TOIMITUSJOHTAJAHUIJAUS

Hakkerointia vai käyttäjän manipulointia?

Risto Ikonen

5/2020

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

Tekijä(t)	Tutkinto
Risto Ikonen	Poliisi (AMK)
Julkaisun nimi Toimitusjohtajahuijaus. Hakkerointia vai käyttäjän manipulointia?	Julkisuusaste Julkinen
Ohjaaja Kujanpää Olavi, ylikomisario Peltoja Jani, erityisasiantuntija	Opinnäytetyön muoto Kirjallisuuskatsaus

Tiivistelmä

Tässä opinnäytetyössä tarkastellaan toimitusjohtajahuijauksia poliisin ja yritysten näkökulmasta. Tavoitteena opinnäytetyössä on kuvata toimitusjohtajahuijauksia ilmiönä ja sitä, miten teot toteutetaan hyödyntäen sekä tietotekniikkaa, että käyttäjän manipulointia. Opinnäytetyö toimii poliisin rikostutkinnalle apuna ymmärtämään ilmiötä, sekä pyrkii avaamaan yrityksille huomioitavia seikkoja, kuten millä voidaan varautua tekoa vastaan, esimerkiksi tietoisuutta lisäämällä.

Toimitusjohtajahuijauksissa yritystä ja työntekijää lähestytään esimerkiksi sähköpostitse väärentämällä lähettäjän sähköpostin osoitetiedot ja tekeydytään näin toiseksi henkilöksi. Maksuista tai rahaliikenteestä vastaava henkilö erehdytetään luulemaan, että hän käy keskustelua tosiasiallisen toimitusjohtajan kanssa. Huijaamalla työntekijää pyritään siihen, että hän suorittaa maksun huijarin määrittelemälle maksutilille.

Opinnäytetyön keskeiset tulokset ovat käyttäjän manipulaation laajamittainen hyödyntäminen huijauksissa ja se, kuinka manipulaatio on suuremmassa roolissa huijauksien varsinaisessa toteuttamisessa, kuin tietotekniikka. Tärkeäksi seikaksi nousee myös yritysten tietoisuus huijauksista ja kuinka tätä parantamalla saavutettaisiin etuja huijausten ennalta-ehkäisyyn.

Opinnäytetyö on muodoltaan kirjallisuuskatsaus, jonka teoriapohjassa on hyödynnetty avoimia lähteitä, tieteellisiä aikakausilehtiä ja artikkeleita, sekä monialaisia tietokantoja. Työn lähteet ovat sekä suomeksi, että englanniksi. Kirjallisten lähteiden tueksi on työssä kerätty kokemuspohjaista tietoa Sisä-Suomen poliisin Tampereen pääpoliisiaseman rikostutkijoilta ja ICT-tutkinnalta.

Sivumäärä	Tarkastuskuukausi ja -vuosi
40	toukokuu 2020

Avainsanat

huijaus, kyberrikollisuus, käyttäjän manipulointi, petos, tietojen kalastelu toimitusjohtajahuijaus

SISÄLLYS

TERMINOLOGIAA

Diskurssi: Puhuttu ja kirjoitettu kielenkäyttö.

Hakkeri: (engl Hacker). Tietojärjestelmään tai tietoverkkoon luvatta tunkeutuva henkilö.

Harrastelijahakkeri: (engl. Script kiddie). Skriptipentu tai harrastelijahakkeri, jolla ei ole kokemusta koodaamisesta.

Kaksivaiheinen tunnistautuminen: (engl. Two-factor authentication, 2FA). Autentikointi tehdään esimerkiksi pankkitunnuksella ja matkapuhelimella, jossa on tunnuslukusovellus.

Kalastelupaketti: (engl Phishing kit). Paketti työkaluja, joilla huijari ilman syventävää tietoteknistä osaamista toteuttaa tietojenkalastelu-sivuston.

Kyberhyökkäys: (engl. Cyber attack.) Hyökkäys, joka kohdistuu kybertoimintaympäristöön.

Kybertoimintaympäristö: (engl. Cyber environment). Yhdestä tai useammasta tietojärjestelmästä muodostuva verkkoympäristö.

Käyttäjän manipulointi: (engl Social engineering). Manipuloinnin avulla hankitaan luottamuksellista tietoa.

Lähetysosoitteen huijaus: (engl. Spoofing). Väärennetään lähettäjän nimikenttä sähköpostiin.

Soittopyyntöurkinta: (engl. Vishing/ Voice phishing). Puhelimitse urkitaan luottamuksellista tietoa.

Tietojen kalastelu: (engl. Phishing). Urkitaan tietoverkossa esimerkiksi pankin nimissä luottokortin numero ja tunnusluku.

Tietoturva-aukko: (engl. Vulnerability). Tietojärjestelmän heikkous, joka altistaa kyberhyökkäykselle.

Toimitusjohtajahuijaus: (engl. Business Email Compromise fraud). Rikollinen tekeytyy toimitusjohtajaksi ja harhauttaa työntekijää siirtämää rahaa huijarin tilille.

Troijalainen: (engl. Trojan horse). Ohjelma, johon on piilotettu haitallista ohjelmistokoodia.

Palvelunestohyökkäys: (engl. DoS, Denial of Service). Verkkohyökkäys, jossa pyritään estämään verkkopalvelun käyttö kuormituksella.

Verkkotunnus: (engl. Domain name): Standardin mukainen maatunnus verkkopalvelussa. Esimerkiksi .fi (Suomi).

1 JOHDANTO

Toimitusjohtajahuijaus kohdistetaan yritykseen tai sen työntekijään. Tekijä pyrkii esiintymään ihmisenä, joka vastaa yrityksen rahaliikenteestä tai vastaavasti toimii päättävässä asemassa yrityksessä kuten toimitusjohtajana. Tekijän tavoitteena on pyytää työntekijää siirtämään rahaa haluamalleen tilille. Tekijä vetoaa erilaisiin keinoihin ja syihin. Yleisin toimintatapa on lähestyä työntekijää sähköpostitse. Tunnusmerkkeinä asiassa esimerkiksi ovat kiireellisyys, vetoaminen arkaluontoisuuteen, kesäloma-aika, työntekijän sijainen tai ettei toimitusjohtaja itse pysty jostain syystä tilisiirtoa nyt juuri tekemään, koska on esimerkiksi ulkomaanmatkalla. (Poliisi 2019a.)

1.1 Opinnäytetyön tarkoitus

Opinnäytetyö kuvaa ilmiötä itsessään. Työ pyrkii avaamaan ilmiön takana olevia tekniikoita ja toimintatapoja. Työssä listataan asioita, miten suhteellisen helposti tätä ilmiötä vastaan pystytään taistelemaan pienilläkin resursseilla esimerkiksi pk-yritysten näkökulmasta kouluttamalla työntekijöitä ja lisäämällä heidän tietoisuuttansa asiasta.

Ajatus tähän opinnäytetyöhön lähti ollessani työharjoittelussa Sisä-Suomen Poliisilaitoksella Tampereella. Toimin silloin Valvonta- ja Hälytyssektorilla kenttävuorossa. Partiomme sai hälytyskeskukselta tehtävän koskien yritykseltä anastettuja varoja. Lähtötiedot tapaukseen ja soitto asianomistajalle varmistivat kyseessä olevan toimitusjohtajahuijaus. Muistan silloin miettineeni, että mitä yksittäinen partio voisi asialle tehdä. Kyseessä oli kesäinen perjantai-ilta mikä sopi täydellisesti teon profiiliin.

Poliisin strategia Suomessa ja EUROPOL:in strategia Euroopassa puoltaa aiheen ajankohtaisuutta tällä hetkellä. Tilastojen varjossa kyseinen huijaus on myös kasvanut suuressa määrin Euroopassa ja Suomessakin (Europol 2019).

Poliisin strategia 2017 – 2020 listaa neljä pääpainopistettä tämänhetkisessä poliisin strategiassa. Nämä ovat turvallisuuden edistäminen, rikollisuuden torjuminen, hyvät palvelut ja avoin toiminta ja vaikuttavuuden edistäminen. Rikollisuuden torjuminen-osiossa poliisi käy läpi toimenpiteitä tietoverkkorikostentorjunnassa ja kyberosaamista poliisissa. Tavoitteina näiden osalta on panostaa Kyberrikostorjuntakeskuksen toimintaan. Näin voidaan tukea paikallisia poliisiyksiköitä ja varmistaa yhteistyö kotimaassa ja ulkomailla niin viranomaisten

kesken, kuin poliisin sisällä. Pyrkimyksenä on myös taata riittävät resurssit, välineistä ja osaaminen Kyberrikollisuuden uhkiin. (Poliisi 2019b.)

EUROPOL:in Internet Organized Crime Threat Assesment (IOCTA)-raportti lokakuulta 2019 listaa lukuisia verkossa tapahtuvia rikollisuuden muotoja ja toimenpiteitä niiden ehkäisemiseksi. Raportissa kuvataan, kuinka uusi teknologia tuo uusia haasteita ja kuinka lainsäädännön pitää pysyä mukana, kun rikolliset kehittävät uusia toimintatapoja. Keinoina rikoksia vastaan viranomaisten tietotaito ja työkalut pitää olla ajan tasalla. Raportti listaa toimitusjohtajapetokset yhtenä alakohtana prioriteettirikoksien-listassa. Haasteena nähdään tässä myös muuttunut rahaliikenne, jota on nopeutettu Euroopan tasolla. Vaikka finanssimaailma hyötyy siitä, että rahat siirtyvät lähes välittömästi Euroopan sisällä, niin se edesauttaa myös rahanpesua ja muita maksuhuijauksia (EUROPOL 2019).

1.2 Tutkimuskysymysten asettelu

Työn tavoitteena on vastata kysymykseen, mikä on toimitusjohtajahuijaus, miten se toteutetaan käyttäjän manipulointia hyödyntäen sekä minkälaisia teknisiä lähestymistapoja siinä käytetään.

1.3 Aiheen rajaaminen

Työ kuvaa ilmiötä koskien pk-yrityksiä ja yhdistyksiä suomessa. Teon muotona on sähköpostilla tai puhelimella tapahtuva huijaus. Ajallisesti teko voi kestää useamman päivän tai on ohitse yhden vastaanotetun sähköpostin jälkeen. Teon tavoitteena on saada yritys tai yksilö siirtämään rahaa huijarin haluamalle tilille. Vaikka teknologia tässä huijauksessa näyttelee isoa roolia, on käyttäjän manipulointi, silti isommassa osassa kokonaisuuteen nähden. Käyn läpi myös tätä elementtiä koskien nimenomaan toimitusjohtajahuijausta.

Työn rajauksessa otin huomioon ilmiön monimuotoisuuden ja vahvan kansainvälisen yhteyden. Rajasin kuvauksen ulkopuolelle isot yritykset, koska heidän toimintansa on monesti kansainvälistä. Halusin nimenomaan katsoa asiaa Suomen mittapuulla ja pienemmässä mittakaavassa.

Rajasin työni pienempiin yrityksiin pk-sektorilla osin siksi, että näissä yrityksissä tietoturva nähdään helpommin välittömänä pahana eikä osana yrityksen arkea. Huijaus on myös tätä

nykyä levinnyt pienempiin yhdistyksiin ja seuroihin. Nämä yhdistykset ovat vähemmän ammattimaisia ja rahaliikennettä pyöritetään monesti oman palkkatyön ohessa. Kuitenkin näille tahoille aiheutetut vahingot ovat mittavia niiden toimintaa kokonaisuutena ajatellen.

1.4 Tutkimusmenetelmät

Opinnäytetyöni on luonteeltaan kuvaileva kirjallisuuskatsaus. Kaksi muuta tärkeintä kirjallisuuskatsauksen muotoa ovat systemaattinen kirjallisuuskatsaus ja meta-analyysi. Kuvaileva kirjallisuuskatsaus on yksi eniten käytetyistä kirjallisuuskatsastuksen muodoista. Tämä muoto mahdollistaa yleiskatsauksen aiheesta ilman, että aineistoa rajataan tiukasti ja kovin tarkasti. Aineiston valintaa ei tässä katsauksessa tarvitse rajata metodisin säännöin. Vaikka kuvaileva kirjallisuuskatsaus ei omaa systemaattisen kirjallisuuskatsastuksen tarkkoja raamituksia aineiston valinnasta, niin sillä pystytään kuvaamaan tutkittava ilmiö laajasti. (Salminen 2011, 6-7.)

Kuvaileva kirjallisuuskatsaus jakautuu vielä kahteen eri orientaatioon. Nämä ovat narratiivinen ja integroiva katsaus. Integroiva kirjallisuuskatsaus on lähempänä systemaattista katsausta. Työssä käsittelen asiaa narratiivisen orientaation kautta. Tämän avulla pyrin antamaan laajan kuvan käsiteltävästä aiheesta. Narratiivinen lähestyminen mahdollistaa sen, että epäyhtenäistä tietoa järjestellään jatkumoksi. Tämä sopii mielestäni hyvin työhön, koska erilaiset artikkelit ja tieto aiheesta on hajautettu useaan eri paikkaan ja eri tieteenaloille. Narratiivinen katsaus pyrkii lopputulokseen, joka olisi lukijalleen helppolukuinen. (Salminen 2011, 6-7.)

Tutkimustekniikkana narratiivinen katsaus pyrkii saamaan tutkimustiedon ajan tasalle, mutta ei tuota analyyttisintä tulosta aiheesta. Voisikin sanoa, että ajankohtaisen tiedon tuottaminen kuvaa hyvin narratiivista katsausta. Selkeänä heikkoutena tässä tavassa voidaan kuitenkin nähdä, että tutkimus voi tuottaa johdattelevaa ja puolueellista tietoa, mikä voi rajata sen pois päätöksenteon tukena käyttämiseen, esimerkiksi poliittisella saralla. (Salminen 2011, 6-7.)

Narratiivinen katsaus voidaan vielä jakaa kolmeen erilaiseen toteuttamistapaan. Nämä ovat toimituksellinen-, kommentoiva- ja yleiskatsaus. Toimituksellinen katsaus on tarkoitettu lähinnä lyhyehkön, alle kymmenen lähteen aineiston käsittelyyn. Kommentoiva katsaus puo-

lestaan pyrkii herättämään keskustelua asiasta. Yleiskatsaus taas puolestaan pyrkii tiivistämään aiempia tutkimuksia. (Salminen 2011, 6-7.) Näistä kolmesta erilaisesta tavasta valitsin lähestymistavakseni kommentoivan katsauksen.

Kirjallisuuskatsauksen muoto tässä opinnäytetyössä tulee olemaa kuvaileva kirjallisuuskatsaus, joka on sekä narratiivinen, että kommentoivan otteen omaava.

1.4.1 Kokemuspohjainen tieto

Työharjoitteluni ohessa Sisä-Suomen Tampereen pääpoliisiasemalla, kävin keskusteluja asiantuntijoiden kanssa toimitusjohtajahuijauksesta ja sen toimintatavoista. Asiaa käytiin läpi niin teoreettisella, kuin käytännön tasolla. Kokemuspohjaisella tiedolla pyrittiin vahvistamaan kirjallisen tiedon lähteitä. Varsinaisia haastatteluja ei ole tehty.

1.4.2 Kieli ja termistö

Suurin osa lähteistä on englanninkielisiä, mutta suomen kielessä on hyviä vakiintuneita vastineita jo paljon olemassa. Rinnakkaisia termejä käytetään jonkin verran Suomessa, mutta lopullisen termin olen tarkistanut termipankista. Käännösten apuna olen käyttänyt TEPA-termipankkia. Käännöskone hyödyntää muun muassa Sanastokeskuksen Tietotekniikan termitalkoot-projektia. Tässä projektissa joukko kielen, viestinnän ja tietotekniikan ammattilaisia kokoaa suosituksia käytetyistä sanastoista. Lisäksi termipankki hyödyntää muun muassa IAET sanastoa, joka hakee EU:n tasolta tietoa käytettävistä termeistä.

1.5 Aineisto

Suoranaista pääteosta ei aineistossa ole käytetty. Aineistoa on pyritty keräämään mahdollisimman laajasti, mutta kuitenkin laatukriteerejä noudattaen. Kotimainen tietokirjallisuus on suhteellisen pienimuotoista aihetta koskien, vaikka hyviäkin teoksia löytyy.

Ilmiön ollessa erityinen, valikoin aineistoksi tiedejulkaisuja, tutkimuksia ja artikkeleita alan lehdistä. Tietokantoina käytin esimerkiksi Ebsco Academic Search, Sage Premier ja Emerald-kantaa. Hakuja näissä kannoissa en lähtenyt rajaamaan erityisesti ja hakukielenä käytin yksinomaan englantia.

1.6 Aiemmat tutkimukset aiheesta

Aiempaa tutkimusta ei Suomessa ole tehty suoraan tähän aiheeseen liittyen näin tarkalla tutkimuskysymyksellä, jossa pureuduttaisiin ainoastaan toimitusjohtajahuijaukseen ilmiönä. Aihetta on kuitenkin sivuttu samankaltaisilla tutkimuksilla, jossa tutkitaan yrityksiin kohdistuneita identiteettivarkauksia, sekä toinen selvitys, jossa tutkitaan pk-yrityksiin kohdistuvia huijauksia. Lisäksi käyttäjän manipulointia koskevia tutkimuksia on laajalti tarjolla.

Ensimmäinen tutkimusraportti on koostettu kesäkuussa 2019. Raportin nimi: Tutkimusraportti Indentiteettivarkauksista: Pienet ja keskisuuret yritykset, on mySafety-yrityksen koostama raportti. Yritys on lähtöisin Ruotsista ja toimii Suomessakin kahdella paikkakunnalla. Toimialana yrityksellä on vakuutuspalvelut rikosten ennaltaehkäisyyn ja haittavaikutusten minimoimiseen verkossa (MySafety 2019).

Raportti tuo esille sen, että Ruotsissa huijauslaskut ovat olleet yritysten riesana jo useamman vuoden mikä toisaalta on edesauttanut yrityksiä jo niiden torjunnassa. Yrityksille on ehditty jo luoda toimintatapoja näiden huijausten estämiseen. Vastaavasti taas Suomessa tilanne on vielä erilainen ja huijauslaskut menevät lävitse hieman helpommin.

Toinen raportti on Kilpailu- ja kuluttajaviraston 2017 teettämä selvitys siitä kuinka pk-yrityksiin kohdistuu erilaisia huijauksia, selvitys on: Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset, kirjoittajana Helena Tuorila. Tässä selvityksessä yhtenä osana käsitellään myös toimitusjohtajahuijauksia, valelaskuja, laskuväärennöksiä ja erilaisia huijaussähköposteihin liittyviä ilmiöitä (Tuorila 2017).

Selvityksessä pohditaan, miten huijauksia analysoidaan ja miten yritykset ja yrittäjät ylipäätänsä ovat joutuneet huijauksen kohteeksi. Miten kiire, harjoittelijat ja tietotaito sekä tiedottamisen puute voivat altistaa huijaukselle. Yhtenä mielenkiintoisena seikkana nostetaan esille se, että pitäisikö huijausten vastaisen toiminnan sisältyä jo perusopetukseen. Tämä seikka on nostettu esille, koska on koettu huijausten olevan integroitu jo hyvin vahvasti sisälle yhteiskuntaan.

Selvitys listaa erilaisia toimia, miten pk-yritysten asemaa saataisiin paremmaksi ja miten huijauksia saataisiin torjuttua. Avaintermejä tässä on tiedottamisen nopeutus, vahva sähköinen tunnistautuminen ja lainsäädännön muutokset.

Näiden lisäksi käyttäjän manipulointia on tutkittu hyvinkin monelta kantilta. Deniz Anttila on tutkinut kandidaatin tutkielmassa 2016 käyttäjän manipulointia organisaation tietoturvauhkana (Anttila 2016). Anttila mainitsee tutkimuksessaan, kuinka käyttäjän manipulaatio vaatii tietoteknisen puolen, joka tukee toimintaa ja tekee siitä entistä vaarallisemman. Anttila toteaa myös, että käyttäjän manipulaatio toimii varsinkin isossa organisaatiossa, joissa työntekijät saavat usein yhteydenottoja entuudestaan tuntemattomilta ihmisiltä. Tässä yhteydessä on myös mainittu, kuinka käyttäjän manipulointi toimii, kun ihmiset eivät tunne toisiaan niin hyvin johtuen suuresta henkilöstömäärästä. Tämä puolestaan toimii hyvin hyökkääjän näkökulmasta, koska identiteetistä ei ole täyttä varmuutta.

Näkemykseni mukaan myös pienemmät organisaatiot saavat paljon yhteydenottoja entuudestaan tuntemattomilta tahoilta. Joten käyttäjän manipulointi on näissä tapauksissa räätälöity eri lailla, kun isojen yritysten kohdalta. Isoissa yrityksissä ihmiset eivät toki tunne toisiaan niin hyvin, kun pienemmissä yrityksissä mutta sähköpostin kautta tapahtuvassa huijauksessa on helpompi piiloutua väärän identiteetin taakse, kun kasvotusten mikä mahdollistaa tämänkaltaisen toiminnan isoissa ja pienissä organisaatioissa.

Anttila kuvaa työssään ilmiötä, jossa katastrofi tai luonnonmullitus saa huijarit liikkeelle. Näissä huijauksissa pyrittiin keräämään rahaa ihmisille, jotka olivat jonkun katastrofin uhreja. Nämä huijaukset toimivat hyvin, koska ihmisten halua auttaa on meihin sisäänrakennettu hyvin perustasolle. Tämänkaltaista toimintaa on ollut havaittavissa myös Suomessa esimerkiksi koronapandemian aikaan.

2 KYBERRIKOLLISUUS

2.1 Määritelmä

Toimitusjohtajahuijauksen toimintaympäristönä toimii pääasiallisesti aina internet jossain muodossa. Tämän rikollisuuden muodosta käytetään termiä kyberrikollisuus. Tämä tarkoittaa tietoverkkoihin ja tietojärjestelmiin tapahtuvia rikoksia, jossa hyödynnetään tietotekniikkaa ja tietoverkkoja. Rikosten tapahtuminen tietojärjestelmissä ja tietoverkoissa on kasvava trendi poliisin tietouteen tulleista rikoksista. (Sisäministeriö 2019.)

Tietoverkkorikoksia ovat palvelunestohyökkäykset eli DoS (Denial of Service) missä esimerkiksi pyritään hidastamaan halutun tietojärjestelmän tai web-sivun toimintaa. Haittaohjelmien asennus, missä tietokoneeseen salaa asennetaan troijalainen, mato tai virus, millä mahdollistetaan tietokoneen etäkäyttö tai saadaan tietokone lähettämään tietoa tietokoneen datasta toiselle tietokoneelle. Hakkerointi yleisesti tarkoittaa tunkeutumista järjestelmään, jolloin syntyy tietomurto. Hakkerointi mahdollistaa esimerkiksi tietojärjestelmän tuhoamisen tai sen, että järjestelmää voidaan käyttää rikollisiin tarkoituksiin. (Sisäministeriö 2019.)

Kyberrikollisuuden rikostyyppeinä yleisimpiä ovat erilaiset omaisuuteen kohdistuvat rikokset. Näitä ovat petokset, maksuvälinepetokset, kiristys ja rahanpesu. Anonyymina tai ainakin osittain anonyymina toimiminen on lisännyt lapsiin ja nuoriin kohdistuvia seksuaalisia hyväksikäyttöjä (Sisäministeriö 2019.). Yhtenä syynä tähän on internetin käytön räjähdysmäinen kasvu, mistä osoituksena on se, että ikäryhmistä 16-44 kaikki käyttävät internettiä (Tilastokeskus 2019).

Yksi huomioimisen arvoinen piirre kyberrikoksissa on kansainvälisyys. Monesti verkossa tapahtuva rikollisuus on kansainvälistä. Tietoverkot ja nykyiset nopeat yhteydet poistavat fyysiset esteet uhrin ja rikollisten väliltä, sekä myös rikollisten itsensä väliltä. Tämä on huomion arvoinen seikka ja hankaloittaa entisestään viranomaisten esitutkinnan suorittamista. (Sisäministeriö 2019.)

Rikoksen perimmäinen muoto ei muutu mihinkään, vaikka se toteutetaan verkossa. Verkossa tehty rikos mahdollistaa nopean tavan hyökätä useamman tahon kimppuun yhtä aikaa ja riippumatta heidän sijainnistaan niin Suomessa kuin Euroopassa. Myös mahdollisuus toimia anonyymisti ainakin tiettyyn rajaan asti, helpottaa rikollista toimintaa ja vähentää kiinnijäämisen riskiä.

2.2 Rikosnimikkeet

Erilaisten rikosten kirjoa tässä kyseissä rikoksessa on vaikea lokeroida yhden tai kahden rikosnimikkeen alle. Monesti kyseessä on useamman rikollisen teon summa, josta kokonaisuus muodostuu. Yleisesti ottaen tämän rikoksen yhteydessä käsitellään törkeää petosta, törkeän petoksen yritystä, petoksen yritystä, identiteettivarkautta ja tietomurtoa (Erkkilä 2018).

Tämä kuvaa hyvin mielestäni sitä, kuinka laaja-alaisesti tämä koskettaa myös yrityksen toimintoja, sekä kuinka monta erilaista petosta ja huijausta teko vaatii toteutuakseen. Omalta osaltaan tämä myös hankaloittaa toimitusjohtajahuijauksen tilastoimista poliisin järjestelmiin.

2.3 Pk-yrityksien raportoimat tappiot ja rikosten määrät

Rahalliset tappiot ovat mittavia toimitusjohtajahuijauksessa. Lehdistä saa lukea isojen yritysten menettämistä summista jatkuvasti ja vaikka Suomen tasolla summat ovatkin pienempiä, ovat ne pk-yritysten sektorilla huomattavia pienille yrittäjille. Suomen Yrittäjät, joka ajaa pienten ja keskisuurten yritysten etuja on teettänyt Kantar TNS Oy:llä yrittäjägallupin. Kantar TNS Oy on osa suurta Kantar TNS konsernia, mikä puolestaan on yksi suurimpia markkinatutkimusyrityksiä maailmassa. Kysely on teetetty syyskuussa 2019 (Lammassaari 2019).

Gallupista käy ilmi, että 52 prosenttia huijatuista tai huijausyrityksen uhreista on menettänyt huijauksessa vähemmän kun 500 euroa. 16 prosenttia on menettänyt 500 – 10 000 euroa. Kolme prosenttia oli menettänyt yli 10 000 euroa. 28 prosenttia ei osaa arvioida huijauksen aiheuttaman vahingon arvoa. Suhteessa kovimmat tappiot ovat tulleet 2-9 henkeä työllistäville yrityksille. Kyselyyn vastasi 1006 pk-sektorin yritystä.

Samassa gallupissa selvitettiin onko yritys joutunut ylipäätänsä huijauksen tai sen yrityksen kohteeksi. 50 prosenttia vastaajista kertoi joutuneensa huijarien kohteeksi.

Gallupin perusteella 21 prosenttia ilmoitti huijauksesta tai sen yrityksestä poliisille. 39 prosenttia näistä ilmoituksista tutkittiin. Gallupissa epäiltiin, että poliisi tutki herkemmin yli 10 työntekijää työllistävien yritysten ilmoitukset.

Suomen Yrittäjien tekemän gallupin ja poliisille raportoitujen rikosten määrässä voi olla aukkoja. Elokuuhun 2019 mennessä poliisille oli raportoitu epäiltyjä toimitusjohtajahuijauksia yhteensä 196 kappaletta. Poliisin arvio on, että yritykset, sekä muut tämän rikoksen kohteeksi joutuneet tahot, ovat menettäneet rahaa arvioituna 4,2 miljoonaa euroa. Vuonna 2018 rikosilmoitusten määrä oli 170 ja vuonna 2017 noin sata kappaletta. (Poliisi 2019e)

Näiden tietojen pohjalta näyttä siltä, että suuri osa toimitusjohtajahuijauksista jää raportoimatta. Tämän lisäksi haasteena on se, miten poliisi saa tilastoitua ilmoitetut rikokset toimitusjohtajahuijaukseksi tekotavan ja luokittelun osalta. Osa toimitusjohtajahuijauksista voidaan tilastoida petoksina, identiteettivarkauksina tai vaikka tietomurtoina.

3 TOIMITUSJOHTAJAHUIJAUS

Toimitusjohtajapetos, toimitusjohtajahuijaus, laskutushuijaus tai valelasku. Teolla on useita hieman vaihtelevia nimiä mitä siitä käytetään. Euroopassa ja Yhdysvalloissa asiasta puhutaan BEC fraud -nimikkeellä eli Business Email Compromise, mikä terminä viittaa mielestäni kuvaavasti siihen, että yrityksen sähköposti on vaarantunut. CEO fraud tai CEO impersonation termit taas ovat lähempänä suomen kielen versiota toimitusjohtajahuijaus. Man-in-the-email-scam ja bogus invoice scheme ovat harvemmin vastaan tulevia termejä asiasta, mutta kuvaavat tekoa myös hyvin.

3.1 Toteutustavat ja tunnusmerkit

Kohteena teossa voi olla isot ja pienet yritykset, koulut, hyväntekeväisyysyritykset ja pienet järjestöt ja urheiluseurat. Yhteistä näille kaikille on se, että heillä on säännöllisiä maksusuoritteita erinäisille tahoille (Poliisi 2019a; Europol 2019).

Seuraavassa käydään läpi, minkälaisia elementtejä huijaukseen yleisesti liittyy ja minkälaisista palasista teko muodostuu. Kaikkia näitä keinoja yhdistää hyvin vahvasti samat lainalaisuudet, jotka koskeva käyttäjän manipulointia, jota käyn läpi myöhemmässä vaiheessa.

3.1.1 Tieto

Kohteesta kerätään mahdollisimman paljon yleisesti saatavilla olevaa tietoa. Tietoa on voitu myös kerätä suoraan yrityksen työntekijöiltä aiemmilla kerroilla, kun yhteyksiä on otettu sähköpostitse tai puhelimitse yritykseen. Yrityksen omilta verkkosivuilta yleensä löytyy nimiä, puhelinnumeroita ja sähköpostiosoitteita. Vaikka sähköpostiosoitteet on pyritty osittain piilottamaan, niin yleensä niissä lukee etu.sukunimi@yritys.fi, mistä voidaan päätellä vastaanottajan sähköpostiosoite. Joskus verkkosivulta nähdään jo suoraan yrityksen avainasemassaa olevien ihmisten nimiä (Poliisi 2019a; Europol 2019).

3.1.2 Yhteydenotto

Tekijä lähestyy yritystä puhelinsoitolla tai sähköpostin välityksellä. Tässä vaiheessa tekijä on voinut valita roolikseen yrityksen korkea-arvoisen henkilön, kuten toimitusjohtajan tai rahaliikenteestä vastaavan henkilön, esimerkiksi talousjohtajan roolin. Yleensä saatu sähköposti tai puhelinsoitto ei ole odotettu yhteydenotto, vaan jopa aika yllättävä. Taho, joka yhteyden ottaa, on sellainen, että uhri ei välttämättä ole tähän normaalisti yhteydessä työn ohessa (Poliisi 2019a; Europol 2019).

3.1.3 Kiireellisyys

Avainsana huijauksessa on monesti yrityselämästäkin tunnettu kiireen tuntu. Tekijä vetoaa siihen, että rahat pitää saada nopeasti liikkumaan. Kiireellisyydessä voidaan vedota siihen, että ”toimitusjohtaja” ei itse juuri nyt asiaa pysty hoitamaan. Tekosyynä voi olla vaikka se, että henkilö itse on ulkomailla tai muuta vastaavaa (Poliisi 2019a; Europol 2019).

3.1.4 Salassapito, palkitseminen ja painostus

Tekijä pyytää pitämään mahdollisen rahasiirron salassa. Tässä voidaan vedota siihen, että kyseessä on yrityskauppoja koskeva maksu, josta ei saa puhua muille tahoille. Vetoaminen luottamukseen ja, että kyseinen rahansiirto on uskottu tietylle henkilölle, imartelee monesti työntekijää (Poliisi 2019a; Europol 2019). Lisäksi voidaan tarjota etuja tai korvauksia, mikäli rahansiirto tapahtuu nopeasti.

Myös yksi vaihtoehto on painostaa seuraamuksilla, mikäli siirto ei tapahdu nopeasti. Kukapa tahtoisi vastustaa esimiesasemassa olevaa henkilöä. Tätä voidaan vielä viedä pitemmälle sillä tavoin, että työntekijä saa puhelinsoiton hieman sähköpostin saamisen jälkeen, jossa lakimies tai muu taho kyselee jo maksusuorituksen perään. Tällä tavoin painostuksen määrä tuplaantuu ja työntekijä entistä helpommin hoitaa asian pyynnöstä eteenpäin (Poliisi 2019a; Europol 2019).

3.1.5 Ohituskaista

Tekijä voi vedota edellä mainittuihin syihin (kiire, arkaluonteisuus) ja pyytää työntekijää ohittamaan normaalit toimintatavat, koskien yrityksen laskutuskäytäntöjä. Pyyntö voi osittain kuulostaa epätavalliselta ja olla pahastikin ristiriidassa yrityksen käytäntöjen kanssa, mitä sisäisesti normaalissa maksuliikenteessä noudatetaan (Poliisi 2019a; Europol 2019).

3.1.6 Toimintaohjeet

Kun alkuun on luotu luottamus ja saatu kommunikaatio kulkemaan tekijän ja työntekijän välillä, voidaan jatko hoitaa edelleen sähköpostitse, jossa annetaan myöhemmin ohjeet maksun suorittamiseen. Tässä voidaan myös hyödyntää kolmatta tahoa, jolle työntekijä voi soittaa tai laittaa sähköpostia varmistaakseen, että kyseessä on oikea maksusiirto (Poliisi 2019a; Europol 2019).

3.1.7 Rahan siirto

Se mihin tekijä loppupelissä tähtää, on tietenkin rahan konkreettinen siirto tekijän tilille. Tässä piilee se pahin kompastuskivi yrityksen kannalta, koska tekijän antama tilinumero on väärä. Yleensä kyseessä on Euroopan ulkopuolinen tilinumero. Tällä pyritään siihen, että Euroopan ulkopuolelle siirretty raha on haastavampi jäljittää tai siirtoa perua (Poliisi 2019a; Europol 2019).

4 KÄYTTÄJÄN MANIPULOINTI

4.1 Määritelmä

TEPA-termipankki määrittelee käyttäjän manipuloinnin (engl. Social engineering) seuraavasti.

> ”Toiminta, jonka tavoitteena on hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi ja käyttämällä hyväksi tiedon käyttöön oikeutettuja henkilöitä. Huomautus: Käyttäjän manipulointi voi kohdistua yhteen tai useampaan henkilöön. Usein manipuloinnilla pyritään selvittämään käyttäjän salasana.”

Kun lähdemme purkamaan termiä paremmin auki, aukeaa sen monipuolisuus mielestäni paremmin. Toiminta ei rajoita tekoa mihinkään tiettyyn ympäristöön, vaan se voi tapahtua kasvotusten, puhelimitse tai internetissä. Tavoitteena luottamuksellisen tiedon hankita lienee itsestäänselvyys, vaikka toisaalta lopullinen tavoite on yleensä rahallinen hyöty. Tämä kuvastaa sitä, kuinka käyttäjän manipulointi itsessään on vain yksi keino muiden joukossa saavuttaa haluttu määränpää.

Luottamuksellinen tieto ei kuitenkaan rajoitu yhteen tietoon tai yhteen henkilöön. Tavoite on tässä muodostaa eräänlainen kartta tai tietopankki erilaisesta tiedosta ja ihmisistä ja näiden avulla toteuttaa tietomurto.

Tekeytyminen toiseksi henkilöksi tai tiedon käyttöön oikeutetuksi on erehdyttämistä sen perimmäisessä muodossa, mikä kuvastaa hyvin petosrikoksen muotoa (Rikoslaki 39/1889 36:1§.)

Kohdistuminen yhteen tai useampaan henkilöön kuvastaa teon suunnitelmallisuutta ja kuinka pienistä informaation palasista saadaan koostettua riittävästi haavoittavaa tietoa. Eli jo hyvinkin pienistä tiedonmuruista koottu luottamuksellinen tieto saattaa olla yrityksen kannalta haavoittavaa.

4.2 Käyttäjän manipuloinnin tarkoitus

Käyttäjän manipulointi on jatkuvasti kasvava uhka. Lähivuosina eri kokoiset ja erityyppiset organisaatiot ovat joutuneet sen uhreiksi. Joukossa on myös yhteiskunnalle kriittisiä palveluita ja toimintoja. Kun organisaatiot ja yritykset panostavat IT-ratkaisuihin ja datan salaamiseen, jotta tieto pysyisi turvassa, palaavat hyökkääjät vanhanmallisiin toimintatapoihin. Nämä ovat niitä tapoja, jolla hyödynnetään ihmisen omia heikkouksia ja isketään käyttäjään suoraan (Jaf ym. 2018).

Käyttäjän manipulointi on psykologinen hyökkäys, jolla saadaan aikaan vaste ja monesti suostumus kohteilta, jotka eivät normaalitilanteessa olisi halukkaita suostumaan toteuttamaan jotain asiaa mihin hyökkääjä pyrkii. Useasti tämä asia on salasana, käyttäjätunnus tai pääsyn antaminen tiettyyn järjestelmään (Jaf ym. 2018).

Tänä päivänä käyttäjän manipulointi on korkealla sijoituksella EUROPOL:in listalla, kun käydään läpi organisaatioihin ja yrityksiin kohdistuvista uhkia (EUROPOL 2019). Paras suoja käyttäjän manipulointia kohtaan saadaan yleisellä ihmisten tietoisuuden parantamisella kyberuhista ja asianmukaisella koulutuksella. Hyvänä esimerkkinä tässä toimii se, että kun käyttäjän manipulointiin kohdistuva hyökkäys ilmenee, eivät mitkään tekniset turvaratkaisut estä käyttäjää antamasta hyökkääjälle salasanaa esimerkiksi puhelimitse. Vastaavasti taas oikein kohdistetulla koulutuksella sama työntekijä voi toimia lenkin vahvimpana yrityksessä tai organisaatiossa ja tällä tavoin pelastaa työnantajansa mahdollisesti suureltakin hyökkäykseltä (Jaf ym. 2018).

4.3 Kevin Mitnick

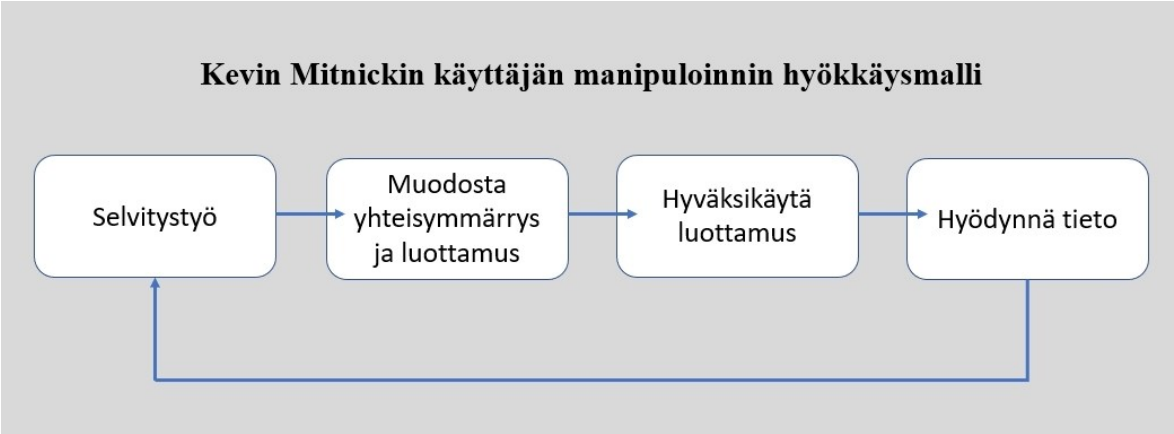
Ainakin julkisuudella mitattuna maailman kuuluisin hakkeri on Kevin Mitnick. Mitnick pääsi julkisuuteen jo 90-luvun puolella, kun hän toteutti erinäisiä tietomurtoja ja pääsi FBI:n etsityimpien listalle. Suomessa hän tuli tunnetuksi, kun hän puhelimitse sai hankittua Nokian Salon verkkopalvelimille käyttäjätunnukset. Sieltä kautta hän pystyi lataamaan Nokian matkapuhelinten lähdekoodit. Käyttäjätunnukset hankitiin puhelimitse ilman minkäänlaista tietoteknistä apua hyödyntäen (Jukam 2015).

Mitnick on sanonut, että vielä nykypäivänäkään ei ole teknologiaa, jota ei pystyttäisi ohittamaan käyttäjän manipulointia hyödyntämällä. Samanlaisia lausuntoja kuulee monesta suunnasta tietoturvaihmisten suusta vielä nykypäivänäkin. Ihminen on edelleenkin se heikoin lenkki tietoturvan suhteen.

4.3.1 Käyttäjän manipuloinnin hyökkäysmalli

Käyttäjän manipuloinnissa hyödynnetään erilaisia taktiikoita, jotta kohde saadaan ansaan ja suorittamaan hyökkääjän vaatima asia. Yksinkertaisimmillaan se voi olla luottamuksen saaminen puhelimitse, jota kautta sitten saadaan tiedusteltua luottamuksellista ja arkaluonteista tietoa.

Yleisesti tunnustetuin malli hyökkäämiseen on Kevin Mitnickin luoma käyttäjän manipuloinnin hyökkäysmalli. Tämä malli kuvataan Mitnickin kirjassa The art of deception: controlling the human element of security (Mitnick 2002). Malli määrittelee neljä vaihetta mitkä tapahtuvat ennen käyttäjän manipulointia ja sen aikana.



Kuva 1. Kevin Mitnickin käyttäjän manipuloinnin hyökkäysmalli (Jaf ym. 2018).

Selvitystyön aikana tietoa kerätään kohteesta ja sen heikkouksista. Lisäksi hankitaan kaikki tieto kohteesta, mikä voi auttaa hyökkäyksen myöhäisemmässä vaiheessa. Toisessa vaiheessa pyritään muodostamaan yhteisymmärrys ja luottamus kohteen kanssa. Tämä luottamus hyödynnetään kolmannessa vaiheessa. Luottamuksen hyväksikäyttäminen ilmenee siten, että saadulla tiedolla kohde saadaan tekemään haluttu toimenpide tai tarjoamaan lisätietoa vaaditusta asiasta. Hyökkäyksen neljäntenä vaiheena oleva tiedon hyödyntäminen on hyökkäyksen viimeinen näytös. Tässä tieto ja saadut resurssit, jotka on kerätty kolmen ensimmäisen vaiheen aikana, pannaan hyötykäyttöön, jotta saavutetaan haluttu tulos (Jaf ym. 2018).

4.3.2 Psykologinen manipulointi

Käyttäjän manipulointi iskee tiettyihin ihmisen luonteenpiirteisiin, jotta hänet saadaan tekemään vastoin tahtoaan ja hyökkääjän tahtotilan mukaan.

Useissa tapauksissa hyökkääjän kohde yrityksissä on työntekijä, joka on vastuussa jonkinasteisesta määräysvallasta tai pitää hallussaan luottamuksellista tietoa, josta on hyötyä hyökkääjälle. Jotta työntekijä on saavuttanut tämän tason, on hänen täytynyt käydä läpi tiettyjä vaiheita yrityksessä. Näiden vaiheiden aikana hän on osoittanut osaamisensa ja tietyn tason ammattimaisuudesta. Joka tapauksessa näitäkin työntekijöitä manipuloidaan luovuttamaan luottamuksellista tietoa. Käyttäjän manipuloinnissa käytetään psykologisen manipuloinnin keinoja, jotta kohde alkaa luottaa hyökkääjään. Metodeina käytetään tunteiden hyödyntämistä, leikittelyä sanoilla, hurmaamista ja tietenkin esiintymistä toisena ihmisenä, jotta kohteen luottamus saadaan muodostumaan (Jaf ym. 2018).

4.3.3 Naiiviuden hyödyntäminen

Hyökkääjä luottaa käyttäjän manipuloinnissa siihen, että ihminen on naiivi, etenkin kun otamme huomioon ne faktat, että jotkut ihmiset ovat epäanalyyttisiä, teknologiavastaisia ja eivät omaa internetin käyttötaitoa. Nämä asiat, kun yhdistetään luontaiseen herkkäuskoisuuteen, huomaamme, että nämä ihmiset pitävät kädessään kylttiä, jossa suorastaan kutsutaan hyökkääjä astumaan peremmälle ovesta (Jaf ym. 2018).

Jos sopiva tilaisuus ilmenee, hyökkääjä toimii ilman viivettä. Luonnon katastrofit, julkisuuden henkilöiden huhut ja päivän polttavat trendit ovat suosittuja tapoja, jolla huijarit saavat huomiota aikaan ja pyrkivät saamaan ihmiset painamaan erinäisiä verkkolinkkejä. Näitä linkkejä voidaan jakaa ympäri internettiä siinä toivossa, että joku aina niitä painaa uteliaisuuttaan. Tämä on varsin toimiva tapa saada haittaohjelmia asennettua tietokoneelle. (Jaf ym. 2018).

4.3.4 Auktoriteettien kunnioitus

Ihmiset ovat lähtökohtaisesti tottelevaisia auktoriteetteja kohtaan. Jo nuoresta iästä alkaen meidät on opetettu vanhempien toimesta kunnioittamaan ja kuuntelemaan ihmisiä, joilla on auktoriteettia. Tämä pitää esimerkiksi sisällään vanhemmat, opettajat ja viranomaiset. Siirryttäessä työelämään tämä sama laajenee esimiehiin, pomoihin ja managereihin, joiden sanaan luotamme ja noudatamme heidän antamiaan käskyjä. Tämä on yksi niistä psykologisista heikkouksista, mitä hyökkääjä innokkaasti hyödyntää. Kohteliaisuus ja kunnioitus ovat tärkeitä, mutta mikäli on ylitotteleva, eikä osaa kyseenalaistaa mitään, on ihminen erityisen helposti huijattavissa. Tätä heikkoutta aktiivisesti myös hyödynnetään hyökkäyksessä. (Jaf ym. 2018).

Auktoriteetti yhdistetään monesti myös univormuihin, erilaisiin tunnuksiin ja käytökseen, jotka ovat symbolisia tai yhdistetään tiettyihin työpaikkojen käytöntöihin. Hyökkääjä voi käyttää tätä ihmisten tottumista näihin ulkoisiin tekijöihin hyödyksi ja pukeutumisella sekä käyttäytymisellään soluttautua työyhteisöön. Tällä tavoin heidän toimintaansa yrityksen sisällä ei niin helposti kyseenalaisteta (Malin ym. 2017, 164 - 165). Esimerkkinä tässä asiassa toimii hyvin huoltomies, jolla on huoltofirman vaatteet, tikkaat kainalossaan ja hän on matkalla tekemään korjauksia yrityksen tiloihin.

4.3.5 Milgramin tottelevaisuuskoe

1960-luvulla Stanley Milgram selvitti yksilöön kohdistuvan auktoriteetin vaikutusta sosiaalipsykologian keinoin. Koehenkilöille ei ollut kerrottu kokeen koskevan auktoriteettia. Heille oli kerrottu, että kokeessa tutkitaan rangaistuksen vaikutusta oppimiseen. Koehenkilö toimi opettajan roolissa, jossa hänen tehtävänsä oli antaa rangaistukseksi sähköisku, mikäli oppilas vastasi tehtävään väärin. Sähköiskun antamisen määräsi kokeen tutkija, joka edusti laboratoriotakissaan auktoriteettia. Sähköiskun voimakkuus koveni pikkuhiljaa testin edetessä. Todellisuudessa oppilaan roolissa toimivat avustajat, jotka eivät oikeasti saaneet sähköiskuja. Oppilaat kuitenkin näyttelivät kärsivänsä sähköiskuista ja anelivat kokeen lopettamista, kun sähköiskut kovenivat. Koehenkilöt kuulivat oppilaiden huudot, mutta eivät nähneet heitä (Milgram 1974). Sähköiskujen voimakkuus vaihteli välillä 15 – 450 volttia.

Kun saavutettiin piste, jossa oppilaat pyysivät lopettamista ja koehenkilö epäröi sähköiskun antamista, määräsi auktoriteetti jatkamaan sähkön antamista. Sähköiskujen teho ilmoitettiin kirjallisesti testilaitteessa varoitustekstein. Asteikon lopussa luki teksti ”vaara” tai ”vakava isku”. Auktoriteetti kuitenkin kertoi sähköiskujen olevan vaarattomia, ja hän lupautuisi ottamaan täyden vastuun seuraamuksista. Koeasetelmassa 65% kokonaisosallistujamäärästä, joka oli 40 henkilöä, ei vastustanut auktoriteettia, vaan jatkoi kokeen loppuun asti. Näissä tapauksissa auktoriteetti oli samassa huoneessa koehenkilön kanssa ja opiskelija oli toisessa huoneessa. Tottelemattomuus oli helpompaa silloin, kun auktoriteetin käskyt tulivat puhelimen välityksellä toisesta huoneesta (Milgram 1974).

Koe on useasti kyseenalaistettu ja eettisyyden vuoksi vastaavaa ei ole lähdetty toistamaan samoin puittein. Vastaavanlaisia testejä on kuitenkin tehty samankaltaisin tuloksin. Yksi näistä on puolalaisten tekemä testi. Tässä testissä eettisyyttä oli pyritty korostamaan ja käytetyt voltit sähköiskuissa olivat pienemmät. Tässä testissä 90% koehenkilöistä oli valmiita antamaan mitta-asteikossa määritellyn kovimman sähköiskun, kun auktoriteetti niin määräsi. Tutkijat analysoivat, että tämä osoittaa sen, kuinka helposti ihmiset toimivat vastoin omatuntoaan, kun heitä auktoriteetti käskee (Doliński ym 2017).

5 TEON TEKNINEN TOTEUTUS

Vaikka yritykset ja organisaatiot ovat nykypäivänä varovaisempia ja tietoisia erilaisista kyberuhista, ovat vastaavasti sitten rikolliset kehitelleet uusia innovaatioita kuinka teknologisia vastatoimia pystytään kiertämään. Tässä käsitellään näitä hyökkäystapoja ja mekanismeja niiden takana, millä monesti toimitusjohtajahuijauksessa toimitaan. Esimerkit sähköposteista perustuvat oikeisiin tapauksiin, mutta yksilöivät tiedot on näistä muutettu. Tarkoitus on näillä visuaalisesti pohjustaa tekstiä.

5.1 Tietojen kalastelu - Phishing

Tietojen kalastelu (engl. Phishing) on yksi keskeisin osa toimitusjohtajahuijausta, kun hyödynnetään tietokoneita ja tietoverkkoja. Tämä siitä syystä, että yksittäinen huijaussähköposti täyttää monesti tietojen kalastelun tunnusmerkit ja tällä yksittäisellä sähköpostilla voidaan käynnistää kokonainen toimitusjohtajahuijaus. Sillä on olemassa muitakin erilaisia muotoja esim. kohdistettu tietojen kalastelu ja soittopyyntöurkinta, joita tässä käydään myös läpi.

Kyseessä on käyttäjän manipulointia hyödyntävä tekniikka, jossa pyritään saamaan arkaluonteista tietoa, kuten esimerkiksi salasanoja, käyttäjänimiä ja taloustietoja yrityksestä. Tekniikka on suhteellisen vanha internetin mittapuulla. Sanaa on alettu käyttämään jo 1996 kun hakkeriryhmät olivat huijanneet isoa amerikkalaista internet yritystä AOL (ent. American Online). Huijaus tapahtui siten, että ryhmä oli satunnaisesti luonut luottokortin numeroita suuret määrät. Näillä korteilla pyrittiin luomaan AOL-tilejä. Kun tilin luonti onnistui, pystyivät he lähettämään roskapostia useille AOL:n muille käyttäjille. Termi syntyi, kun lähetetiin sähköpostia suurille massoille ja osa tarttui koukkuun. Eli kalustustermein tässä oli käytössä syötti ja koukku. (Infosec 2020a).

Tietojen kalastelusähköposti pitää sisällään elementtejä, joita hyödynnetään perinteisessä taikuudessakin. Eli pyritään kohdistamaan huijattavan katse ja huomio ihan muualle missä huijaus tapahtuu. Sähköpostin pitää näyttää viralliselta ja mikäli yritys käyttää sähköpostin allekirjoitukseen logoja tai vastaavia, pitää ne huijaussähköpostista myös löytyä (Malin ym. 2017, 150).

Yksi tärkeimpiä luotettavuuden mittareita huijauksessa on saada lähettäjän sähköpostiosoite näyttämään siltä, että se tulisi luotettavalta taholta. Tässä hyödynnetään sähköpostiosoitteen

lähetysosoitteen huijausta (engl. Spoofing). Tässä saadaan sähköposti näyttämään siltä, että lähettäjänä on tuttu ja luotettu taho, esimerkiksi toimitusjohtajan nimi kuvassa 1. Tässä kuvataan esimerkkiä, jossa yrityksen työntekijöiltä pyritään saaman tieto ihmisestä kuka vastaa yrityksen maksuliikenteestä. (Infosec 2020b.)

LÄHETTÄJÄ: **Matti Meikäläinen** <matti.meikalainen@e.mail.fr>
LÄHETETTY: maanantaina 9. joulukuuta 2019 10.27
VASTAANOTTAJA: Maija Miettinen <maija.miettinen@yritys.fi>
AIHE: Laskujen hyväksyntä

Hei Maija,

Muistatko kuka vastaa laskujen hyväksynnästä teidän osastolla? Vastaa nopeesti.

Terveisin
Matti Meikäläinen
Toimitusjohtaja

Kuva 1. Esimerkki huijaussähköpostista

Normaalisti sähköpostiohjelmat saattavat vain näyttää lähettäjän nimen ilman, että siinä on tarkemmin eritelty lähettäjän oikea sähköpostiosoite. Kuvassa 1 näkyvä sähköpostin alkuperä @e.mail.fr omaa maatunnuksen Ranskasta ja kyseessä on siellä toimiva ilmainen sähköpostipalvelu. Tässä tapauksessa on siis luotu vain toimitusjohtajan etu- ja sukunimeä käyttämällä tili kyseiseen palveluun. Kyseessä on siis hyvin yksinkertainen tapa koostaa tiedonkalustelusähköposti, kun tiedossa vain on oikea henkilö, jonka nimeä voidaan hyödyntää huijauksessa. Tässä hyödynnetään juuri sitä, että ihmisen katse kohdistuu tuttuun ja luotettuun nimeen ilman, että tarkemmin lähdetään tutkimaan lähettäjän alkuperää (Malin ym. 2017, 150). Toimitusjohtajan nimen selvittäminen ei vaadi nykypäivänä, kuin yhden verkkohaun, eikä sinällään vaadi käyttäjän manipuloitiin vaadittavia keinoja. Yritysten taloustiedot ovat myös monesti vapaasti tarjolla erilaisissa verkkopalveluissa. Näistä tiedoista voidaan helposti poimia useita yrityksen työntekijöitä, jolle voidaan lähettää kalastelupostia massalähetyksenä. Tässä riittää se, että yksi ihminen tärppää pyydykseen ja kertoo tarvittavan tiedon millä huijausta voidaan viedä eteenpäin.

Tietojen kalastelu luottaa lisäksi siihen, että suurin osa ihmisistä haluaa tehdä asiat oikein ja mikäli luotettava taho pyytää jotain toimenpidettä tekemään ei sitä pidetä mitenkään ihmeellisenä, mikäli sisältö ei liikaa poikkea normaalista. Lisäksi harva jättää reagoimatta pyyntöön varsinkin, jos pyynnön jättämättä tekemisellä voisi olla jotain negatiivisia vaikutuksia ihmiselle itselleen. (Malin ym. 2017, 151).

5.1.1 Kohdistettu tietojen kalastelu - Spear phishing

Kehittyneempi tietojen kalastelun muodoista on kohdistettu tietojen kalastelu. Tässä pyritään nimenomaan tavoittamaan tietty taho tai ihminen, jolle pyyntö voidaan kohdistaa. Tästä voidaan myös käyttää englannin kielistä termiä ”Whaling” eli valas, mikä viittaa siihen, että henkilö, johon tietojen kalastelu kohdistetaan, omaa merkittävän aseman, statuksen tai rahaa ja valtaa. Tällä tavoin tietojen kalastelun tuotto kasvaa huomattavasti ja raha tai tiedot, joita saadaan kalasteltua voivat olla miljoonien eurojen arvoisia. (Malin ym. 2017, 153).

Kohdistetussa tietojen kalastelussa käyttäjän manipulointi näyttelee jo huomattavasti suurempaa roolia. Tässä hyödynnetään keinoja, jota on kuvattu aiemmin. Yksi tärkeimpiä näistä on kiireen tuntu ja miellyttämisen halu. Vaikka työntekijällä olisi tiedossa, että rahat eivät välttämättä siirry heti eteenpäin esimerkiksi viikonlopun vuoksi, pyrkii työntekijä kuitenkin miellyttämään toimitusjohtajaa toimimalla nopeasti. Mikään ei huijaa ihmistä paremmin, kuin ihmisen itselleen kertomansa valhe. (Malin ym. 2017, 154).

LÄHETTÄJÄ: Matti Meikäläinen <matti.meikalainen@yrityss.fi>
LÄHETETTY: perjantaina 3. tammikuuta 2020 15.38
VASTAANOTTAJA: Pekka Miettinen <pekka.miettinen@yritys.fi>
AIHE: Lasku 06122

Hei Pekka,

Voitko tehdä kansainvälisen siirron EU-maahan tänään? Tämä koskee odottavaa laskua ja pitää hoitaa nopeasti ennen viikonloppua.

Haluan tietää sitten voin lähettää sinulle pankin tiedot.

Terveisin
Matti Meikäläinen
Toimitusjohtaja

Kuva 2. Esimerkki kehittyneestä huijaussähköpostista.

Mitä enemmän tuttuja elementtejä sähköpostissa on, sen helpommin ihmistä pystyy huijaamaan. Silmä hakeutuu tuttuihin seikkoihin ja pienet kauneusvirheet voivat jäädä huomiotta. Lähettäjän sähköpostiosoitteessa ylimääräinen s-kirjain jää vähälle huomiolle, mikäli muuten oikeat elementit ovat sähköpostissa olemassa.

Ilmaisen sähköpostitilin luominen esimerkin mukaisessa tapauksessa ei vaadi enempää aikaa kun 15 minuuttia ja tietokoneen peruskäyttäjän taidot. Ilmaisia palveluita on tarjolla lukuisia aina perinteisestä Gmail-palvelusta alkaen ja näissä palveluissa on mahdollista käyttää haluamaansa lähettäjän nimeä. Tähän perusmuotoiseen huijaukseen kuitenkin moni lankeaa, vaikka verkkotunnus (engl. domain name) ei vastaakaan yrityksen nimeä. Hieman vaativampi lähestyminen vaatii yleensä maksullisen palvelun, jonka kautta luoda palvelimen nimi mikä muistuttaa hyvin paljon alkuperäistä sähköpostin lähettäjän nimeä. Tästä esimerkkinä mainittu @yrityss.fi-sähköpostiosoite.

5.1.2 Soittopyyntöurkinta – Vishing

Tietojen kalastelun muodoista toimitusjohtajahuijauksissa myös sähköpostin lisäksi hyödynnetään perinteisiä puhelinsoittoja. Erityisen tehokasta tämä on silloin, kun lähestytään sekä sähköpostitse ja puhelimitse mahdollista uhria.

Vishing tai voice phishing on käyttäjän manipulointia hyödyntävä lähestymistekniikka, jolla saadaan puhelimitse arkaluonteista tietoa yrityksestä, salasanoista ja muista luottamuksellisista tiedoista. Tässä soittaja esiintyy toisena henkilönä tai tunnettuna yrityksenä huijatakseen ihmisiä. Pelottelun ja muiden manipulointikeinojen avulla pyritään saamaan ihminen luovuttamaan tarvittava tieto. Samankaltaista toimintaa on hyödynnetty suomessakin nähdyssä valepoliisi-ilmiössä, missä varsinkin ikäihmisiltä on huijattu rahaa (Iltasanomat 2019).

Perinteinen vishing on ollut automatisoitua ja siinä on hyödynnetty robottipuheluita ja nauhoituksia, mutta yhdistettynä toimitusjohtajahuijaukseen, täytyy soittajan olla ihminen, joka hallitsee käyttäjän manipulointia vaativia keinoja. (FraudWatch International 2019).

5.1.3 Diskurssi – kielellinen ilmaisu osana tietojen kalastelua

Kielenkäyttö on osa toimitusjohtajahuijauksia niin kirjoitetussa muodossa, kuin puhuttuna. Tunnusmerkistössä ei välttämättä kielenkäyttö liity rikosasiaan, mutta osa rikosta se kuitenkin on. Varsinkin kun kielellisin keinoin teon yhteydessä pyritään huijaamaan ihmisiä. Toimitusjohtajahuijauksessa pyritään kuitenkin pääasiallisesti valehtelemaan ja manipuloimaan uhria puheen ja kirjoitetun tekstin kautta (Rentola 2019, 9-10).

Olemme ehkä hieman tuudittautuneet siihen ajatusmalliin, että meidän ainutlaatuinen suomen kielemme antaisi lisäturvaa huijauksia vastaan. Tämä on osin totta ja kaikista epäammattimaisimmat huijarit käyttävät esimerkiksi ilmaisia kääntäjiä, kuten Goole Translate-palvelua ja paljastuvat siten suhteellisen helposti.

Vaikka rikolliset olisivatkin alkuperältään jotain muuta, kun syntyperäisiä suomalaisia, on heillä mahdollisuus käyttää muuleja (Poliisi 2019c). Tällöin saadaan kieli- ja paikkatuntemus hyödynnettyä. Sopivaa maksua vastaan muuli voi hoitaa muitakin pienimuotoisia toimia rikollisten hyväksi. Toki vaikka kyseessä olisi kansainvälinen rikollisorganisaatio, voi siinä myös toimia paljonkin suomalaisia toimijoita. Tällöin kielen tarjoamat haasteet on helppo ohittaa.

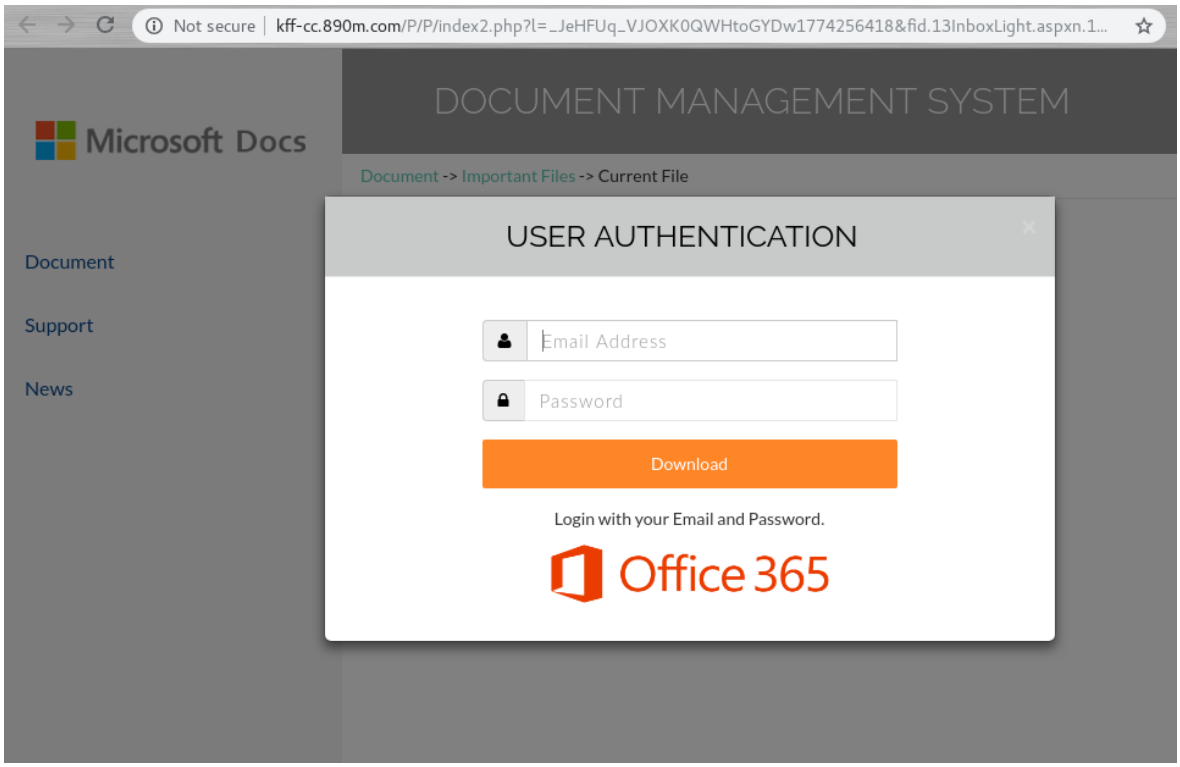
5.2 Microsoft Office 365-huijaus

Toinen merkittävä sähköpostihuijaus tässä huijauksen lajissa on Outlook käyttäjätunnuksen ja salasanan kaappaaminen. Tässä huijauksessa on monta eri tapaa sen toteuttamiseen, mutta tavoite niissä kaikissa on sama, eli saada käyttäjän käyttäjätunnus ja salasana rikollisten haltuun.

Microsoft Office 365-huijaustapaus kuuluu toimitusjohtajahuijauksen alle, vaikka sillä voidaan muunlaisiakin tietomurtoja suorittaa. Huijaustapana se on kuitenkin teknisempi ja sitä vastaan voidaan laajemmin suojautua IT-osastojen toimesta. Nämä suojaustavat ovat kuitenkin enemmän isompien yritysten kontolla, jossa on keskitetty IT-tuki. En ole lähtenyt tässä työssä avaamaan niitä seikkoja sen tarkemmin.

Teko alkaa sillä, että oletettavasti luotetusta lähteestä tulee sähköposti, jossa pyydetään sähköpostin lukijalta erilaisia toimenpiteitä suoritettavaksi. Käyttäjän pyydetään avaamaan linkki tai tiedosto sillä verukkeella, että hänen tilillensä on hyökätty, tai käyttäjä joutuu jostain syystä kirjautumaan uudelleen Office 365-järjestelmään. Yksi huijauskeino on myös, että käyttäjä saa aidolta näyttävän sähköpostin, jossa on tieto siitä, että joku käyttäjän lähettämä sähköposti ei ole mennyt perille vastaanottajalle (engl. undeliverd message). Todellisuudessa käyttäjä ei tämänkaltaista sähköpostia ole koskaan edes lähettänyt (Kyberturvallisuuskeskus 2019).

Näissä huijauksissa käyttäjän painettua väärennettyä linkkiä tai avatessaan liitetiedoston hän ohjataan väärennetylle web-palvelimelle, joka kysyy käyttäjätunnusta ja salasanaa. Websivu tällä palvelimella näyttää täysin samalta, kun aito Outlook kirjautumisikkuna, mutta sillä poikkeuksella, että palvelimen osoite on aivan jotain muuta, kun Microsoftin palvelimet käyttävät. Tämä huijauspalvelin voi olla rikollisten oma palvelin tai usein he ovat kaapanneet jonkun palvelimen käyttöönsä missä turvataso on ollut heikko. Useasti ajan tasalla olevat internet-selaimet, jotka avaavat tämän kaltaisen sivun, voivat huomata jotain outoa sivun ulkoasussa ja tekstissä. Tätä kautta selain voi varoittaa käyttäjää, joka tämänkaltaisen sivuston avaa. Haaste on siinä, huomaako käyttäjä tätä varoitusta, kun keskittyminen on puhtaasti kohdistettu käyttäjätunnuksen ja salasanan antamiseen sivustolle (Tietosuojavaltuutetun toimisto 2020).



Kuva 3. Esimerkki Outlook-kirjautumisesta. Lähde Kyberturvallisuuskeskus 2019.

Outlook-huijauksen toteuttaminen vaatii jo keskimääräistä hieman enemmän tietotekniikan hallintaa. Toisaalta tähänkin on saatavilla valmiita paketteja, millä jo perustaidoillakin varustettu motivoitunut hyökkääjä saa tuhoa aikaan. Tähän tarkoitukseen on valmistettu niin sanottuja tietojen kalastelun paketteja (engl. Phishing kit), joissa on valmiita sivustopaketteja, esimerkiksi sellaisille sivustoille kuin Outlook 365, Google, Facebook ja vaikka DropBoxia varten (Kyberturvallisuuskeskus 2019).

5.3 Hakkerit

Tietojen kalastelupaketin käyttäjä voi monesti olla harrastelijahakkeri/skriptipentu (engl. script kiddie). Tässä on kyseessä henkilö, joka ei omaa itse koodaamiseen vaadittavia taitoja eikä välttämättä ole niitä valmis edes opettelemaan. Kuitenkin hän omaa riittävän motivaation etsiäkseen ja käyttääkseen muiden tekemiä valmiita koodi- ja skriptipaketteja. Nämä paketit muotoutuvat helposti käyttäjän tarpeisiin pienillä muutoksilla (Putman 2020).

Vaikka henkilön osaamistaso ei ole välttämättä huomattava, ei häntä silti pidä aliarvioida. Sopivilla kontakteilla ja ostetuilla palveluilla on mahdollista saada isojakin toimijoita polvilleen, jos motivaatio haitan tekemiseen vain on korkea (Putman 2020).

Vaikka harrastelijahakkerit omalla toimellaan aiheuttavat suurtakin haittaa, ei heitä välttämättä lasketa niin sanottuihin oikeisiin hakkerityyppeihin. Varsinaisia hakkerityyppejä on kolme: Valkohatut, Mustahatut ja Harmaahatut, mutta variaatiota on toki enemmänkin ja verkossa haittaa sekä tuhoa tekeviä tahoja on useita muitakin.

Valkohatut ovat niitä, jotka yrityksen toimeksiannon mukaisesti kartoittavat minkälaisia tietoturvauhkia yrityksen järjestelmissä on. Heidän tehtävänsä on raportoida tietoturva-aukoista ja mahdollisesti antaa kehitysehdotuksia aukkojen korjaamiseen. Näiden hakkerien toiminta on tässä kategoriassa eettisintä (Norton 2020).

Harmaahatut ovat etiikaltaan häilyviä. Välillä Harmaahattu voi toimia kuten Valkohattu ja kartoittaa uhkia toimeksiannosta. Välillä he taas voivat julkaista tietoturva-aukon ja tällä tavoin pakottaa sovelluskehittäjän tai yrityksen korjaamaan vian. Tämä tekee heidän toiminnastaan arvaamatonta ja tietyllä tapaa saa heidät näkymään enemmänkin aktivisteina, jotka paljastavat yrityksien asioita oman aatteensa vuoksi (Norton 2020).

Mustahattu-hakkerilla on yleisesti tietotaitoa murtautua tietoverkkoihin. Yleensä nämä henkilöt luovat haittaohjelmia, mitkä edesauttavat verkkoihin murtautumisia. Yleinen motivaatio heillä on raha tai vietti verkkorikollisuuteen. Nämä hakkerit pyrkivät nimenomaan anastamaan luottamuksellista tietoa, kuten henkilökohtaista arvokasta tietoa (Norton 2020).

Yhteistä Valkohatuille, Harmaahatuille ja Mustahatuille on se, että he yleensä osaavat luoda ohjelmistokoodia alusta alkaen. Tämä johtaa siihen, että he pystyvät rakentamaan työkaluja tilanteen mukaan itselleen ja muille. Kuten aiemmin mainittu, niin tämä on suuri ero näillä hakkereilla verrattuna harrastelijahakkereihin, joilla ei yleensä tämän kaltaista osaamista ole. Yhteistä näille kaikille on se, että heidän käyttämänsä työkalut ovat usein samoja riippumatta missä roolissa he toimivat.

6 SUOJAUTUMINEN JA ENNALTAEHKÄISY

> ”Sodan doktriini on olla olettamatta, ettei vihollinen tule, ja luottaa omaan valmiuteensa kohdata hänet, olla uskomatta, ettei hän hyökkää ja tehdä itsestään voittamaton.” (Tzu, Sun 2007, 121)

Sun Tzun opetukset näemmä kantavat 2000-2500 vuoden jälkeen vielä kyberturvallisuuteenkin asti. Kantava ajatus on tässä se, että hyökkäyksen todennäköisyys ei ole se mitä pitää laskelmoida, vaan pyrkiä miettimään mikä on oma valmius hyökkäystä vastaan (Limnéll ym. 2014, 76).

Tilanteesta riippumatta tulee olla olemassa toimintakyky, jolla vastata haasteisiin. Kaikkien tietoturvan kanssa tekemisissä olevien tulisi ymmärtää, että kyberhyökkäys voidaan kohdistaa ketä tahansa vastaan ja koska tahansa. Hyökkäyksen todennäköisyyden ja kohteen kiinnostavuuden määrittelee hyökkääjän näkökulma, joka vaihtelee tilanteen mukaan (Limnéll ym. 2014, 76). Hyökkääjä toimii silloin, kun parhaaksi näkee, ei silloin, kun yritys on parhaiten valmistautunut.

Varautuminen, työntekijöiden tiedottaminen ja tietoisuus uhista ovat ne tärkeimmät tekijät, jotta tätä hyökkäysmallia vastaan voidaan puolustautua.

6.1 Tietoisuuden lisääminen Suomessa

Suomessa toimii useita tahoja, jotka pyrkivät parantamaan yleistä tietoisuutta uhista ja tiedottamaan ajankohtaisista vaaroista verkossa. Näitä tahoja ovat esimerkiksi Kyberturvallisuuskeskus, Kuluttajaliiton huijausinfo.fi sekä Jyväskylän Ammattikorkeakoulun CYBERDI-hanke.

Huijausinfo.fi on Kuluttajaliiton hanke, joka pyrkii lisäämään tietoisuutta erityyppisistä huijauksista nimenomaan verkossa. Hankkeen rahoittaa tällä hetkellä Sosiaali- ja terveysjärjestöjen avustuskeskus (STEA). Verkkosivusto tarjoaa tietoa, miten huijauksen voi tunnistaa ja minkälaisia huijauksia ylipäätänsä on olemassa (Kuluttajaliitto 2020).

Huijausinfo järjestää aiheesta verkkokoulutuksia ja kursseja, jotka ovat maksuttomia. Lisäksi tarjolla on paljon itseopiskelumateriaalia ja vertaistukiryhmä, jossa tarjotaan tukea ihmisille, jotka ovat huijauksen uhreiksi joutuneet. Yhtenä tapana tietoisuuden jakamiseen toimii Twitter ja siellä #huijausinfo sekä #varohuijareitaverkossa hastagit (Kuluttajaliitto 2020).

Jyväskylän Ammattikorkeakoulun CYBERDI-projektin tavoitteena on kehittää käytäntöjä, miten toimia kyberrikoksien estämisessä, kuinka näitä tutkitaan sekä selvitetään. Tietoisuuden parantaminen käyttäjälähtöisesti on myös merkittävässä roolissa projektilla. Tutkimus- ja kehitystyötä CYBERDI:ssä kohdistetaan yhteistyössä eri tahojen kanssa. Näitä tahoja ovat esimerkiksi Poliisiammattikorkeakoulu, Kuluttajaliitto ja Keski-Suomen kauppakamari (CYBERDI 2020).

CYBERDI:n tietopankissa korostuu käyttäjälähtöisyys siten, että sinne on laadittu tiiviitä kortteja erilaisista huijaustyypeistä. Nämä kortit ovat vapaasti kenen tahansa hyödynnettävissä ja kertovat erilaisten huijausten tunnusmerkit selkokielisesti. Tämän lisäksi myös CYBERDI hyödyntää muuan muassa Twitteriä tietoisuuden levittämiseen uhista. Hashtag #oletietoinen jakaa ajankohtaista tietoa kulloinkin verkossa esiintyvistä uhista (CYBERDI 2020).

Näiden tahojen tuottama materiaali ja koulutusinfo on helposti lähestyttävää ja käyttäjäystävällistä. Suurin haaste lienee näillä toimijoilla on se, miten saada hyödyllinen informaatio sitä eniten tarvitseville. Yritystoiminnassa tämänkaltaisen tiedon seuraaminen on välttämätöntä, mutta koska myös yksityishenkilöillä on lähes kaikki palvelut nykyään verkossa, tulisi heidänkin saada ajankohtaista tietoa erilaisista verkkoon kohdistuvista uhista.

6.2 Tekniset varmistuskeinot

Yrityksen tulisi tarkistaa nettisivuillaan näkyvät tiedot ja miettiä onko kaiken sen informaation julkisesti tarjoaminen tarkoituksenmukaista. Tämä koskee myös sosiaalista mediaa. Yrityksen hierarkian avaaminen ulospäin tekee yrityksestä myös helposti haavoittuvan.

Käytetty laitteisto ja tietoturva tulisi aina pitää ajan tasalla. Tällä tavoin järjestelmissä ei ole vanhoja tietoturva-aukkoja, jotka vaarantavat kokonaisturvaa. Tämä koskee yhtä lailla käytössä olevia tietokoneita ja niissä pyöriviä ohjelmistoja, sekä tietenkin verkon infrastruktuuria.

Yrityksen ulkopuolelta tuleville sähköposteille on mahdollista asettaa merkintä tai huomioväri, joka osoittaa sähköpostin tulevan ulkopuolelta. Tällä tavoin huijaussähköposti voi tarttua helpommin työntekijän silmään. Yritys voi myös asettaa sähköpostin lähettäjäkentän

aukeamaan kokonaisuudessaan sähköpostin saapuessa, jolloin työntekijä pystyy näkemään, mikäli joku sähköpostin osoitekentässä poikkeaa normaalista.

Yksittäisen työntekijän tai yrityksen tietoturvaihmisten tulisi seurata minkälaisia uudelleenohjaussääntöjä Outlook sähköpostiohjelmaan on asetettu. Näillä pyritään ohjaamaan takaisin sähköpostiin tulevat viestit rikollisen haltuun, sekä piilottamaan ne työntekijän näköpiiristä esimerkiksi ohjaamalla ne johonkin piilossa olevaan kansioon Outlook-ohjelmassa.

Kaksivaiheisen tunnistautumisen asettaminen Microsoft-tilille antaa lisää turvaa sähköpostin käyttöön. Näin pystytään seuraamaan paremmin, mikäli jostain tuntemattomasta tai uudesta laitteesta kirjaudutaan tilille. Kirjautumisesta tulee tietoa mobiililaitteeseen mistä kirjautuminen pitää erikseen hyväksyä. Näin on mahdollisuus estää jo anastettujen käyttäjätunnusten väärinkäyttö.

6.3 Kuinka uhka voidaan tunnistaa yksittäisestä sähköpostista

Tärkeää olisi järjestää ennakoivia koulutuksia yrityksen työntekijöille ja sivistää itseään, sekä muita kollegoita väärennettyjen sähköpostien vaaroista. Myös säännölliset muistutukset asian tiimoilta auttavat parantamaan tietoisuutta uhista.

Mikäli tietomurtoa ei vielä ole päässyt tapahtumaan esimerkiksi toimitusjohtajan tai laskutuksesta vastaavan henkilön sähköpostiin, on vielä mahdollisuus tunnistaa väärennetty sähköposti suhteellisen yksinkertaisesti

Tärkeää on varmistaa lähettäjän sähköpostin alkuperä. Onko sähköpostin osoite varmasti oikea. Onko kirjaimia mahdollisesti vaihtunut. Onko esimerkiksi iso i-kirjain ”I” vaihdettu pieneksi L-kirjaimeksi ”l”. Onko osoite jollain lailla väärinkirjoitettu (Hornetsecurity 2019).

Epävarmuuden iskiessä jonkun tietyn asian suhteen sähköpostissa, voi ottaa yhteyttä kollegaan. Mikäli henkilön, joka on sähköpostin lähettänyt, pitäisi istua lähellä, niin hänen kanssaan kannattaa keskustella asiasta kasvotusten tai soittamalla hänelle numeroon, joka on varmistetusti oikea (Europol 2019; Hornetsecurity 2019).

Kirjoitusvirheet paljastavat paljon. Esimerkiksi vastaanottajan nimi on kirjoitettu väärin tai varsinainen teksti on laiskaa eikä tunnu sopivan yrityksen kulttuuriin. Myös automaattisen käännöskoneen aiheuttamat virheet on syytä huomioida (Hornetsecurity 2019).

Sähköpostin linkkejä ei pitäisi painaa miettimättä. Sen sijaan, että avataan tutun oloinen linkki painamalla sitä sähköpostista, voi sen avata suoraan internet-selaimesta. Kun hiiren vie linkin päälle (engl. hover over) näyttää se kohteen mihin linkki avataan sen sijaan, että se näyttäisi vain tekstin mikä linkille on annettu nimeksi (Europol 2019; Hornetsecurity 2019).

6.4 Yleiset varmistusmekanismit

Mikäli teknisistä varmistuskeinoista huolimatta huijaussähköposti tulee perille asti ja työntekijä uskoo sen sisällön, on vielä mahdollisuus estää huijauksen tapahtuminen. Tietyllä tapaa viimeisenä suojamuurina toimii myös yrityksen laskutuksen sisäisesti sovitut käytännöt. Hiemankin epäilyttäviin maksupyyntöihin tulisi aina suhtautua suurella varauksella (Poliisi 2019d).

Vakiintuneet käytännöt laskutuksen suhteen ovat tässä avainasemassa. Yrityksen pitää muodostaa tarkistuskäytännöt, joilla varmistetaan se, että onko sähköpostitse saapuva maksu aito ja oikea. Onko lähettävä taho oikea ja ennen kaikkea se, mille tilille maksu ollaan suorittamassa. Mikäli tilinumero on poikkeava verrattuna siihen mitä on sovittu laskuttavan tahon kanssa aiemmin, pitää asia tutkia tarkkaan miksi tilinumero on muuttunut. Varsinkin uusien työntekijöiden ja sijaisten kanssa asiaan pitäisi paneutua sen vaatimalla vakavuudella, ettei huijauksia pääse syntymään (Poliisi 2019d).

Yrityksen tulisi myös laatia raportointi sen suhteen, mikäli epäiltyjä huijauksia ilmaantuu, jotta niiden suhteen voidaan tehdä seurantaa ja tarkkailla trendejä. Samalla tavoin kaikista huijauksista pitäisi raportoida poliisille, vaikka huijaus pystyttäisiinkin välttämään. Nopea toiminta ja yhteys omaan pankkiin voi vielä pelastaa siirrettyjen rahojen kohtalon (Poliisi 2019d).

7 YHTEENVETO JA POHDINTA

Kirjallisuuskatsauksen tarkoituksena oli kuvata toimitusjohtajahuijausta ilmiönä. Tavoitteena oli saada työstä sujuvaa luettavaa sekä varmistaa, että tieto olisi mahdollisimman hyvin ajantasaista.

Opinnäytetyön kantavat tutkimuskysymykset olivat toimitusjohtajahuijauksen kuvaaminen ilmiönä sekä miten teko toteutetaan. Teon toteuttamisen jaoin vielä tekniseen toteuttamiseen ja käyttäjän manipulointia hyödyntäviin alakohtiin. Rajaamisen pyrin pitämään suhteellisen tiukkana siitä syystä, että tiesin riskin siitä, kuinka helposti asia lähtisi rönsyilemään.

Toimitusjohtajahuijauksen kuvaamisessa yritin ottaa näkökulmaksi yrityksen katsantokannan. Pyrin selostamaan tekoa ja sen tunnusmerkistöä siten, että asiasta saisi helposti luettavaa ja käsityksen mistä on kysymys. Tähän käytin paljon poliisin, Europolin ja kyberturvallisuuskeskuksen materiaaleja, joissa asiaa on avattu selkokielisesti. Työssä listataan tunnusmerkkejä mitä huijaus yleisesti ottaen pitää sisällään.

Teon tekninen toteuttaminen avautui materiaalin myötä siten, että siinä yhdisteltiin erilaisia teknisiä keinoja murtaa tietojärjestelmiä. Voisikin sanoa, että toimitusjohtajahuijaukseen on selvästi tietty työkalupaketti, mistä voidaan poimia tilanteeseen sopivat hyökkäyskeinot, kuten esimerkiksi tietojen kalastelu. Nämä samat keinot toistuivat poikkeuksetta kaikissa lähdemateriaaleissa. Tästä voi vetää yhteen sen johtopäätöksen, että teko itsessään on teknisen toteutuksen puolelta lähes aina samoja tekniikoita hyödyntävä. Tätä päätelmää tukee myös se, että niin suomen poliisin, Kyberturvallisuuskeskuksen kuin Europolin tunnusmerkit ja suojautumiskeinot pohjautuivat samanlaisiin päätelmiin ja ohjeistukset asian suhteen kulkivat käsi kädessä. Tämä antaa varmuutta siihen, että kirjallisuuskatsaus on reliaabeli ainakin näiltä osin.

Käyttäjän manipulointi osoittautui työn edetessä hyvin laajaksi kokonaisuudeksi. Asiassa pääsi pureutumaan psykologisiin seikkoihin ja keinoihin mitä toimitusjohtajahuijauksissa hyödynnetään. Kirjallinen materiaali aiheesta oli laajaa ja asiaa on tutkittu moneltakin eri kantilta. Huomiolle pantavaa oli se, että vaikka käyttäjän manipulointi on niin sanotusti vanha keksintö, jota Kevin Mitnick on hyödyntänyt jo silloin, kun käytössä ovat olleet vain puhelimien lankalinjat, ei se kuitenkaan ole perusperiaatteeltaan vanhentunut. Nykypäivänä

tämä keino on osoittautunut varsin hyvin toimivaksi. Tästä osoituksena ovat toimitusjohtajahuijauksetkin, joissa käyttäjän manipulointi on varsin suuressa roolissa.

Ohjeistus hyökkäykseltä suojautumiseen ja sen ennaltaehkäisemiseksi syntyi osin opinnäytetyöni sivutuotteena, vaikka olin sen alun perin suunnitellutkin mukaan työhön. Kun tutkin asiaa ja ilmiöitä, niin havaitsin sen, että hyökkäyksissä käytettiin hyvin samankaltaisia toimintatapoja. Tunnusmerkkien ja tekotapojen listaaminen ja niiden avaaminen tuntuivat luonnollisesta ratkaisulta tässä vaiheessa. Pyrin tähän kokonaisuuteen keräämään eri lähteistä saatuja huomioita asian tiimoilta ja koostamaan niistä tiiviin paketin. Täysin mahdollista on, että tämä paketti jäi opinnäytetyössä melko suppeaksi kokonaisuudeksi, mikä puolestaan tarkoittaisi sitä, että osio ei palvele sitä tarkoitusta, mitä varten se on luotu. Osion pitäisi avata silmiä siitä, kuinka yksinkertaisilla toimilla huijausta voidaan välttää yrityksissä yksittäisen työntekijän toimesta.

Koska kyseessä ei kuitenkaan ollut toiminnallinen opinnäytetyö, en pureutunut asiaan niin syvällisesti, että olisin lähtenyt koostamaan yleispätevää ohjetta asiasta. Tästä syystä en myöskään lähtenyt keksimään pyörää uusiksi. Esimerkiksi Microsoft Office 365-huijauksen osalta on olemassa erinomainen Kyberturvallisuuskeskuksen opas aiheesta (Kyberturvallisuuskeskus 2019b). Ohje toimii hyvin ihmisille, jotka vastaavat yrityksen tietoliikenteen valvonnasta, tietoturvasta ja infrastruktuurista.

Tieto mitä aiheesta löytyi, oli pääasiallisesti hyvin ajan tasalla ja sitä oli kiitettävästi tarjolla. Haasteeksi muodostui se, että tieto oli hyvin pitkälti ripoteltu sinne tänne johtuen siitä, että varsinaisia pääteoksia kyseisestä huijausmallista ei ollut tarjolla. Palapeli kuitenkin alkoi pikkuhiljaa koostua kasaan. Työssä piti ymmärtää yhdistellä eri tieteenaloja, kuten esimerkiksi käyttäjän manipulointia, joka istuu psykologian alle, kun taas vastaavasti tietojen kalastelu on tietotekniikan alaisuudessa.

Tieto mitä alan artikkeleista, lehdistä ja tiedejulkaisuista oli saatavilla, oli lähtökohtaisesti sellaista tietoa, mihin pystyi luottamaan, koska kyseessä oli esimerkiksi yliopistojen yleisesti hyväksyttyjä ja käyttämiä tietokantapalveluja. Tämä lisää suurelta osin kirjallisuuskatsauksen validiutta. Kuitenkin osa tiedosta mitä kaupalliset toimijat, esimerkiksi tietoturvayhtiöt olivat asiasta kirjoittaneet, osoittautuivat käyttökelpoisiksi. Lähtökohtaisesti, kun yritys markkinoi palvelujaan blogi- tai asiantuntijan, kirjoituksina ei se välttämättä ole kovin ob-

jektiivista. Pystyin kuitenkin tarkistamaan näiden tietojen oikeellisuuden ja samalla huomasin, että tietoturvayhtiöiden kirjoituksissa oli paljon faktatietoa tarjolla, vaikka sitä ei tietenkään ole vertaisarvioitu.

Haaste työssä oli pyrkiä kääntämään alalla vallitsevia termejä suomeksi, kun moni termeistä on iskostettu suuhun englanninkielisenä. Tässä suurena apuna toimi TEPA-termipankki, joka kattaa hyvin tietoteknisen alan sanastoa. Ihan kaikkeen sekään ei taipunut, mutta suurimpaan osaan käännöksiä se kyllä vastasi oikeellisuudellaan. Suunnitteluvaiheessa olin luomassa alkuun sanastoa, joka avaisi terminologiaa erikseen, mutta luovuin kuitenkin tästä ajatuksesta. Tämän tein siksi, että pyrin tietoisesti siihen, etten viljelisi alalle ominaista ammattikieltä liikaa tai ainakin avaisin sen merkityksen paremmin asian käsittelyn yhteydessä.

Alun perin opinnäytetyöhön oli suunniteltu yksi tai kaksi asiantuntijahaastattelua poliisin hallinnosta. Tein jossain vaiheessa tietoisen ratkaisun jättää haastattelut pois. Syynä tähän oli puhtaasti se, että pääsin puheyhteyksiin työharjoittelun aikana poliisin rikostutkijoiden ja ICT-tutkinnan henkilöiden kanssa tästä aiheesta, enkä nähnyt tarpeellisuutta varsinaiselle haastattelulle. Näissä keskusteluissa sain tukea kirjalliselle materiaalille mielestäni riittävästi. Nämä keskustelut täyttivät myös tiettyjä aukkoja mitä kirjallinen materiaali ei ollut täyttänyt. Jälkikäteen ajateltuna tutkimuksellisesti se, että varsinaista haastattelua ei tullut tehtyä ja litteroitua, osittain heikentää tutkimuksen tulosta. Tämä siltä osin, että kokemuspohjainen tieto ei siirry tähän työhön sellaisenaan, vaan sen alkuperäinen muoto häviää hiukan tutkijan omien sanojen ja sanamuotojen taakse. Toisin sanoen tiedon lähde katoaa joltain osin mutta toisaalta, jos kokemuspohjainen tieto voidaan vahvistaa kirjallisilla lähteillä, on lopputulos hyvin samankaltainen.

7.1 Tulosten hyödyntäminen

Kirjallisuuskatsastus ei tarjoa yhtä ainoaa ratkaisua tai tulosta toimitusjohtajahuijauksien suhteen. Kuitenkin se mielestäni osoittaa vahvasti sen seikan, että yritysten ja yhteisöjen tietoisuutta asian suhteen pitää parantaa huomattavasti. Tiedottamisella ja tietoisuuden lisäämisellä voidaan jo saavuttaa suuri parannus nykytilanteeseen, jossa huijaukset tuntuvat menevän suhteellisen helposti läpi yrityksissä. Varsinkin jos tätä tiedottamista saadaan kohdistettua pieniin yrityksiin, missä henkilömäärät ovat luokkaa 2-9 henkilöä, kuten Suomen Yrittäjien tekemässä gallupissa todetaan. Suomessa on tahoja, jotka tätä tiedottamista hoitavat,

mutta haasteena on miten se tieto tavoittaisi vielä paremmin sitä tarvitsevat organisaatiot ja muut tahot.

Tiedottamisen lisäämisen seurauksena selvä parannuskohde yrityksille on tietenkin koulutus uhkien tunnistamiseen ja suojautumiseen. Selvää on tietenkin se, että tiedottamisen kustannustehokkuus vie voiton koulutuksista. Isompien yrityksien kohdalla koulutus on paremmin jo perusteltavissa, koska ennaltaehkäisevä koulutus on aina halvempaa, kuin suuremman luokan tietomurrot ja rahan menetys rikoksen yhteydessä.

Yritysten tekemien rikosilmoitusten määrät asian suhteen olivat myös asia mihin kiinnitin huomiota. Suomen Yrittäjien gallupkysely toi ilmi sen seikan, että vain 21 % kyselyn yrityksistä ilmoitti tehdystä tai yritetystä huijauksesta poliisille. Tämä on huomattavan pieni määrä ja se kiistatta kertoo siitä kuinka paljon huijauksista jää täysin pimentoon. Se mistä tämä vähäinen rikosten ilmoittamisten määrä johtuu, vaatisi jo laajemman tutkimuksen aiheesta.

7.2 Jatkotutkimusaiheet

Opinnäytetyöni nosti esiin pari omasta mielestäni mielenkiintoista jatkotutkimusaihetta, joita voisi jalostaa jatkotutkimuksen muodossa.

Toimitusjohtajahuijauksissa isoa roolia näyttelee rahaliikenne. Tähän voisi pureutua siltä osin, että miettisi minkälaisia mahdollisuuksia niin poliisin, kuin pankkien puolelta on jäädyttää tilisiirtoja. Tässä asiassa helposti tulee vastaan toki yrityssalaisuudet ja salassapitovelvoitteet. Asiassa kuitenkin pitäisi käydä läpi viranomaisten pyyntöjä pankkien suuntaan ja samalla avata pankkien vasteaikaa jäädytysten osalta. Myös virtuaalivaluutat huijauksen rahasiirroissa ovat nykypäivää, joten tätä näkökulmaa voisi myös pohtia rahojen alkuperän häivyttämisen osalta.

Kuka ja mikä taho toimitusjohtajahuijauksia toteuttaa. Lisäksi tutkimuksessa voisi avata sitä, minkälainen on organisaatio tai järjestäytyneen rikollisjärjestön ryhmittymä mikä tekoja toteuttaa. Millaiset ovat heidän hierarkiansa, maakohtainen henkilöstö ja toimeenpaneva porras. Jo se pelkästään, miten tekoa varten valikoidaan sopivia yrityksiä, olisi hyödyllinen tieto huijauksen ennalta-ehkäisyssä.

Tietyllä tapaa melko erillään omasta opinnäytetyöstä selvisi, että yritykset raportoivat ainakin huijaustyyppisiä rikoksia huonosti poliisille. Tämän taustaa voisi myös mahdollisesti miettiä. Aiheena se on toki laaja, kun aletaan miettiä kuinka yritykset ylipäätänsä raportoivat rikoksen poliisille.

7.3 Loppusanat

Lähdin työstämään opinnäytetyötä hyvin pitkälti sen ajatuksen pohjalta, että vihamielinen hakkerointi (engl. black hat hacker), tietoturva-aukot, haittaohjelmat ja tekninen osaaminen ovat ne asiat, mihin työssäni tulen paneutumaan. Tämä siitä syystä, että kuvittelin niiden olevan avainasemassa toimitusjohtajahuijauksien toteuttamisessa.

Itsenäni yllätti eniten sen, että teko on enimmäkseen käyttäjän manipulointia ja siinä on paljon samankaltaisuuksia, kuin valepoliisi-ilmiössä, jossa auktoriteetin voimalla pyritään uskottelemaan ihmisille valheita ja huijaamaan heiltä rahaa. Tämä mielestäni myös osoittaa sen, että tietotekniikan saralla tehtävät rikokset ovat hyvin samanlaisia rikoksia, kuin ilman tietotekniikkaa toteutetut rikokset. Joissain rikoksissa tietotekniikka on avuksi teon toteuttamisessa mutta pohjimmiltaan itse rikos ei muutu mihinkään.

Oppimiskäyrä toimitusjohtajahuijauksien osaamisen suhteen on omalta osaltani ollut nousujohteinen. Uskon, että syventävä kirjallinen materiaali on avannut toimitusjohtajahuijauksista paljon erityisiä seikkoja ja yksityiskohtia. Olen päässyt hyödyntämään näitä seikkoja myös työharjoitteluni aikana käytännön rikostutkinnassa. Tältä osin opinnäytetyön teko on antanut paljon, koska olen pystynyt hyödyntämään oppimaani teoriaa käytännön tasolla

7.3.1 Koronapandemia

Pandemia on hyvin nopealla vauhdilla saanut aikaan ilmiöitä, mitkä ovat ilmenneet erilaisina huijauksina. Suomessa tämänkaltainen esimerkki on tullut ilmi, kun ihmisten asuntoihin on tultu sisään tekemään niin sanottua Korona-tarkistusta. Tätä kautta huijaamalla on anastettu omaisuutta ihmisten kodeista. Tässä hyödynnetään käyttäjän manipuloinnin keinoin auktoriteettien luomaa tilannetta, jonka takia erinäiset ”tarkastajat” ovat päässeet kynnyksen ylitse.

Tietoturvayhtiö F-Secure on myös raportoinut verkossa tapahtuvista huijauksista, jossa Koronan luomaa poikkeustilaa on käytetty hyväksi. Huijauksissa on luvattu infoa taistelussa Koronaa vastaan tai esimerkiksi myyty hengityssuojaimia. Taktiikka näissä hyökkäyksissä on hyvin samankaltainen, kuten kerroin aiemmin. Niissä ihmisten naiiviutta hyödynnetään luonnonkatastrofeissa ja poikkeavissa tilanteissa. Ihmiset on näissä huijauksissa erehdyksissään painaneet verkkolinkkejä, joita ovat saaneet sähköpostiinsa (Syrjäläinen 2020).

LÄHTEET

Anttila, Deniz 2016 kandidaatintutkielma: Käyttäjän manipulointi organisaation tietoturvauhkana. Luettavissa https://jyx.jyu.fi/handle/123456789/52459 Luettu 20.4.2020

CYBERDI 2020: Kansallista & kansainvälistä kyberosaamista kasvattamassa. Luettavissa https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/Projektiesittely/ Luettu 26.4.2020

Doliński, D. et al. 2017: Would You Deliver an Electric Shock in 2015? Obedience in the Experimental Paradigm Developed by Stanley Milgram in the 50 Years Following the Original Studies, Social Psychological and Personality Science, 8(8), pp. 927–933. doi: 10.1177/1948550617693060.

Erkkilä, Jorma 2018: Poliisi varoittaa sähköpostin välityksellä tehtävistä toimitusjohtajapetoksista. Luettavissa: https://www.salkunrakentaja.fi/2018/05/poliisi-varoittaa-sahkopostin-valityksella-tehtavista-toimitusjohtajapetoksista/ Luettu 10.12.2019

EUROPOL 2019: Internet Organized Crime Threat Assesment (IOCTA). Luettavissa: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 Luettu 20.12.2019

FraudWatch International 2019: What is vishing? Luettavissa https://fraudwatchinternational.com/vishing/what-is-vishing/ Luettu 16.1.2020

Hornetsecurity 2019: Social engineering – How hackers get at your data without programming skills: Luettavissa: https://www.hornetsecurity.com/en/security-information/social-engineering/ Luettu 18.3.2020

Infosec 2020a: Phishing Definition and History. Luettavissa: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/ Luettu 6.1.2020

Infosec 2020b: Email spoofing and Spams. Luettavissa: https://resources.infosecinstitute.com/email-spoofing-spams/ Luettu 6.1.2020

Iltasanomat 2019: Valepoliisi-ilmiö. Luettavissa: https://www.is.fi/kotimaa/art-2000006252500.html Luettu 16.1.2020

Jaf, S., Ghafir, I., Prenosil, V., Saleem, J., Hammoudeh, M., Faour, H., Baker, T. 2018: Security threats to critical infrastructure: the human factor. Journal of Supercomputing, 74(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Jukam, Kelsey 2015: World's most famous hacker. Luettavissa https://www.caymancompass.com/2015/12/31/world-s-most-famous-hacker-to-speak-in-cayman/ Luettu 7.5.2020

Kyberturvallisuuskeskus 2019a: Uusin Microsoft Office 365-huijaus ohjaa uhrin murretulle SharePoint-tilille. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusin-microsoft-office-365-huijaus-ohjaa-uhrin-murretulle-sharepoint-tilille Luettu 16.2.2020

Kyberturvallisuuskeskus 2019b: Organisaatio! Torju Office 365 -tunnusten kalastelu oppaamme avulla. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/organisaatio-torju-office-365-tunnusten-kalastelu-oppaamme-avulla Luettu 21.3.2020

Lammassaari, Jari 2019: "Uusi työntekijämme maksoi 9350 euron huijauslaskun" – Puolet yrittäjistä joutunut huijauksen kohteeksi. Luettavissa: https://www.yrittajat.fi/uutiset/612988-puolet-yrittajista-joutunut-huijauksen-kohteeksi-uusi-tyontekijamme-maksoi-9350-euron#d6982e51 Luettu 19.3.2020

Limnéll, Jarno & Majewski, Klaus & Salminen Mirva 2014: Kyberturvallisuus, Jyväskylä, Docendo Oy

Malin, Cameron H, Gudaitis, Terry; Holt, Thomas J.; Kilger, Max. 2017: Deception in the digital age: exploiting and defending human targets through computer-mediated communications, San Diego, Academic Press

Milgram, Stanley 1974: Obedience to authority: An experimental view. New York, NY: Harper and Row

Mitnick, Kevin D. & Simon William L 2002: The art of deception: Controlling the human element of security, Indianapolis, Wiley

MySafety 2019: Tutkimusraportti Indentiteettivarkauksista: Pienet ja keskisuuret yritykset. Luettavissa: https://www.mysafety.fi/sites/mysafety.fi/files/mysafety_tutkimusraportti_yritysten_identiteettivarkauksista_kesa_2019.pdf Luettu 12.12.2019

Norton 2020: What is the Difference Between Black, White and Grey Hat Hackers? Luettavissa: https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html Luettu 26.4.2020

Poliisi 2019a: Cyberscams. Luettavissa: https://www.poliisi.fi/rikokset/huijaukset/cyberscams Luettu 15.2.2020

Poliisi 2019b: Poliisin strategia 2017-2020 Luettavissa: https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/poliisiwwwstructure/57642_POL_ST_esite_suomi_210x280_LR.pdf?1ba9169f36d0d588
Luettu 18.12.2019

Poliisi 2019c: Muuli-ilmiö. Luettavissa: https://www.poliisi.fi/rikokset/rikosilmioita/muuli_ilmio Luettu 18.2.2020

Poliisi 2019d: Toimitusjohtajahuijauksia taas runsaasti liikkeellä. Luettavissa: https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/toimitusjohtajahuijauksia_taas_runsaasti_liikkeella_81785 Luettu 18.3.2020

Poliisi 2019e: Yrityksiin ja yhdistyksiin sataa valelaskuja – jopa harrastusseurat rikollisten kohteina. Luettavissa: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/yrityksiin_ja_yhdistyksiin_sataa_valelaskuja_jopa_harrastusseurat_rikollisten_kohteina_83699?language=fi Luettu 22.3.2020

Putman, Patrick Script Kiddie: Unskilled Amateur or Dangerous Hackers? Luettavissa: https://www.uscybersecurity.net/script-kiddie/ Luettu 16.2.2020

Rentola, Roosa 2019: Kielestä kiinni. Tyrvää-Vammala-Sastamala, Warelia

Salminen, Ari 2001: Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa, Vaasan yliopisto

Sisäministeriö 2019: Kyberrikollisuus. Luettavissa: https://intermin.fi/poliisiasiat/kyberrikollisuus Luettu 11.12.2019

Syrjäläinen, Sanna 2020: F-Secure - Koronavirus-aiheiset sähköpostihyökkäykset kehittyvät viruksen kanssa samaa tahtia. Luettavissa: https://blog.f-secure.com/fi/koronavirus-aiheiset-sahkopostihyokkaykset-kehittyvat-viruksen-kanssa-samaa-tahtia/ Luettu 27.4.2020

TEPA-termipankki 2019: Luettavissa: http://www.tsk.fi/tepa/fi/

Tietosuojavaltuutetun toimisto 2020: Tietojen kalasteluun perustuvat tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietojenkalastelu Luettu 16.2.2020

Tilastokeskus 2019: Suomalaisten internetin käyttö 2019. https://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_kat_001_fi.html Luettu 1.11.2019

Tuorila, Helena 2017: Pieniin ja keskisuuriin yrityksiin kohdistuvat huijaukset. Luettavissa: https://www.kkv.fi/globalassets/kkv-suomi/julkaisut/selvitykset/2017/kkv-selvityksia-2-2017-pk-yrityksiin-kohdistuvat-huijaukset.pdf Luettu 20.12.2019

Tzu, Sun 2007: Sodankäynnin Taito. Juva, Tietosanoma Oy