjen viimeisimpänä kerroksena on henkilön tai osaston määrittäminen, joka riskin toteutuessa osaa tutkia hyökkäyksen suuruutta sekä palauttaa tilanteen normaaliksi. Tämä on hyvä olla sovittuna ennen riskin toteutumista, jotta reagointiaika hyökkäyksen toteutuessa ei pitkittyisi vastuuhenkilöiden puutteen vuoksi. (Gragg 2002, 10–19.)

Kirjoittajan ehdottama “sipulimainen” runko, jonka tiivistin edellisessä kappaleessa, on mielestäni erinomainen pohja organisaatiolle oman tietoturvapolitiikan luomiselle, joka olisi mahdollisimman varautunut myös sosiaalisia manipulointihyökkäyksiä vastaan. Se mahdollistaa organisaation omien sisäisien käytäntöjen ja muiden sääntöjen kategorisointia ja implementointia osana kerroksittaista kokonaisuutta, joka selkeästi myös määrittelee eri käytännöille tärkeysjärjestyksen. Tämä puolestaan taas selkeyttää koko tietoturvapolitiikkaa organisaation työntekijöille. Pidän myös ideasta rajata selkeästi, mikä on arkaluontoista tietoa ja mikä ei. Tällä menettelytavalla on mielestäni muutama selkeä hyöty: mikäli kyseinen määrittely tehdään organisaatiotasolla, väistyy käyttäjäkohtainen subjektiivinen näkemys tiedon arkaluontoisuudesta. Näin poistuu myös oletus siitä, että käyttäjät valmiiksi tietäisivät miten kyseistä luokittelua tulisi tehdä, pohjautuen kunkin käyttäjän yleissivistykseen. Kyseinen määrittely myös edesauttaa yhtenäisten toimintatapojen luomista, mikä puolestaan vahvistaa entisestään tietoturvakäytäntöjen tehokkuutta.

Jotkut kirjoittajan ehdottamat ideat kyseisen “politiikkarungon” implementointiin ovat kuitenkin mielestäni liian radikaaleja ja saattavat aiheuttaa enemmän haittaa kuin hyötyä. Aikaisemmin viitatussa tutkimuksessa Gragg (2002, 10-19) ehdottaa yhdeksi koulutuskeinoksi sosiaalisen manipulointihyökkäyksen kohdistamista organisaatioon ja tämän tulosten läpikäynti erillisessä koulutustilaisuudessa, jossa jokaiselle käyttäjälle kerrotaan mitä tietoa hyökkääjä on häneltä onnistunut saamaan. Koulutuksen tavoitteeksi hän asettaa tietoisuuden lisääminen, jota kyseinen koulutus kieltämättä saavuttaisi nimetyillä menetelmillä, mielestäni kuitenkin tämän kaltainen tapahtuma olisi käyttäjille lähinnä hyvin nöyryyttävä kokemus. Mielestäni organisaatio saattaa tämän kaltaisella lähestymistavalla vahingoittaa työntekijän asennetta koko organisaatiota sekä omaa työtä kohtaan. Olen tämän asian kannalta samaa mieltä Bada ym. (2019, 3) kanssa, jotka tutkimuksessaan väittävät uhkailuiden ja pelottelukeinojen olevan tehottomia keinoja tietoisuuden lisäämiseksi, jotka voivat pahimmillaan johtaa stressiin ja välinpitämättömyyteen käytäntöjä kohtaan. Tehokkaampi tapa lisätä tietoisuutta tämän kaltaisia hyökkäyksiä kohtaan voisi olla Hadnagyn ja Wilsonin (2010, 340) esittämä keino, jossa käyttäjille näytetään sosiaalisten manipulointihyökkäysten vaikutukset organisaatioon niiden onnistuessa. Näin käyttäjä pääsee näkemään hyökkääjän käyttämät keinot ja osaa varautua näitä vastaan sekä ha-

vaitsee vakavat seuraukset organisaatioon. Tällä keinolla sosiaalinen manipulointihyökkäys ei jää abstraktiksi käsitteeksi, vaan todistetaan, mitä haittaa niistä pahimmillaan voi koitua ja miten jokaisen rooli on erittäin tärkeä kaikkien tietoturvatason ylläpitämiseksi. Käyttäjä saa itselleen arvokasta tietoa oman ja organisaation suojaustason ylläpitämiseksi ilman henkilökohtaista nöyryytystä koulutustilaisuudessa.

Eräs tapa selvittää oman organisaation valmiustasoa sosiaalisia manipulointihyökkäyksiä vastaan on toteuttaa tietynlainen “auditointi”, jonka tarkoitus on koetella työntekijöiden sisäisien käytäntöjen noudattamista. Orgill, Romney, Bailey ja Orgill suorittivat tämän kaltaisen “auditoinnin” toteuttamalla sosiaalisen manipulointihyökkäyksen, joka kohdistui organisaation työntekijöihin. He valitsivat auditoijan, joka oli organisaation ulkopuolinen henkilö, ja hänelle annettiin kokeen alussa mahdollisuus hakea tietoa organisaatiosta ja sen avainhenkilöistä. Auditoija asetti testin tavoitteeksi selvittää, kuinka moni työntekijä noudattaa lähes universaalia sääntöä olla antamatta salasanaansa kolmansille osapuolille. Hän valmisti lyhyen kyselyn, jossa käyttäjiä pyydettiin muiden kysymysten ohella antamaan käyttäjätunnuksensa ja salasanansa sillä tekosyyllä, että organisaatiossa olisi käynnissä suuri verkon tietoturvatason arviointi. Hän onnistui löytämään kulkukortin ja pääsi tämän avulla organisaation toimistotiloihin toteuttamaan kyselyn kohtaamalla työntekijöitä henkilökohtaisesti. Tulokset ovat huolestuttavia: keskimäärin lähes 60 % kyselyyn vastanneista kirjoitti “auditoijan” kyselykaavakkeelle salasanansa ja joissain osastoissa kaikki kyselyyn osallistuneet työntekijät kirjoittivat kaavakkeelle sekä käyttäjätunnuksensa että salasanansa. (Orgill, Romney, Bailey & Orgill, 1–5.)

Tutkimuksen toteuttajat eivät ottaneet kantaa syihin, miksi niin moni käyttäjä päätti vapaaehtoisesti luovuttaa sisäänkirjautumistietonsa. Uskallan väittää, että korkea onnistumisprosentti johtuu myös kyselyn toteutustavasta, jossa auditoija päätti henkilökohtaisesti toteuttaa kyselyn kohtaamalla organisaation työntekijöitä. Valitulla keinolla hän pääsi luomaan aidolta vaikuttavan luottamussuhteen kyselyyn osallistuviin henkilöihin, onnistuen näin manipuloimaan kyselyn osallistujien käytöstä auditoinnin aikana. Uskon myös vahvasti, että mikäli hän olisi päättänyt toteuttaa kyselyn verkkolomakkeella tai sähköpostitse, sekä kyselyn kokonaisvastausprosentti että salasanan luovuttajien prosentti olisi ollut huomattavasti pienempi. Perustelen tämän väitteen sillä, että mielestäni useampi käyttäjä olisi osannut odottaa ja varoa verkon kautta tulevia tiedonkalasteluviestejä. Oman havainnon mukaan kyseiset toteutustavat ovat yksinkertaisesti enemmän esillä tietoturvakeskustelussa, niin organisaatioiden virallisissa käytännöissä kuin esimerkiksi uutisissa, jonka seurauksena käyttäjien varautumistaso tämän kaltaisia hyökkäyksiä vastaan on korkeampi.

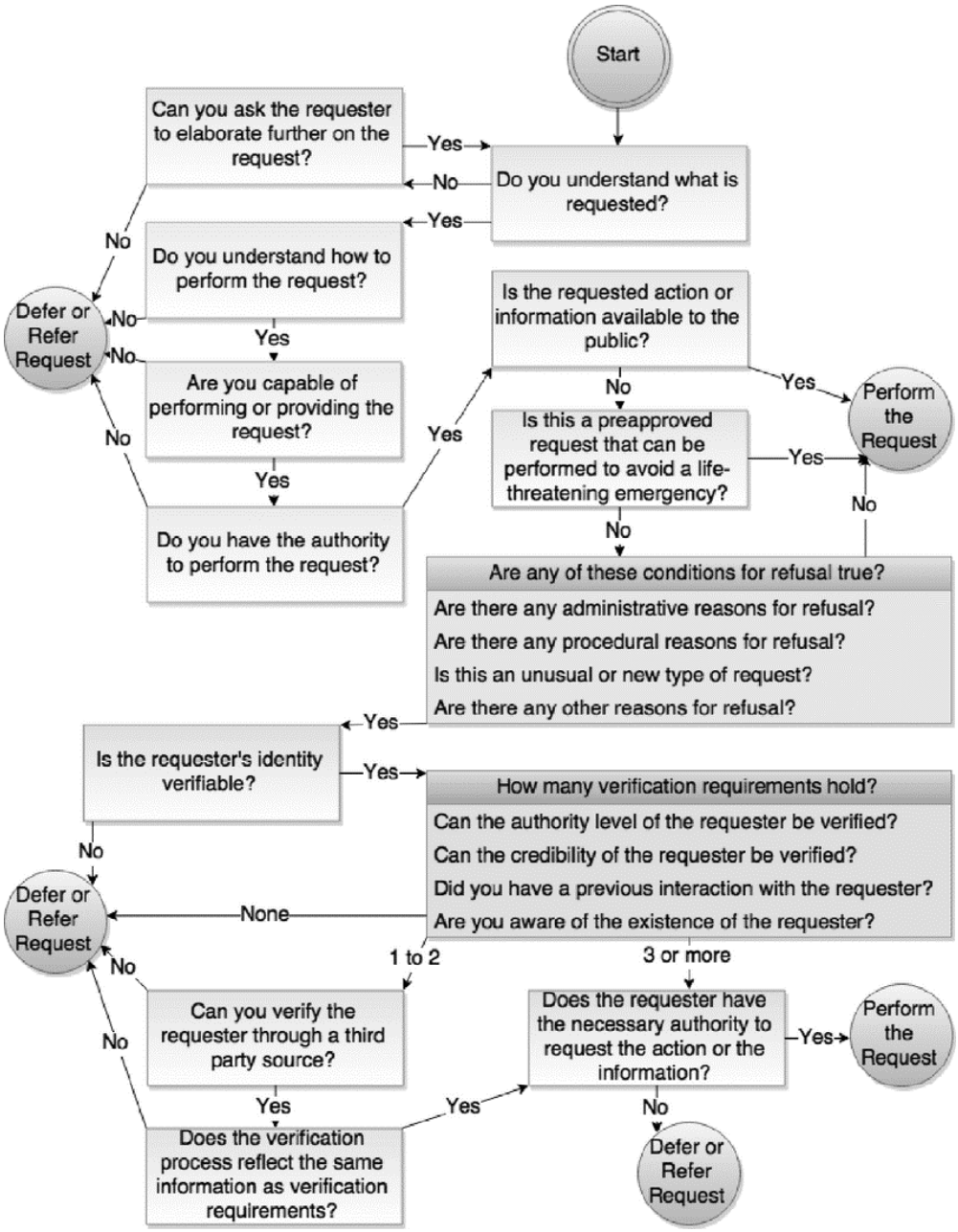
Aikaisemmassa kappaleessa mainitsin Hadnagyn ja Wilsonin (2010, 340) ehdotuksen demonstroida sosiaalisen manipulointihyökkäyksen etenemistä ja sen seurauksia käyttäjille. Auditointituloksia analysoimalla nousee väistämättä mieleen kysymys olisiko kyseinen koe tuottanut erilaisia tuloksia, mikäli käyttäjät olisivat ennakkoon osanneet varautua tämän kaltaisiin manipulointihyökkäyksiin. Mielenkiintoinen idea koulutukselle olisi näiden kahden konseptin yhdistäminen yhdeksi kokonaisuudeksi: organisaatio voisi toteuttaa tutkimuksen kaltaisen auditoinnin, jonka tuloksia analysoidaan erillisessä koulutustapahtumassa. Tilaisuuden sisältö tuloksien lisäksi olisi sosiaalisessa manipuloinnissa käytettyjen tekniikoiden läpikäynti ja sosiaalisen manipuloinnin mahdollistama vahingon toteaminen käyttäen pohjana kyseistä auditointia. Koulutuksen jälkeen, myöhempänä ajankohtana, organisaatiossa toteutetaan toinen vastaavanlainen auditointi. Auditoinnin rakenteen ei tarvitsisi olla täysin vastaava, mutta siinä käytettyjen tekniikoiden kuuluisi kuitenkin olla käyttäjien tunnistettavissa. Tämän kaltaisen syklin toistamisella useamman kerran olisi mielestäni selkeästi hyötyä käyttäjille sekä organisaation tietoturvatasolle. Toisto itsessään tuo myös hyötyjä, sillä se auttaa työntekijöitä muistamaan oikeat käytännöt sekä kehittää heidän havainnointikykyänsä.

Mielestäni esimerkin kaltainen “auditointi” on erinomainen tapa testata organisaation suojaustasoa sekä parantaa organisaation suojaustasoa mahdollisien sosiaalisten manipulointihyökkäysten varalta. Tuloksien anonymisointi ennen analysoimista, kuten meneteltiin yllä olevassa tutkimuksessa, on mielestäni perusteltua. Kokeen tavoitteena ei ole tunnistaa ja rankaista yksittäisiä käyttäjiä tai osastoja, vaan tarkoitus on tarjota organisaatiolle laajan kokonaiskuvan sillä hetkellä voimassa olevien käytäntöjen pätevyydestä ja toimivuudesta yleistasolla sekä identifioida tärkeimmät kehityskohteet paremman suojaustason saavuttamiseksi. Lisäksi kokeessa käytetyt psykologiset menetelmät ovat samat, joita hyökkääjä hyödyntäisi aidossa sosiaalisessa manipulointihyökkäyksessä, joten näin saatu data on lähes suoraan verrattavissa oikean hyökkäyksen seurauksena tapahtuneeseen vahinkoon.

Tässä luvussa esitettyjen tutkimuksien ja teoksien tekijöistä moni uskoo, että paras suojautuminen sosiaalisia manipulointihyökkäyksiä vastaan edellyttää jatkuvaa kouluttamista sekä koulutuksessa opitun tiedon toistamista. Näistä kahdesta tekijästä on mielestäni myös huomattavasti vaikutusta siihen, miten hyvin onnistutaan organisaatiossa sisällyttämään tietoturvakäytäntöjä ja oikeaoppisia toimintamalleja osana henkilöstön normaaleja työtapoja.

Koulutuksien ja auditointien lisäksi käyttäjille on tarjolla myös työkaluja, joiden avulla he pystyvät tapauskohtaisesti analysoimaan kohtaamiaan epäselviä tai epäilyksiä herättäviä

pyyntöjä ja päättelemään, kuuluuko niihin vastata ja jos, niin miten. Loogisen päättelyn tueksi on ehdotettu eräänlaista rakennetta, jossa lähtökohtana on saapunut viesti ja oikeaoppinen toimintatapa määräytyy rakenteessa olevien kysymyksien vastauksen perusteella. Rakenteessa on otettu huomioon neljä elementtiä, joiden ominaisuudet vaikuttavat lopputulokseen: itse pyynnön lisäksi pyynnön lähettäjä, pyynnön vastaanottaja ja kolmas osapuoli, joka voi tarvittaessa tarkistaa ja varmistaa kysyjän identiteetin. Viestin sisältö on rakenteen lähtökohta, jossa vastaanottajan kuuluu pohtia, ymmärtääkö hän tarkalleen mikä kysyjän pyyntö on vai tarvitseeko hän tähän lisätietoja. Tämän kysymyksen vastauksen perusteella vastaanottaja etenee seuraaviin kysymyksiin: onko hänen mahdollista ymmärryksensä ja asemansa perusteella suorittaa mitä pyynnössä halutaan, onko pyynnössä haluttu tieto julkisesti saatavilla, onko pyyntö tietoturvakäytäntöjen tai muiden ohjeistuksen vastainen, onko kysyjän mahdollista asemansa perusteella kysyä haluttua tietoa ja niin edelleen. Kysymyspuun eri vaiheissa käyttäjä päätyy joko toteuttamaan alkuperäisen pyynnön tai hylkäämään sen sellaisenaan. (Mouton, Leenen & Venter 2015, 2–3.)



Kuva 5. Sosiaalisten manipulointiyritysten analysointia helpottava kysymysrakenne (mukaillen Mouton, Leenen & Venter 2015)

Tämän kaltainen työkalu on mielestäni loistava apukeino auttaa käyttäjiä päättelemään oikeat toimintatavat eri tilanteissa. Rakenne käsittelee laajasti erilaisia skenaarioita, joiden perusteella pyyntö voidaan hyväksyä tai hylätä. Rakenteen läpikäyminen ei vie huomattavia määrää aikaa ja tämä antaa mahdollisuuden suhtautua saapuneeseen viestiin analyyttisesti myös tilanteissa, joissa kyseessä on aidosti nopeita toimenpiteitä vaativa hätätilanne. Tämä on mielestäni rakenteen tärkein ominaisuus, sillä olen edellisissä kappaleissa tuonut usein esiin, miten sosiaalinen manipuloija pyrkii luomaan hätätilanteelta vaikuttavan tilanteen, joka herättämään vastaanottajassa voimakkaita tunteita ja joka saa hänet käyttäytymään virallisten ohjeistuksien vastaisesti. Lisäksi rakenteen avulla voidaan

analysoida niin verkosta saapuvia pyyntöjä kuin myös henkilökohtaisia yhteydenottoja. Ehdottaisin kyseisen analysointikeinon lisäämistä Graggin (2002, 10–19) ideoiman sipulimaiseen suojausrakenteeseen erityisesti sopivana työkaluna henkilöille, jotka asemansa vuoksi kohtaavat usein asiakkaiden tai muiden työntekijöiden pyyntöjä. Gragg itse painottaa kohdennetun koulutuksen tärkeyttä näissä asemissa oleville työntekijöille, yllä oleva rakenne voi tuoda huomattavia etuja tällaisessa asemassa työskenteleville henkilöille päätöksentekoa vaativissa epäselvissä tilanteissa.

Kokeilin tästä työstä löytyvien sosiaalisten manipulointiesimerkkien pyyntöjen analysoimista tämän rakenteen avulla, ja jokaisen kohdalla kysymysten perusteella päädyin tulokseen, jossa pyyntö kuuluisi hylätä tai selkeän kuvan muodostamiseksi olisi tarpeen pyytää lisätietoja. Mainittavaa on myös, että jokaisen kohdalla en olisi voinut varmistaa pyynnön lähettäjän identiteettiä eikä myöskään varmentaa tätä kolmannen osapuolen kautta. Esimerkkiotos on pieni, mutta tästä huolimatta rakenne vaikuttaa olevan hyvä apukeino sosiaalisten manipulointihyökkäyksiä vastaan.

Mielestäni organisaation hyviin tietoturvakäytänteisiin olisi lisättävä eräs suojauskeino, jota en onnistunut löytämään hyväksi havaituista tietoturvakäytänteistä tai muista aiheeseen liittyvistä tutkimuksista sen yksinkertaisuudesta huolimatta. Tämä on sääntö, jossa kielletään sähköpostitse saapuvien linkkien avaamista kaikissa tilanteissa, joissa sähköpostiviestissä olevaa tietoa on mahdollista varmistaa suoraan viestin oletetulta lähettäjältä itseltään. Tämän tutkimuksen ensimmäisessä luvussa esittelin erään pankin nimissä lähetetyn kalastelusähköpostin sekä esimerkeissä listasin PayPalin, Applen sekä toisen pankin nimissä lähetettyjä sähköpostiviestejä, joiden avulla onnistuttiin anastamaan käyttäjiltä heidän kirjautumistietojaan. Näissä tilanteissa, käyttäjät olisivat voineet suojautua manipulointihyökkäykseltä yksinkertaisesti tarkistamalla sähköpostissa olevan tiedon oikeellisuuden suoraan palveluntarjoajalta itseltään. Mikäli kyseessä olisi aito, välittömiä toimia vaativa tilanne, tämä olisi ilmennyt myös palveluntarjoajan kotisivuilla tai palvelun omasta käyttäjäportaalista. Vaihtoehtoisesti käyttäjä huomaa, että kyseessä on huijaus, ja välttää avaamasta linkkejä tai muutoin kommunikoimasta hyökkääjän kanssa.

3.2. Tekniset keinot

Yksi teknisistä keinoista suojata resursseja sosiaalisten manipulointihyökkäyksien seurauksista on monivaiheisen tunnistautumisen käyttöönotto. Ideaalitilanteessa autentikointiin tarvittava lisätunniste olisi kertakäyttöinen sekä saapuisi käyttäjän erilliselle laitteelle tunnistautumisvaiheessa. Näin kirjautuminen pelkästään varastetuilla kirjautumistiedoilla ei olisi mahdollista. Dokumenttien kategorisointi tiedon arkaluonteisuuden perusteella ja

tämän luokittelun perusteella toteutettu pääsynhallinta voi onnistuessaan suojata organisaation kriittisimmän datan tietomurron sattuessa. Kaikista kriittisimmät järjestelmät voidaan myös suojata estämällä julkisesta verkosta tulevia pyyntöjä, tosin tällä tavalla toteutettu pääsynhallinta saattaa vaikuttaa huomattavasti myös järjestelmän käytettävyyteen. (Mann 2008, 171–176.)

Yksinkertainen ja tehokas tekninen suojauskeino on ohjelmistojen säännöllinen päivittäminen. Vanhentuneissa ohjelmistoversioissa saattaa piillä kymmeniä haavoittuvuuksia, jotka voivat edesauttaa hyökkääjän tietomurtoa. Ohjelmistoversioiden päivityksissä on yleensä mukana myös kriittisiä tietoturvapäivityksiä, joissa korjataan julki tulleita haavoittuvuuksia. (Hadnagy & Wilson 2010, 347.)

Työasemien monitorointi sekä vain ennalta hyväksyttyjen ohjelmistojen käytön salliminen helpottaa käyttäjien tietoliikenteen seuraamista sekä ehkäisee turvattomien ohjelmistojen asentamisen seurauksena johtuvat tietoturvaloukkaukset (Gulati 2003, 7).

Erilaiset sähköpostifiltterit auttavat käyttäjiä suojautumaan sähköpostitse tulevilta manipulointihyökkäyksiltä. Sähköpostifiltterin toiminta voi perustua esimerkiksi otsakkeissa oleviin tietoihin tai itse viestissä oleviin avainsanoihin. Sähköposteja voidaan myös suodattaa lähettäjän osoitteen tai käyttäjän asettaman säännön perusteella. Joidenkin filttereiden toiminta perustuu havaittujen kalasteluviestien ominaisuuksien analysointiin, jonka tuloksen perusteella filtteri jatkossa suodattamaan ei-toivottuja sähköpostiviestejä. (Anslinger 2013; Almomani, Gupta, Atawneh, Meulenberg & Almomani 2013, 2.)

Sähköpostifiltterin käyttöönotto on hyvä keino suojautua sähköpostitse leviäviltä tietoturvauhkilta, jotka voivat levittää haittaohjelmia tai saastuttaa verkon laitteita. Sähköpostitse saapuvia sosiaalisia manipulointihyökkäyksiä vastaan se ei tosin yksinään riitä. Mikäli manipulointihyökkäysyritys sisältää tiettyjä avainsanoja ja tulee tunnetusta roskapostia lähettävästä osoitteesta, filtteri mahdollisesti suodattaa viestin ennen viestin päätymistä vastaanottajalle. Ohjelmisto ei tosin pysty päättelemään kaikkien viestien kohdalla, onko kyseessä normaali yhteydenotto vai manipulointiyritys. Mielestäni tosin näissäkin tapauksissa olisi mahdollista kuitenkin varoittaa vastaanottajaa siitä, että viestin lähettäjä on oman organisaation ulkopuolinen henkilö ja kehottaa häntä varovaisuuteen etenkin linkkien ja liitteiden osalta. Tämä voisi toteuttaa esimerkiksi lisäämällä varoitustekstin ennen sähköpostiviestin alkuperäistä sisältöä. Vaikka varoitusteksti yksin ei toki ehkäise haittaohjelmia leviämistä, se voi vähentää käyttäjän riskiä joutua manipulointihyökkäyksen uhriksi.

Edellisissä kappaleissa esitetyn tiedon perusteella voi päätellä, että sosiaalisen manipulointia vastaan kehitetty tekniset ratkaisut ovat enimmäkseen suunnattuja ehkäisemään tai lievittämään onnistuneen teknisen tai sosioteknisen sosiaalisen manipulointihyökkäyksen seurauksia. Sosiaalisia manipulointihyökkäyksiä ei ole mahdollista kategorisoida matemaattisesti aina tietyn kaavan perusteella, joten ohjelmiston on mahdotonta tulkita jokaisen viestin sisältöä. Vaikka hyökkäyksissä käytetyissä menetelmistä on mahdollista löytää yhteneväisyyksiä, nämä eivät mielestäni läheskään riitä luomaan johdonmukaista kaavaa hyökkäyksien rakenteesta, jonka avulla voidaan varmuudella kategorisoida yhteydenotot viattomiksi tai vaarallisiksi. Teknisten ratkaisujen käyttöönotosta on kuitenkin hyötyä organisaatioille. Esittelin luvussa 2.1, miten sosiaalinen manipulointihyökkäys ei ole tietomurtohyökkäys vaan kyseisten hyökkäyksen tietynlainen esiaste, jossa yritetään saada haltuun informaatiota itse tietomurtoa varten. Vaikeuttamalla kirjautumista kohteeseen esimerkiksi monivaiheisella tunnistuksella, voidaan hidastaa tai jopa kokonaan ehkäistä sosiaalisesta manipuloinnin ansioista saatujen kirjautumistietojen hyödyntämistä.

On olemassa teknisiin toteutustapoihin perustuva ratkaisu, joka voi auttaa suojaamaan organisaatiota myös itse sosiaalisten manipulointihyökkäyksien tiedonkalasteluyrityksiltä: niin kutsuttu zero trust –malli. Kyseinen toimintatapa perustuu siihen, että kirjautumistunnukset, joille on myönnetty laajat oikeudet kirjautumiskohteessa, säilytetään erillisessä holvissa. Täältä ne voidaan väliaikaisesti myöntää työntekijöille tarpeen mukaan, vaihtoehtona admin-tunnuksien myöntämiselle jokaiselle ylläpitäjälle. Lisäksi kirjautumiseen järjestelmiin tarvitaan aina erillinen syy sekä esimiehen tai muun tarkastajan hyväksyntä. Joissain tapauksissa hyväksyjän on jopa mahdollista valvoa sekä väärinkäyttötilanteissa katkaista istuntoja. Istunto voidaan tallentaa videomuodossa mahdollista tulevia auditointia varten. (Cyberark.)

Kyseisen mallin perusteella toteutettu tekninen ratkaisu on hyvä keino suojautua sosiaalista manipulointia vastaan, sillä tämän kaltaisella toteutustavalla viedään hyökkääjien ulottumattomiin juuri sen tiedon, minkä ne sosiaalisella manipulointihyökkäyksellä toivoo saavuttavansa. Olen työni puolesta ollut tekemisissä järjestelmän kanssa, joka tarjoaa juuri zero trust-mallin mukaisia ratkaisuja organisaatiolle. Mielestäni kyseisellä tavalla toteutettu kriittisten järjestelmien tunnuksien hallinta nostaa organisaation tietoturvatasoa ja vähentää mahdollisten virheiden määrää kohdejärjestelmässä. Perustelen tämän väittämän sillä, että kirjautumiseen zero trust –mallin mukaan tarvitaan myös syy sekä erillinen hyväksyntä. Tämä ehkäisee kirjautumista epähuomiossa väärään järjestelmään sekä sen seurauksena tapahtuvia virheellisiä ylläpitotoimenpiteitä.

Edellisessä luvussa esittelin sipulimaisen suojausrakenteen, jonka avulla on mahdollista luoda kattava organisaation tietoturvapolitiikka perustuen käytäntöihin, koulutuksiin ja erilaisiin ohjeistuksiin (Gragg 2002, 10–19). Rakenne ei juurikaan sisältänyt teknisiä ratkaisuja, mutta mielestäni rakenteen eri “kerrokset” voisivat kuitenkin hyötyä teknisistä suojaus- ja havainnointikeinoista. Nämä voisivat tukea käyttäjien toimia, auttaa heidät havainnoimaan epäilyttävät yhteydenotot sekä hälyttää tarvittavat henkilöt epäselvän yhteydenoton seurauksena.

Sipulirakenteen ytimen osana on tietoturvapolitiikan lisäksi tiedon luokittelu salaiseksi ja ei-salaiseksi: tämän vuoksi zero trust –mallin mukainen admin-tunnuksien hallinta olisi luonnollinen lisäys osaksi suojauspolitiikan ydintä. Zero trust –mallin voisi nähdä myös tiedonluokittelun eräänä muotona, joissa arkaluontoisimmat kirjautumistunnukset erotellaan muista kirjautumistunnuksista. Toisen kerroksen, käyttäjien koulutusten tueksi voisi asettaa ohjelmistojen ja käyttöjärjestelmien säännölliset päivitykset. Koulutusten tavoite on jo saadun tiedon kertaamisen lisäksi myös tiedon päivittäminen sekä uuden tiedon oppiminen, samankaltaiset vaatimukset voisi asettaa myös organisaation järjestelmille ja työasemille. Näin mahdollistetaan uusimman saatavilla olevan tiedon hyödyntäminen niin laitteiston käyttäjiltä kuin itse laitteistolta. “Sipulirungossa” esiteltiin erilliset koulutusvaatimukset työntekijöille, jotka ovat asemansa vuoksi muita useammin yhteyksissä ulkopuolisiin kanssa - nämä henkilöt mielestäni hyötyisivät erityisesti sähköpostifilttereistä sekä erilaisista viestien varoitusteksteistä, jotka auttavat erottelemaan tunnetusta verkosta tai tunnetulta lähettäjältä saapuvia yhteydenottoja muista. Lisäksi, mikäli mahdollista, näille henkilöille voisi myöntää muita vähemmän oikeuksia kohdejärjestelmiin, esimerkiksi vain lukuoikeuden: perustelen väittämän sillä, että sosiaalisen manipulointihyökkäyksen kohdistuessa näihin henkilöihin, vuodetutuilla tunnuksilla olisi mahdollista rajata järjestelmässä sijaitsevan datan turmelemismahdollisuutta. Rakenteen seuraava kerros ehdottaa koulutusmateriaalien ja käytänteiden säännöllistä toistamista oppimisen tueksi. Vastaavaksi tekniseksi ratkaisuksi ehdottaisin säännöllistä prosessien lokitusta sekä näiden auditointia: tällä varmistetaan järjestelmien konfigurointien toimivuuden sekä mahdollisesti voidaan havaita epäilyttäviä toimia nopeasti. Viimeisimpänä turvapolitiikan kerroksena on henkilön tai osaston määrittäminen, joka mahdollisimman nopeasti pääsee suojaamaan järjestelmää ja korjaamaan sattuneita vahinkoja: palvelimien kahdennuksella voidaan nopeasti korjata tarvittavat ympäristöt hyökkäystä edeltävälle tasolle itse korjaustoimenpiteiden ajaksi. Päivystävä henkilö voisi olla sama henkilö, jolla on valtuudet myös zero trust –holviin. Näin tarvittavat ylläpitotunnukset voivat olla nopeasti saatavilla, eikä hyökkäyksen torjumista varten tarvitse viivytellä ja odottaa kolmatta osapuolta.

Vaikka teknisillä keinoilla ei ole mahdollista suojautua itse manipulointihyökkäyksiä vastaan, niillä on mahdollista tukea organisaation tietoturvakäytäntöjä sekä vahvistaa järjestelmiä mahdollisen tietomurron varalta. Tämän perusteella voi tulla johtopäätökseen, että tekniset keinot ovat myös tärkeässä asemassa sosiaalisten manipulointihyökkäyksien vastaisessa taistelussa. Tämä korostuu entisestään, jos tekninen suojauskeino asetetaan yksittäisten tietoturvakäytäntöjen tueksi, kuten edellä esitetyn sipulimaisen rakenteen tapauksessa.

4. Pohdinta

Sosiaalinen manipulointi on verkkorikollisten käyttämä tekniikka, jonka kohde on aina ihminen ja jonka tavoite on saada uhri toimimaan tietyllä tavalla. Yleensä hyökkääjä tavoittelee tällä hyökkäystavalla uhrin tiedossa olevaa tietoa, kuten esimerkiksi erilaisia kirjautumistietoja ja luottokorttinumeroita, mutta myös muu henkilökohtainen tieto kiinnostaa hyökkääjiä. Hyökkääjät osaavat hyödyntää tehokkaasti eri kommunikointikanavia ja voivat toteuttaa hyökkäyksen myös kasvotusten. Kyseisten tietoturvahyökkäyksien suosion trendi on nouseva. Lisäksi sosiaalisista manipulointihyökkäyksistä on vuosien saatossa tullut kehittyneempiä, niillä tavoitellaan rahallista voittoa sekä näitä toteuttavat myös valtiolliset toimijat.

Sosiaalisia manipulointihyökkäyksiä ei toteuteta impulsiivisesti eikä niiden onnistuminen ole riippuvainen onnesta, vaan hyökkääjä suunnittelee hyökkäyksen jokaista vaihetta tarkasti. Hyökkääjän yhteydenotot ovat myös strukturoitu niin, että hyökkääjän ja uhrin välinen kommunikointi on mahdollisimman luontevan ja viattoman oloinen. Tämän takia sosiaalisia manipulointihyökkäyksiä on vaikea tunnistaa. Hyökkääjät suunnittelevat tarkasti yhteydenottonsa sisältöä, hyödyntäen erilaisia psykologisia keinoja, jotta uhri päättäisi luottaa hyökkääjään. Luottamussuhteen luominen on sosiaalisen manipulointihyökkäyksien tärkeimpiä välitavoitteita, sillä tätä hyväksikäyttämällä hyökkääjän on mahdollista suostutella uhria paljastamaan tavoiteltua tietoa. Hyökkääjällä on huomattava määrä keinoja, joilla hän onnistuu luomaan luottamussuhteen uhriin. Sosiaalinen manipulointi vaatii taitavan toteuttajan, joka osaa luontevasti ja rennosti kommunikoida uhrin kanssa ja edistää hyökkäystä herättämättä uhrin epäilyksiä.

Suojautuminen kyseisiltä hyökkäyksiltä on haastavaa. Myös manipulointihyökkäyksiltä suojautumisessa on kyse kompromissista ja riskin minimoimisesta, aivan kuten muidenkin tietoturvauhkien kohdalla. Organisaatiotasolla hyvä suojautuminen kyseisiä hyökkäyksiä vastaan edellyttää hyvän tietoturvakulttuurin luomista. Tämän tavoite on tehdä hyvistä käytänteistä osa normaaleja työtapoja. Käyttäjien jatkuva koulutus ja koulutuksessa opitun tiedon ylläpitäminen ovat hyvin tärkeitä suojauskeinoja, joilla varmistetaan tietoturvakäytäntöjen ymmärrys sekä näiden jatkuvaa soveltamista osana päivittäistä tekemistä. Myös eri käytäntöjen, sääntöjen ja toimintatapojen kategorisointi voi auttaa käyttäjiä selkeyttämään organisaation tietoturvapolitiikkaa kokonaisuutena. Organisaatiossa voidaan mitata käytäntöjen ja sääntöjen tehokkuutta erilaisilla auditoinneilla, näistä syntyviä tuloksia voidaan hyödyntää koulutuksissa sekä omien tietoturvakäytänteiden kehittämisessä. Mikäli organisaatiossa on työntekijöitä, jotka työkuvansa vuoksi kommunikoivat muita useammin

asiakkaiden tai ulkopuolisten henkilöiden kanssa, näille kuuluisi tarjota erityiskoulutusta ja lisätyökaluja sosiaalisten manipulointihyökkäyksien suojautumiseen. Tekniset keinot voivat tukea käyttäjien toimia sosiaalisten manipulointihyökkäyksien havainnoinnissa ja ehkäisyssä, mutta nämä yksin eivät tarjoa riittävää suojaustasoa.

Tämä tutkimusprosessi sai alkunsa halusta luoda omaa tutkimusprojektia, johon voisin kerätä oleellisimmat tiedot kyseisestä tietoturvailmiöstä sekä keinoja ehkäistä näistä syntyviä tietomurtoja ja tietoturvaloukkauksia. Halusin analysoida projektiini tutkijoiden sekä kirjailijoiden havaintoja sosiaalisesta manipuloinnista ja siltä suojautumiseen. Ajatuksenani oli, että kyseinen lähestymistapa olisi mahdollistanut laajan kokonaisuuden luomisen, joka keskittyisi itse ilmiön ja suojauskeinojen ominaisuuksiin. Lisäksi tämä oli mielestäni tehokkain menetelmä tuottaa tarvittavia tuloksia projektin aikataulusta ja laajuudesta johtuvien rajoituksien vuoksi. Tutkimuksessani en hyödyntänyt kyselyitä, sillä halusin välttää henkilöiden mielipiteiden vaikutusta sisältöön. Toiveenani oli luoda yleinen katsaus aiheeseen, joka perustuisi ammattilaisten havaintoihin ja tutkimuksiin ja jota olisi mahdollista soveltaa mahdollisimman moneen käyttötarkoitukseen.

Suhtaudun näillä menetelmillä tuotetuilla tutkimuksen tuloksiin terveen kriittiseesti. Ymmärrän, että tämä projekti on minun tekemä rakennelma näillä lähteillä ja lähteiden tulkintatavoilla; näin ollen myöskään tutkimukseni tulokset eivät ole täysin objektiivisia eivätkä edusta absoluuttista totuutta. Ilmiön tutkimustieto itsessään perustuu havaintoihin, joten myös käyttämäni lähteiden kirjoittajien näkemykset vaikuttavat osittain tutkimuksen tuloksiin. Näistä asioista huolimatta, tämän tutkimuksen tulokset kuvaavat mielestäni ilmiötä sekä suojauskeinoja pääosin hyvin ja oikein.

Ilmiön laajuus sekä moniulotteisuus pääsivät yllättämään tutkimuksen edetessä. Tutkimus onnistui vastaamaan tutkimuskysymyksiin sekä tuotti yleisen katsauksen ilmiöön tavoitteen mukaisesti. Tästä huolimatta ilmiöstä jäi vielä hyvin paljon kerrottavaa sekä tutkimuskysymyksien vastauksiin olisi mahdollista perehtyä vielä perusteellisemmin. Jouduin paikoin tekemään vaikeita päätöksiä ja valitsemaan mitä haluan sisällyttää tutkimukseen, jotta projekti itsessään olisi pysynyt aikataulussa ja toivotussa laajuudessa.

Edellä mainitusta huolimatta, projektin tutkimustuloksia on mielestäni mahdollista hyödyntää laajasti. Organisaatioiden tietoturvavastaavat sekä hallinnollisen tietoturvan vastuuhenkilöt voivat pohtia nykyisten käytäntöjen, koulutuksien ja teknisten ratkaisujen riittävyyttä organisaatiossa. Työssä esitetään laajasti myös hyväksi havaittuja suojauskeinoja sekä rakenteita, jotka helpottavat käyttäjiä omaksumaan hyviä tietoturvakäytäntöjä sekä mahdollistavat sosiaalisten manipulointihyökkäyksien havainnointia. Näitä rakenteita voi

myös soveltaa luomaan organisaatiolle vahvan, mutta omiin tarpeisiin räätälöidyn tietoturvapolitiikan. Hyökkäyksien ominaisuuksien kuvausta voi hyödyntää koulutuksissa sekä niiden avulla voidaan auttaa käyttäjiä havaitsemaan ja raportoimaan organisaatioon kohdistuvia sosiaalisia manipulointihyökkäyksiä. Teknisen tietoturvan vastuuhenkilöt voivat käyttää tuloksia omien ympäristöjen suunnittelussa sekä oikeanlaisten teknisten ratkaisujen valinnassa. Erilaiset palveluntarjoajat voivat myös käyttää tutkimusta selkeyttämään ja parantamaan heidän asiakasviestintäänsä sekä käytettyjä viestintäkanavia. Oma toiveeni olisi, että jokainen työn lukija hyödyntäisi tutkimustuloksia omalla kohdalla ja arvioisi omaa verkkokäyttäytymistä ja suhtautumista tuntemattomien ihmisten pyyntöihin. Jokainen lukija voi tässä projektissa olevan tiedon avulla parantaa omaa tietoturvaa sekä suojautua hyökkääjiltä.

Pääsen myös itse hyödyntämään tutkimustuloksia työssäni. Voin omien työskentelytapojen pohtimisen lisäksi myös vaikuttaa eri kehitysprojektien määrittelyihin niin, että näissä huomioitaisi sosiaalisten manipulointihyökkäyksien vaikutuksia heti projektin työstämisen alusta. Voin kehittää omaa asiakasviestintääni selkeämmäksi. Voin helpommin havaita minuun kohdistuvia sosiaalisia manipulointihyökkäyksiä ja raportoida näistä oikealle taholle, näin parantaen organisaationi tietoturvaa ja suojautumista kyseisiä hyökkäyksiä vastaan.

Olisin toivonut löytäväni lähteen, jossa vertaillaan hyvin suunniteltu ja kohdennettu manipulointihyökkäys ja massaviestinä lähetetyn tiedonkalastelusähköpostin välillä. En tähän projektiin löytänyt luotettavia lähteitä, jotka olisivat analysoineet myös massaviestinä lähetettyjä kalasteluviestejä. Mielestäni olisi ollut mielenkiintoista vertailla kohdistetun ja ei-kohdistetun hyökkäyksen yhteneväisyyksiä ja eroavaisuuksia, vertailla hyökkäyksien onnistumisprosenttia sekä käyttäjien suhtautumista ja varautumista eri tavalla toteutettujen sosiaalisten manipulointihyökkäyksien välillä. Olisin myös toivonut löytäväni tilastoja, joista olisi ilmennyt ilmiön laajuus Euroopassa, Pohjoismaissa tai Suomessa. Projektia varten lähetin sähköpostia erään teleoperaattorin turvallisuusjohtajalle sekä eräälle verkkopetoksiin erikoistuneelle toimittajalle, jossa kyselin heidän näkemyksiänsä sosiaalisiin manipulointihyökkäyksiin liittyen. Valitettavasti kumpikaan ei vastannut yhteydenottopyyntööni. Heidän havaintojaan ja kokemuksiaan olisi voinut verrata alan kirjallisuuteen ja tutkimuksiin. Lisäksi heidän vastauksensa perusteella olisi mielestäni ollut mahdollista luoda edes osittainen katsaus ilmiön laajuudesta ja vakavuudesta Suomessa.

Ilmiöstä jäi vielä runsaasti tutkittavaa: aihetta voisi lähestyä tutkimalla perusteellisemmin tietyn kanavan tai tiettyihin henkilöihin kohdistuvia hyökkäyksiä ja näiden ominaisuuksia.

Vaihtoehtoisesti voisi tutkia kulttuurin vaikutusta sosiaalisiin manipulointihyökkäyksiin. Sosiaalista manipulointia voisi melkein kutsua antropologiseksi ilmiöksi, jossa hyökkäyksen sisältö sekä toteutumistapa määräytyvät suuresti keskustelijoiden kulttuurin ja tapojen mukaan: tätä näkökulmaa olisi mielestäni mielenkiintoista tutkia lisää. Kohdistettujen ja eikohdistettujen yhteydenottojen välisien erojen tutkiminen tuottaisi mielestäni tuloksia, joita olisi mahdollista hyödyntää suojauskeinojen kehittämisessä. Lisäksi tuottamani suojausrungon tehokkuutta ja toimivuutta organisaation toteuttaessa tietoturvapolitiikan sen mukaisesti olisi hyvä mitata. Teknologian kehityksen vaikutusta sosiaalisiin manipulointihyökkäyksiin olisi myös mahdollinen tutkimusaihe: olisi mielenkiintoista tutkia miten esimerkiksi tekoälyä voitaisiin soveltaa niin itse hyökkäykseen kuin siltä suojautumiseen.

Kokonaisuutena, tämä projekti on ajoittain ollut haastava. Edistymistä hidasti huomattavasti kokopäivätyöni, jonka seurauksena arkipäivisin harvoin jaksoin työstää opinnäytetyötä kovin pitkään. Opinnäytetyön haasteellisuutta lisäsi myös se, etten ole syntynyt Suomessa enkä ole opiskellut suomen kieltä. En ollut myöskään aikaisemmin työstänyt näin laajaa kokonaisuutta suomeksi. Tämän seurauksena työ eteni ajoittain erittäin hitaasti, sillä halusin tuottaa mahdollisimman hyvää ja sujuvaa tekstiä, joka taas tarkoitti moninkertaista tuotetun tekstin tarkistamista. Kirjoittaminen on minulle tosin mielekästä, joten kielitaidosta johtuvista hidasteista huolimatta pidin opinnäytetyön työstämisestä ja minua kiinnostavan aiheen tutkimisesta.

Edellä kerrottujen haasteista huolimatta saavutin mielestäni hyvin projektille asetetut tavoitteet. Aiheesta löytyy kattavasti luotettavaa tietoa erilaisista lähteistä: aiheeseen perehtyneiltä tutkijoilta, alan huippuammattilaisilta sekä entisiltä huijareilta itseltään. Tämä taas mahdollisti laajan katsauksen ilmiöön hyödyntämällä eri asemassa olevien näkemystä hyökkäyksen rakenteesta, toteutustavoista sekä keinoista suojautua sosiaaliselta manipuloinnilta. Työstä löytyvät omat havainnot ja päätelmät saavat myös tukea työssä esitetystä kirjallisuudesta. Yksi työn päätavoitteista oli kerätä samaan työhön ilmiötä tutkineiden henkilöiden näkemyksiä ilmiöstä ja siitä suojautumiselta: siinä tämä työ onnistuu mielestäni hyvin. Lisäksi ammatillinen kehittymiseni tämän työn ansiosta on ollut huimaa. Olen oppinut sosiaalisista manipulointihyökkäyksistä sekä tietoturvasta huomattavan määrän asioita, joita voin suoraan hyödyntää jokapäiväisessä työssäni. Olen tyytyväinen tuotettuun kokonaisuuteen ja toivon, että tästä projektista olisi hyötyä myös muille.

Lähteet

Almomani, A. Gupta, B. Atawneh, S. Meulenberg, A. & Almomani, E. 2013. A survey of phishing email filtering techniques. Luettavissa: https://www.researchgate.net/publication/236250451_A_Survey_of_Phishing_Email_Filtering_Techniques Luettu: 14.4.2020

Anslinger, J. 2013. How do email spam filters work? Luettavissa: https://www.ltnow.com/email-spam-filters-work/ Luettu: 24.4.2020

Bada, M. Sasse, A. & Nurse, J. 2019. Cyber security awareness campaigns: why do they fail to change behavior? Luettavissa: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf Luettu: 3.4.2020

Baggett, D. & Alibe, B. 3.4.2020. Phish Friday - COVID-19 Phishing Scams. Webinaari. https://www.brighttalk.com/webcast/18067/396310

Computer Gaming World. 1994. Got a modem? 121, 117–118. Luettavissa: http://www.cgwmuseum.org/galleries/issues/cgw_121.pdf Luettu: 1.5.2020

Cyberark. Standard Core PAS. Luettavissa: https://www.cyberark.com/products/privileged-account-security-solution/core-privileged-account-security/ Luettu: 11.5.2020

FBI. 2015. 2015 Internet crime report. Luettavissa: https://pdf.ic3.gov/2015_IC3Report.pdf Luettu: 12.4.2020

FBI. 2017. 2017 internet crime report. Luettavissa: https://pdf.ic3.gov/2017_IC3Report.pdf Luettu: 12.4.2020

FBI. 2019. 2019 Internet crime report. Luettavissa: https://pdf.ic3.gov/2019_IC3Report.pdf Luettu: 12.4.2020

Gillaerts, P & Gotti, M. 2008. Genre Variation in Business Letters. Peter Lang AG. Luettavissa: https://books.google.fi/books?hl=fi&lr=&id=QugwjS-RiuQoC&oi=fnd&pg=PA257&dq=419+scam&ots=IpG6YjOLJS&sig=zzxCQGiawxon6f1qSpknZH7HcKg&redir_esc=y#v=onepage&q=419%20scam&f=false. Luettu: 10.4.2020

Grabosky, P. 2017. The evolution of cybercrime, 2006-2016. Teoksessa Holt, T. Cybercrime through an interdisciplinary lens, s. 15- 36. Routledge, New York. Luettavissa:

https://books.google.fi/books?hl=fi&lr=&id=0T8lDwAAQBAJ&oi=fnd&pg=PA15&dq=evolution+of+information+security&ots=cXmfnsVbEK&sig=0pmmjQr_VupzVyhcjrEfSIrEitY&redir_esc=y#v=onepage&q=evolution%20of%20information%20security&f=false. Luettu: 6.4.2020.

Gragg, D. 2002. A Multi-Level Defense Against Social Engineering. Luettavissa: http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf Luettu: 11.4.2020

Gulati, R. 2003. The threat of social engineering and your defense against it. Luettavissa: https://cdn.preterhuman.net/texts/underground/info/The%20Threat%20of%20Social%20Engineering%20and%20Your%20Defense%20Against%20It.pdf Luettu: 14.4.2020

Hadnagy, C. & Wilson, P. 2010. Social engineering: the art of human hacking. John Wiley & sons. Indianapolis.

Kangasniemi, J. 2020. Facebookissa kiertää nyt viattoman näköisiä kyselyitä, joissa piilee riski – Asiantuntija kertoo, miksi kannattaa harkita tarkasti, ennen kuin listaa somessa entiset työpaikkansa. Luettavissa: https://www.hs.fi/teknologia/art-2000006488268.html Luettu: 1.5.2020

Keizer, G. 2015 Sony hackers targeted employees with fake Apple ID emails. Luettavissa: https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html Luettu: 29.3.2020

Krombholz, K. Hobel, H. Huber, M. & Weippl, E. 2014. Advanced social engineering attacks.

Kyberturvallisuuskeskus. 2020. Korona-aiheisia huijauksia on liikkeellä - mieti mitä klikkaat. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/korona-aiheisia-huijauksia-liikkeella-mieti-mita-klikkaat Luettu: 20.4.2020

Mann, I. 2008. Hacking the Human: Social Engineering Techniques and Security Countermeasures. Gower Publishing Limited. Hampshire.

Mouton, F. Leenen, L. & Venter, H. 2015. Social Engineering Attack Detection Model: SEADMv2.

Mouton, F. Leenen, L. Malan, M. & Venter, H. 2014. The Social Engineering Attack Framework. Luettavissa: https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework Luettu: 4.4.2020

Orgill, G. Romney, G. Bailey, M. & Orgill, P. The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems. Luettavissa: https://dl.acm.org/doi/pdf/10.1145/1029533.1029577 Luettu: 2.4.2020

Peltier, T. 2006. Social Engineering: Concepts and solutions.

Rekouche, K. 2011. Early Phishing. Luettavissa: https://arxiv.org/ftp/arxiv/papers/1106/1106.4692.pdf Luettu: 28.3.2020

Rosencrance, L. 2002. Online Payment Service PayPal hit by scam. Luettavissa: https://www.computerworld.com/article/2579316/online-payment-service-paypal-hit-by-scam.html Luettu: 16.4.2020

Rusch, Jonathan. 1999. The “social engineering” of internet fraud. Luettavissa: https://web.archive.org/web/20080617150031/http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm#s2 Luettu: 8.3.2020

Singer, B. 2012. Feds Catch Their Illegal Limit In Operation Phish Phry. Luettavissa: https://www.forbes.com/sites/billsinger/2012/05/15/feds-catch-their-illegal-limit-in-operation-phish-phry/#16dabd646265 Luettu: 5.4.2020

Singh, Rahul. 2013. Kali Linux Social Engineering. Packt Publishing, Limited. Birmingham.

Thornburgh, T. Social engineering: The “Dark Art”. Luettavissa: https://dl.acm.org/doi/pdf/10.1145/1059524.1059554 Luettu: 29.2.2020

Van Der Werff, E & Lee, T. 2015. The 2014 Sony Hacks, explained. Luettavissa: https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea Luettu: 29.3.2020

Wozniak, S. Simon, W & Mitnick, K. 2003. The Art of Deception: Controlling the Human Element of Security. Wiley. Indianapolis.