Tekstiviestit sähköpostiperustaisen tietojenkalastelun tehokeinona

Keski-Pukkila, Pontus

2019 Laurea

Laurea-ammattikorkeakoulu

Tekstiviestit sähköpostiperustaisen tietojenkalastelun tehokeinona

Keski-Pukkila, Pontus
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2019

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma

Keski-Pukkila, Pontus

Tekstiviestit sähköpostiperustaisen tietojenkalastelun tehokeinona

Vuosi 2019 Sivumäärä 37

Erilaiset sosiaaliseen manipulointiin perustuvat tietojenkalasteluhyökkäykset ovat yritysmaailmassa laajalle levinnyt uhka, jolle ei ole absoluuttista suojautumiskeinoa. Ihmisten kouluttaminen ja heidän valveutuneisuuden lisääminen on tällä hetkellä tehokkain suojautumiskeino tietojenkalasteluhyökkäyksiä vastaan. Jatkuvan tietoturvakoulutuksen myötä ihmisten kyky tunnistaa ja torjua perinteiset sähköpostitse saapuvat tietojenkalasteluhyökkäykset paranevat.

Kun ihmisten tietoisuus lisääntyy ja heidän kykynsä tunnistaa ja torjua perinteiset sähköpostitse saapuvat tietojenkalasteluhyökkäykset kehittyvät, on verkkorikollisten muutettava taktiikoitaan. Yksi mahdollinen kanava on matkapuhelimiin lähetettävät tekstiviestit. Tekstiviesteillä voi tukea perinteistä tietojenkalastelusähköpostia ja luoda yksinkertaiseenkin sähköpostiin uskottavuutta, jonka avulla hyökkääjä parantaa mahdollisuuksiaan hyökkäyksen onnistumisessa.

HoxHunt tarjoaa yritysasiakkailleen pelillistettyä tietojenkalastelukoulutusta, jossa asiakasyrityksen työntekijät oppivat tunnistamaan ja raportoimaan sähköpostitse tulevia tietojenkalasteluhyökkäyksiä. Toimeksiantaja haluaa kehittää palveluitaan ja laajentaa nykyisen tuotteen ominaisuuksia. Tätä varten työssä selvitettiin toimeksiantajan tarpeisiin parhaiten sopiva tekstiviestinvälityspalvelu, joka täyttäisi toimeksiantajan vaatimat ominaisuudet ja jonka toimeksiantaja voisi ottaa tulevaisuudessa osaksi tarjoamaansa palvelua. Uusilla ominaisuuksilla toimeksiantaja voi saada teknistä etumatkaa mahdollisten kilpailijoiden tuotteisiin nähden ja pysyy jatkuvasti muuttuvan tietoturvakentän relevanttina toimijana.

Opinnäytetyön ensimmäisessä vaiheessa suoritettiin simuloitu hyökkäys, jolla pyrittiin selvittämään, onko tekstiviestien käyttämisellä osana tietojenkalastelua vaikutusta tietojenkalastelun onnistumiseen? Voiko ulkopuolinen hyökkääjä parantaa onnistumismahdollisuuksiaan hyökätessään koulutettuja työntekijöitä vastaan käyttämällä tekstiviestejä osana sosiaaliseen manipulointiin perustuvaa hyökkäystään? Työn ensimmäisessä osassa valikoitui toimeksiantajan tarpeisiin sopiva palveluntarjoaja tekstiviestien lähetystä varten. Työn empiirisessä osassa toteutettiin tietojenkalasteluhyökkäys sekä haastattelu ja kyselytutkimus.

Työssä tehty testi osoitti, että tekstiviestillä voidaan luoda uskottavuutta sähköpostitse lähetettävään tietojenkalasteluviestiin ja näin parantaa tietojenkalasteluhyökkäyksen onnistumista. Testiin osallistuneista henkilöistä 47% avasi sähköpostin liitteenä olleen potentiaalisesti haitallisen tiedoston.

Asiasanat: Kyberturvallisuus, tietoturva, tietojenkalastelu, sosiaalinen manipulointi

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's degree

Keski-Pukkila, Pontus

Using Text Messages to Increase the Success of Email Phishing Attacks

Year 2019 Pages 37

Attacks utilising malicious social engineering tactics are a widespread threat against businesses. Currently there are no bulletproof solutions against these threats and the most effective solution is continuous security awareness training. People learn to spot and report malicious phishing attacks when they are engaged in a continuous security awareness training.

When the effectiveness of basic phishing attacks deteriorates, the malicious social engineers need to adapt and improve their tactics. One possible attack vector could be text messages. Text messages could be used to create a highly believable pretext that raises the possibility of a successful phishing attack. When an employee is trained against phishing attacks, a phish that has been validated via SMS will most likely result in a business email compromise.

HoxHunt offers gamified phishing awareness training to corporate customers. HoxHunt's awareness training is currently only focusing on social engineering attacks utilising email based phishing attacks. Therefore, the commissioner of this thesis wanted to research if SMS pretexting constitutes a real threat and if there is a need to train employees to recognize SMS based social engineering attacks. The second purpose of this thesis was to find the best 3rd party service provider for sending SMS messages where the sender address could be spoofed.

HoxHunt wants to create a competitive advantage over its rivals and stay on the leading edge of cyber security awareness training. In this thesis a simulated social engineering attack was conducted using SMS pretexting and phishing email against a small group of employees working in a cyber security company. All subject employees are enrolled in a continuous security awareness training that focuses on email phishing and social engineering. It is safe to assume that the subject employees participating in this simulated attack are more resilient than employees not working in the field of cyber security or whom are not enrolled in a security awareness training. The results of the study indicate that the use of SMS pretexting in conjunction with email-based phishing creates a more believable social engineering attack that results in 47% of the study participants opening a potentially malicious email attachment.

Keywords: cybersecurity, information security, phishing, social engineering

Sisällys

Lyhenteet ja termit

API	Application programming interface. Rajapinta, jonka avulla eri palvelut voivat vaihtaa tietoja ja keskustella keskenään.
APT	Advanced Persistent Threat. Yleisnimitys verkkorikollisryhmille, jotka käyttävät hienostuneempia menetelmiä, joilla voidaan olettaa olevan ulkopuolinen rahoitus, jotka ovat valtion tukemia tai jotka kohdistavat hyökkäyksensä yhtämittaisesti tiettyyn organisaatioon.
HTTP	Hypertext Transfer Protocol. WWW-palvelinten käyttämä tiedonsiirtoprotokolla.
Hyökkäysvektori	Menetelmä tai polku, mitä kautta hyökkääjä lähestyy kohdettaan. Voi olla esimerkiksi sähköpostitse tai tekstiviestitse.
PDF	Portable Document Format. Adoben kehittämä dokumenttiformaatti, joka on suunniteltu ohjelmistoriippumattomaksi siirrettäväksi tiedostomuodoksi ja on laajasti käytössä.
Phishing	Nimitys sosiaaliseen manipulointiin perustuville hyökkäyksille, jossa kohdetta huijataan luovuttamaan arkaluontoista tietoa kuten, salasanoja, käyttäjätunnuksia, henkilötietoja tai muuta arkaluontoista materiaalia.
Pretexting	Valheellisen pohjan tai taustan luominen tietojenkalasteluhyökkäykselle.
RCS	Rich Communications Services. Matkapuhelinverkon kautta lähetettävä multimediasisältöä tukeva protokolla. Uudempi versio perinteisestä SMS protokollasta.
REST	Representational State Transfer. HTTP-protokollan päälle rakennettu hajautettujen sovellusten väliseen kommunikointiin tarkoitettu arkkitehtuurinen tyyli.
Smishing	SMS phishing. Tekstiviestitse tapahtuva tietojenkalastelu.
SMS	Short Messaging Service. Matkapuhelinverkon kautta lähetettävä lyhyt tekstiä sisältävä viesti.
SMSC	Short Messaging Service Center. Teleoperaattorin verkossa oleva palvelin, jonka tarkoitus on välittää matkapuhelinverkossa liikkuvaa dataa.
Sosiaalinen manipulointi	Manipuloidaan kohdetta tekemään toimenpide, jota kohde ei normaalisti tekisi. Sosiaalisen manipuloinnin tarkoituksena on saada uhri paljastamaan arkaluontoista materiaalia tai antaa hyökkääjälle pääsy salattuihin tietoihin.

1 Johdanto

Elämme aikaa, jolloin kaikki tieto on tallennettuna digitaalisessa muodossa elektronisissa laitteissa. Tietojen varastaminen ei vaadi enää fyysistä ryöstöä vaan rikolliset voivat etänä murtautua ja varastaa tietoa lähes mistä vain internettiin kytketystä laitteesta. Tietomurtojen estämiseksi kehitetään jatkuvasti tehokkaita teknisiä tietoturvaratkaisuja. Silti tietomurtoja tapahtuu lähes päivittäin. Ongelmana ei ole tietoturvaratkaisut vaan tietoturvan heikoin lenkki on ihminen. Yrityksen työntekijöihin kohdistuvat sosiaaliseen manipulointiin perustuvat hyökkäykset eivät ole uusi ilmiö, mutta niiden jatkuva kasvu voidaan selittää ihmisen laiskuudella. Sosiaalista manipulointia hyödyntävät hyökkäykset ovat usein teknisesti yksinkertaisempia kuin muut hyökkäysmetodit. Silti jopa valtion rahoittamat edistyneet rikollisryhmät, kuten esimerkiksi Advanced Persistent Threat (APT) käyttävät kohdennettuja tietojenkalasteluhyökkäyksiä apunaan teollisuuden valvontajärjestelmiin murtautumisessa. (Bere, M. Bhunu-Shava, F. Gamundani, A. Nhamu, I. 2015.) Miksi rikollinen käyttäisi valtavasti vaivaa ja aikaa kohteen monimutkaisten teknisten ratkaisujen murtamiseksi, kun kohteen työntekijä antaa hänen omat tunnuksensa rikolliselle niitä pyydettäessä tai ajaa haitallista koodia yrityksen verkossa sitä käsiin saatuaan?

Sähköposti on tärkeä osa päivittäistä kommunikointia yritysmaailmassa ja sen ulkopuolella. (Radicati Group 2017.) Lähes kaikki yritysten sisäinen sekä ulkoinen kommunikointi tapahtuu sähköpostin välityksellä. Yli 205 miljardia sähköpostiviestiä lähetettiin ja vastaanotettiin vuonna 2015. (Radicati Group 2017.) Henkilökohtainen työsähköposti on yleensä yksi ensimmäisistä asioista mitä uusi työntekijä saa työnantajaltaan sillä monet palvelut vaativat sähköpostiosoitteen palveluun kirjautumista varten. (Radicati Group 2017). Näistä syistä sähköposti on edelleen suosituin sosiaalista manipulointia hyödyntävä hyökkäyskanava. Vaikka hyökkäykset sähköpostin kautta toimivat edelleen, on ihmisten varovaisuus ja kyky tunnistaa ja torjua tietojenkalasteluhyökkäyksiä parantunut tietoturvakoulutusten ansiosta. Tämä pakottaa verkkorikolliset kehittämään hyökkäystaktiikoitaan. Yksi mahdollinen kanava voi olla tekstiviestit. On tärkeää, että puolustava osapuoli mukautuu rikollisten käyttämiin taktiikoihin.

1.1 Motivaatio ja työn tilaajan tausta

Työn toimeksiantaja HoxHunt tarjoaa asiakasyrityksilleen palvelun, jonka tarkoitus on kouluttaa yrityksen työntekijät tunnistamaan ja raportoimaan kohdistettuja tietojenkalasteluhyökkäyksiä. HoxHunt eroaa kilpailijoistaan tarjoamalla koko tuotteen palveluna, jolloin asiakas ei tuhlaa omia resurssejaan koulutusmateriaalin suunnittelemiseen, tuottamiseen ja lähettämiseen. HoxHuntin tuote tekee tietoturvasta mielenkiintoisempaa ja hauskempaa tarjoamalla pisteitä, kun työntekijä tunnistaa ja raportoi sähköpostiohjelmaan asennettavalla lisäosalla simuloidun hyökkäyksen. Yksittäiset työntekijät kilpailevat toisiaan vastaan organisaatiotasolla. Pelillistetyn taktiikan ansiosta HoxHuntin tuotetta käytetään aktiivisemmin ja jatkuva

hyökkäyssimulaatio saa käyttäjissä aikaan muutoksen heidän tietoturvatietoisuudessaan, jolloin jokaiseen saapuvaan sähköpostiviestiin suhtaudutaan mahdollisena simuloituna hyökkäyksenä.

Toimeksiantaja tutkii mahdollisuutta laajentaa nykyistä tuoteperhettään ja tarjota asiakkailleen entistäkin parempaa ja monipuolisempaa palvelua. Tällä hetkellä toimeksiantajan päätuote toimii sähköpostin välityksellä, mutta nykypäivän työntekijää uhkaavat hyökkäykset eivät rajoitu vain yhteen kommunikointikanavaan. Toimeksiantaja haluaa tarjota nykyistä vastaavaa palvelua myös tekstiviestitse.

1.2 Tutkimusongelma

Tutkimuksen kohteena on tekstiviestien vaikutus tietojenkalasteluhyökkäysten vaikuttavuuteen. Tutkimuksella pyritään selvittämään, onko tekstiviestien käyttämisellä osana tietojenkalastelua vaikutusta tietojenkalastelun onnistumiseen?

2 Tietojenkalasteluhyökkäykset

PhishMe:n vuonna 2016 tekemän tutkimuksen mukaan 91% kyberhyökkäyksistä ja niistä johtuvista tietomurroista saa alkunsa kohdennetuista tietojenkalasteluhyökkäyksistä. (PhishMe 2016.). Verizon:in mukaan vuonna 2018 sähköpostin välityksellä tehtiin 96% kaikista sosiaaliseen manipulointiin perustuvista hyökkäyksistä. (Verizon 2018). Sähköpostitse tulevalla kalasteluviestillä pyritään joko saamaan vastaanottaja luovuttamaan omat kirjautumistunnuksensa erilaisiin palveluihin, ajamaan liitetiedoston mukana tulevaa haitallista koodia tai tekemään jokin muu potentiaalisesti haitallinen toimenpide. Kalastettuja tunnuksia hyväksikäyttäen hyökkääjä voi murtautua organisaation järjestelmiin ja lähettää murretun tilin kautta lisää kalasteluviestejä organisaation muille työntekijöille tai muihin organisaatioihin. Hyökkääjä voi myös varastaa arkaluontoista materiaalia ja päästä käsiksi muihin palveluihin, joita murretun sähköpostitilin kautta on rekisteröity. Verizon:in mukaan 92.4% haittaohjelmista levitetään sähköpostin liitetiedostona, joista yli 82% oli joko kiristysohjelmia tai pankkitroijalaisia vuonna 2017. (Verizon 2018).

Hyökkääjän on helpompi ohittaa yrityksen tietoturvamekanismit sähköpostin välityksellä, sillä sähköposti on yleinen ja yleensä välttämätön kommunikointikanava yrityksessä sekä sisäisesti että ulkoisesti. Sähköpostiliikenteeseen on kehitetty lukuisia teknisiä tuotteita ja palveluita, joiden tarkoitus on ollut automaattisesti suojata työntekijöitä haitalliselta sisällöltä ja karsia roskapostia. Tietojenkalastelua ei ole kuitenkaan kokonaan saatu torjuttua erilaisilla sähköpostinsuodatusohjelmilla. Ongelmana on yleensä ollut liian tiukka tai vapaa sähköpostinsuodatus. Jos suodatin on liian tiukka, voi tärkeä ja turvallinen viesti jäädä suodattimeen, eikä saavu vastaanottajalle. Jos suodatin on liian vapaa, tulee vastaanottajalle jatkuvasti roskapostia.

Regner & al. (2016) kertovat verkkorikollisilla olevan monia eri motiiveja hyökkäysten toteuttamiseksi. He luettelevat esimerkkejä kuten uteliaisuus, hauskanpito, mielihyvä, julkisuus, manipulointi, tuhoaminen, kosto, egon kohottaminen, haktivismi, nationalismi, radikalismi, uskonto, politiikka sekä taloudellinen hyöty.

2.1 Tietojenkalastelu sosiaalisessa mediassa sekä tekstiviestitse

Tulevaisuudessa voidaan olettaa hyökkääjien siirtyvän sähköpostin rinnalla enemmän myös muihin kanaviin, koska lisääntyvän koulutuksen myötä sähköpostitse tuleviin viesteihin suhtaudutaan varauksella. Näitä voi olla erilaiset sosiaalisen median kanavat (Facebook, Twitter, Instagram), pikaviestipalvelut (Whatsapp, Facebook Messenger, WeChat ja Telegram) ja tekstiviestit. Proofpointin mukaan sosiaaliseen mediaan perustuvat hyökkäykset kasvoivat 500% vuoden 2016 aikana. (Proofpoint 2016).

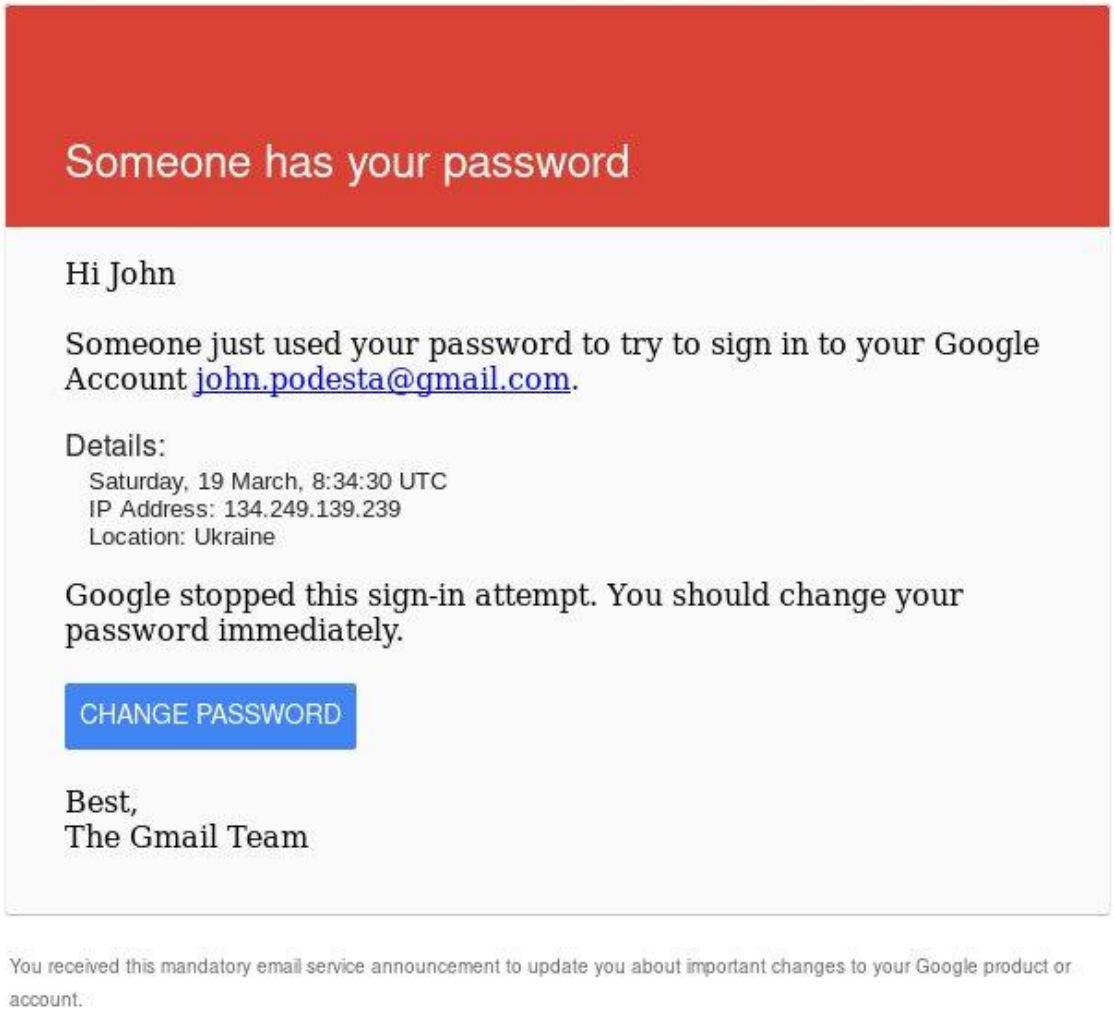
Osaa yllämainituista sosiaalisesta mediasta ja pikaviestipalveluista käytetään pääosin tai pelkästään älypuhelimella. Usein älypuhelimeen ei ole asennettu tai älypuhelimiin ei ole saatavilla samanlaisia tietoturvaominaisuuksia ja palveluita, mitä yrityksen tietokoneilla on. Älypuhelinten pienen näyttöpinta-alansa takia ohjelmistojen kehittäjien täytyy tehdä kompromisseja ja jättää mahdollisesti tärkeää tietoa pois, kuten oikea lähettäjän osoite, oletusnäkymästä. Kaikkea tietoa ei saa näkymään älypuhelimen ruudulla tai informaation löytäminen on vaikeaa. Kolmas syy hyökkääjien siirtyminen sosiaaliseen mediaan tai tekstiviesteihin on matkapuhelimien laaja käyttö. Deloitten vuonna 2017 julkaistun raportin mukaan 80% kehittyneiden maiden kansalaisista omisti älypuhelimen ja yli 90% omisti matkapuhelimen. (Deloitte 2017).

2.2 Tietojenkalasteluhyökkäysten vaikutus yrityksille

Tietomurtojen yleisin syy on ihmisluonteen heikkous. Ihmistä on helppo huijata. Verizonin vuonna 2018 julkaistun raportin mukaan kaikista tietomurroista 93% saa alkunsa tietojenkalasteluhyökkäyksistä ja erilaisia verukkeita (pretexting) hyödyntämällä. (Verizon 2018). Sähköpostitse tapahtuu edelleen 96% kaikista sosiaaliseen manipulointiin perustuvista hyökkäyksistä. (Verizon 2018). Ihmisiä ei voi kuitenkaan pelkästään syyttää sillä ihmiset on vuosien saatossa opetettu klikkaamaan linkkejä ja avaamaan liitetiedostoja. Verkkorikolliset käyttävät ihmisille opetettuja normeja ja ihmisluonnetta hyväkseen sosiaaliseen manipulointiin perustuvien hyökkäyksien tukena.

Tietomurto on aina erittäin haitallinen yrityksen liiketoiminnalle. Tietomurron yhteydessä mahdollisesti menetetty maine ja taloudelliset kulut voivat koitua jopa koko yrityksen liiketoiminnan päättymiseen. Ponemon Instituten tekemän raportin mukaan tietomurtojen jälkeisten toimenpiteiden kulut nousevat vuosittain 6.4%. Vuonna 2018 keskivertohinta tietomurrolle oli 3.86 miljoonaa dollaria ja tietomurron kärsineen yrityksen todennäköisyys joutua uuden tietomurron uhriksi seuraavan kahden vuoden aikana oli 27.9%. Yritysten kyky todeta ja eristää hyökkäys on keskimääräisesti 266 päivää. Yritykset, jotka onnistuivat eristämään hyökkäyksen alle 30 päivässä, säästivät yli 1 miljoonaa dollaria verrattuna yrityksiin, joilla kesti yli 30 päivää hyökkäyksen eristämisessä. (Ponemon Institute LLC 2018).

Onnistuneella tietojenkalasteluviestillä voi olla suuri vaikutus myös maailmanpoliittisesti. Kuviossa 1 on esimerkiksi maaliskuussa vuonna 2016 tapahtuneesta kohdistetusta tietojenkalasteluhyökkäyksestä, jonka johdosta Yhdysvaltain presidenttiehdokkaan Hillary Clintonin presidenttikampanjan puheenjohtajan John Podestan sähköpostiviestit vuotivat julkisuuteen. Hyökkäyksellä saattoi olla vaikutus presidenttikampanjan lopputulokseen.



Kuvio 1: Tietojenkalasteluviesti Hillary Clintonin presidenttikampanjan puheenjohtajalle. (Wikileaks 2016).

2.3 Tekstiviestin luotettavuus mediana

Shift Communicationsin tekemän tutkimuksen mukaan 82% tutkimukseen vastanneista sanoo avaavansa jokaisen heille saapuneen tekstiviestin. 17% sanoo avaavansa tekstiviestin vain, jos viesti on tullut henkilöltä, jonka he tietävät. (Shift Communications 2015). Tämä tarkoittaa 99% saavutettavuutta, jos tekstiviesti lähetetään vastaanottajan tuntemasta numerosta. Lisäksi 90% tekstiviesteistä luetaan 3 minuutin sisällä viestin vastaanottamisesta. (Sendmode 2017).

Pew Research Centerin tekemän tutkimuksen mukaan sähköpostilla lähetettyyn kyselyyn vastanneita henkilöitä oli 13 prosenttia enemmän ensimmäisen päivän aikana, kun sähköpostin lisäksi tutkimukseen osallistuneille henkilöille lähetettiin myös tekstiviesti. (Pew Research Center 2016). TextMagicin mukaan kuluttajat suosivat tekstiviestejä sähköpostin tai äänipuheluiden sijasta. Kuluttajat haluavat myös kiireelliset ilmoitukset mieluummin tekstiviesteinä

kuin sähköpostilla tai äänipuheluilla. Voidaan olettaa, että ihmiset luottavat enemmän tekstiviesteihin suuren sähköpostiin saapuvan roskapostimäärän takia ja äänipuheluina tulevien robottipuheluiden takia. (TextMagic 2018.). Flowrouten tekemän tutkimuksen mukaan 82% tutkimukseen osallistuneista luki heille lähetetyn tekstiviestin 5 minuutin sisällä sen vastaanottamisesta. (Flowroute, Inc 2016).

2.4 Kirjallisuutta tietojenkalastelun alalta

Kirjallisuudesta on jossain määrin löydettävissä esimerkkejä, joissa tekstiviesti on pääasiallinen tietojenkalastelun kanava ilman erillistä sähköpostia. (Goel D, Jain A. K. 2017). Kirjallisuudesta ei ole löydettävissä esimerkkejä, jossa tekstiviestejä olisi käytetty osana sähköpostiviestin uskottavuuden lisäämistä ja jossa olisi käytetty tekstiviestin ja sähköpostin yhdistelmää.

Aiheesta löytyy tieteellistä kirjallisuutta niukasti. Ensimmäinen artikkeli liittyen tietojenkalasteluun tekstiviestitse löytyy vuodelta 2005. William Enck, Patrick Traynor, Patrick McDaniel, Thomas La Porta mainitsi asian artikkelissa. Artikkeli löytyi Google Scholarin tietokannasta hakusanalla ”sms phishing”. Artikkelien määrä kasvaa vuoteen 2018 asti. ProQuestin tietokannasta löytyy selvästi eniten artikkeleita vuodelta 2017 ja 2018. Suurin osa internetissä olevasta materiaalista on uutisia ja tieteellistä tutkimusta on selvästi vähemmän. Yleisimmin lähteissä kerrotaan tietojenkalastelusta yleisesti ja tietojenkalastelu tekstiviestitse on vain pieni osa kokonaisuutta, jolloin aihe käydään läpi lyhyesti. Kirjallisuuden osalta on mainittava, että phishingistä on huomattavasti enemmän kirjallisuutta englanniksi kuin smishingistä. Phishingillä tarkoitetaan sähköpostitse tapahtuvaa tietojenkalatelua. Smishing on lyhenne sanoista SMS phishing joka puolestaan tarkoittaa tekstiviestitse tapahtuvaa tietojenkalastelua.

3 Tutkimusmenetelmät

Tutkimustrategiana käytettiin tapaustutkimusta. Tapaustutkimus eli case-tutkimus on yksi tutkimusstrategia kokeellisen tutkimuksen ja survey-tutkimuksen ohella. Se on laadullista tutkimusta, jolla kuvataan olemassa olevia ilmiöitä syvällisesti ja kattavasti. Tapaustutkimuksella vastataan seuraaviin kysymyksiin: miten ja miksi? (Kananen 2013, 54; Yin 2009, 10-11).

Keskeistä tapaustutkimuksessa on määriteltävä tutkimuskysymys, tutkimusasetelma ja aineistojen analyysit. Tutkimuskysymykseen liittyy sen ratkaiseminen, mistä tapaus kertoo ja mitä tapauksen avulla voidaan oppia. Tapaustutkimusta suositellaan käytettäväksi siinä vaiheessa, kun tapauksesta tai ilmiöstä on tehty vain vähän empiiristä tutkimusta. Tämän työn aiheesta ei empiiristä tutkimusta löydy ja siksi se on erityisen sopiva tämän työn tapaukseen. Tapaustutkimus soveltuu hyvin ilmiöiden arviointiin.

Tapaustutkimusprosessi sisältää seuraavat vaiheet: Tutkimuskysymysten muotoileminen, tutkimusasetelman suunnittelu, tapausten määrittely ja valinta sekä tietojen keruu, saatujen tietojen analysointi ja raportointi.

Tapaustutkimuksen tekijän on syytä perehtyä seuraaviin asioihin: haastattelu ja kuuntelutaito, tilanteisiin mukautuminen, joustavuus ja puolueettomuus. (Yin 2009, 69-72).

3.1.1 Tiedonkeruumenetelmät

Osana hyökkäyssimulaatiota pyrittiin selvittämään työntekijöiden suhtautuminen tekstiviestitse tapahtuviin hyökkäyksiin. Työssä käytettiin kahta eri menetelmää tiedon keräämiseen simulaatioon osallistuneilta henkilöiltä. Ensimmäisenä menetelmänä käytettiin haastattelua, joka tehtiin jokaiselle simulaatioon osallistuneelle henkilölle erikseen hyökkäyksen toteutuspäivänä. Toisena menetelmänä käytettiin kyselytutkimusta, jonka linkki lähetettiin henkilöiden sähköpostiosoitteeseen noin 2 viikkoa simulaation jälkeen.

Haastattelussa osallistujilta pyrittiin saamaan mahdollisimman nopeasti tietoa heidän mietteistään ja tunteistaan simulaation toteutuksesta. Haastattelu oli vapaamuotoinen, missä henkilöiltä kysyttiin tiettyjä kysymyksiä, joihin toivottiin vastausta. Haastattelun aikana haastateltavat saivat myös vapaasti kertoa mietteitään ja kokemuksiaan hyökkäyksen kulusta.

Kyselytutkimuksella haluttiin saada tarkempaa ja henkilökohtaisempaa tietoa simulaatioon osallistuneilta henkilöiltä. Kyselytutkimuksessa käytettiin apuna Google Forms-työkalua. Kyselyssä käytettiin Likert-asteikkoa työntekijöiden asenteiden tutkimiseen sekä binäärisiä kyllä ei vastauksia. Asteikossa on väittämiä, jotka ilmaisevat sekä kielteistä, että myönteistä suhtautumista kysymykseen. Vastaajat arvioivat kysymyksiä 5-portaisella asteikolla ääripäiden ollessa esimerkiksi: en luottanut ollenkaan ja luotin täysin.

3.1.2 Tiedon analysointimenetelmät

Tutkimus toteutettiin kolmivaiheisena: 1. Simuloidun tietojenkalasteluhyökkäyksen valmistelu ja lähettäminen käyttäen CLX Communicationin ja HoxHuntin alustaa. 2. Simuloidun hyökkäyksen ensimmäisten tulosten tarkastelu hyödyntäen haastattelua ja taulukkolaskelmaohjelmistoa. 3. Simuloidun hyökkäyksen tarkempien tulosten kerääminen ja tarkastelu kyselytutkimuksella.

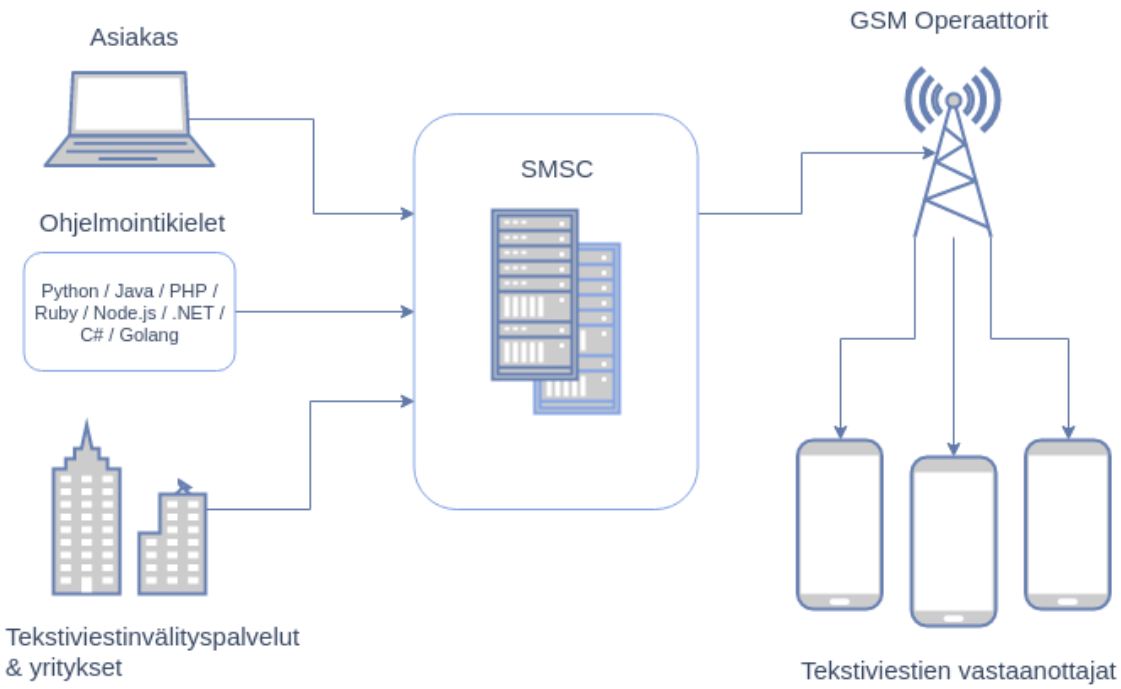
Yleisesti tuloksia analysoitiin yksinkertaisin menetelmin taulukkolaskentaohjelmistoa käyttäen. Simulaatiodatasta laskettiin suhdeluku niistä käyttäjistä, jotka avasivat sähköpostissa olleen liitetiedoston.

Simuloidusta hyökkäyksestä kyselytutkimuksella kerätyn tiedon analysointi tapahtui Google Forms-työkalun käyttöliittymässä. Tulosten tulkinnassa hyödynnettiin Google Forms alustan valmiita visualisointi ja analysointityökaluja. Haastattelututkimuksessa käytettiin laadullista analyysiä ja kyselytutkimuksessa käytettiin tilastollista analyysiä.

4 Tutkimusympäristön kuvaus

Tekstiviestin välityspalveluilla välitetään tekstiviestejä yritysten palveluiden ja loppukäyttäjien välillä. Tekstiviestejä välittävillä yrityksillä on joko pääsy teleoperaattorien verkkoon SMPP-protokollan välityksellä tai teleoperaattorin ja välityspalvelun välillä on kolmas taho, joka tarjoaa palveluitaan molemmille osapuolille. Useimmat välityspalvelut tarjoavat sovellusohjelmointirajapinnan, joka integroidaan asiakkaan omaan järjestelmään ja jonka kautta asiakasyritykset lähettävät viestejä ohjelmallisesti.

Alla olevassa kuvassa (kuvio 2) yksinkertaistettu polku, jossa asiakas käyttää tekstiviestinvälityspalveluntarjoajan tuotetta tekstiviestin lähettämiseen. Tekstiviestinvälityspalvelut tarjoavat asiakkailleen epäsuoran pääsyn Short Messaging Service Centerin (SMSC) kautta lähetettäviin tekstiviesteihin. SMSCt ovat teleoperaattoreiden verkossa. Asiakkaat käyttävät palveluntarjoajan tuotetta selaimen tai ohjelmistorajapinnan kautta. Yleensä palveluntarjoajilla on ohjeet palvelun integroimisen eri ohjelmointikielien avulla. SMSCn kautta asiakkaiden määrittelemät viestit kulkeutuvat teleoperaattoreiden ja heidän telemastojen kautta vastaanottajien matkapuhelimiin.



Kuvio 2: SMS API palvelun infrastruktuuri yksinkertaistettuna

Tekstiviestinvälityspalveluita käytetään useisiin eri tarkoituksiin. Esimerkiksi markkinointiin lähettämällä palveluiden asiakkaille mainoksia alennuksista ja uusista tuotteista, suojaamaan

tilejä varmistamalla kirjautuminen tekstiviestitse saapuvalla koodilla, ilmoittamaan teknikoille kiireellisistä vikailmoituksista, keräämään asiakaspalautetta ja ilmoittamaan asiakkaita erääntyvistä parkkimaksuista.

4.1 Vaatimusmäärittely

Osana työn tarkoitusta oli löytää toimeksiantajalleni paras mahdollinen kolmannen osapuolen palvelu, jonka kautta toimeksiantajani voisi lähettää tietojenkalastelutekstiviestejä asiakasyrityksiin osana toimeksiantajani tarjoamaa tietoturvakoulutusta. Toimeksiantajani haluaa laajentaa palveluaan mukautumaan mahdollisiin tulevaisuudessa yleistyviin uhkiin ja tarjota asiakkailleen parempaa palvelua. Tekstiviestinvälityspalvelu on tulevaisuudessa tarkoitus integroida toimeksiantajan nykyiseen järjestelmään, jota tällä hetkellä käytetään sähköpostiviestien lähettämiseen.

Application Programming Interface (API) on erilaisissa palveluissa käytettävä rajapinta, jolla sovellukset voivat kommunikoida keskenään. API voi antaa ulkoiselle sovellukselle tai henkilölle mahdollisuuden käyttää taustalla olevaa palvelua ilman, että APIa käyttävä tietää miten taustalla oleva sovellus on tehty. API yksinkertaistaa palveluiden integroinnin ja tiedonvälityksen sekä mahdollistaa kolmannen osapuolen sovelluskehityksen. Rajapinnan avulla palvelun käyttäjille ei tarvitse antaa suoraa pääsyä taustalla oleviin palveluihin. Tämä parantaa palvelun tietoturvaa. APIn luomiseen ja käyttöön sisältyy vahvasti rajapinnan dokumentointi. Ilman kunnollista dokumentaatiota rajapinnan hyödyntäminen on huomattavasti työläämpää.

Vertailussa mukana olevista palveluista kaikissa on avoin API, joka mahdollistaa palvelun integroimisen HoxHuntin järjestelmiin. Ilman avointa rajapintaa, tekstiviestien lähettäminen ja hallinnointi olisi pakko tehdä käyttäen palveluntarjoajan omaa käyttöliittymää.

Tekstiviestinvälityspalvelun tulisi täyttää vähintään seuraavat kriteerit: helppo integroitavuus, tekstiviestin lähettäjäkentän muokkaaminen ilman rajoitteita, edullinen hinta, toiminnallisuus Euroopassa, palvelun laadukas ja kattava dokumentointi, helppokäyttöisyys, lisäominaisuudet

4.2 Tekstiviestinvälityspalveluiden vertailu

Ennen varsinaisen tutkimuksen aloittamista ja palveluiden vertailua kartoitettiin palvelulta vaadittavat pakolliset ominaisuudet. Ensimmäinen pakollinen ominaisuus oli lähettäjäkentän muokkaaminen ilman rajoituksia ja toinen pakollinen ominaisuus oli palvelun tarjoama REST API. Muut vertailussa olevat ominaisuudet eivät olleet pakollisia, mutta toivat vertailuun syvyyttä ja auttoivat valitsemaan myös pitkällä tähtäimellä parhaan palvelun.

Tutkimuksen ensimmäisessä vaiheessa kartoitettiin suosituimmat SMS-yhdyskäytäviä tarjoavat palveluntarjoajat. Suosituimmat palvelut otettiin lähempään tarkasteluun, jossa arvioitiin

pintapuolisesti palvelun soveltuvuus juuri toimeksiantajan käyttötarkoitukseen. Suosituimpien vaihtoehtojen joukosta karsittiin pois palvelut, joista ei löytynyt tarpeeksi tietoa, jotka olivat saaneet huonoja arvosteluja tai jotka eivät tarjonneet työn toteutuksen mahdollistavia ominaisuuksia. Tämän lisäksi vertailussa pyrittiin suosimaan palveluntarjoajia, jotka mahdollistaisivat tekstiviestien lisäksi vielä laajempaa palvelua, kuten äänipuheluja tai SMS Associationin kehittämän perinteisen tekstiviestiprotokollan mahdollisesti korvaavan RCS protokollan hyödyntämistä osana toimeksiantajani laajempaa palvelua myös tulevaisuudessa. Tämä helpottaisi tietyn palvelun käyttöönottoa ja siihen sitoutumista, sillä uuteen palveluntarjoajaan ei välttämättä tarvitsisi perehtyä jokaisen mahdollisen uuden ominaisuuden käyttöönotossa.

4.3 Tekstiviestinvälityspalveluiden valinta

Vertailu alkoi tarjonnan kartoittamisella, joka tehtiin internetin hakukoneita hyödyntämällä. Vertailuun otettiin aluksi mukaan 6 palveluntarjoajaa, josta 2 karsittiin pois niiden tarjoamien palveluiden niukkuuden, kotisivujen laadun ja keskustelupalstoilla saadun huonon arvostelun mukaan. Lopulliseen vertailuun otettiin mukaan 4 jäljelle jäänyttä palveluntarjoajaa. Valitut palveluntarjoajat kuuluvat maailmanlaajuisesti suosituimpien palveluiden joukkoon.

Lopullisessa vertailussa jokaisen palveluntarjoajan palveluun luotiin tili. Lähes kaikissa palveluissa tekstiviestin pystyi lähettämään ilmaiseksi tiettyyn numeroon, mutta lähettäjäkentän osoitetta ei pystynyt muuttamaan. Tästä syystä kaikille tileille siirrettiin pieni määrä rahaa, jolla pystyi varaamaan oman numeron ja määrittämään lähettäjän osoitteen ja vastaanottajan numeron itse. Samalla tutustuttiin palveluntarjoajan muihin ominaisuuksiin, kuten: SMS, MMS, RCS, äänipuhelut, pikaviestit, vastaanottajan numeron validointi.

Palveluiden ominaisuuksien tarkemassa kartoituksessa CLX Communications ja Nexmo tarjosivat ominaisuuksiltaan, helppokäyttöisyyksiltään ja hinnaltaan toimeksiantajan käyttöön parhaimmat vaihtoehdot. Vertailun viimeisessä vaiheessa tuli kuitenkin ilmi, että suomalaiset operaattorit käyttäytyvät keskenään eri lailla Nexmon ja CLX Communicationsin kautta lähetettäviin tekstiviesteihin, joissa lähettäjän osoite on vapaasti määritetty. Nexmon kautta Telian liittymiin lähetetyt tekstiviestit saapuivat vastaanottajan matkapuhelimeen lähettäjän nimellä NXSMS, jos lähettäjän numero vastasi jo olemassa olevaa rekisteröityä numeroa. CLX Communications ei kärsinyt samasta ongelmasta, jolloin toimeksiantajan tarkoitukseen parhaimmaksi palveluksi valikoitui CLX Communications. Oheisessa taulukossa tarkemmin eri palveluntarjoajien ominaisuudet vaatimusmäärittelyn mukaan.

Ominaisuudet	CLX Communications	Nexmo	Twilio	Plivo
Tekstiviestit				
Hinta (SMS lähetys suomen sisällä)	0.0600€	0.0700€	0.0820€	0.0725€
Tukee lähettäjäkentän muokkaamista Numerot/Nimet	Telia: Numerot/Nimet Elisa: Numerot/Nimet DNA: Numerot/Nimet	Telia: Nimet Elisa: Numerot/Nimet DNA: Numerot/Nimet	Telia: Ei Elisa: Ei DNA: EI	Telia: N/A Elisa: N/A DNA: N/A
API				
Rest API	☑	☑	☑	☑
Ohjelmistokehityspakkaus	Python / Java / PHP	Python / Java / PHP / Ruby / Node.js / .NET	Python / Java / PHP / Ruby / Node.js / C#	Python / Java / PHP / Ruby / Node.js / .NET / Golang
Formaatti	JSON	JSON	JSON	JSON
Lisäominaisuudet				
SMS	☑	☑	☑	☑
MMS	☑	☑	☑	☐
RCS	☑	☐	☑	☐
Äänipuhelut	☑	☑	☑	☑
Pikaviestit	☐	☑	☑	☐
Numeron validointi	☑	☑	☑	☐
Skaalautuvuus				
SMS lähetys, maiden lukumäärä	N/A	224	210	Yli 200

Taulukko 1: SMS välityspalveluiden vertailutaulukko

5 Empiirinen tutkimus ja sen toteutus

Hyökkäys toteutettiin 15 tietoturva-alalla työskentelevälle henkilölle, jotka kaikki työskentelevät samassa tietoturva-alan yrityksessä. Testissä oli mukana henkilöitä, joiden pääasiallisiin työtehtäviin kuului myyntiä, rekrytointia, tuotekehitystä, graafista suunnittelua sekä asiakastyytyväisyyden hallinnointia. Kaikki testiin osallistuneet työntekijät ovat mukana tietojenkalasteluun erikoistuneessa jatkuvassa tietoturvakoulutuksessa, joten voidaan olettaa, että kohdehenkilöiden tietoturvatietoisuus on keskivertotyöntekijää parempi.

Hyökkäys pyrittiin toteuttamaan mahdollisimman aidosti ulkopuolisen hyökkääjän näkökulmasta. Hyökkääjän päämääränä oli saada mahdollisimman moni valituista työntekijöistä avaamaan sähköpostin liitteenä oleva PDF-liitetiedosto, jonka kautta hyökkääjä olisi voinut ajaa haitallista koodia vastaanottajan päätelaitteella. Hyökkäys toteutettiin seuraavassa järjestyksessä:

1. Kohteelle lähetetään tekstiviesti, jonka lähettäjä näyttää olevan yrityksen työntekijä taloushallinnosta

2. Noin minuutin päästä tekstiviestin lähetyksestä kohteelle lähetettiin sähköpostiviesti, jossa liitteenä PDF-tiedosto. PDF-liitetiedostossa oli tietoa kokeilusta ja ohjeet ottamaan yhteyttä testin tekijään

Testissä oletettiin kaikkien liitetiedoston avaavien henkilöiden ilmoittavan liitetiedoston avaamisestaan vapaaehtoisesti testin suorittajalle. Liitetiedoston ohjeissa pyydettiin testiin osallistuvia olemaan kertomatta mitään testiin liittyvää muille organisaation työntekijöille ennen kuin testi olisi suoritettu kokonaisuudessaan ja tulokset olisi julkaistu.

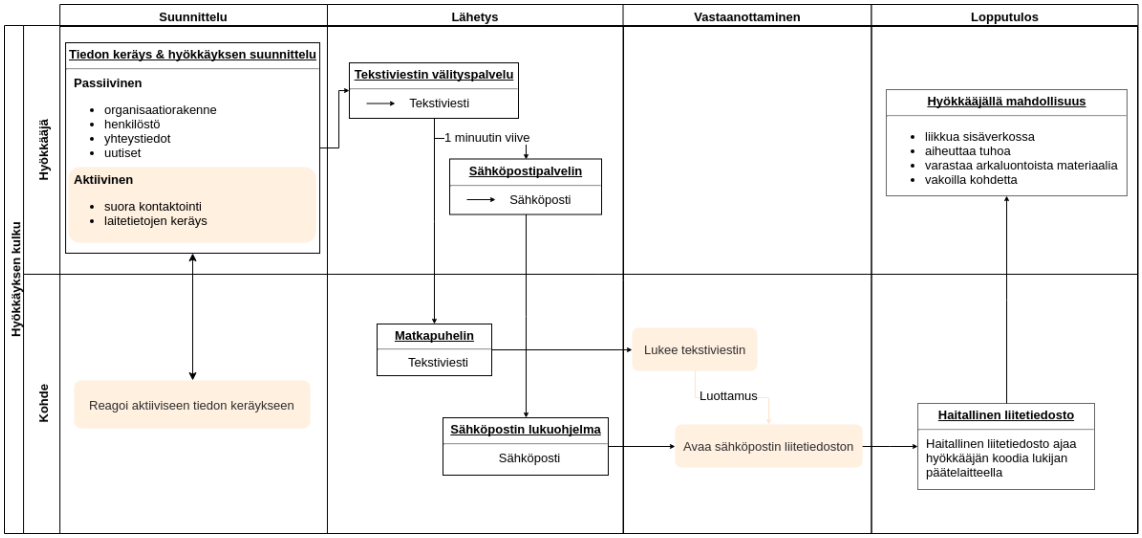
Hyökkäys lähetettiin portaittain kahden päivän aikana ja kaikille vastaanottajille erikseen. Ensimmäiset 8 hyökkäystä lähetettiin keskiviikko aamuna kello 8:30-10 välisenä aikana, seuraavat 3 hyökkäystä lähetettiin kello 14-15 välisenä aikana ja seuraavana päivänä viimeiset 4 hyökkäystä lähetettiin kello 14-15 välisenä aikana.

Viestien lähetyksen jälkeen odotettiin yhteydenottoja ohjeissa mainittuun kanavaan. Jos vastaanottaja ei ottanut yhteyttä, voitiin olettaa, että vastaanottaja oli tunnistanut hyökkäyksen, eikä ollut avannut liitetiedostoa. Näille henkilöille ilmoitettiin testistä jälkikäteen ja todettiin oletuksen paikkansapitävyys.

Suurimmalle osalle hyökkäys lähetettiin aamulla. Hyökkäyksissä käytetty sisältö oli täysin sama jokaiselle kohdehenkilölle. Hyökkäyksen tarkoituksena oli käyttää kahta eri yhteydenottokanavaa, jolla luodaan vastaanottajalle varmistus jälkimmäisen viestin aitoudesta. Tekstiviestissä pyrittiin luomaan kiireellisyyden tunne, jotta tekstiviestiin tai sähköpostiviestiin ei

kiinnitettäisi ylimääräistä huomiota. Mitä nopeammin kohdehenkilö reagoi viesteihin, sitä vähemmän hänellä on aikaa validoida viestien aitoutta. Tekstiviestillä pyrittiin saamaan vastaanottaja odottamaan sähköpostitse saapuvaa viestiä, jolloin saapuvaan sähköpostiin muodostuu vahvempi luottamus, kuin sähköpostiviestiin, jota vastaanottaja ei odota.

Kuvassa 3 on kuvattu onnistuneen hyökkäyksen kulku asteittain ja yksinkertaistettuna. Kuvat tekstiviestistä ja sähköpostiviestistä ovat suuntaa antavia esimerkkejä oikeista, simulaatiossa käytetyistä viesteistä. Hyökkääjä aloittaa hyökkäyksen suunnitteluvaiheesta, jossa kerätään tietoa kohteen järjestelmistä, työntekijöistä ja mahdollisista muista aiheista, joita hyökkääjä voisi hyödyntää uskottavan kontekstin luomisessa. Myös molemmat hyökkäysvektorit kirjoitetaan suunnitteluvaiheessa. Seuraavaksi valmiit hyökkäysvektorit lähetetään valituille kohteille tai kohteelle. Tutkimuksessa tehdyn hyökkäyksen onnistumisen kannalta on tärkeää, että kohde lukee tekstiviestin ennen sähköpostiviestiä. Sähköpostin ja tekstiviestin välillä on 1 minuutin viive. Seuraavassa vaiheessa kohde lukee vastaanotetut viestit. Jos kohde luottaa molempiin viesteihin, hän avaa sähköpostiviestissä olleen haitallisen liitetiedoston. Tutkimuksessa kävi ilmi, että sähköpostiviestin ei aina tarvitse olla täysin uskottava, sillä joissain tapauksissa kohdehenkilö luotti sähköpostiin pelkän aikaisemmin luetun tekstiviestin takia, vaikka olisi pitänyt sähköpostiviestiä hieman epäilyttävänä. Viimeisessä vaiheessa kohteen avaama haitallinen liitetiedosto on ajanut hyökkääjän määrittelemää haittakoodia kohteen päätelaitteella ja näin ollen hyökkääjän on mahdollista suorittaa vapaasti komentoja kohdehenkilön päätelaitteella. Ohessa kuvio 3, jossa hyökkäyksen kulku visualisoituna.

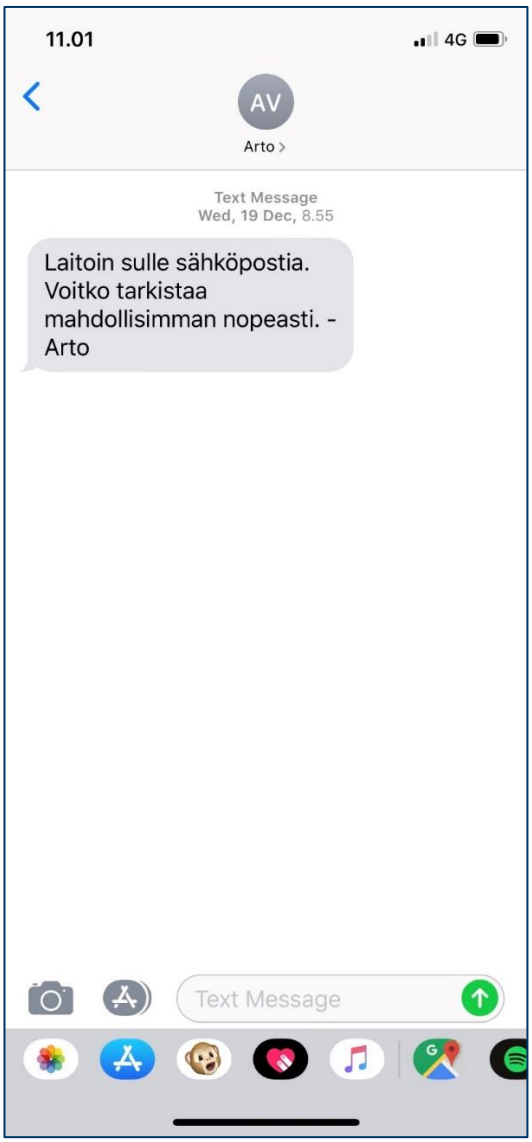


Kuvio 3: Hyökkäyksen kulku

Tekstiviestin lähettäjäkentän osoite on helposti väärennettävissä, eikä hyökkäyksessä käytetyn tekstiviestin aitoutta pystynyt pintapuolisesti varmistamaan. Hyökkäystekstiviesti ilmestyy

vastaanottajan matkapuhelimeen. Viesti näkyy vastaanottajan matkapuhelimessa samalla nimellä, jolla vastaanottaja on puhelinnumeron tallentanut. Jos vastaanottaja on lähettänyt tai vastaanottanut hyökkäyksessä käytetyn puhelinnumeron kanssa aikaisempia viestejä, saapuu hyökkäystekstiviesti samaan keskusteluhistoriaan aikaisempien aitojen viestien joukkoon. Tekstiviestin olisi voinut todeta hyökkäykseksi, jos vastaanottaja olisi erikseen varmistanut viestin aitouden sen oletetulta lähettäjältä. Kuviossa 4 on esimerkki simuloidussa hyökkäyksessä käytetystä samankaltaisesta viestistä.

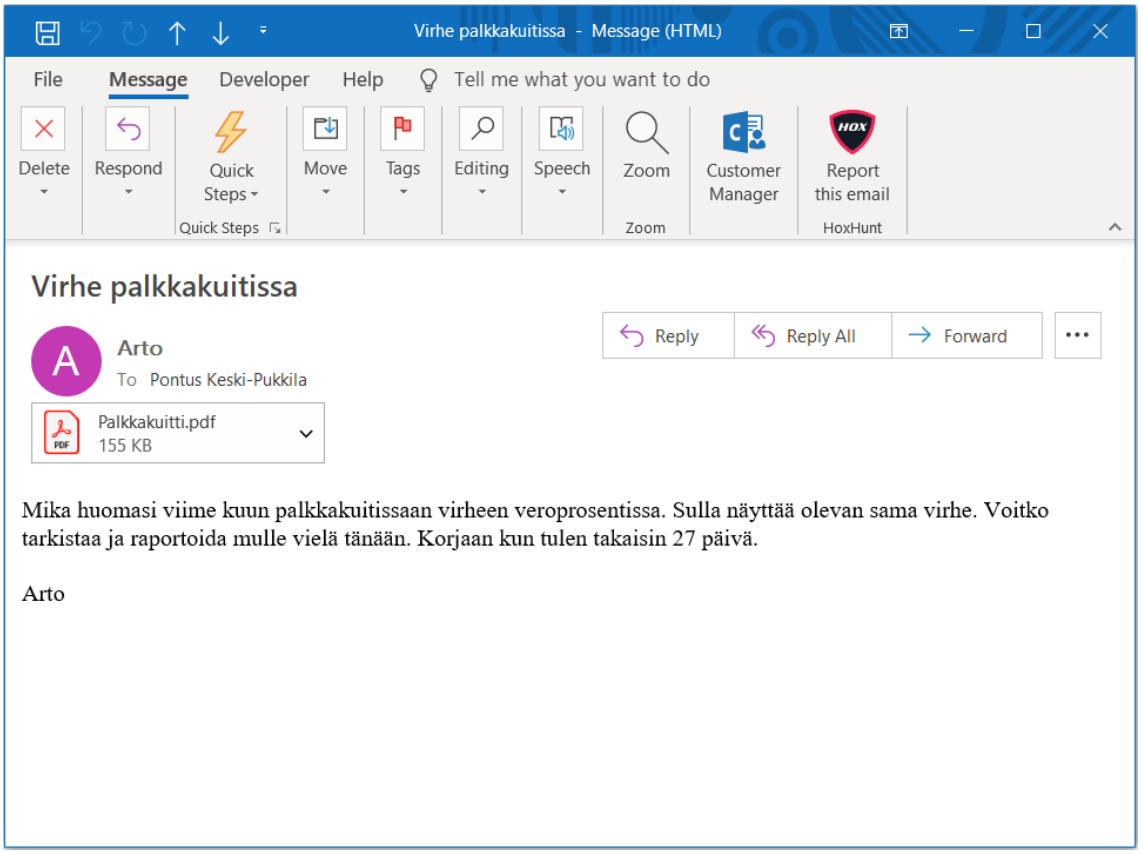
Tässä työssä esitetyt teksti- ja sähköpostiviestit ovat vain esimerkkejä eivätkä vastaa todellisessa simuloidussa hyökkäyksessä käytettyjen viestien sisältöä.



Kuvio 4: Esimerkki kohdeyrityksen työntekijän numerosta lähetetystä tekstiviestistä

Lähettäjän osoite on vastaanottajan itse määrittelemä, koska puhelin näkee vastaanotetun viestin saapuneen samasta puhelinnumerosta kuin aikaisemmat viestit. Tämä tekee hyökkäystekstiviestistä persoonallisemman, koska vastaanottaja on itse päättänyt lähettäjän nimen tallentaessaan hänen puhelinnumeronsa. Testissä ei voitu olettaa kaikkien vastaanottajien tallentaneen hyökkäyksessä käytetyn puhelinnumeron matkapuhelimeensa, joten viestin loppuun lisättiin oletetun lähettäjän etunimi. Tekstiviesti on lyhyt, jotta lukija olettaa viestin olevan kirjoitettu kiireessä. Tätä tunnetta vahvistaa viestissä oleva kehote, jossa pyydetään vastaanottajaa tarkistamaan hänelle lähetetty sähköpostiviesti mahdollisimman nopeasti.

Kuviossa 5 on esimerkki tekstiviestin jälkeen lähetetystä sähköpostiviestistä. Hyökkääjä on ostanut vapaan verkkotunnuksen, joka matkii kohdeorganisaation oikeaa verkkotunnusta. Viestin liitteenä näkyy tutkimuksessa käytetty PDF liitetiedosto. Kyseisessä liitetiedostossa oli ohjeet, kuinka kohdehenkilön tulisi toimia, kun liitetiedosto on avattu.



Kuvio 5: Esimerkki testiin osallistuneille lähetetystä sähköpostiviestistä, jossa PDF liitetiedosto

Sähköpostiviestissä on enemmän tekstiä, kuin tekstiviestissä. Sähköpostiviestissä pyritään käyttämään hyökkääjän aikaisemmin keräämää ja ulkopuoliselle vapaasti saatavilla olevaa tietoa. Tiedolla pyritään luomaan sähköpostiviestiin lisää uskottavuutta. Viestissä mainitaan kolmas henkilö, joka on osa organisaation henkilöstöä. Lisäksi viestissä on fakta, joka voidaan

mahdollisesti olettaa olevan tiedossa vain organisaation sisällä. Viestissä pyydetään tarkistamaan liitteenä oleva tiedosto saman päivän aikana, jotta lukijan tunne asian tärkeydestä ja kiireellisyydestä voimistuu.

5.1 Haastattelu hyökkäyksen jälkeen

Kaikilta simuloituun hyökkäykseen osallistuneilta henkilöiltä kysyttiin haastattelussa seuraavat kysymykset:

- Luitko tekstiviestin ennen sähköpostia?

  Sähköposti yksin saattaa herättää helposti epäilyksiä ja kokenut henkilö todennäköisesti tarkistaa lähettäjän verkkotunnuksen, jos hänellä on syytä epäillä sähköpostin autenttisuutta. Tämän olettamuksen vahvistamiseksi kohdehenkilöiltä varmistettiin, ovatko he lukeneet tekstiviestin ennen sähköpostiviestiä.

- Luotitko tekstiviestiin?

  Jos tekstiviesti herättää lukijassa epäilyksiä, ei sähköposti todennäköisesti vahvista luottamusta. Tarkoituksena oli selvittää vastaanottajan aikaisempi tietämys tietojenkalastelusta tekstiviestitse. Kysymyksellä saatiin varmuus olettamukseen minkä mukaan vastaanottaja ei todennäköisesti usko sähköpostiviestiin, jos on aikaisemmin epäillyt tekstiviestiä.

- Luitko sähköpostiviestin?

  Jos kohdehenkilö ei lukenut sähköpostiviestiä, ei hyökkäyksen tehokkuudesta voinut tehdä tarkempia loppupäätelmiä, koska kohdehenkilöllä ei ollut mahdollisuutta raportoida sähköpostiviestiä tai avata liitetiedostoa.

- Jos luit sähköpostin, millä päätelaitteella sen luit?

  Yleensä matkapuhelimella on työläämpi tarkistaa lähettäjän verkkotunnus pienen näyttöpinta-alan takia. Matkapuhelimella sähköpostia luettaessa verkkotunnus ei näy lukijalle suoraan. Sähköpostiohjelman työpöytäversiolla verkkotunnus näkyy suoraan ja on helposti tarkastettaessa.

- Mistä tunnistit hyökkäyksen?

  Minkä perusteella kohdehenkilö päätti, että hänen saamansa viestit voivat olla osa verkkorikollisen hyökkäysyritystä. Kysymyksellä voidaan erotella tekstiviestin ja sähköpostiviestin väliset erot vastaanottajan näkökulmasta. Onko tekstiviesti uskottavampi?

Liitetiedoston avanneilta henkilöiltä kysyttiin edellisten kysymysten lisäksi seuraava kysymys:

- Mitä ajatuksia testi herätti?

  Tarkoituksena saada selville mahdolliset testin herättämät tunteet. Herättikö testi vihaa, oliko testi liian henkilökohtainen, yllättikö testi ja osaisitko tunnistaa vastaavanlaisen testin tulevaisuudessa?

5.2 Kyselytutkimus hyökkäyksen jälkeen

Vastaajat arvioivat kysymyksiä 5-portaisella asteikolla ääripäiden ollessa esimerkiksi: en luottanut ollenkaan ja luotin täysin. Kyselytutkimukseen valittiin seuraavat kysymykset:

- Tunnistitko simuloidun hyökkäyksen?

  Kysymyksessä luokitellaan vastaajat kahteen eri ryhmään; henkilöihin, jotka tunnistivat hyökkäyssimulaation ja henkilöihin, jotka luottivat hyökkäyssimulaatiossa lähetettyihin viesteihin.

- Oletko aikaisemmin saanut tietojenkalasteluviestejä tekstiviestitse?

  Kysymyksen avulla selvitetään, kuinka yleistä ja tuttua tietojenkalastelu tekstiviestitse on kyselyyn vastanneiden henkilöiden keskuudessa.

- Luotitko tässä simulaatiossa lähetettyyn tekstiviestiin?

  Kysymyksellä selvitetään simulaatiossa lähetetyn tekstiviestin luotettavuus verrattuna simulaatiossa lähetettyyn sähköpostiviestiin.

- Luotitko tässä simulaatiossa lähetettyyn sähköpostiviestiin?

  Kysymyksellä selvitetään simulaatiossa lähetetyn sähköpostiviestin luotettavuus verrattuna simulaatiossa lähetettyyn tekstiviestiin.

- Luotatko tekstiviesteihin enemmän kuin sähköpostiviesteihin?

  Kysymyksellä selvitetään kyselyyn vastanneiden henkilöiden yleinen luottamuksen taso tekstiviestien ja sähköpostiviestien kesken.

- Kuinka paljon luotit tekstiviesteihin ennen simuloitua hyökkäystä?

Kysymyksellä selvitetään kyselyyn vastanneiden henkilöiden luottamuksen taso tekstiviesteihin enne simuloitua hyökkäystä.

- Muuttuiko luottamuksesi tekstiviesteihin?

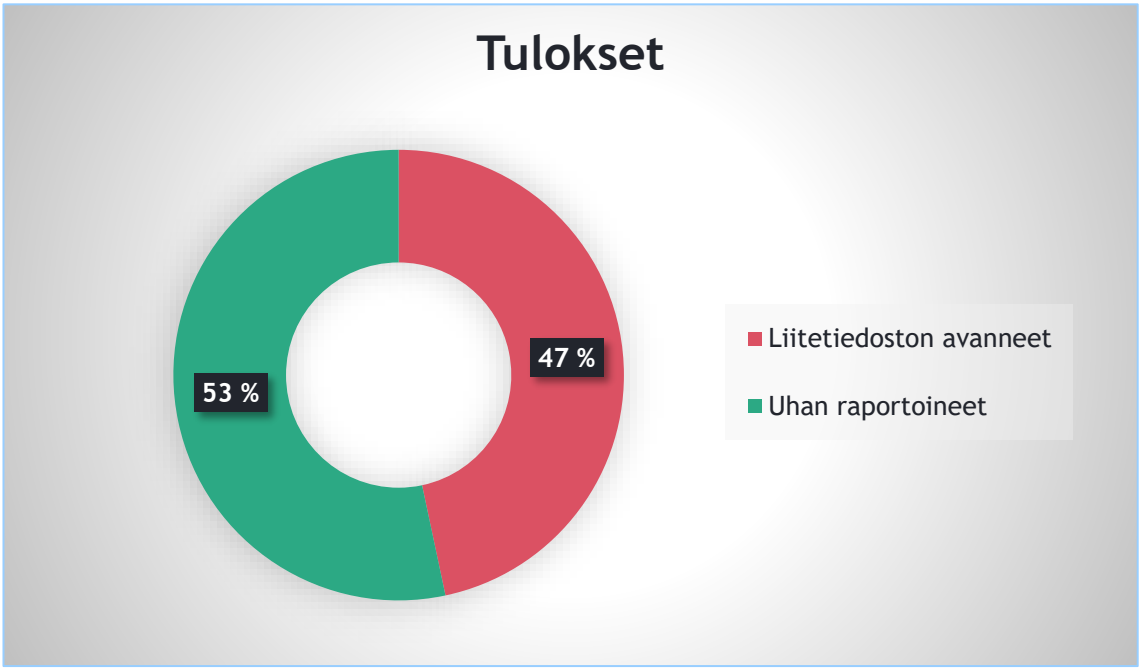
  Kysymyksellä haluttiin selvittää henkilön luottamuksen kehittymistä ennen ja jälkeen simuloidun hyökkäyksen.

- Paraniko tietoisuutesi tekstiviestitse tulevien uhkien tunnistamisessa?

  Kysymyksellä haluttiin selvittää henkilön asennetta tekstiviestien luotettavuuteen.

6 Tietojenkalasteluhyökkäyksen tulokset

Testissä mukana olleesta 15 henkilöstä 7 avasi sähköpostin liitteenä olevan PDF tiedoston. Luku on huomattava, sillä jo yhdellä potentiaalisesti haitallisella tiedostolla voi luoda kohdeorganisaation järjestelmissä suurta taloudellista vahinkoa. Kuviossa 6 on esitetty simuloidun hyökkäyksen tulokset.



Kuvio 6: Hyökkäyksen tulokset

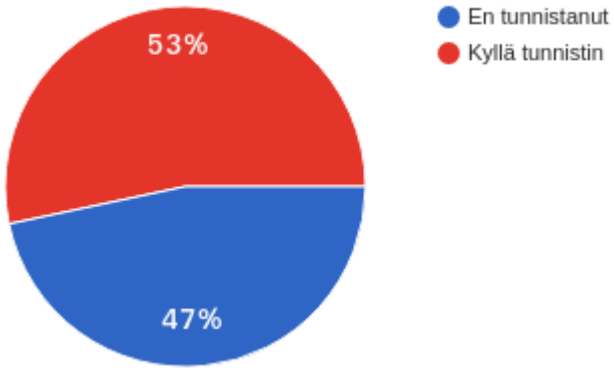
Tulokset osoittavat, että tekstiviestin käyttäminen lisää tietojenkalasteluhyökkäyksen tehoa, koska lähes puolet avasi lopullisen sähköpostin liitteenä olevan PDF-tiedoston.

6.1 Kyselytutkimuksen tulokset

Kyselytutkimukseen vastasivat kaikki simuloidun hyökkäyksen saaneet henkilöt. 15 osallistujaa vastasi kahdeksaan eri kysymykseen. Tuloksista käy ilmi simulaatioon osallistuneiden henkilöiden aikaisempi tietämys tekstiviestitse saapuvista mahdollisista tietojenkalasteluviesteistä ja kuinka luotettavaksi he kokevat tekstiviestit ja sähköpostiviestit.

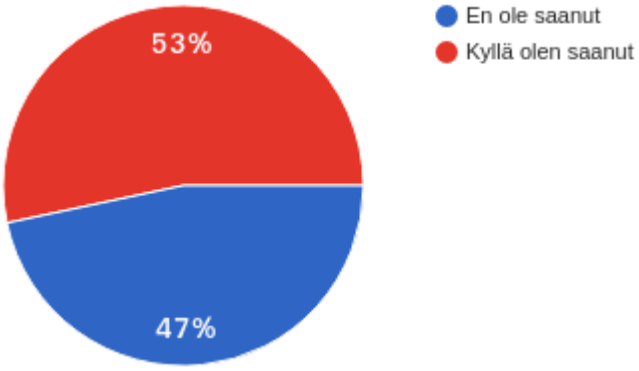
Alla olevissa kuvissa kaaviot testiin osallistuneiden vastauksista. Kysymykset ovat kuvoiden kuvateksteinä.

Kuviossa 7 selvitetään kuinka moni testiin osallistuneista tunnisti simuloidun hyökkäksen. 47% osallistuneista avasi sähköpostin liitteenä olleen potentiaalisesti haitallisen tiedoston.



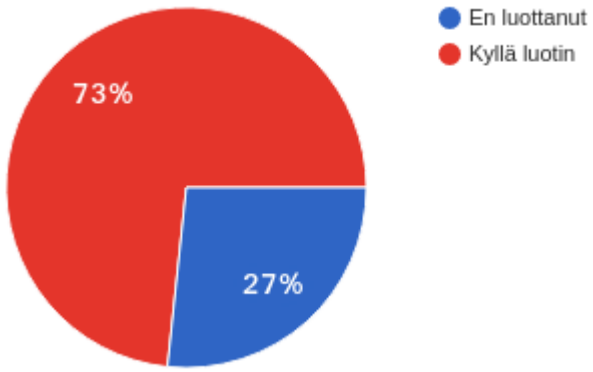
Kuvio 7: Tunnistitko simuloidun hyökkäyksen?

Kuviossa 8 selvitetään, onko vastaaja saanut aikaisemmin tietojenkalasteluviestejä tekstiviestitse. Oliko tutkimuksessa tehty simuloitu hyökkäys vastaajan ensimmäinen henkilökohtainen kosketus tekstiviestitse saapuvaan sosiaaliseen manipulointiin?



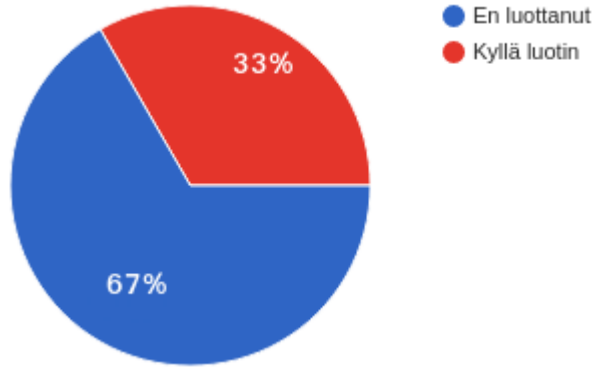
Kuvio 8: Oletko aikaisemmin saanut tietojenkalasteluviestejä tekstiviestitse?

Kuviossa 9 selvitetään vastaajan luottamus simuloidussa hyökkäyksessä lähetettyyn tekstiviestiin. 73% vastaajista luotti tekstiviestiin, joka on huomattavasti enemmän, kuin simulaatiossa lähetettyyn sähköpostiviestiin.



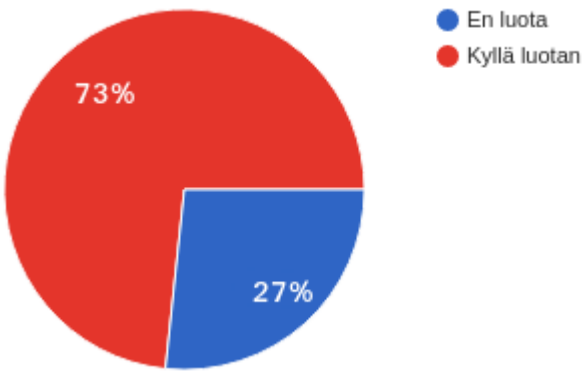
Kuvio 9: Luotitko tässä simulaatiossa lähetettyyn tekstiviestiin?

Kuviossa 10 selvitetään vastaajan luottamus simuloidussa hyökkäyksessä lähetettyyn sähköpostiviestiin. Vain 33% vastaajista luotti sähköpostiviestiin.



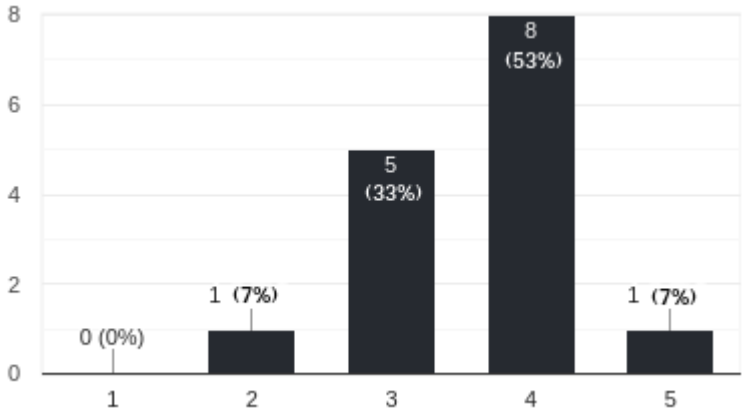
Kuvio 10: Luotitko tässä simulaatiossa lähetettyyn sähköpostiviestiin?

Kuviossa 11 erotellaan simulaatiossa lähetetyn tekstiviestin ja sähköpostiviestin luotettavuus vastaajittain. Vain 27% vastaajista sanoi, ettei luota tekstiviesteihin enemmän, kuin sähköpostiviesteihin. Kysymysten tuloksista voidaan päätellä tekstiviestin luoman tekosyyn vaikutus sähköpostiviestiin.



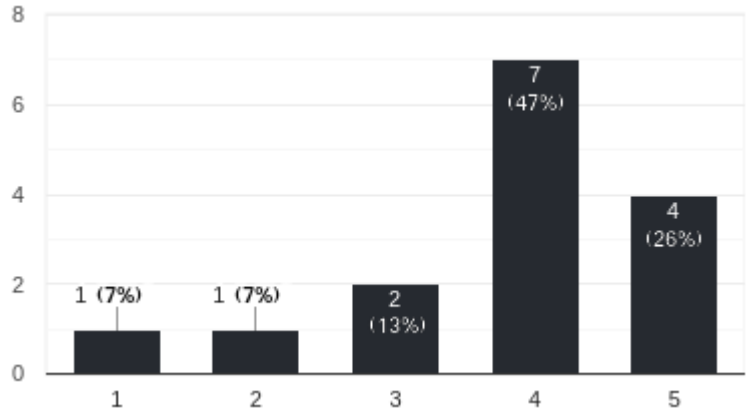
Kuvio 11: Luotatko tekstiviesteihin enemmän kuin sähköpostiviesteihin?

Kyselytutkimuksen mukaan enemmistö vastaajista luotti tekstiviesteihin ennen simuloitua hyökkäystä. Asteikolla 1-5, yhteensä 9 vastaajaa vastasi numeron 4 tai suuremman ja 1 vastaaja vastasi numeron 2 tai pienemmän (Kuvio 12). Asteikko 1 tarkoitti en luottanut ollenkaan ja asteikko 5 luotin täydellisesti.



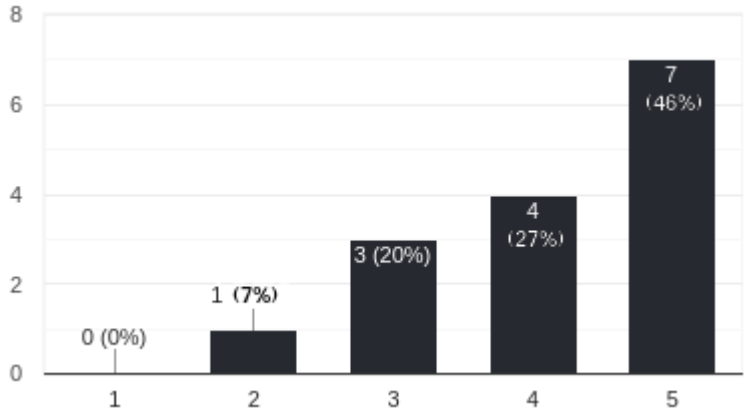
Kuvio 12: Kuinka paljon luotit tekstiviesteihin ennen simuloitua hyökkäystä?

Kuviossa 13 likert-asteikolla 4-5, 73% vastaajista oli sitä mieltä, että heidän luottamus tekstiviesteihin muuttui simuloidun hyökkäyksen jälkeen. Asteikko 1 tarkoitti ei muuttunut ollenkaan ja asteikko 5 muuttui huomattavasti.



Kuvio 13: Muuttuiko luottamuksesi tekstiviesteihin?

Kuviossa 14 likert-asteikolla 4-5, 73% vastaajista sanoi tietoisuutensa parantuneen tekstiviestitse tulevien uhkien tunnistamisessa simulaation jälkeen. Asteikko 1 tarkoitti ei parantunut ollenkaan ja asteikko 5 tarkoitti parantui huomattavasti.



Kuvio 14: Paraniko tietoisuutesi tekstiviestitse tulevien uhkien tunnistamisessa?

6.2 Haastattelun tulokset

Haastattelun perusteella käy ilmi, että osa (33%) uskoi sähköpostiin, koska he eivät olleet tietoisia, että tekstiviestin lähettäjäkentän voi väärentää ja että tekstiviesti näkyy samassa keskusteluhistoriassa aikaisempien keskustelujen jatkona. Liitetiedoston avanneiden haastattelusta käy ilmi, että osa (13%) epäili sähköpostia, mutta avasivat liitetiedoston, koska luottivat tekstiviestiin. He olivat mahdollisesti huomanneet, että sähköposti ei tule täysin samasta verkkotunnuksesta, kuin normaalisti sama sähköpostiviesti tulisi. Tekstiviestillä voitiin siis ohittaa tietoturvakoulutuksessa saadut ohjeet sähköpostin lähettäjän verkkotunnuksen tarkistamisesta ja normaali tietoturvallinen käytös ei enää pätenyt, kun luottamus oli ensin luotu tekstiviestillä.

7 Johtopäätökset

Kuten kuviot 9 ja 11 osoittavat, tutkimukseen osallistuneista henkilöistä 73% luottivat tekstiviesteihin enemmän kuin sähköpostiviesteihin. Tämä tulos osoittaa, että tietojenkalastelu-hyökkäyksen onnistuminen on todennäköisempää, jos tietojenkalastelusähköpostin lisäksi käytetään tekstiviestejä.

Huomioitavaa on kuitenkin, että otanta on pieni (15 henkilöä), mutta kohdehenkilöiden tietojen tasoa tietojenkalasteluhyökkäyksistä ja niiden uhista voidaan pitää tavanomaisen työntekijän tietojen tasoa parempana ja siksi testiin osallistuneet henkilöt olivat normaalia haastavampi kohderyhmä hyökkääjän näkökulmasta.

Organisaatioiden reagointikyky on rajoitettu jatkuvasti muuttuvien kyberuhkien suhteen. Ennaltaehkäisyyn pyritään, mutta harvemmin lähes tuntemattomiin hyökkäyksiin pystytään varautumaan etukäteen. Testiin osallistuneet henkilöt ovat mukana jatkuvassa tietojenkalasteluhyökkäysten tunnistamiskoulutuksessa, joka keskittyy vain sähköpostitse tuleviin tietojenkasteluhyökkäyksiin. Tutkimuksessa käy ilmi henkilöiden kyvyttömyys tunnistaa tietojenkalasteluhyökkäystä, mikäli hyökkäys poikkeaa vastaanottajalle tutusta metodista, eikä sen tunnistamista ei ole koulutettu etukäteen. Tietomurtojen aiheuttamat vahingot ovat usein suurempia kuin ennaltaehkäisevän koulutuksen kustannukset.

Tietoisuus mahdollisista tekstiviestitse saapuvista tietojenkalasteluhyökkäyksistä on huomattavasti alhaisempi kuin sähköpostitse saapuvista tietojenkalasteluhyökkäyksistä. Simuloituun hyökkäykseen osallistuneista henkilöistä 73% luotti tekstiviestiin, joten voidaan olettaa, että he eivät olleet tietoisia tekstiviestin lähettäjäkentän väärentämisen olevan mahdollista samaan tapaan kuin sähköpostiviestin.

Sosiaaliseen manipulointiin perustuvat hyökkäykset ovat tällä hetkellä erittäin suosittu metodi yksityishenkilöiden, yritysten ja jopa valtiollisen tason järjestelmiin murtautumisessa. Koska hyökkäyksessä käytettiin enimmäkseen hyväksi sosiaaliseen manipulointiin perustuvaa taktiikkaa, oli hyökkäyksen lopullista tulosta erittäin vaikea ennustaa. Perinteiseen sähköpostitse lähetettävään tietojenkalasteluviestiin voidaan luoda täysin uusi elementti, kun hyökkäykseen lisätään hyökkäyksen tueksi melko yksinkertainen tekstiviesti.

Uskon, että tehokkain ratkaisu organisaatioiden suojaamisessa tekstiviestejä apuna käytettävissä hyökkäyksissä on lisätä tietoisuutta ja kouluttaa yritysten työntekijöitä suhtautumaan myös tekstiviesteihin varauksella.

Lähteet

Painetut

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Yin, Robert K. 2009. Case Study Research, Design and Methods. 4. Painos. Thousand Oaks, CA: SAGE Publications.

Sähköiset

Bere, M., Bhunu-Shava, F., Gamundani & A. Nhamu, I 2015. How Advanced Persistent Threats Exploit Humans. Viitattu kesäkuu 2018. https://search-proquest-com.nelli.laurea.fi/central/docview/1752642724/fulltextPDF/1358BC050CF341D6PQ/3

Deloitte. 2017. Global mobile consumer trends, 2nd edition. Viitattu joulukuu 2018. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-global-mobile-consumer-survey-second-edition.pdf

Flowroute, Inc. 2016. Flowroute Survey Finds Consumers Overwhelmingly Prefer SMS to Email and Voice for Business Interactions. Viitattu tammikuu 2019. https://www.flowroute.com/press-type/flowroute-survey-finds-consumers-overwhelmingly-prefer-sms-to-email-and-voice-for-business-interactions/

Goel D, Jain A. K. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. 2017. Viitattu helmikuu 2019. https://www-sciencedirect-com.nelli.laurea.fi/science/article/pii/S0167404817302717

Pew Research Center. 2016. Text Message Notification for Web Surveys. Viitattu tammikuu 2019. http://www.pewresearch.org/methods/2016/09/07/text-message-notification-for-web-surveys/

PhishMe, Inc. 2016. Enterprise Phishing Susceptibility and Resiliency Report. Viitattu marraskuu 2018. https://cofense.com/enterprise-phishing-susceptibility-report/

Ponemon Institute LLC. 2018. 2018 Cost of a Data Breach Study: Global Overview. Viitattu joulukuu 2018. https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf

Proofpoint. 2016. Quarterly Threat Summary. Viitattu joulukuu 2018. https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final.pdf

Radicati Group. 2017. Email Statistics Report, 2015-2019. Viitattu kesäkuu 2018. https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. Viitattu marraskuu 2018. http://www.ijcncs.org/published/volume4/issue6/p1_4-6.pdf

Sendmode. 2017. All You Need To Know about Bulk Text Marketing. Viitattu tammikuu 2019. https://www.sendmode.com/all-you-need-to-know-about-bulk-text-marketing

Shift Communications. 2015. What is the open rate of SMS text messaging? Viitattu tammikuu 2019. https://www.shiftcomm.com/blog/what-is-the-open-rate-of-sms-text-messaging/

TextMagic. 2018. 52 Text Messaging Statistics for Businesses. Viitattu tammikuu 2019. https://www.textmagic.com/blog/text-messaging-statistics-for-businesses/

Verizon. 2018. Data breach investigation report 2018. Viitattu joulukuu 2018. http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

Wikileaks 2016. Viitattu toukokuu 2019. https://wikileaks.org/podesta-emails/emailid/36355

Kuviot

Taulukot

Liitteet

Liite 1: Kyselytutkimuksen kysymykset

Tunnistitko simuloidun hyökkäyksen? *

- ○ En tunnistanut
- ○ Kyllä tunnistin

Oletko aikaisemmin saanut tietojenkalasteluviestejä tekstiviestitse? *

- ○ En ole saanut
- ○ Kyllä olen saanut

Luotitko tässä simulaatiossa lähetettyyn tekstiviestiin? *

- ○ En luottanut
- ○ Kyllä luotin

Luotitko tässä simulaatiossa lähetettyyn sähköpostiviestiin? *

- ○ En luottanut
- ○ Kyllä luotin

Luotatko tekstiviesteihin enemmän kuin sähköpostiviesteihin? *

- ○ En luota
- ○ Kyllä luotan

Kuinka paljon luotit tekstiviesteihin ennen simuloitua hyökkäystä? *

	1	2	3	4	5	
En luottanut ollenkaan	○	○	○	○	○	Luotin täydellisesti

Muuttuiko luottamuksesi tekstiviesteihin? *

	1	2	3	4	5	
Ei muuttunut ollenkaan	○	○	○	○	○	Muuttui huomattavasti

Paraniko tietoisuutesi tekstiviestitse tulevien uhkien tunnistamisessa? *

	1	2	3	4	5	
Ei parantunut ollenkaan	○	○	○	○	○	Parantui huomattavasti

SUBMIT