Tallinna Ülikool

Digitehnoloogiate instituut

Siim Karoman

SOTSIAALMANIPULATSIOONI PÕHIVÕTTED JA VASTUMEETMED

Seminaritöö

Juhendaja: Kaido Kikkas

Tallinn 2016

SISUKORD

SISSEJUHATUS

Töö teema on sotsiaalmanipulatsioon ja selle vastumeetmed. Eesmärk on kirjeldada, kuidas inimesi sotsiaalmanipulatsiooni kaudu mõjutatakse, mis on selle eesmärk ja kuidas rünnakute vastu võidelda. Valisin selle teema, sest see on aktuaalne ja muutub tänapäeva infoühiskonnas järjest olulisemaks. Ma arvan, et ettevõtte töötajaid on oluline sel teemal harida, kuid praegu tundub, et seda ei tehta piisavalt. Võib-olla ei ole olnud mingeid suuremaid probleeme, mis paneks kiirelt tegutsema või eeldatakse, et töötajad ise on piisavalt teadlikud.

Inimesed võivad sotsiaalmanipulatsiooni kogeda nii tööelus kui ka vabal ajal. Me veedame väga palju aega internetis. Paljudel on internet ka telefonis ja seetõttu oleme kogu aeg ühendatud ja kättesaadavad. Vaatamata sellele peaks internetis surfama vastutustundlikult. Info hulk on väga suur ja seepärast ei pruugita tähele panna ohukohti, mis meid internetis varitsevad. Kui inimesed teadvustavad endale võimalikud ohud ja riskid, siis kergem võimalikke rünnakuid vältida.

Töö koosneb neljast suuremast peatükist. Esimeses peatükis kirjeldatakse sotsiaalmanipulatsiooni eesmärke ja selle kasutajaid. Teises peatükis keskendutakse sotsiaalmanipulatsiooni viisidele. Tuuakse välja seitse võimalikku andmete hankimise meetodit ja mõned näited. Kolmandas peatükis kirjeldatatakse tegevusi, mida tuleks teha sotsiaalmanipulatsiooni ennetamiseks. Viimases peatükis on punktide kaupa toodud välja soovitused, mida järgides on võimalik end sotsiaalmanipulatsiooni rünnakute eest kaitsta.

1 MIS ON SOTSIAALMANIPULATSIOON?

Peatüki eesmärk on kirjeldada, mis on sotsiaalmanipulatsioon, mis on selle eesmärk ja kuidas seda igapäevaelus kasutatakse.

Social engineering ehk sotsiaalmanipulatsioon on üks kurjategija ründe viisidest, kuidas saada ligi tundlikule infole. Selleks kasutatakse ära inimeste loomust ja selle nõrkasid kohti. Sotsiaalmanipulatsiooni tehnikat kasutatakse, et saada infot ja teadmisi, mille abil oma rünnakut plaanida. Selle asemel, et kasutada keerukaid programme, millega süsteemi otse rünnata, üritab manipulaator saada infot otse inimese käest. Proovitakse ennast esitleda asutuse töötaja, kliendi, ülemuse või mõne muu isikuna, kes on seotud asutuse või selle klientidega. Ründaja proovib saada teada võimalikult palju infot: töötajate nimesid, kasutajaid, serveri nimesid, IP-sid, paroole jne. Peale selle võib ta üritada uurida üldiselt asutuse süsteemi ülesehituse kohta ja selle võimalikke nõrkasid kohti. Asutuse süsteem võib olla väga turvaline ja murdmatu, aga inimese faktor jääb alati. (Greavu-Şerban & Şerban 2014, 5.)

Sotsiaalmanipulatsiooni eesmärk on inimesi manipuleeirda avaldama infot nii, et nad ise ei saaks arugi, et on avaldanud midagi, mida nad ei tohiks. Neile jääb mulje, et midagi pahatahtlikku ei ole toimunud. Enamasti ei jää see hetk, kui rünnak on toimunud ja info avaldatud, meeldegi, kuna inimeste jaoks midagi kahtlast ei juhtunud ja see oli osa igapäeva tegevustest. (Greavu-Şerban & Şerban 2014, 6.)

Sotsiaalmanipulatsiooni on hakatud kasutama üha rohkem, sest traditsionaalsete rünnakute efektiivsus on kahanenud. Inimestest sõltumatute turvasüsteeme on hakatud järjest rohkem kasutama ja need on muutunud tõhusamaks. Ründajad on võtnud tarvitusele alternatiivmeetodid, mis kasutavad ära nii tehnoloogia vead, kui ka inimeste omad. Samuti on probleemiks see, et sotsiaalmanipulatsiooni levikust ei olda veel nii teadlikud. (Janczewaki & Fu 2010.)

Turvatunne on tihti illusioon, mida võimendab veel kergeuslikkus, naiivsus või ignorantsus. Lõppkokkuvõttes saab sotsiaalmanipulatsioon toimida siis, kui inimesed ei pööra tähelepanu headele turvakommetele. Paljud IT-firmad on arvamusel, et nad on teinud oma ettevõtte rünnakutele immuunseks, kui nad on võtnud kasutusele standardturvameetmed. Näiteks tulemüür, liikumisandurid ja tugevamad autentimissüsteemid, nagu ajapõhised *token*'id ja

biomeetrilised *smart*-kaardid. Need kes arvavad, et ainuüksi turvatoodetest piisab täielikuks turvalisuseks, petavad ennast. Varem või hiljem kogevad nad turvavigu. Arendajad parendavad koguaeg turvalisustehnoloogiat ja see teeb järjest raskemaks ründajatel tehnoloogilises pooles nõrkusi leida. Seega pööravad ründajad järjest rohkem tähelepanu inimlikele nõrkustele, mida saaks ära kasutada, sest seda kergem leida kui nõrkust tulemüüris. (Mitnick & Simon 2002, 12-13.)

Ohu hindamisel tuleb kasuks ründaja motivaatsiooni teadmine ning tema oskuse tase. Inimene peaks teadma mis info peaks kindlalt olema kaitstud, et luua süsteemid selle kaitsmiseks. Üldiselt jagunevad ründajad kaheks: professionaalid, kes teenivad raha om rünnakutega ja amatöörid, kes tahavad tõestada oma oskuski või saada tunnustatud/nähtud läbi oma tegude. (AL-Johani & AL-Msloum 2013, 235.)

Amatöörhäkkerite alla kuuluvad näiteks häkkerid kes ei tee seda rahalisel või väljapressimise eesmärgil, vaid näiteks niisama huvi pärast või et tekitada pahandust. Nende motivatsioon on näidata oma oskuski ja näidata, et nad saavad seda teha. Siia alla kuuluvad ka aktivistid, kes oma tegevusega võitlevad millegi ideoloogilise või regligioosse eest. Enamasti on nad rohkem professsionaalid kui amatöörhäkkerid. (AL-Johani & AL-Msloum 2013, 235.)

Üks suurimaid ajendeid rünnakuteks on rahaline kasu. Ründaja soovib saada lihtsalt rohkem raha või tunneb, et ta väärib rohkem raha. Sellistele eesmärkidele võivad kallutada ka rahalised probleemid. Ajendiks võib olla ka kättemaks. Kätte saab maksta nii inimesele, kui ka kogu asutusele. Näiteks inimene, kes on vallandatud või mingit muud moodi väärkoheldud võib tahta maksta oma tööandjale kätte. Ta on firmas töötanud ja teab firmasisest infot ja asjade käiku. Seega on tal lihtsam kahju tekitada. Lisaks aitavad tööl oldud ajal saadud tutvused ja sõbrad. (Allen 2007, 6.)

Enamjaolt on sotsiaalmanipulaatorid hea suhtlemisoskusega. Nad on sarmikad, viisakad ja nendega on lihtne suhelda. Need on omadused mis aitavad luua usaldust. Kogenud sotsiaalmanipulaator on võimeline saama ligi põhimõtteliselt igale infole kasutades oma strateegiaid ja meetodeid. Tehnikatargad on vaeva näinud, et luua informatsiooni kaitse lahendusi, et minimaliseerida riske, mis kaasnevad arvuti kasutamisega. Nad on aga jätnud suuresti arvestamata suurima vea – inimfaktori. Inimese intellektuaalsusele vaatamata on inimene ikkagi kõige suurem turvarisk. (Mitnick & Simon 2002, 16-17.)

Üheks tuntuimaks sotsiaalmanipulaatoriks võib pidada Kevin Mitnicki, kes on raamatute „The Art of Deception“ ja „Ghost in the Wires: My Adventures as the World's Most Wanted Hacker“ autor.

Aastal 1983, olles üliõpilane, suutis Mitnick saada sissepääsu ARPANet-i, mis oli Interneti eelkäija, mida kasutasid suured korporatsioonid, ülikoolid ja USA sõjavägi. ARPANet-i pääsemine andis talle ligipääsu Pentagoni ja kõikidele kaitseministeeriumi failidele. Mitnick tegelikult minigeid andmeid ei varastanud. See oli pigem võimalus ennast tõestada. Hiljem, kui sellest teada saadi, Mitnick arreteeriti ja ta kandis lühikest karistust noorte kinnipidamisasutuses. See oli tema esimene karistus illegaalselt arvuti süsteemi sissemurdmise eest. Pärast seda oli Mitnick jätkuvalt FBI radaril ja sattus mitmete uurimiste huviorbiiti. (Iozzio 2008.)

1994 aasta suutis Mitnick, olles üleriigiliselt tagaotsitav, aastaks tööle saada advokaadibüroose, kus ta esitles ennast nime all Eric Weiss. Mitnick läks oma kuritegude eest siiski lõpuks vangi. Nüüdseks on ta oma karistuse ära kandnud ja töötab edukalt turvanõustajana, kasutades oma varem hangitud teadmisi ja kogemusi. (Mitnick & Simon 2011.)

2 SOTSIAALMANIPULATSIOONI PÕHIVÕTTED

Pragusel infoühiskonna ajastul on väga palju erinevaid võimalusi, kuidas inimeste käest tundlikku teavet kätte saada. Ühelt poolt võib läheneda inimesele otse, teisalt võib appi võtta digitaalsed vahendid.

Meetodi valik oleneb enamasti ründaja ajast, kannatusest, isiksusest ja järjepidevusest. Samuti tuleb siin mängu petmise oskus. Et murda süsteemi, peab ründaja leidma viisi, kuidas saada kätte info süsteemi kasutaja käest. Ründaja saab kätte tundliku info või petab/manipuleerib ta tegema midagi, mis tekitab suure turvaaugu süsteemis, mida ründaja saab ära kasutada. Ükski tehnoloogia ei saa sellise tegutsemise eest kaitsa. Sotsiaalmanipulaatorid kasutavad ära töötajaid ja süsteemi kasutajaid, et läbi murda turvasüsteemidest. (Mitnick & Simon, 2002, 16.)

Järgnevalt on välja toodud levinumad sotsiaalmanipulatsiooni viisid, mida manipulaatorid kasutavad.

2.1 Vaatlemine

Lihtne vaatlus võib anda palju infot. Vaatluse teel on võimalik tuvastada, kas rünnatav asutus kasutab võtmeid, kaarte, või muid lukustusviise. Saab teada, kas asutusel on väljas suitsunurk, kas sinna pääseb ligi ilma, et peaks kuskilt midagi avama või kellelgi mingit dokumenti näitama. Peale selle on võimalik näha, kui suur on asutuseväline turvatase, kas ja kus on kaamerad, kas on valvureid, kas majast väljas asub väliseid seadmeid, nagu elektrikilbid või ventilatsioon. Lihtsa vaatluse abil on veel palju muud võimalik teada saada, eriti kui olla kannatlik ja dokumenteerida oma vaatlusi. (Hadnagy 2013, 67.)

2.2 Üle õla vaatamine (*shoulder surfing*)

See on oskus saada ligi informatsioonile lihtsalt vaadates kasutaja arvuti ekraani ja jälgides tema tegevust (nt vaadelda mida ja kuhu trükitakse). Seda on võimalik teha aknast sisse vaadates, ukse vahelt või koridorist piiludes või lihtsalt vestlust pealt kuulates. Inimesed, kes tegelevad tundliku infoga, peavad olema teadlikud oma ümbrusest. Tähele tuleks panna, kes on lähedus ning kes võib kuulata või vaadelda. Parooli trükkimisel tuleks seda võõraste pilkude eest varjata. Inimesed, kes teevad tööd või tegelevad tundliku infoga avalikus kohas,

peaksid jälgima, kuhu nende ekraan on suunatud. Tuleks vältida arvuti ekraani suunamist kellegi vaatevälja. (Cyber Security Tips 2012, 1.)

2.3 Prügikastis tuhnimine (*dumpster diving*)

See tähendab sihtmärgi prügi läbi otsimist. Eesmärk on leida kasulikku infot. Info mis prügist leitakse võib olla väga kasulik. Enamus inimesi ei pööra suurt tähelepanu sellele, mis nad kodus ära viskavad: telefoniarved, krediitkaardi andmed, ravimikarbid, pangakaardi/kontoga seotud paberid, tööga seotud dokumendid jne. Tööl peaks töötajatele selgeks tegema, et prügist on võimalik leida infot, mida saab pahatahtlikult ära kasutada. (Mitnick & Simon, 2002: 147.)

2.4 Sappavõtmine (*tailgating*)

Sappavõtmine tähendab maja sisenemist inimesele järel, kellel on õigused majja sisenemiseks. Asutused võivad investeerida kümneid tuhandeid dollareid uste turvasüsteemidele, mida on võimalik läbida ainult uksekaardi või koodiga. Nii saavutatakse olukord, kus ukse saab avada ainult inimene, kellel on selleks õigus. Selle süsteemi nõrkuseks on, et süsteem ei kontrolli mitu inimest siseneb, kui uks on avatud. Kui üks õigustega inimene avab ukse, siis temale võib järgneda keegi veel, kellel ei ole õigusi ise siseneda. (Cimapa 2011, 64.) Samuti on inimese loomus ja viisakus siin olulised faktorid. Keegi ei taha teisel nina ees ust kinni lüüa. Kui liigutakse kellegagi koos, siis ikka hoitakse ust enda taga kauem lahti, et järgnev inimene saaks uksest sisse. (Kikkas 2016, 2.)

2.5 Maskeerimine

Töötaja ei ole ainuke, kelleks ründaja ennast maskeeruda võib. Kulleriks, töömeheks või isegi külaliseks riietamine annab ründajale hea võimaluse, kuidas majja sisse pääseda. Enda kulleriks maskeerumine on suhteliselt lihtne. Lihtsaim viis on lihtsalt tunked osta. Peale selle on võimalik osta ka mõne tuntud kullerfirma riideid. Need on saadaval näiteks e-bays või mõnel muul veebioksjonisaidil. (Jones 2004, 10.)

Üks tüüpiline tehnika on läheneda sissepääsule raskete kastidega ja loota, et leidub abivalmis inimene, kes ukse avab. Kui töötaja peaks ründajaga rääkima hakkama siis veenab ründaja töötajat, et tal on vaja sisse pääseda. Alati võib aidata mõne kõrgemal kohal töötava inimese

nime mainimine. Samuti võib majja pääsemiseks end remondimeheks riietada. Selleks tuleb hankida endale tunked või mõne teenust pakkuva firma logoga särk. Administraatorile öeldakse, et tuldi telefoni, tualetti vms parandama. Kui võimalik, siis valitakse aeg, kus haldusjuht pole majas. Samuti võib rõhutada, et tegemist on kiireloomulise asjaga (Jones 2004, 10.) Sarnaselt eelpool nimetatud tööriietele võib sama mõju olla ka tavalisel helkurvestil.

2.6 Küsimustike kasutamine

Me kõik oleme kindlasti täitnud varem küsimustikke internetis. Enamjaolt on need kellelgi reaalse uurimuse tarvis valmistatud. Kuid leidub ka selliseid, mille eesmärk on pahatahtlik. Küsimustikud võivad sisaldada küsimusi sinu töökoha kohta, selle infrastruktuuri või näiteks turvameetmete kohta. (Cyber Security Tips 2012, 2.)

2.7 USB-mälupulga mahajätmine

Ründajad võivad kasutada ka USB-mälupulka, et pääseda ligi tundlikule infole, mida talletatakse arvutis või võrgus. Ründaja võib nakatada USB-mälupulga viiruse või Troojaga. Kui mälupulk ühendatakse arvutiga, siis annab see ründajale ligipääsu sisselogimistele, paroolidele ja muule teabele kasutaja arvutis või võrgus, kus kasutaja arvuti on ühendatud. Ründaja võib jätta USB-mälupulga näiteks põrandale või kuhugi arvutite lähedusse. Tavaliselt valitakse koht, kus liigub palju inimesi. Inimene, kes leiab mälupulga, sisestab tihti selle enda arvutisse, lootuses, et leiab infot, kellele see mälupulk kuuluda võib. (Information Security Office.)

2.8 Sotsiaalmeedia ja veebisaitide kasutamine

Sotsiaalmeediasse millegi postitamise või mõne postituse kommenteermisega peaks olema ettevaatlik. Kui info on üles pandud on põhimõtteliselt kõigil võimalus seda lugeda. Hiljem ei pruugi enam olla võimalik seda infot maha võtta või on juba liiga hilja. Mida rohkem infot postitada, seda suurem võimalus on seda rünnaku tegemiseks kuritarvitada. Veebilehti on võimalik ära kasutada mõtlematute inimeste käest tundliku teabe, nagu näiteks meiliaadresside või paroolide, saamiseks. Näiteks võib veebisait pakkuda võimalust osaleda loosimisel või kampaanias. Sait võib paluda sisestada oma meiliaadressi ja parooli. Parool,

mis sisestatakse, võib olla sama või sarnane tema muude paroolidega, näiteks töö e-posti aadressi parooliga. (Cyber Security Tips 2012, 2; Allen 2007, 8.)

Üks näide Interneti kaudu inimeste mõjutamise kohta on *phishing*. Ründaja saadab võltsitud meili, mis sarnaneb mingi firma või panga ametliku e-posti vormiga. Samuti võib kasutada võltsitud veebilehti, mis on tehtud välimuselt võimalikult sarnaseks. Näiteks seal on link http://www.facebook.com, mis tegelikult suunab sind lingi peale vajutades hoopis mingile muule veebilehele, kus kasutaja juba sisestab oma andmed. (Allen 2007, 8.)

2.9 Telefoni teel info saamine

Enamus sotsiaalmanipulatsiooni rünnakuid toimub telefoni teel. Helistaja esitleb ennast inimesena, kellel on õigus saada infot. Näiteks võib pettemanöövriks kasutada selle sama asutuse töötaja identiteeti. Helistaja palub kolleegilt abi ja tuge mõne probleemi lahendamiseks. Kõige lihtsam koht alustamiseks on tehniline tugi. Põhjus on väga lihtne – see ongi tehnilise toe töö, pakkuda töötajatele abi. (Allen 2007, 7.)

Siin on toodud üks näide telefoni teel info saamisest. Suurfirma tegi kampaania, kus pakkus liitumise eest uut telefoni ühe sendi eest. Paljud ostlejad peaksid ennem sellise plaaniga liitumist tegema kindlaks, mis täpsemalt plaanis sisaldub, ilma, et hakkaksid kohe uue telefoni pärast liituma. Sotsiaalmanipulaator, kellele meeldis ühe sendi eest pakutav telefon, aga kellele ei meeldinud üldse pakutav plaan, lahendas olukorra omamoodi. (Mitnick & Simon, 2002: 50.)

Ta helistas ühte peoketi elektroonikapoodi ja väitis, et oli mõned päevad varem rääkinud ühe töötajaga plaanist ning pidi temaga uuesti ühendust võtma, kuid unustas tema nime. Ta viis oma jutuga kõne vastuvõtja selleni, et see ütles ühe töötaja nime (William). Seda sama nime kasutades helistas sotsiaalmanipulaator hiljem keti teise firmasse ja esitles end nüüd Williamina. Ta ütles, et tegi ühe inimesega lepingu, kuid neil on telefonide varu otsa saanud. Kuna teises poes, kuhu ta helistas, neid veel oli, siis olidki nemad nõus selle telefoni väljastama. Seega läkski sotsiaalmanipulaator poodi ja talle anti telefon ilma, et ta oleks pidanud tegelikult ühegi plaaniga liituma. (Mitnick & Simon, 2002: 50-51.)

2.10 Tähtsa juhi identiteedi kasutamine

Rünnaku tegija esitleb ennast kui kõrgemat juhti selles organisatsioonis, kellel on tähtis tähtaeg. Nii saab inimest sundida endale kasulikku infot jagama. Nagu näiteks, millist kaughaldustarkvara nad kasutavad, kuidas seda seadistada, vajalikud sisselogimisandmed serverile ligipääsemiseks jms. Sellise info kättesaamise järel on ründajal võimalik luua ühendus organisatsiooni võrguga. Ründaja võib paar tundi hiljem tagasi helistada ja öelda, et ta on unustanud oma parooli ja paluda see uuesti lähtestada. (Allen 2007, 7.)

3 SOTSIAALMANIPULATSIOONI ENNETAMINE

Eelnevalt on kirjeldatud sotsiaalmanipulatsiooni mõiste, selle eesmärk ja põhilised kasutusviisid. Selles peatükis vaadeldakse lähemalt seda, kuidas end sotsiaalmanipulatsiooni rünnakute eest kaitsta ja kuidas neid ennetada.

3.1 Töötajate koolitamine

Esimene samm sotsiaalmanipulatsiooni rünnakute vältimisteks on teada, mis need on ja õppida nende kohta. Teadmised ei pea olema sügavad, nagu näiteks teadmine, kuidas neid ise läbi viia. Pigem peaks omandama teadmised selle kohta, milliseid rünnakuid on olemas ja mis juhtub, kui nende ohvriks langeda. Lisaks on vaja kindlasti teada olulisi tähelepanekuid, mis vihjavad, et tegemist võib olla pahatahtliku tegevusega. (Hadnagy 2013, 403-404.)

Oluline on, et see teadmine oleks omandatud juba enne seda, kui rünnak on toimunud, mitte õppida toimunud rünnakust. Hea oleks informeerida oma töötajaid sotsiaalmanipulatsiooni uutest teemadest. Näiteks võib lugeda mingit raamatut sel teemal, näidata õppevideoid või kutsuda spetsialistid pidama õppekoosolekuid. Põhimõtteliselt võib öelda, et mida rohkem sa tead sotsiaalmanipulatsioonist, seda kergem on ära tunda võimalikke rünnakuid. (Hadnagy 2013, 403-404.)

3.2 Info väärtuse hindamine

Üks hea soovitus on see: ole teadlik info väärtusest, mida sul võidakse paluda avaldada. Enne kui edastad informatsiooni, mõtle, kas see inimene peaks seda üldse teadma. Inimestel on sisse ehitatud tahe aidata hädasolijaid. See on üks viise, mida kasutatakse inimeste manipuleerimiseks. Töötaja peaks teadma ja suutma aru saada, kas tegelikult on vaja avaldada sellist infot. Ka kõige väiksemad infokillud võivad aidata kaasa rünnakule. Kui küsimused äratavad kahtlust on üks lihtsamaid viise öelda lihtsalt, et „Vabandust, ma ei või seda infot avaldada“ või lihtsalt öelda, et te ei tea täpselt selle kohta ja suunata nad edasi üldinfosse. (Hadnagy 2013, 408.)

Töötajate jaoks on hea luua nn stsenaarium. See tähendab, et luuakse küsimustikud/käitumisviisid, mida saab teatud olukordades kasutada. Näiteks kui keegi

helistab ja väidab, et on mingi osakonna juht või on administraator, siis tuleks küsida, kas inimese ID-d või muud sellist identifitseerimise võimalust. (Hadnagy 2013, 412-413.)

3.3 Andmete klassifikatsioonid

Iga ettevõtte peaks reguleerima andmete väljastamist. Ettevõtte infovarade kaitsmiseks on vaja paika panna andmete klassifikatsiooni poliitika. See poliitika loob raamistiku, tänu millele on töötajad teadlikud andmete tundlikkuse tasemest. Kui neid eeskirju pole, siis peavad suurema osa otsuseid tegema töötajad ise. Töötajate otsused põhinevad enamasti pigem subjektiivsetel aspektidel kui teabe väärtusel. (Mitnick & Simon 2002, 248–249.)

Andmete klassifikatsiooni poliitika paneb paika kindlad juhised, mille abil antakse väärtuslikule informatsioonile üks kindel tase. Pärast seda saavad töötajad juba jälgida kindlaid andmete käsitlemise protseduure, et kaitsta ettevõtet hooletu väärtusliku info avalikustamise eest. Juhatus peab paika panema ka info omaniku. Info omanik vastutab väärtuslikud info kaitse eest, otsustab, milline klassifikatsioonitase määrata, vaatab infole määratud tasemeid aeg-ajalt üle ja vajaduse korral uuendab neid. (Mitnick & Simon, 2002, 249.)

Kõige üldisemalt võib andmed jagada nelja kategooriasse: konfidentsiaalne, privaatne, sisemine, avalik. Konfidentsiaalne kategooria sisaldab kõige tundlikumat teavet. Seda ei tohi mitte mingil juhul ettevõttest välja anda ja enamasti teab sellest ainult teatud inimestering. Privaatse kategooria alla kuuluvad andmed, mis on isiklikku laadi ja mida tohib kasutada ainult asutuse sees (nt töötajate haiguslood, palga või pangakonto info). Sisemine kategooria hõlmab andmeid, mida võib vabalt jagada kõigi ettevõtte töötajatega. Avaliku info alla kuulub teave, mis on loodud spetsiaalselt asutuse väliseks kasutamiseks. Siia alla kuuluvad pressiteated, tootevoldikud jms). (Mitnick & Simon, 2002, 249–251.)

Peale andmete klassifikatsiooni on veel oluline teada, kuidas tundlikku infot hävitada. Tähtsad dokumendid ja tundlik info tuleks ära viskamise asemele purustada ja muuta selle lugemine võimatuks. Lisaks peaks hoidma oma prügi ka asutuse väliselt kättesaamatus kohas, et keegi võõras sellele ligi ei pääseks. (Edmead 2008, 4.)

3.4 Tarkvara uuendamine

Asutused peaksid hoidma oma tarkvara alati uuendatud. Oma rakenduste uuendamisega tagatakse, et töötajatel oleks olemas hetkel kõige turvalisem versioon. Enamus turvaauke, mis avastatakse, parandatakse ja lisatakse uuendusse. Juba vanema Internet Exploreri kasutamine loob palju uusi turvaauke juurde. Kindlasti ei tohiks anda isikutele, kelle identiteedis te kindlad ei ole, infot selle kohta, milliseid veebibrauserit kasutate või mis formaadis tekste avate. (Hadnagy 2013, 411–412.) Näiteks võib juhtuda, et sotsiaalmanipulatsiooni rünnaku tegija helistab töötajale ja esitleb end IT-osakonna töötajana, et saada teavet veebibrauseri versiooni kohta. Kui ta saab teada, et kasutatakse uuendamata versioone, siis saab ründaja vastavalt sellele oma rünnakut planeerida.

3.5 Turvaeeskirjad

Turvaeeskirjad on täpsed juhised töötajatele, et võidelda potentsiaalsete turvariskide vastu. Samuti on need olulised sotsiaalmanipulatsiooni rünnakute ennetamiseks ja tuvastamiseks. Turvaeeskirjad ei taga, et alati saab kõiki rünnakuid ennetada. Pigem on eesmärk vähendada riski tasemeni, mis on vastuvõetav. Samuti on oluline, et asutuse kõrgem juhatus näitaks oma tugevat toetust turvaeeskirjade arendamisele. Töötajad peavad nägema, et info turvalisus ja andmete kaitse on ettevõtte toimimise jaoks elutähtis. (Mitnick & Simon 2002, 246.)

Infoturbe eeskirjade kirjutamisel ei tohi kasutada keerulist tehnilist keelt. Peale selle on tähtis kirja panna, miks mingi reegel või protseduur oluline on. Muidu võivad töötajad neid reegleid lihtsalt eirata, sest nad peavad seda ajaraiskamiseks. Töötajatele tuleb teada anda, miks need reeglid on olulised ja millist kahju see võib tuua, kui neid reegleid ei järgita. Lisaks tuleb töötajaid teavitada tagajärgedest, mis neid ootavad, kui nad eeskirju rikuvad. (Mitnick & Simon 2002, 247.)

Infoturbe eeskirjad ei saa olla muutumatud. Kuna ettevõte ja turvatehnoloogiad võivad muutuda, siis tuleb ka eeskirju regulaarselt üle vaadata ja täiendada. Eeskirjad tuleb panna siseveebi töötajatele kättesaadavasse kohta, et nad sealt vajadusel kiirelt küsimustele vastuseid leiaks. Nõrkade kohtade leidmiseks tuleb perioodiliselt testida eeskirjade järgmist, kasutades sotsiaalmanipulatsiooni meetodeid. (Mitnick & Simon 2002, 247-248.)

3.6 Turvaauditid

Asutus võib täiendada küll turvaeeskirju ja töötajaid koolitada, kuid mis siis, kui neid ei võeta tõsiselt või eiratakse. Samuti ei pruugi ettevõte teada, kas ettevõetud toimingud on adekvaatsed või mitte. Sellepärast tulekski teha turvaauditeid. Turvaauditid aitavad tuua välja võimalikke vigu ning tänu sellele saab eeskirju täiendada. Sotsiaalmanipulatsioonile keskenduvate auditite kaudu saab töötajatele näidata, et ka nemad võivad olla sihtmärgiks. (Jones 2004, 6-7.)

Enne auditi tegemist on oluline selleks eelnevalt hoolikalt ette valmistada. Kõigepealt tuleks panna paika eesmärk, miks üldse auditit tehakse. Selleks võib olla näiteks uute eeskirjade testimine või ebasobivate toimingute avastamine. Enne testi tegemist tuleb saada nõusolek juhtkonnalt. Samuti on oluline teavitada töötajaid, et selline turvatest tehakse, kuid te ei pruugi öelda, millal ja keda täpselt testitakse. (Jones 2004, 7.)

Üks võimalus sotsiaalmanipulatsiooni testi tegemiseks on saata töötajale testmeil. Esmalt kirjutatakse meil, mis sarnaneb tavaliste andmepüügi stsenaariumidega. Seejärel pannakse koostöös IT-osakonnaga üles üks vale veebiaadress, kuhu kasutaja kirjas oleva lingi kaudu suundub. Veebisaidil küsitakse sisse logimiseks vajalikke andmeid. Meil saadetakse töötajatele ja hiljem saab monitoorida, kes nendest lingil klikkisid. (Pyzik 2015, 21.)

4 SOOVITUSED SOTSIAALMANIPULATSIOONI ENNETAMISEKS

Peatükis on välja toodud konkreetsed soovitused, mida inimesed peaksid jälgima, et mitte sattuda sotsiaalmanipulatsiooni rünnaku ohvriks. Vajaduse korral saab need näiteks välja printida ja koju, kooli või töö juurde seinale panna.

- Ära avalda tundlikku informatsiooni inimesele, kelle identiteedis sa ei ole täiesti kindel. Nii emaili ja telefoni teel, kui ka näost näkku. (Hadnagy 2013, 408.)
- Mõtle selle peale, mida sinult küsitakse. Kui küsimus tundub kuidagi imelik või ei ole asjakohane, ära avalda infot.
- Hoia oma kasutatav tarkvara alati kõige uuemal versioonil. Kaasa arvatud antiviirus ja muud turva tarkvarad. Uuendustega tulevad turvaaukude parandused. (Hadnagy 2013, 408.)
- Ära viska tundliku infoga dokumente lihtsalt prügikasti. Purusta need või muuda mingil muul viisil loetamatuks. Ära viska kindlasti dokumente avalikesse prügikastidesse. (Edmead 2008, 4.)
- Ära kunagi jaga oma parooli.
- Ära kasuta üht ja sama parooli igal pool. Kui keegi saab teie parooli teada, siis saab ta ligipääsu ka teistele teie kontodele.
- Ära ava tundmatuid ja kahtlaseid manuseid.
- Ära kunagi sisesta oma parooli kahtlasel veebisaidil (OSAC, 2015)
- Pööra tähelepanu veebilehe aadressile. Veendu, et veebiaadressiribal oleks olemas luku ikoon ja et aadressi ees oleks *https*. See tagab turvalise ühenduse.
- Jälgi oma ümbruskonda, kui arvutis oled. Veendu, et ükski võõras või inimene, kellel ei ole vaja, ei jälgiks sinu arvuti ekraani. (Cyber Security Tips 2012, 1.)
- Ära räägi töö asjadest kõva häälega avalikes kohtades. Kunagi ei tea, kes pealt võib kuulata.
- Ära jäta külalisi kontorisse omapäi, alati peab kaasas olema saatja. (Edmead 2008, 4.)
- Kui märkad majas üksi liikuvat võõrast, siis uuri, mis asjus ta seal viibib.

KOKKUVÕTE

Töö andis ülevaate sotsiaalmanipulatsioonist, selle peamistest viisidest ja vastumeetmetest. Lähemalt vaadeldi veel, kes on sotsiaalmanipulaatorid ja mis neid selleks tegevuseks ajendab. Peale selle antakse näpunäiteid, kuidas vältida sotsiaalmanipulatsiooni rünnaku ohvriks langemisest.

Sotsiaalmanipulatsioon on probleem, mis levib infoühiskonnas järjest enam. Tööst järeldub, et ründajatel on järjest raskem teha kahju tehnoloogiliste vahendite kaudu. Kõige suurem turvarisk on siiski inimene ise. Näiteks on viimastel kuudel levinud juhtumid, kus inimestele saadetakse meile, mis sisaldavad linki ja pärast sellele klikkimist krüpteeritakse inimese arvuti. Arvuti vabastamiseks tuleb maksta ründajatele lunaraha. See on samuti üks näide sotsiaalsest manipulatsioonist.

Sotsiaalmanipulatsiooni ennetamine peaks algama ettevõttes peast. See tähendab, et ettevõtte juhid peaksid mõistma teema olulisust ja selle jaoks vajalikke toiminguid tegema. Teine etapp on kindlasti töötajate koolitamine. Samuti on tähtis aeg-ajalt auditeid teha, et leida ettevõtte turvariskid ja kitsaskohad. Inimesed ei tohiks kaotada kriitilist mõtlemist, mis tahes olukordades.

Kuna Eestis ei ole seda teemat väga palju uuritud, siis võikski uurida sotsiaalmanipulatsiooni hetkeolukorda Eestis. Näiteks kui teadlikud inimesed on sotsiaalmanipulatsioonist, kas ja kui palju on nad sellega kokku puutunud või kui kerge oleks nende käest tundliku teabe saamine.

KASUTATUD KIRJANDUS

AL-Johani, A. A., & AL-Msloum, A. S. (2013). Social engineering risks in the contemporary reality and methods of fighting these risks. International Journal of Academic Research Part A, 5(6), 265-272. doi: 10.7813/2075-4124.2013/5-6/A.33

Allen, M. (2007). Social Engineering: A Means To Violate A Computer System. SANS Institute Reading Room. Vaadatud aadressil: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529 (12.03.2016).

Ciampa, M. 2011. Security+ Guide to Network Security Fundamentals, Fourth Edition. 3 Course Technology, Cengage Learning. Vaadatud aadressil http://faculty.olympic.edu/kblackwell/docs/cmptr236/Online%20Book%20Preview/Chapter%202/1111640122_303078.pdf (20.03.2016).

Cyber Security Tips. (2012). Social Engineering: You are at Risk! From the Office of Angel Cruz, Chief Information Security Officer, State of Texas, 6 (7). Vaadatud aadressil https://www.tamiu.edu/oit/documents/socialengineering1.pdf (12.03.2016).

Edmead, M. T. 2008. Social engineering attacks: What we can learn from Kevin Mitnick. Vaadatud aadressil http://gauss.ececs.uc.edu/Courses/c6056/pdf/social-engineering-prevent-attacks.pdf (12.03.2016).

Greavu-Şerban, V., & Şerban, O. (2014). Social Engineering a General Approach. Informatica Economica, 18 (2), 5-14. doi: 10.12948/issn14531305/18.2.2014.01

Hadnagy, C. (2013). Social Engineering: The Art of Human Hacking. Indianapolis, Indiana: Wiley Publishing Inc. Vaadatud aadressil https://sin.thecthulhu.com/library/security/social_engineering/The_Art_of_Human_Hacking.pdf (12.03.2016).

Information Security Office. Social Engineering Using a USB Drive. Garnegie Mellon University. Vaadatud aadressil https://www.cmu.edu/iso/aware/be-aware/usb.html (18.03.2016).

Iozzio, C. 2008. The Cyber Crime Hall of Fame. Vaadatud aadressil http://www.cs.clemson.edu/course/cpsc420/material/Papers/The%20Cyber%20Crime%20Hall%20of%20Fame.pdf (20.03.2016).

Janczewski, L. J., & Fu, L. (2010). Social Engineering-Based Attacks: Model and New Zealand Perspective. Proceedings of the International Multiconference on Computer Science and Information Technology pp. 847–853. Vaadatud aadressil https://fedcsis.org/proceedings/2010/pliks/36.pdf (12.03.2016).

Jones, C. 2004. Social Engineering: Understanding and Auditing. SANS Institute. Vaadatud aadressil https://www.sans.org/reading-room/whitepapers/engineering/understanding-auditing-1332 (12.03.2016).

Kikkas, K. 2016. Lihtsalt küsi, ehk turvaründed ilma arvutita. Nutiajakiri 30 pluss, märts.

Mitnick, K. D., Simon, W. L. 2002. The Art of Deception. Controlling the Human Element of Security. John Wiley & Sons. Vaadatud aadressil http://www.scis.nova.edu/~cannady/ARES/mitnick.pdf (12.03.2016).

Mitnick, K. D., Simon, W. L. 2011. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Little, Brown and Company. Vaadatud aadressil http://www.pdf-archive.com/2015/10/07/ghost-in-the-wires-kevin-mitnick/ghost-in-the-wires-kevin-mitnick.pdf (20.03.2016).

OSAC. 2015. U.S. Department of State Overseas Security Advisory Council. Social engineering: threts and best practises. Vaadatud aadressil http://www.pacific.edu/Documents/risk_management/OSAC%20Social%20Engineering%20Guide.pdf (18.03.2016).

Pyzik, K. 2015. Shutting the door on social engineering. Internal Auditor. 72 (5), 20-21. Vaadatud aadressil http://web.a.ebscohost.com.ezproxy.tlu.ee/ehost/pdfviewer/pdfviewer?sid=ef9c52f9-4b4f-4120-9017-34c6fb02ef96%40sessionmgr4001&vid=11&hid=4107 (12.03.2016).