



Opas sosiaalisen manipuloinnin välttämiseen

Tietoturvan inhimillinen puoli

Seemi Hintsanen

Haaga-Helia ammattikorkeakoulu

Tietojenkäsittelyn koulutusohjelma

Opinnäytetyö

2022

Tiivistelmä

Tekijä(t) Seemi Hintsanen
Tutkinto Tradenomi
Raportin/Opinnäytetyön nimi Opas sosiaalisen manipuloinnin välttämiseen – Tietoturvan inhimillinen puoli
Sivu- ja liitesivumäärä 8 + 18 (opas)
<p>Opinnäytetyö on toiminnallinen. Tuotos on tietoturvaohje. Sen taustana on pääasiassa Christopher Hadnagy'n kirjat The human Hacking book ja The art of social engineering. Jälkimmäisen kirjan tietoperusta perustuu myös neljään eri tutkimukseen, jotka hakevat vastauksia käytösmallien ja muiden ominaisuuksien vaikutuksesta sosiaalisen manipulaation kohteille.</p> <p>Opinnäytetyössä tuotettiin opas, joka toimii mahdollisimman selkokielisenä, konkreettisenä ja perusteleva tietoturvaohjeena. Opasta on voi hyödyntää tietoturvakoulutusten pohjana. Oppaan avulla voidaan myös parantaa yritysten työntekijöiden tietoisuutta sosiaalisen manipulaation riskeistä ja yleistymisestä. Opas on tärkeä, koska harmittomalta ja mukavalta vaikuttava manipulaatiohyökkäys voi johtaa vakaviin seurauksiin. Mikäli kaikkia hyökkäyksiä ei pystytä tunnistamaan, niitä voidaan ainakin hankaloittaa erilaisilla käytännöillä.</p> <p>Opas käsittelee hakkerointia, sen tunnistamisesta sekä käytäntöjä, jotka toimivat hakkerointia suojaavina mekanismeina. Opas keskittyy hakkerointiin, joka kohdistuu ihmisiin - ei teknisiin järjestelmiin. Opas käsittelee sosiaalisen manipuloinnin aihetta yleisellä tasolla. Oppaassa käydään läpi teknisiä käytäntöjä vain siltä osalta, miten ne liittyvät sosiaalisten manipulaatiohyökkäyksen torjumiseen.</p> <p>Opas on toteutettu perehtymällä tietoturva-alan ammattikirjallisuuteen, jossa opetetaan sosiaalista manipulaatiota ja sen perusteella kirjoitettiin opas, siltä suojautumisesta.</p>
Asiasanat Tietoturva, Sosiaalinen manipulaatio, Tietoturvan parhaat käytännöt, Tietojenkalastelu, Huijaminen, Hakkerointi

Sisällys

1 Johdanto	1
2 Teoriatausta	2
3 Empiirinen osa ja oppaan teko	5
4 Pohdinta	7
Lähteet.....	8

1 Johdanto

Tämä raportti on osa opinnäytetyötä. Opinnäytetyössä on kaksi osaa, raportti ja toiminnallinen tuotos. Tässä raportissa kerrotaan tietoperustaa, jonka pohjalta tietoturvaopas on kirjoitettu. Raportti kuvailee tutkimuksia, joista oli hyötyä oppaan näkökulmien laatimisessa ja faktapohjan luomisessa. Raportin tietoperustaosassa kerrotaan myös kahdesta Christopher Hadnagy'n kirjasta, jotka toimivat oppaan päämateriaalina ja suurena inspiraationa. Raportissa kerrotaan myös, mitä kirjat käsittelevät. Vaikka kirjat ovat hyvin samanlaisia, ne eroavat toisistaan ja ne kummatkin toimivat tärkeinä lähteinä itse oppaan kirjoittamisessa.

Oppaan empiirisessä osassa perustellaan tarkemmin, miksi opas on suunnattu sekä pienien että suurien yritysten käyttöön. Opasta voivat hyödyntää kuluttajatkin, mutta eniten siitä hyötyvät yritykset, joiden tietojärjestelmissä on hakkereita kiinnostavaa arkaluontoista materiaalia. Empiirisessä osassa perustellaan myös oppaan tarpeellisuutta kyberrikollisuuden siirtyessä ihmis-kohteiseksi sekä oppaan tavoitetta lisätä tietoisuutta sosiaalisen manipulaation ilmiöstä ja toimia ymmärrettävänä pohjana työntekijöiden tai yksityishenkilöiden tietoturvallisuuden parantamiseksi.

2 Teoriatausta

Aiheeseen perehdyttiin tieteellisestä näkökulmasta tutustumalla seuraaviin tutkimuksiin:

A multi-level defense against social engineering

David Gragg, Sans-instituutista on kirjoittanut artikkelin, josta saatiin hyvä malli ohjeistuksen tekemiseen. Artikkelista löytyy paljon samankaltaisuuksia, kuin oppaasta. Se avaa ensin aihetta - mitä sosiaalinen hakkerointi on? - ja käy hieman läpi sosiaalisen hakkeroinnin keinoja. Tämän jälkeen eritellään loogisesti muodostettu malli, jolla suojaudutaan sosiaaliselta hakkeroinnilta korostaen tiedostamista sekä hyviä käytäntöjä koulutuksien ja tietoturvapoliitikan kautta. (Gragg, D. 2021)

A Personality Based Model for Determining Susceptibility to Phishing Attacks

Tämä on tutkimus, jossa tutkitaan miten persoonallisuus vaikuttaa alttiuteen langeta kalasteluvies-teihin. Tutkimuksen tekivät James L. Parrish ja Janet L. Bailey, Arkansanin yliopistosta sekä James F. Courtney, Louisiana Tech -yliopistosta. Tämä tutkimus tehtiin, koska uudet tutkimukset ovat osoittaneet, että eräät henkilöt ovat toisia alttiimpia tietojenkalastelulle. Tutkimuksessa pyrittiin löytämään yhteys ison viiden (The big five) persoonallisuusmallinnuksen ja tietojenkalastelulle alttiuden välillä. (Parris, J., Bailey, J., Courtney, J. A)

Who falls for phis? A Demographic analysis og phishing susceptibility and effectiveness of interventions

Tässä tutkimuksessa analysoidaan tietojenkalastelun kohderyhmää ja demografian vaikutuksia alttiuteen kalastelulle. Tutkimuksessa selvitetään myös, miten tehokkaasti koulutusmateriaalit ja tietoisuuden lisääminen vähentää alttiutta tietojenkalastelulle. Tutkimuksen tulokset olivat yllättäviä ja antoivat hyvää suuntaa oppaan tieto-osioon. Tutkimuksen tekivät Garnegie Mellon -yliopiston tutkijat Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor ja Julie Downs. (Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J. 2010)

Behavioral Response to Phishing Risk

Tämän tutkimuksen ovat tehneet Garnegie Mellon -yliopiston tutkijat Julie Downs, Mandy B. Lanyon ja Lorrie Cranor. Tutkimus antoi hyödyllistä vertailudataa demografian vaikutukseen tietojenkalastelussa, sekä mielenkiintoisia näkökulmia miten ihmisten erilaiset käytösmallit vaikuttavat alttiuteen langeta tietojenkalasteluun. Tutkimus antoi myös näyttöä miten tietoisuuden lisääminen auttaa estämään hyökkäyksen onnistumista. Tutkimuksessa testattiin osallistujia roolileikin avulla. Tutkimuksen tulosten perusteella verkkoympäristön laajempi ymmärtäminen vähentää siihen liittyviä riskejä paremmin kuin pelkkä riskien tiedostaminen. (Downs, J., Lanyon, M., Cranor, L. 2007)

Työn tietopohjana käytettiin myös Christopher Hadnagyn Social Engineer -podcastia, jota hänen Social Engineer -yrityksensä tuottaa. Podcastissa Christopher Hadnagy kertoo hänen hakkerointiuransa villeimpiä tarinoita. Hadnagy tekee valkohattuhakkerointia ja suorittaa penetraatiotestauksia ja kalastelukampanjoita yrityksille, jotta ne voivat testata omaa tietoturvaansa. Mikäli Hadnagyn tiimi onnistuu hakkeroinnissaan, he järjestävät yritykselle koulutuksen. Siinä käydään läpi parannusehdotukset ja toimineet tietoturvaprotokollat. Christopher Hadnagy on myös tietoturvakirjailija ja hän on kirjoittanut aiheesta useita kirjoja. Kirjojen painotus on hakkeroinnin kannalta inhimillisissä haavoittuvuuksissa, joita hän tiiminsä kanssa hyödyntää. Hadnagy on perehtynyt psykologiaan ja erityisesti sosiaalipsykologiaan ja hän onkin tiivistänyt niiden periaatteista ja tutkimuksista konkreettisia työkaluja ihmisten sosiaaliseen hakkerointiin. Nykypäivänä tekninen tietoturva on monesti monikerroksista. Siksi onkin usein paljon helpompi murtautua järjestelmiin ja paikkoihin hyödyntämällä ihmisten pyyteetöntä, hyvää tarkoittavaa toimintatapaa tai välinpitämättömyyttä.

Opas pohjautuu pääosin Christopher Hadnagyn kahteen kirjaan:

- The science of human hacking (Hadnagy, C. 2018.)
- The Art of Social Engineering (Hadnagy, C. 2014.)

Myös Christopher Hadnagyn Social Engineer LLC -yrityksen verkkosivujen materiaaleja on käytetty tietopohjana.

The science of human hacking

Kirjassa Christopher Hadnagy opettaa tapoja vaikuttaa ihmisiin positiivisuuden kautta. Kirjan vaikutustapoja voisi ajatella samalla tavalla kuin karman lakia – tee hyvää ja saat hyvää. Kirja on hyödyllinen kaikille, jotka haluavat parantaa omia kommunikaatitaitojansa jokapäiväisessä elämässään. (Hadnagy, C. 2018.)

The art of social engineering

Tämä kirja on suunnattu enemmän turvallisuusalan ammattilaisille. Kirjassa käsitellään vaikuttamisen tapoja ja keinoja tarkemmin ammattimaisemmalla näkökulmalla sekä paneudutaan syvällisemmin kommunikaation eri aspekteihin. (Hadnagy, C. 2014.)

Security Through Education

Tämä Social engineering LLC -yrityksen ylläpitämää verkkosivu (Social engineer) tarjosi myös materiaalia ja kokonaiskuvaa oppaan sisällölle. Verkkosivulla on julkaistu paljon sosiaalinen manipulaatioon liittyvää materiaalia. Sivusto sisältää eräänlaisen laajan viitekehyksen ja pyrkii yksityiskohdistaisesti selittämään ja opettamaan sosiaalisen manipulaation keinoja ja taitoja. Sivusto sisältää laajasti materiaalia. Sivuston kohdeyleisönä on sekä turva-alan ammattilaiset että alan ulkopuoliset henkilöt.

Lisäksi lähteinä käytettiin tietoturvamateriaalia Ciscolta (Cisco. 2018) sekä Purple Sec (Purple Sec) ja Comparitech -yhtiöiltä (Purple Sec) käytettiin varmistamaan ja tarkistamaan faktojen oikeudellisuutta. Lähteistä saatiin tilastollisia perusteluja vahvistettua tarkalla numeraalisella datalla.

Oppaassa haluttiin kiteyttää oppaan sanomaan tietoturva-asiantuntija Panu Palmun sitaatilla – *”Ihminen on tietoturvan heikoin lenkki”* (Palmu, P. 2020).

3 Empiirinen osa ja oppaan teko

Tuotoksen vaiheistus

Oppaan teon ensimmäinen vaihe oli oppaan formaatin ja kohdeyleisön valinta. Oppaan formaatiksi valittiin vapaamuotoinen ja esitelmätyyppinen muoto. Näin opas on kaikille mahdollisimman selkeästi luettavissa. Oppaan viesti on tärkeä ja pääasia on, että jokainen ymmärtää mitä oppaassa tarkoitetaan. Oppaan pääsääntöiseksi kohdeyleisöksi valittiin keskisuurten yritysten kaikki työntekijät. Opas soveltuu yrityksille, jotka eivät käsittele erittäin arkaluontoista tietoa. Oppaan kohdeyleisö valittiin sillä perusteella, että kohdeyleisö on tietämättömyyden takia haavoittuvainen manipulatiohyökkäykselle.

Projektin toinen vaihe oli tietoperustan ja lähdemateriaalin valinta. Christopher Hadnagy henkilönä oli oppaan kirjoittajalle entuudestaan tuttu hänen yrityksensä podcastien kautta. Hän on alan asiantuntija, joka on kirjoittanut aiheesta kiinnostavalla ja selkeällä tavalla. Oppaan tuottamisessa haluttiin yksi päälähde, jotta opas pysyisi mahdollisimman selkeänä. Oppaan muut lähteet valittiin faktojen tarpeellisuuden ja luotettavuuden perusteella. Oppaan muut lähteet perustelevat tutkimustuloksillaan oppaan väittämiä.

Tuottamista rajaavat ja hankaloittavat tekijät

Oppaan rajaaminen oli hankalaa, sillä sen tarkoituksena oli kattaa koko sosiaalinen manipulaatio. Koska oppaan kattaa melko laajan aihealueen, ei yksittäisiin aiheisiin voitu paneutumaan kovin tarkkaan. Mikäli oppaan rajaus olisi ollut tarkempi, esimerkiksi kalastelusähköpostit, olisi oppaassa jäänyt paljon kiinnostavia ja tärkeitä aihealueita pois. Oppaassa ei käsitellä kaikkia teknisiä tietoturva-protokollia. Ainoastaan niitä protokollia käsitellään, joilla estetään tai hankaloitetaan hakkerien sosiaalista manipulaatiohyökkäystä. Käsiteltyjen tietoturva-protokollien teknisiä toimintoja ei myöskään avata sen enempään kuin on oleellista. Oppaan kirjoittamista rajoitti myös sen yleishyödyllisyys. Oppaan tuottaminen olisi ollut selkeämpään, jos se olisi tehty toimeksiantona jollekin yritykselle. Toimeksianto yritykseltä olisi tarkentanut oppaan hyödynnettävyyttä ja muita oppaan laatukriteerejä. Oppaan tuottamista rajoitti myös aikataulu, sillä lähdemateriaalin kääntäminen englannista suomeksi hidasti sisällöntuottamista.

Kenelle opas on suunnattu

Opas on kohdennettu niin, että siitä hyötyisi erityisesti keskisuuret ja suuriin yritykset. Opasta voi kuitenkin hyödyntää kuka tahansa yksityishenkilöstä aina ison yrityksen tietoturvavastaavaan. Sosiaalinen manipulaatiohyökkäys on huolellisesti valmisteltu eikä spontaani massahyökkäys ja siksi

niitä ei yleensä kohdistu yrityksiin, joilla ei ole tietoturvan kannalta arkaa materiaalia. Toki hyökkäyksen syinä voi olla esimerkiksi raha tai kosto, mutta näissä kohteen valitsemiselle on moninaisempia syitä.

Oppaan tavoite

Oppaan tavoite on parantaa tietoisuutta koko ajan kasvavasta ongelmasta ja tarjota ongelmaan neuvoja ja ratkaisuja. Opas on tarpeellinen, koska sosiaalinen manipulaatio on yleistynyt viime vuosikymmenen ajan ja kasvaa koko ajan isommaksi tietoturvauhaksi. Kyberrikokset ovat valtava kuluerä yritysmaailmassa ja hyvin usein rikoksissa hyödynnetään myös sosiaalista hakkerointia. Aiheesta löytyy paljon englanninkielistä kirjallisuutta, mutta huomattavasti vähemmän suomenkielistä kirjallisuutta. Suomenkielisen oppaan kirjoittaminen voi tuoda lisää selkeyttä aiheeseen ja madaltaa kynystä aiheeseen perehtymiseen. Oppaan tavoitteena on antaa jokaisen ymmärtämiä järkiperusteita, jotta lukija käsittää tietoturvaprotokollien ja niiden huolellisen noudattamisen tärkeyden. Oppaassa kerrotaan myös konkreettisia esimerkkejä tavoista, joilla hakkerit hyödyntävät sosiaalista manipulaatiota. Näin lukijat voivat tunnistaa niitä paremmin sekä ymmärtää niistä aiheutuvia seurauksia.

Opas voi toimia joko yrityksen työntekijöille jaettava itsenäisenä koulutusmateriaalina tai opas voi toimia koulutustilaisuuden pohja- tai lisämateriaalina. Yritys voi arvioida itse tilannekohtaisesti koulutusmallin ja -tavan. Koska opasta voi käyttää myös itsenäiseen aiheeseen perehdytykseen, se mahdollistaa joustavat aiheen koulutustavat sekä niiden mukanaan tuomat mahdolliset säästöt yrityksen koulutuskustannuksissa.

Opas on onnistunut tavoitteessaan, mikäli yritys pystyy sen pohjalta luomaan konkreettisen tietoturvapolitiikan ja -koulutuksen. Opas on myös onnistunut, mikäli yrityksen suomenkieliset työntekijät, joille tietoturva on jokseenkin tuntematon aihealue, kokevat oppaan luettuaan pystyvänsä paremmin varautumaan sosiaaliseen manipulaatioon.

4 Pohdinta

Opinnäytetyön tulos oli suunnitelman mukainen opas, joka yleisellä tasolla esittelee, mitä on sosiaalinen manipulointi tietoturvan kontekstissa ja kertoo faktoja sen vaikutuksista nykyisessä kyberrikollisuuden maailmassa. Esittelyn jälkeen se mainitsee tapoja tunnistaa manipulaatiohyökkäys ja hyökkäyksen keinoja. Opas alkaa hyödynnettävimmällä osalla, jossa käydään läpi esimerkein käytäntöjä, joiden pohjalta yritykset ja yksityishenkilöt voivat laatia tietoturvapoliittikoja.

Opas itsessään kertoo tietoturvasta pintaraapaisun ja siihen voisi olla hyvä jatkomahdollisuus ottaa jostain yrityksestä toimeksianto ja opasta hyödyntäen luoda yritykselle tietoturvapoliittikka ja -koulutus.

Opinnäytetyöprosessin ja oman oppimisen arviointi

Opas ei juurikaan ole eri mieltä Christopher Hadnagy tai muidenkaan lähteiden kanssa. Päinvastoin, oppaassa hyödynnetään tutkimuksia ja Christopher Hadangyn kirjoja perustelemaan oppaan sanomaa. Aihetta tutkiessani opasta varten opin paljon lisää siitä, miksi monet käytännöt oikeasti ovat olemassa. Sainkin useammankin ”ahaa” -elämyksen ymmärtäessäni, miksi aiemmin ihmettelämäni käytännöt olivat luotu. Kokonaisuudessaan opinnäytetyöprojekti tarjosi hyvää lisäoppia ajanhallintaan ja projektityöhön liittyen. Opinnäytetyön itsenäinen työskentely ja oman tietoturvaoppaan tekeminen vahvistivat myös aiheen konkreettista asiantuntemustani.

Lähteet

25+ password statistics. Luettavissa: <https://www.comparitech.com/blog/information-security/password-statistics/>. Luettu 20.2.2022

Cisco. 2018. Luettavissa: <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>. Luettu 12.2.2022

Downs, J., Lanyon, M., Cranor, L. 2007 Behavioral Response to Phishing Risk. Luettavissa: https://www.researchgate.net/publication/221462245_Behavioral_response_to_phishing_risk. Luettu 2.2.2022

Gragg, D. 2021. A Multi-Level Defense Against Social Engineering. Luettavissa: <https://www.sans.org/white-papers/920/>. Luettu 3.2.2022

Hadnagy, C. 2018. Social Engineering: The science of human hacking. 2nd ed. Hoboken, NJ: Wiley Publishing. Äänikirja

Hadnagy, C. 2014. Social Engineering: The art of human hacking. Brilliance audio, unabridged edition. Äänikirja

Palmu, P. 2020. Eteväen tietoturva-asiantuntija: Ihminen on tietoturvan heikoin lenkki! Luettavissa: <https://www.etevat.fi/blogi/ihminen-on-tietoturvan-heikoin-lenkki>. Luettu 16.3.2022

Parris, J., Bailey, J., Courtney, J. A Personality Based Model for Determining Susceptibility to Phishing Attacks. Luettavissa: https://www.academia.edu/48717594/A_Personality_Based_Model_for_Determining_Susceptibility_to_Phishing_Attacks. Luettu 22.1.2022

Purple Sec. Luettavissa: <https://purplesec.us/resources/cyber-security-statistics/> Luettu 2.2.2022

Roshental, M. 2022. Tessian. Luettavissa: <https://www.tessian.com/blog/phishing-statistics-2020/> Luettu 5.2.2022

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J. 2010 Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Luettavissa: https://www.researchgate.net/publication/221514257_Who_falls_for_phish_A_demographic_analysis_of_phishing_susceptibility_and_effectiveness_of_interventions. Luettu 30.1.2022

Social engineer. Luettavissa: <https://www.social-engineer.org/>. Luettu 21.3.2022



Opas sosiaalisen manipuloinnin välttämiseen

Tietoturvan inhimillinen puoli

Sisällysluettelo

1. Johdanto	3
<i>Oppaan tarkoitus</i>	3
<i>Kuka hyötyy tästä oppaasta?</i>	4
2. Sosiaalisen manipuloinnin tunnistaminen	5
<i>Mitä on sosiaalinen manipulointi?</i>	5
<i>Sosiaalisen manipulaation tunnistaminen ja välttäminen käytäntöjen kautta</i>	6
<i>Tunnistamisen ja välttämisen ero</i>	7
<i>Tunnistaminen ja reagointi</i>	8
3. Vaikuttamisen keinoja ja esimerkkejä	9
<i>Hyökkäyksen valmistelu</i>	9
<i>Tiedon johdattelu (eliciting)</i>	11
4. Hyökkäyksen välttäminen käytäntöjen kautta	12
<i>Mitä ovat parhaat käytännöt?</i>	12
<i>Tietoturvakäytännöt käytännössä</i>	12
5. Tekninen tietoturva	16
<i>Käyttöoikeuksien rajaaminen</i>	16
<i>Salasanakäytännöt</i>	17
<i>Ulkoisten laitteiden liittäminen</i>	17
Lähteet	18

1. Johdanto

Teknologia kehittyy jatkuvasti ja tietoturva on kyberrikollisten ja tietoturva-ammattilaisten kilpajuoksua. Uusia keinoja estää tietomurtoja kehitetään jatkuvasti. Samaa aikaan myös rikolliset keksivät jatkuvasti uusia keinoja ohittaa palomuuureja ja virustorjuntia. Yleinen tietotekninen tietotaito kehittyy kuitenkin hitaammin, kuin tietoturvateknologia ja sen erilaiset moniportaiset tietoturvaratkaisut.

Yleistyvässä määrin rikolliset hyödyntävät sosiaalista manipulaatiota, ainakin osana tietomurtoa. Purple sec -tietoturvayhtiön mukaan, jopa 98% tietomurroista nojautuu nykyään ainakin osittain sosiaaliseen manipulaatioon.

Ihmiset ovat aina huijanneet ja tulevat aina huijaamaan toisiaan. Viimeisten 15 vuoden aikana ihmisten huijaamisesta on tullut yhä isompi ongelma myös tietoturvan saralla.

Tämä opas pyrkii kuvaamaan, mistä tässä merkittävässä ilmiössä on kyse.

Oppaan tarkoitus

Tämä opas käsittelee tietoturvaa vähemmän tiedostetusta sosiaalisesta manipuloinnista näkökulmasta. Oppaassa käydään läpi, mitä sosiaalisella manipulaatiolla tarkoitetaan tietoturvan kontekstissa, sekä minkälaisilla keinoilla sitä voidaan estää ja välttää.

Tämä opas painottaa sosiaaliselta manipulaatiolta suojautumista pääosin käytäntöjen kautta. Hyökkäyksen tunnistaminen ja huomaaminen on todella hyödyllistä. Kun hyökkäysyritys tunnistetaan, siihen voidaan myös reagoida. Hyökkäysyrityksien tunnistaminen edellyttää tiedon siitä, miten ne tyypillisesti tehdään.

Hyökkäyksen tunnistaminen vaatii myös eri kriittistä suhtautumista erilaisiin interaktioihin ja sopivan annoksen vainoharhaisuutta. Toimivat tietoturvakäytännöt sekä hyökkäysyritysten tunnistaminen helpottavat myös siksi, ettei kaikessa toiminnassa tarvitse olla jatkuvasti vainoharhainen.

Tilanteet, joissa tietoturvakäytännöistä joutuu joustamaan, tulee kuitenkin aina arvioida mahdollisen hyökkäyksen kannalta. Käytännöistä saadaan siis hyvää tasapainoa luottamuksen ja tarpeellisen epäilyn välille. Ihmisten välinen kanssakäyminen vaatii aina tietyn verran luottamusta, joka pitää suhteuttaa tilanteeseen.

Sosiaalinen manipulaatiohyökkäys perustuu siihen, että kohde toimii hakkerin haluamalla tavalla ilman, että kohde suhtautuu hakkerin pyyntöön liian kriittisesti ja epäluuloisesti. Hyvällä käytäntöpolitiikalla ja käytäntöjen tiukalla noudattamisella vaikeutetaan hakkerointia merkittävästi. Hyvillä käytännöillä on siis tarkoitus estää vahingossa tapahtuvat tietoturvariskit.

Hyökkäykselle paras esto on mahdollisimman moniportainen tietoturva, joka on yhdistelmä sekä teknisiä että sosiaalisia ratkaisuja ja käytäntöjä. Hyvillä käytännöillä voidaan estää ja vaikeuttaa hakkerointiyrityksiä huomattavasti, ilman että itse hakkerointiyritystä aina edes huomataan. Tietoturva perustuu ajatukseen, että mikään ei ole murtovarmaa. Mitä hankalammaksi murtautumisen voi tehdä, sitä parempi on suojaus.

Kuka hyöttyy tästä oppaasta?

Opas on kohdistettu ensisijaisesti pienille ja keskisuurille yrityksille, jotka käsittelevät arkaluontoista dataa ja voivat siten olla potentiaalisia tietomurron kohteita. Oppaan käytännöistä voivat myös yksityishenkilöt ottaa mallia ja soveltaa oppaan periaatteita omaan arkeensa. Suuret yritykset voivat laajentaa käytäntöjensä esimerkkien perusteella ja hyödyntää opasta lisänä henkilöstön tietoturvakoulutuksissa.

Oppaasta hyötyvät myös yritykset, joilla ei ole suurta tarvetta tiukalle tietoturvalla, sillä monet oppaan käytännöt ovat yleishyödyllisesti sovellettavissa. Tämän oppaan käytännöt ovat yleisiä esimerkkejä, joita voidaan tarvittaessa soveltaa yritys- ja tilannekohtaisesti.

2. Sosiaalisen manipuloinnin tunnistaminen



Mitä on sosiaalinen manipulointi?

Sosiaalinen manipulointi tai hakkerointi ei ole mikään uusi tai erikoinen asia. Ihmiset ovat tiedostaen ja tiedostamatta aina tehneet sosiaalista manipulointia. Sosiaalisessa hakkeroinnissa erityistä on kuitenkin se, että kommunikaatiotapahtuma tapahtuu tiedostetusti ja johtaa tarkoituksenmukaisesti kohti hakkerin tavoitetta. Christopher Hadnagy'n kirjassa, *The art of social engineering*, esitellään Shannon-Weaver -kommunikaation teoria. Teoriasta Hadnagy nostaa viisi pääosa-aluetta:

- Lähde
- Viesti
- Kanava
- Vastaanottaja
- Palaute

Lähteellä tarkoitetaan viestin välittävää tahoa. *Viestillä* viestin sisältöä. *Kanavalla* tapaa, jolla signaali välitetään vastaanottajalle. *Vastaanottajalla* tahoa, joka käsittelee signaalit ja kääntää ne informaatioksi ja *palautteella* jotain kuittausta viestin vastaanotosta tai vastausta viestin

sisältöön. Tämä sama viestinvälityksen ketju pätee kaikessa kommunikaatiossa, oli sitten kyse ihmisten tai tietokoneiden välisestä kommunikaatiosta.

Sosiaalisessa hakkeroinnissa nämä viisi elementtiä on mietitty tarkkaan. Lähdeosassa hakkeri esimerkiksi miettii tilannekohtaisesti miltä hänen tulisi näyttää, mitä hänen kehonkielensä tulisi välittää. Hakkeri miettii myös mitä viestejä hänen pukeutumisensa tai muut tavaransa viestittävät. Hakkeri muotoilee siis oman olemuksensa viestin kanavan ja vastaanottajan perusteella. Kanava on viestinvälitystapa ja hakkeri muotoilee viestinvälitystavan samoin, kuin itse viestin sisällön. Jos viestin kanavana on puhe, hakkeri tekee tiedostettuja valintoja äänensävyystään. Jos taas kanavana toimii sähköposti, hakkeri valitsee ja muotoilee tarkasti sähköpostin kirjoitusasun. Vastaanottajaan ja palautteeseen hakkeri ei voi suorasti vaikuttaa. Hakkerin pyrkii siksi käyttämällä lähdettä, viestiä ja kanavaa siten, että vastaanottaja antaisi hakkerin tavoittelemaa palautetta. Hakkeri onkin jo ennen viestin välitystä varautunut ennalta erilaisiin palautteisiin sekä suunnitellut parhaat reagoitavat eri palautteisiin.

Ihmisten reagointia eri tilanteissa ei voi koskaan täysin varmasti ennustaa. Sosiaalisen hakkeroinnin ideana on suunnitella interaktio mahdollisimman tarkkaan etukäteen ja sen perusteella rakennetaan kommunikaatio, jolla lopulta saavutetaan hakkerin toivoma tavoite.

Sosiaalisen manipulaation tunnistaminen ja välttäminen käytäntöjen kautta

Sosiaalinen manipulaatiohyökkäys on hakkerien käyttämä tapa, joko kerätä tietoa tai saavuttaa ihmisen kautta, jotain sellaista mikä olisi vaikeampaa tai mahdotonta toteuttaa teknisillä keinoilla. Sosiaalisen manipulaatiohyökkäyksen tunnistaminen voi olla hyvinkin hankalaa, sillä se yleensä yritetään naamioida tuiki tavalliseksi ja jopa oikein mukavaksi keskusteluksi.

Tämän oppaan tarkoitus on lisätä tietoisuutta hakkerien käyttämästä nykyaikaisista tavoista kerätä salaista tietoa ja tunkeutua sisäisiin verkkoihin, hyödyntämällä ihmiselle luontaista hyväntahtoisuutta. Englannissa aiheesta puhuttaessa vältetään sanaa manipulaatio ja suositetaan termiä "social engineering". Usein sosiaaliset hakkerit puhuvatkin aiheesta vaikkapa positiivisena vaikuttamisena.

Manipuloinnin skaala on hyvin laaja, eikä kaikki sosiaalinen manipulointi lainkaan toimi edellä mainitulla mukavalla tavalla. Sosiaalinen hakkerointi käsitteenä sisältää kaiken hakkeroinnin, missä hyödynnetään sosiaalista kanssakäymistä. Myös manipuloinnin synkemmät puolet, kuten uhkailu ja kiristys tai mikä tahansa muu ikävä tapa, jolla hakkeria haluaa vaikuttaa yrityksen työntekijöihin.

Tämä opas painottuu enemmän huomaamattomampaan sosiaaliseen manipulointiin, sillä sen avulla hakkeri voi saavuttaa tavoitteensa täysin jälkiä jättämättä. Hakkeri, joka käyttää rikollisia tai muuten säälimättömiä keinoja jättää jälkiä uhrinsa käyttöön. Tämän vuoksi huomaamattomampi tapa mukavalla interaktiolla, jossa uhri saa itselleen jotain kanssakäymisestä, on paljon tehokkaampi.

Sosiaalisen manipulointihyökkäyksen tunnistamisen vaikeuden takia parhaiden käytäntöjen noudattaminen onkin yritysten ja yksityishenkilöiden tietoturvan kannalta ensiarvoisen tärkeää. Christopher Hadnagy korostaa, että ensimmäinen vaihe tietoturvan kannalta on turhan tiedon levittämisen välttäminen. Vähintään yhtä tärkeitä ovat toimivat tietoturvakäytännöt. Parhaiden käytäntöjen kautta voidaan vähentää sosiaalisen manipuloinnin hyödyntämis-

mahdollisuuksia. Tämä vaatii tietoisuuden lisäämistä erityisesti viranomaistahoille, pankeille yms. kohteille, joiden hallussa on paljon arvokkaita tietojamme.

Yritykset sekä yksityishenkilöt saavat päivittäin kalasteluviestejä, joten niitä varten järjestettävät koulutukset ovatkin parhaita tapoja hakkeroinnin onnistumisprosentin pienentämiseksi. Kun tarkastellaan lukuja, rahasummia, vahinkoja ja mainehaittoja viimeisien vuosien ajalta, käy ilmi, että kyseessä on laaja ja vakava uhka. Yksittäisen kansalaisen tulisi itsekkin olla varuillaan, sillä manipulaatiohyökkäykset eivät kohdistu pelkästään yrityksiin. Yksittäisiin ihmisiin kohdistuvat hyökkäykset keskittyvät lähinnä sähköposteihin.

Kalastelusähköposteja varten on lukuisia teknisiä filttäreitä, mutta ne eivät voi estää riittävän hyvin tehtyjä viestejä, sillä samalla ne estäisivät myös oikeata sähköposteja. Ihmisten vastuulle jää päätellä, kuka lähestyy häntä hyvällä tarkoituksella ja kuka taas lähestyy pahoilla tarkoituksilla.

Tekniset tietoliikenne-estot voivat olla tietyn sähköpostipalvelimen estäminen tai suuremmassa mittakaavassa alueellisen dataliikenteen rajaaminen. Esimerkiksi Venäjältä estetty tietoliikenne lopetti 95 prosenttia Kanadaa kohdistuneesta koronavastaisesta disinformaatiosta.

Tunnistamisen ja välttämisen ero

- luota vaistoon ja hälytyskelloihin
- kirjaa ylös aina, jos jostain syystä tilanteessa sinun olisi pitänyt ohittaa tietoturvaprotokolla ja miksi et sitä ohittanut. Tällaisten tilanteiden raportointi auttaa tunnistamaan kaavoja toistuvista tapahtumista.

Tässä oppaassa tarkoitetaan tunnistamisella sitä, että kohde tajuaa häntä manipuloitavan tai vähintäänkin hänellä soi hälytyskellot - että nyt kaikki ei ole hyvin tai tämä kysely tehdään minulta tiedonsaamistarkoituksella. Välttelyn tarkoitus on opastaa parhaiden käytäntöjen noudattamisen tärkeyttä, jotta voidaan välttää luottamuksellisten tietojen antaminen tai esimerkiksi pääsy ei-sallitulle alueelle.

Välttelykäytännöllä tavoitellaan myös sitä, että työntekijöiden ei tarvitsisi olla koko ajan karvat pystyssä varuillaan ja epäillä jokaista asiakasta tai ihmistä ylipäänsä. Käytäntönä voi esimerkiksi olla, että asiakkaan sähköpostia varmistettaessa sitä ei kerrota asiakkaalle vaan asiakas kertoo sen itse. Näin vältetään automaattisesti luovuttamasta asiakastietoja, vaikka asiakasta ei olisi varmennettu.

Huomaamisen ja tunnistamisen tärkeyttä ei tässä oppaassa ole tarkoitus vähätellä laisinkaan, koska niistä saatava hyöty voi olla todella merkittävä. Vain tunnistetut tapaukset voidaan raportoida ja niihin reagoida ja vaikuttaa. Tietoturvallisen ajattelun ei kuitenkaan tarvitse johtaa siihen, että sosiaalisissa kanssakäymisissä jokaista vastaan tulijaa tarvitsisi aina erityisesti epäillä.

Miten löytää tasapaino terveen vainoharhan ja normaalin altruistisen auttamishalun välille?

Hyvä neuvo on noudattaa käytäntöjä suorastaan robottimaisesti, koska hakkerit hyödyntävät muun muassa empatiaa. Nämä käytännöt tulisikin olla vain rajattuna tietoturvan kannalta tärkeisiin tietoihin ja tiloihin. Empaattisen ja inhimillisen palvelun pitäisi toteutua muilla osa-alueilla, mutta tietoturvan kannalta käytännöistä ei voi joustaa.

Tunnistaminen ja reagointi

Christopher Hadnagy antaa *Human Hacking book* -kirjassa seuraavan esimerkkitapauksen:

Hadnagy menee vastaanottoaulaan alakuloisen oloisena ja kantaa kahvista vettyneitä papereita kansiossa. Hadnagyn lähestyessä vastaanottotiskiä virkailija huomaa hänen alakuloisen ilmeensä ja kehonkielensä ja kysyy kuinka hän voisi auttaa. Hadnagy kertoo pre-tekstinsä, jossa hänellä on työhaastattelu alkamassa ja miten tärkeä työmahdollisuus hänelle on. Matkalla haastatteluun ajaessaan autoa tielle juoksi koira ja hän äkkiä koira väistäessään läikytti kahvit hänen ansioluettelolleen. Hadnagy kertoo vastaanottovirkailijalle, että hänellä on USB-muistitikulla ansioluettelo ja kysyy voisiko virkailija tulostaa hänelle uuden ansioluettelon, koska hän ei millään ehdi enää muualle sitä tulostamaan. Hadnagyn sympaattisen tarinan ja kiireellisen tilanteen vuoksi virkailija tuntee empatiaa häntä kohti ja suostuu tulostamaan hakkerin ansioluettelon, vaikka tulostaessaan hän huomaa tarran, joka kieltää ulkopuolisten USB-laitteiden liittämisen tietokoneeseen. Hadnagyn USB-muistitikulle oli ladattu haittaohjelmalla, joka antaa Hadnagyn tiimille etähallinnan virkailijan tietokoneeseen.

Esimerkkitapauksessa vastaanottovirkailija siis tietoisesti ohitti tietoturvakäytännön, jonka tarkoitus on suojata juuri tämän kaltaisilta hyökkäyksiltä. Ohittaessaan mitättömältä tuntuvan käytännön, virkailija vaaransi koko yrityksen tietoturvan. Selkeiden tietoturvakäytäntöjen hyvä puoli on siinä, että ne voidaan nähdä absoluuttisina. Esimerkiksi tässä tapauksessa kieltä ulkoisten USB-laitteiden liittämisestä on selkeä. Virkailija olisi voinut vedota siihen, että ei voi auttaa, vaikka kuinka olisi halunnut. Vaikka virkailija tilanteessa tuntisikin syyllisyyttä, voisi hän silti vedota tietoturvakäytäntöjen noudattamiseen.

Miksi tällaisesta mitättömän oloisesta tapauksesta pitäisi kirjoittaa raportti?

Otetaan esimerkiksi skenaario, jossa hakkeriryhmä yrittää vastaavaa temppua ja vastaanottovirkailija toimii käytäntöjen mukaan ja kieltäytyy tulostamasta ansioluetteloa ja liittämästä USB-muistitikkaa virkailijan tietokoneeseen. Kun manipulaatiohyökkäys epäonnistuu tiukkojen käytäntöjen takia, hakkeri poistuu paikalta tarkoituksenaan kokeilla seuraavana päivänä uudestaan. Aikaisemman selvitystyönsä perusteella hakkeri on saanut selville, että seuraavana päivänä on eri virkailija töissä. Kun hakkeri yrittää samaa uudestaan, on uusi virkailija lukenut edellisen päivän raportin ja tunnistaa tilanteen. Näin hän suhtautuu hakkerin aiheuttamaan empatiaryöppyyn kriittisesti ja noudattaa samaa käytäntöä. Kun myös uusi vastaanottovirkailija kirjoittaa lyhyen raportin ja kaava tunnistetaan, voidaan varoittaa yrityksen muita työntekijöitä yrityksistä saada ulkoisia USB-laitteita liitettyä yrityksen laitteisiin.

3. Vaikuttamisen keinoja ja esimerkkejä

Hyökkäyksen valmistelu

Koska sosiaalinen manipulaatiohyökkäys on huolellisesti suunniteltu hakkerointioperaatio, on luonnollisesti sen ensimmäinen vaihe itse valmistelu.

Disc on yksi työkalu, jolla hakkerit mukailevat omaa käytöstänsä kohdehenkilöön vaikuttamista varten. *Disc*-mallin esitti jo vuonna 1928 professori William Molton Marston, *Emotions of normal people* -kirjassa. *Disc*-mallissa ihmiset jaetaan neljään persoonallisuustyyppiin. Nämä neljä persoonallisuustyyppiä ovat:

- hallitseva (dominant)
- vaikuttaja (influencer)
- vakaa (steady)
- harkitseva (conscientious)

Disc-termi on lyhenne tyyppien englanninkielisistä alkukirjaimista.

Hakkerit tunnistavat oman *disc*-profiilinsa ja yrittävät selvittää kohteensa *disc*-profiilin ja tilanteen tarpeen mukaan hyödyntää näitä persoonallisuuspiirteitä tavoitteensa saavuttamiseksi. Esimerkiksi hallitsevalle tyyppille persoonalle hakkeri voi esiintyä kuuliaisena ja nöyränä tai vaikuttaja -tyypille vastaavasti esiintyä määrätietoisena tai jopa aggressiivisena. Vakaa tyyppille hakkeri voisi taas mukailla käytöstään ystävälliseen ja empaattiseen suuntaan ja pyytää häneltä suoraan apua. Harkitsevalle tyyppille hakkeri voisi taas esittää tarpeensa perustellusti ja rationaalisella tekosyillä. Persoonallisuustyypit ovat vain hyviä yleistyksiä, mutta jokainen meistä kallistuu edes vähän johonkin näistä persoonallisuustyypeistä. Mitä paremmin hakkeri pystyy tunnistamaan kohteensa persoonallisuuspiirteitä, sitä paremmin hakkeri voi *pre*-tekstin sopeuttaa kohteelle sopivaksi.

Sig (social intelligence gathering) tarkoittaa sosiaalista tiedon keräämistä. Helpoin tapa hakkerille on yleensä kerätä tietoa sosiaalisesta mediasta, jonne ihmiset anteliaasti jakavat hyvinkin henkilökohtaisia asioita. Vaikka sosiaalisessa mediassa työntekijä ei kertoisikaan yrityksestä suoraan, voi sieltä silti saada selville hyödyllistä tietoa myös hänen työelämästään. Vaikkapa kollegoista, joita hänellä on Facebook-kavereina. Hakkeri voi myös ottaa aktiivisemman roolin tiedonkeruussa, esimerkiksi luomalla valeprofiilin LinkedIn-palveluun ja lähestyä yrityksen työntekijöitä siellä viesteillä. Tiedonkeruu voi tapahtua myös harmittoman oloisena keskusteluna kahvilassa tai kadulla.

Pre-teksti -termiillä tarkoitetaan tiedon hankkimista valheellisin tai väärin perustein. Tässä yhteydessä *pre*-teksti -käsite laajenee - ei pelkästään arkaluontoisten tietojen saamiseen vaan tilannekohtaisen tavoitteen saavuttamiseen. Hakkeri voi hyödyntää *pre*-tekstiä esiintymällä auktorisoituna henkilönä tai luomalla valheellisesti surullisen tapahtuman herättääkseen vastaanottovirkailijan empatian.

Osana hakkerin luomaa roolia on roolin sopiva itseluottamus ja rekvisiitta. On siis tärkeä suhtautua vastaantulijoihin kriittisesti, vaikka kuinka he näyttäisivät kuuluvansa joukkoon. Eli pelkkään ulkomuotoon ei voi luottaa ja arkaluontoisista asioista ei tule keskustella tuntemattomien kuullen, vaikka kuinka asianmukaisilta he vaikuttaisivatkaan.

Pre-teksti -esimerkki

Christopher Hadnagy kertoo *Human Hacking book* -kirjassa seuraavan tarinan kehittämästään tehokkaasta pre-tekstistä:

Hadnagyn tiimi oli testaamassa erään yrityksen asiakaspalvelun tietoturvaa ja tehtävänä oli saada asiakaspalvelusta puhelimitse sellaista tietoa, mikä ei heille kuulunut. Hadnagyn tiimi oli kehittänyt pre-tekstin, jossa puhelimesta puhuu HR-esihenkilön avustaja ja taustalla HR-esihenkilö huutaa tuskissaan synnytyksen aikana. He loivat tilanteeseen tekosyn tietojen saamiseksi. He tarvitsivat tietoja, koska synnyttävän esihenkilön piti saada palkat laitettua maksuun ajoissa.

Tämän pre-tekstin avulla he välttivät tunnistamisen ja henkilöllisyyden varmistamisen, kun asiakaspalvelija ei saanut synnyttävää esihenkilöä puhelimeen vaan keskustelun kävi avustaja. Tällä pre-tekstillä Hadnagyn tiimi herätti asiakaspalvelijassa empatiaa synnyttävää naista kohtaan ja syyllisyyden tunteita siitä, että asiakaspalvelija joutuisi olemaan esteenä palkkojen maksamiselle ajoissa. Palkkojen maksun aikataulun luoma kiireen tunne ja synnytystilanteen luoma paine saivat työntekijän paljastamaan tiedot joita Hadnagyn tiimi kalasteli.

Sosiaalisessa hakkerointioperaatiossa, tai ylipäättään hakkerointioperaatiossa, on monia vaihtelevia vaiheita. Jokainen hakkerointi, jossa on osana sosiaalinen puoli, alkaa tiedonkeruulla ja toimivan pre-tekstin rakentamisella.

Kalastelusähköpostit ovat viestejä, joissa hakkeri yrittää saada vastaajan klikkaamaan haitallista linkkiä, lataamaan haitallisen tiedoston tai muuten saada häntä hyödyttävää tietoa luomalla vakuuttava sähköposti, jossa lähettäjä esiintyy asiallisena tahona. Hyvin luodut kalastelusähköpostit voivat vaikuttaa hyvin aidoilta.

Spooffaus on termi, joka tarkoittaa, että lähettäjä muuntaa lähetysosoitteensa esimerkiksi niin, että sähköposti näyttää tulleen työntekijän esimieheltä. Siksi pelkkä lähettäjän osoitteen tarkistus ei vielä ole riittävä vahvistus viestin aitoudesta.

Vishing on puhelimitse tapahtuvaa tietojenkalastelua. Vishingillä kerätään tietoja tai pohjustetaan vaikka haittaohjelman lähettämistä sähköpostilla. Vishingissä voidaan myös hyödyntää spooffausta ja vaihtaa numero näyttämään tuttua numeroa.

Smishing on tekstiviestitse tapahtuvaa tietojenkalastelua. Toimintamalli on samanlainen kuin sähköpostien kanssa. Lähinnä on tärkeä tiedostaa, että tekstiviestikään ei ole automaattisesti luotettava kanava. Samalla tavalla, kun puhelimitse, myös smishingissä voi lähettäjän numeron spooffata.

Spooffauksen välttämiseksi paras käytäntö on itse ottaa yhteys, joko soittajaan tai sähköpostin lähettäjään. Spooffaus on hyvä tiedostaa mahdollisuutena esimerkiksi, jos puhelimesta ääni ei kuulosta tutulta, mutta asiaan ei tarvitse alkaa vainoharhaisesti suhtautumaan.

Whaling ja *spreaphishing* ovat kalastelusähköpostien muotoja, jossa kohteen valintaan panostetaan ja kohteeseen tutustutaan etukäteen. Kerättyjen tietojen perusteella kalastelusähköpostit muotoillaan alusta asti kohteelle mahdollisimman kiinnostavaksi. Näissä viesteissä huomioidaan muun muassa kohteen kommunikaatitapa. Jos esimerkiksi kyse on johtajasta, joka kommunikoi lyhytsanaisesti ja pelkästään asiaa, hänelle lähetetään lyhyt ja ytimekäs viesti. Viestissä kerrotaan selkeästi mitä lähetetyn linkin takana on ja miksi se häntä kiinnostaa.

Tiedon johdattelu (eliciting)

Hyvän suhteen luominen kohteen ja hakkerin välille sisältää huolellisesti rakennetun kommunikaation. Tiedon johdattelu (eliciting) on keino, jolla hakkeri keskustelun yhteydessä johdattelee kohteen kertomaan haluamiansa tietoja. Hakkeri voi esimerkiksi jakaa itse kohteelle luottamuksellisen oloista tietoa, jotta kohde vastavuoroisuuden takia kertoisi hakkerille luottamuksellista tietoa. Samassa yhteydessä tai erikseen hakkeri voi normalisoida luottamuksellista tietoa tai vähätellä sitä. Hakkeri voi esimerkiksi mainita miten salasanat ovat nykyään jo tarpeettomia ja kirjautumiset vahvistetaan jollain muulla tavalla. Sitten hakkeri kertoo kohteelle oman keksityn salasanansa. Näin hakkeri on herättänyt kohteen vastavuoroisuudenhalun sekä vähätellyt salasanan kertomisen tärkeyttä ja normalisoinut niiden jakamista jakamalla omansa. Kohde ei tietenkään välttämättä vastaa tähän keskusteluun omalla salasanallaan, mutta yksinkertaisuudessaan näin helposti joltain kohteilta voi sen saada.

Ihmiset toimivat luonnostaan vastavuoroisesti. Jos joku pitää sinulle ovea, pidät sinä hänelle auki seuraavaa ovea. Vastavuoroisuuden periaate on yksi keino, jolla hakkerit yrittävät myös hankkia tietoja kohteista. Luottamuksellisen tiedon johdattelun välttäminen on hyvin haastavaa, mikäli kyseessä on taitava hakkeri. Tällöin pitää vain seurata tietoturvakäytäntöjä tiedon jakamisesta, vaikka hakkeri saisi ne kuulostamaan turhilta tai saisi kohteen vakuutettua, että hänen pitää tehdä hakkerille vastapalvelus.

4. Hyökkäyksen välttäminen käytäntöjen kautta

Mitä ovat parhaat käytännöt?

Tietoturvassa *parhaat käytännöt* -termillä tarkoitetaan yleisiä ohjeistuksia jokapäiväiseen toimintaan niin kotona kuin töissä. Parhaat käytännöt ovat protokollia, jotka tulee suhteuttaa tietoturvan tasoon. Tietoturvaso määräytyy kohteen tärkeyden perusteella. Yrityksen etuovilla tietoturvan taso on pienempi kuin yrityksen palvelinhuoneessa.

Esimerkki kulunvalvontaprotokollasta pääovella

Matkapuhelimia valmistava yrityksen etuovella on vartija, joka päästää työntekijät ja vierailijat sisään tunnistamisen jälkeen. Vartijalla on nimilista työntekijöistä ja vierailijoista. Työntekijät ja vierailijat näyttävät kuvallisen henkilötunnuksen, jota verrataan nimilistaan. Pääoven protokolla on tiukka, koska yritykseltä voi saada tärkeitä tietoja pelkästään fyysisellä pääsillä rakennukseen.

Esimerkki kulunvalvontaprotokollasta palvelinhuoneessa

Yrityksen palvelinhuoneessa tietoturvan tärkeys on merkittävämpi ja protokollat tiukemmat. Yrityksen palvelinhuoneeseen pääsyn yhteydessä työntekijän tavarat tarkistetaan ja sinne saa viedä vain tavaroita, jotka ovat hyväksytyjen listalla. Listalta voidaan rajata pois esimerkiksi kamerat ja matkapuhelimet. Turvaluokitustarkistuksen jälkeen työntekijät päästetään portista, josta mahtuu yksi kerrallaan.

Tietoturvaso suhteuttaminen kohteen tärkeyteen johtuu siis siitä, että tietoturvasuus ei saisi kohtuuttomasti hankaloittaa jokapäiväistä toimintaa. Mikäli tietoturvaprotokollat ovat kohtuuttomia, voi se johtaa välinpitämättömyyden suhtautumiseen niihin. Siksi on myös tärkeää, että protokollia valvovat työntekijät ymmärtävät mitä varten protokollat ovat olemassa. Asiaa voidaan koulutuksissa havainnollistaa riskikuvilla ja protokollia testata palkkaamalla valkohattuhakkereita suorittamaan tunkeutumistestausta.

Tietoturvakäytännöt käytännössä

Kulunvalvonta

Kulunvalvontakäytäntö tulee toteuttaa tapauskohtaisesti ja siksi sitä ei tässä voi tarkasti rajata. Kulunvalvonnassa on hyvä määritellä valvontakamerat kuvaamaan tärkeitä pisteitä ja tiedostaa niiden katvealueet. Kohteen turvaso riippuen, kulunvalvonnalla tulisi estää vanavedessä kulkeminen, sillä se on yksi kätevistä tavoista, joita hakkerit käyttävät ohittaakseen avainkortteja ja lukittuja ovia. Käytäntöä voi varmentaa portilla tai vastaavalla, joka päästää yhden henkilön kerrallaan. Työntekijöiden on kuitenkin helppo ohittaa porttikäytäntöjä ja taitava hakkeri voi ahtaa itsensä samaan aikaan portista läpi. Mikäli resurssit riittävät, on protokolla hyvä kahdentaa turvamiehellä.

Kulunvalvonnassa tulee huomioida myös pääsy asiakirjoihin ja mappeihin, jotka helposti jäävät lojumaan, tai ovat lukollisessa toimistokaapissa mutta kaappi onkin jäänyt auki. Tietoturvakäytäntöksi tulee ottaa, että kaappi tulee aina lukita käytön jälkeen. Helposti voi ajatella, että kaapit ovat toimistossa missä vierailijat eivät pyöri. Tässäkin tapauksessa osaava

hakkeri, vaikka remonttimiehenä esiintyessään, voi kuitenkin päästä toimistokäytävälle vapaasti liikkumaan.

Saattajakäytäntö

Saattajakäytäntö, kuten muutkin, on hyvin riippuvainen kohteen turvaluokituksesta. Mikäli kohteessa on tarkka kulunvalvonta, se ei saisi tarkoittaa, että etuovesta päästyään vierailijat saisivat vapaasti liikkua talossa. Jo pelkästään sillä, että vierailijoita saattaa koko ajan joku yrityksen työntekijöistä, hankaloitetaan suuresti hakkerin toimintaa. Tällä käytännöllä pystytään hyvin estämään vahingollisten, esimerkiksi USB-muistitikun jättäminen näkyville siinä toivossa, että yrityksen työntekijä itse laittaisi sen kiinni tietokoneeseen. USB- muistitikut ovat myös yksi yleisimmistä tavoista saada haittaohjelma yrityksen tietokoneelle. Christopher Hadnagy kertoo *Human Hacking book* -kirjassaan useammankin kerran hyödyntäneensä tätä keinoa, jos hän on saanut pääsyn sisään rakennukseen tai saanut vaikka tilapäisen luvan käydä vessassa. Hän on jättänyt sinne kirjekuoressa USB-muistitikun, jonka yrityksen työntekijä on löytänyt ja laittanut työkoneeseensa kiinni ja haittaohjelma on alkanut toimia.

Tietämystarveperiaate

Christopher Hadnagyn mukaan tietoturvan ensimmäinen askel on turhan tiedon levittämisen välttäminen. Yritysten olisi hyvä muodostaa työntekijöitä varten selkeä tietämystarveperiaate eli tiedon levittämisen periaate. Yritykset eivät tietenkään voi kontrolloida mitä työntekijät puhuvat vapaa-ajalla. Siksi yrityksen olisi tärkeä myös avata tiedonlevittämisen periaate esimerkiksi koulutustilaisuudessa. Koulutuksessa voidaan käydä läpi mitä tietoa ei kannata levittää ja esimerkkien kautta havainnollistaa minkälaisista aiheista työntekijät voivat puhua. Mitä yleistä tietoa voi kertoa työpaikastaan ja voiko esimerkiksi kertoa työntekijöiden aikatauluista. Toimivalla tiedon levittämisen periaatteella voidaan rajoittaa tietoja, joita hakkeri voisi mahdollisesti hyödyntää.

Tietämystarveperiaate kattaa myös sisäisen tiedon levittämisen. Eli kerrotaan vain se tieto niille työntekijöille, jotka sitä tarvitsevat. Mitä ei tiedä ei voi vahingossa paljastaakkaan.

Tietämystarveperiaate kattaa myös tiedon jakamisen asiakkaille. Tästä ensimmäisen käytännön tulee olla asiakkaan tunnistaminen ja vahvistaminen. Luonnollisesti mitään asiakastietoja ei saa kertoa kuin asiakkaalle itselleen. Tätä hakkerit hyödyntävät esiintymällä esimerkiksi asiakkaan lähiomaisina tai asiakkaana itsenään. Sen takia asiakkaan vahvistaminen on tärkeää, eikä lähiomaisillekaan asiakkaan tiedot kuulu. Asiakkaillekaan ei tarvitse kertoa muuta kuin niitä tietoja kuin mitä kyseisen asiakkaalle kuuluu tietää. Jos asiakas esimerkiksi keskustelun yhteydessä kysyy miten yritys säilyttää roskiensa, ei kysymykseen tule automaattisesti vastata. Vaikka tieto roskien säilyttämisestä saattaa kuulostaa mitättömältä, ei se välttämättä sitä ole. Se on tietoa mikä ei normaalisti asiakkaalle kuulu. Työntekijä voi ajatella, että asiakas ei tiedolla mitään tee. Monessa Hadnagyn esimerkissä mainitaan juuri tämän tyyllisen mitättömältä vaikuttavan tiedon olleen kriittistä hyökkäyksen onnistumiselle. Eräs Hadnagyn tuttava onnistui sisällyttämään haittaohjelman kalastelusähköpostiin ja sai yrityksen johtohenkilön avaamaan linkin, koska sai selvillä johtohenkilön keräilevän postimerkkejä. Hakkerille mikään tieto ei ole mitätöntä. Siksi yrityksen asioista tai henkilöistä ei tulisi ulkopuolisille tai sidosryhmille jakaa mitään tarpeetonta tietoa.

Sähköpostikäytäntö

Yritykset ja yksityishenkilöt voivat helposti hyödyntää yleisiä sähköpostipalveluita, kuten Outlook tai Gmail. Yleiset sähköpostipalvelut sisältävät automaattisesti hyvät spam- ja kalastelufiltterit. Mikäli yritys haluaa käyttää jotain vähemmän tunnettua sähköpostiratkaisua, pitäisi silloin myös tarkemmin paneutua sähköpostifilttereiden rakentamiseen. Sähköpostifiltterit ja selaimet eivät kuitenkaan pysty rajaamaan huolellisesti tehtyjä kalasteluhyökkäyksiä tai sivuja, jotka ovat varta vasten kohdennettu osana sosiaalista manipulaatiohyökkäystä. Siksi työntekijöille koulutettu käytäntö antaa kerroksen lisäsuojaa.

Christopher Hadnagy'n kirjoissa mainitaan useampi onnistunut kalasteluhyökkäys, joissa onnistumiseen johti työntekijöiden henkilökohtaisten asioiden hoitaminen työkoneilla. Tämän rajaaminen pois hankaloittaa kalasteluhyökkäyksiä, kun työntekijöiden omiin intresseihin ei pystytä vetoamaan. Tämän käytännön tiukka noudattaminen olisi estänyt aikaisemmin mainitun postimerkkikeräilyn kautta tapahtuneen kalasteluhyökkäyksen johtohenkilöä kohtaan.

Muita hyviä käytäntöjä sähköpostin käytön turvaamiseksi on vieraiden linkkien välttäminen ja kursorin pitäminen linkin päällä ennen sen klikkaamista. Tällöin näkyy koko osoite, jonne linkki vie hyperlinkin sijaan. Sähköpostifiltterit ja tietoturvaohjelmat pystyvät joitain tunnettuja haittaohjelmia estämään, mutta sähköpostin liitetiedostojen avaamisessa on silti hyvä noudattaa varovaisuutta, jos viestin lähettäjä ei ole tunnettu.

Koskaan ei kuitenkaan voi olla varma lähettäjän aitoudesta spoofauksen takia. Tässäkin tapauksessa on hyvä luottaa vaistoon, mikäli viestissä joku asia herättää epäilyksiä. Esimerkiksi jos esihenkilö, joka muutoin käyttää huoliteltua kieltä lyhytsanaisesti, lähettää huolimattomasti kirjoitetun viestin ja vaisto varoittaa omituisuudesta, voi aina lähettäjältä varmistaa tuliko viesti varmasti häneltä.

Kuten muissakin sosiaalisen manipuloinnin tilanteissa, sähköposteissa voidaan hyödyntää kiirettä tai nopean toiminnan tärkeyttä. Tässä tapauksessa hyvä käytäntö on pysähtyä hetkeksi ja ajatella onko asia oikeasti kiireinen vai saako viestin lähettäjä luotua vain vaikutelman kiireestä. Muita hyviä vaaran merkkejä, joista kalasteluyritystä voi tunnistaa ovat:

- lähettäjän vetoaminen luottamuksellisuuteen, eli viestin vaihdosta ei saisi kertoa muille
- viestissä pyydetään jostain syystä joko ylittämään omia valtuuksia tai muuten tekemään jotain normaaliin työnkuvaan kuulumatonta

Koulutuksissa voidaan myös painottaa kriittisyyttä, mikäli viestin sisältö tai lähettäjä omaa piirteitä, jotka altistavat kalastelusähköposteille. Tästä tutkittu esimerkki on miehille kohdistetut viestit, joiden lähettäjänä on erityisen viehättävä nainen. Tämän tyylinen hyökkäystapaa voidaan pohjustaa ottamalla kalastelusähköpostin vastaanottajaan yhteyttä esimerkiksi LinkedIn -palvelun kautta, jossa hakkeri esiintyy viehättävänä naisena. Palvelun kautta tapahtuvassa viestittelyssä hakkeri kertoo lähettävänsä vastaanottajalle sähköpostilla jotain.

Kalastelusähköpostit ovat suuri uhka yrityksen tietoturvalle. Cisco -yrityksen datan mukaan noin 90% tietomurroista johtuu kalastelusähköposteista. Kalastelusähköposteja tulee massiivisia määriä ja ne yleistyvät koko ajan. Joillain aloilla ne saattavat ovat yleisempiä kuin toisilla aloilla. ESET -yrityksen teettämän tutkimuksen mukaan pelkästään vuoden 2021 toukokuun ja elokuun välisenä aikana kalastelusähköpostit yleistyivät 7,3%.

Vuonna 2021 tehdyssä Tessian -yrityksen tutkimuksessa todettiin työntekijöiden saavan keskimäärin 14 haitallista sähköpostia vuodessa. Mikäli näistä edes yksi johtaisi onnistuneeseen tietomurtoon tarkoittaisi se yhtä tietomurtoa työntekijää kohtaan vuosittain. Siksi kalastelusähköpostien tuomaan uhkaan tulisi suhtautua erittäin vakavasti ja noudattaa käytäntöjä huolellisesti.

Who falls for phis. A demographig analysis of phis -tutkimus osoitti, että koulutusmateriaaleilla pystyttiin vähentämään jopa 40% kalastelusivuille syötetystä datasta. Sama tutkimus myös havaitsi yllättäen, että 18-25 -vuotiaat olivat haavoittuvaisin ikäryhmä kalastelusähköposteille. Tämä osoittaa, että koulutuksissa ei kannata tehdä olettamuksia ja niitä tulisi järjestää ihan kaikille työntekijöille.

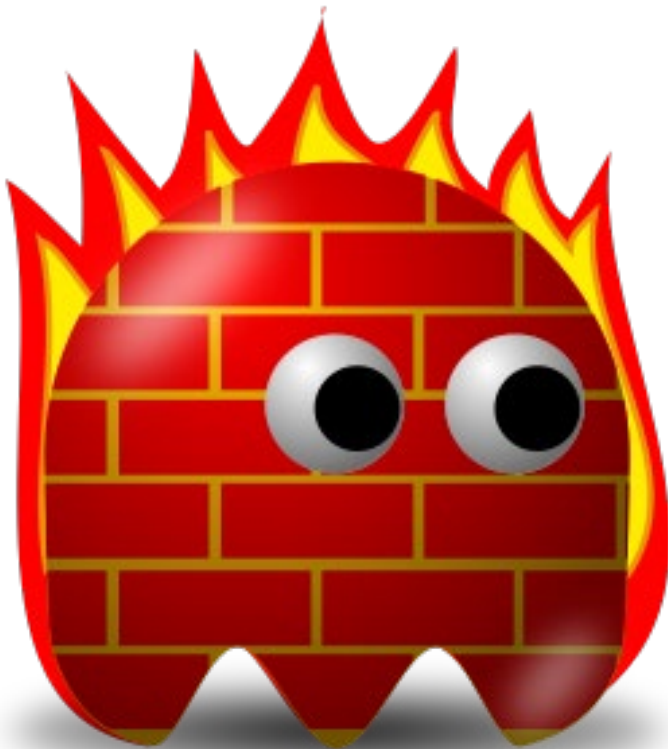
A Personality Based Model for Determining Susceptibility to Phishing Attacks -tutkimus jakaa kalasteluhyökkäyksen kolmeen vaiheeseen, jotka ovat:

- Koukku, eli sähköposti, joka vaikuttaa aidolta
- Houkutin, eli viestin sisältö, joka on muotoiltu saamaan vastaanottajan klikkaamaan linkkiä hakkerin sivustolle
- Saalis, eli sivustolle syötetty data

Edellä mainituissa kahdessa tutkimuksessa huomattiin, että vaikka koulutusmateriaali vähentää vain hiukan linkkien klikkausten määrää, saadaan koulutusmateriaaleilla kuitenkin merkittävästi estettyä kalastellun datan syöttämistä mahdollisesti klikatulle huijaussivustolle.

Kaikkia haitallisia sähköposteja ei koskaan onnistuta estämään. Koulutusten avulla voidaan kuitenkin merkittävästi vähentää arkaluontoisten tietojen syöttämistä kalastelusivustoille ja siten ottaa merkittävä askel kohti tietoturvalisempaa työyhteisöä.

5. Tekninen tietoturva



Käyttöoikeuksien rajaaminen

Tämä periaate on tietyllä tavalla samanlainen kuin aikaisemmin esitelty tietämystarveperiaate. Työntekijöille ei tulisi antaa käyttöoikeuksia, joita he eivät tarvitse. Luonnollisesti työntekijät tarvitsevat tarvittavat riittävät käyttöoikeudet, jotta työn teko ei estyisi käyttöoikeuksien takia. Jos IT-ylläpitovastaava joutuu monta kertaa päivässä sallimaan jonkin käyttöoikeuden työntekijöille, madaltaa se kriittisyyttä kyseisen käyttöoikeuden myöntämiseksi eri tapauksissa.

Käyttöoikeuksia rajaamalla minimoidaan myös haavoittuvuutta. Mitä vähemmän tunnuksia laajoilla käyttöoikeuksilla on, sen vaikeampi niitä on saada käsiin. Mikäli hakkeri saa käsiinsä perustason tunnuksia, pääsee hän käsiksi infrastruktuuriin ja voi mahdollisten haavoittuvuuksien avulla nostaa myös käyttäjätunnuksiensa oikeuksia.

Tietoturva rakentuu kerroksista ja käyttöoikeuksien rajaaminen on käytännöllinen keino luoda jälleen yksi este hakkereille. Kuitenkin tapauskohtaisesti myös hyvin rajattu käyttäjätunnus voi olla sosiaalisen hakkerin hyökkäyksen mahdollistava kanava, jos hän pystyy tunnuksella kirjautuneena esiintymään työntekijänä ja lähettämään viestejä sisäisissä järjestelmissä. Juuri tämän takia jokaiseen tietoturvan kerrokseen, eli tässä tapauksessa rajatuimpiinkin käyttäjätunnuksiin, tulee suhtautua vakavasti.

Kaksivaiheinen tunnistus on yksi tehokkaimmista käytännöistä hankaloittaa hakkerien toimintaa. Kaksivaiheisessa tunnistuksessa on kaksi eri vahvistustapaa, joista toinen voi olla salasana ja toinen esimerkiksi tekstiviestillä tullut vahvistuskoodi. Kaksivaiheinen tunnistus tuo hieman lisähankaluutta arkeen, mutta kaikki tieto mitä et haluaisi kertoa muille pitäisi olla suojattu kaksivaiheisella tunnistuksella.

Salasanakäytännöt

Moni muodostaa salasanojaan omien yksityisten tietojen pohjalta, kuten syntymäpäivä, lemmikin nimi tai lempibändi. Monet ajattelevat kyseiset tiedot yksityiseksi tai sellaisiksi, joita vain hänet tuntevat ihmiset tietävät. Sosiaaliset hakkerit ovat kuitenkin kommunikaation mestareita ja voivat keskustelun yhteydessä saada täysin huomaamatta nämä tiedot selville. Tämän takia salasanakäytännöt auttavat myös ehkäisemään sosiaalista manipulaatiohyökkäystä. Toimiva käytäntö tähän on satunnaisesti generoitu salasana, joka vaihtuu säännöllisesti ja salasanahallintatyökalujen käyttäminen.

Comparitech -yrityksen keräämän статистиikan mukaan, jopa 42% yrityksistä käytetään salasanan hallintaan tarralappuja. Mikäli hakkeri pääsee fyysisesti yritykseen sisälle, saa hän helposti katsottua tarralapuilta työntekijöiden salasanoja. Salasanojen säännöllinen vaihtaminen auttaa, jos hakkeri on keskustelun yhteydessä onnistunut saamaan salasanan selville. Isommat hakkerointioperaatiot voivat olla todella pitkäkestoisia ja näin ollen säännöllinen salasanan vaihtaminen voi joissain tapauksissa olla toimiva este hakkereille. Salasanahallintatyökalut auttavat ylläpitämään hyvinkin monimutkaisia salasanoja, joita hakkerit eivät pysty arvaamaan tai pakkosyöttämällä (brute force) ohittamaan.

Ulkoisten laitteiden liittäminen

Vieraita laitteita ei tulisi missään tapauksessa liittää yrityksen järjestelmiin. Christopher Hadnagy hyödyntää kirjoissaan pariakin eri tapaa viedä haittaohjelma yrityksen laitteisiin hyödyntämällä USB-muistitikkuja. Hyödyntämällä kekseliästä pre-textiä, hän sai vastaanottovirkailijan printtaamaan Hadnagyn muistitikulta hänelle ansioluettelon ja samalla lataamaan tietokoneelleen muistitikulla olleen haittaohjelman. Mikäli Hadnagy pääsee kohderakennukseen sisään, hän jättää USB-muistitikkuja tiloihin lojumaan. Näitä muistitikkuja työntekijät sitten, joko uteliaisuudesta tai auttamishalustaan, liittävät usein laitteisiinsa selvittääkseen niiden sisällön. USB-muistitikut sisältävät haittaohjelman, joka latautuu automaattisesti ja huomaamattomasti. Tärkein keino estää tällainen tapa haittaohjelmapaketin toimittamiselle, on noudattaa tiukasti tietoturvakäytäntöä, jossa koskaan ei saa vieraita USB-muistitikkuja liittää yrityksen laitteisiin.

Lähteet

25+ password statistics. <https://www.comparitech.com/blog/information-security/password-statistics/>

Hadnagy, C. 2018. Social Engineering: The science of human hacking. 2nd ed. Hoboken, NJ: Wiley Publishing.

Hadnagy, C. 2014. Social Engineering: The art of human hacking. Brilliance Audio, unabridged edition.

Cisco. 2018.

<https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>

Parolo, E. 2020. Sosiaalisen manipuloinnin keinot ja niiltä suojautuminen.

<https://urn.fi/URN:NBN:fi:amk-2020052613632>

What is social engineering? <https://www.social-engineer.org/about/>

Palmu, P. 2020. Eteväen tietoturva-asiantuntija: Ihminen on tietoturvan heikoin lenkki!

<https://www.etevat.fi/blogi/ihminen-on-tietoturvan-heikoin-lenkki>

Gragg, D. 2021. A Multi-Level Defense Against Social Engineering.

<https://www.sans.org/white-papers/920/>

Parris, J., Bailey, J., Courtney, J. A Personality Based Model for Determining Susceptibility to Phishing Attacks.

https://www.academia.edu/48717594/A_Personality_Based_Model_for_Determining_Susceptibility_to_Phishing_Attacks

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J. 2010 Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.

https://www.researchgate.net/publication/221514257_Who_falls_for_phish_A_demographic_analysis_of_phishing_susceptibility_and_effectiveness_of_interventions

Downs, J., Lanyon, M., Cranor, L. 2007 Behavioral Response to Phishing Risk

https://www.researchgate.net/publication/221462245_Behavioral_response_to_phishing_risk

Ellis, W. 2019. How spam and phishing filters works.

<https://www.mailpoet.com/blog/how-spam-and-phishing-filters-work/>

25+ password statistics. <https://www.comparitech.com/blog/information-security/password-statistics/>

Purple Sec. <https://purplesec.us/resources/cyber-security-statistics/>

Roshental, M. 2022. Tessian. <https://www.tessian.com/blog/phishing-statistics-2020/>