Socialni inženiring in kako se pred njim ubraniti?

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice pojasnjujejo dejstva o socialnem inženiringu, različne situacije oz. oblike socialnega inženiringa (načini pridobivanja osebnih podatkov) ter strategije, ki jih lahko ubere posameznik, da se pred tovrstnimi oblikami internetne (tudi telefonske ali drugačne) prevare ubrani.
Ciljne javnosti:	Upravljavci zbirk osebnih podatkov v javnem in zasebnem sektorju, zaposleni pri upravljavcih zbirk osebnih podatkov v zasebnem in javnem sektorju, splošna javnost.
Status:	Javno.
Verzija:	1.0
Datum verzije:	4. 9. 2009
Avtorji:	Informacijski pooblaščenec.
Ključne besede:	Smernice, socialni inženiring, osebni podatki, zloraba zaupanja, internet, varnostne politike,…

VSEBINA

>>>

O smernicah Informacijskega pooblaščenca

Namen smernic Informacijskega pooblaščenca (v nadaljevanju Pooblaščenec) je podati skupne praktične napotke za upravljavce zbirk oseb-nih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1-UPB1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1-UPB1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- *Mnenja Pooblaščenca*:
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/

- *Brošure Pooblaščenca*:
  http://www.ip-rs.si/publikacije/prirocniki/

Smernice Pooblaščenca so objavljene na spletni strani:

http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Uvod

V današnjem, modernem času si ne moremo več zatiskati oči pred drvečim vlakom tehnologije. Vendar če si - sami pri sebi, predvsem pa zakonodajalec in nadzorni organi - vsaj za trenutek ne zamrznemo slike tega drvečega vlaka in premislimo, ali ga lahko utirimo v "pravo" smer, lahko vlak prehitro odpelje mimo, ne da bi ga pravočasno usmerili v želeno smer. Drveči vlak je seveda metafora za hitro spreminjajoče se možnosti, ki jih nudi tehnologija, ki nam poleg obilice pozitivnih stvari, prinaša tudi nekaj negativnih, s katerimi se moramo pravočasno in ustrezno soočiti, biti nanje pripravljeni in se pravilno odzvati.

Eden od pojavov modernega časa, ki je zlasti uspešen v povezavi z uporabo modernih tehnologij, je socialni inženiring. Gre za prakso, ki bo najverjetneje vse bolj pogosta, predvsem zaradi možnosti hitrega zaslužka s pomočjo internetnih goljufij in počasnih reakcij zakonodajalca. V nadaljevanju Informacijski pooblaščenec predstavlja dejstva o socialnem inženiringu, različne situacije oz. oblike socialnega inženiringa ter strategije, ki jih lahko ubere posameznik, da se pred tovrstnimi oblikami internetne (tudi telefonske ali drugačne) prevare ubrani.

Socialni inženiring

1.1 Kaj je socialni inženiring?

Socialni inženiring po svoji naravi pomeni predvsem pridobivanje nekih koristi z zlorabo zaupanja posameznika oz. z manipulacijo.

V literaturi se za opis tega dvostranskega razmerja uporabljata predvsem besedi "žrtev" in "napadalec", slednjemu pa lahko rečemo tudi socialni inženir. Socialni inženir torej **z zlorabo zaupanja**, z uporabo **socialnih veščin** oziroma **psiholoških tehnik**, kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva ipd., pridobi od žrtve osebne podatke (najpogosteje ime, priimek, št. transakcijskega računa, razna gesla, EMŠO, št. potnega lista …) in jih **uporabi za pridobivanje večinoma premoženjske koristi**. Redkeje od zasledovanja premoženjskih koristi, pa vendar ne zanemarljivo, se zgodi, da napadalec žrtev s pridobljenimi osebnimi podatki **izsiljuje, grozi**, jo šikanira ali kako drugače spravlja v slabši položaj.

Kevin Mitnick, svetovno znani heker in avtor knjige o socialnem inženiringu "Umetnost prevare" (*Art of Deception*), je zapisal:

"Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Posledica tega je, da lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologije[1]."

V literaturi se seveda pojavljajo različne opredelitve socialnega inženiringa, skupno domala vsem pa je, da opisujejo socialni inženiring kot uporabo socialnih ali psiholoških trikov (v nasprotju z uporabo tehničnega oz. računalniškega znanja), z namenom pridobivanja osebnih podatkov.

Pooblaščenec je o socialnem inženiringu v smernicah o kraji identitete (http://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Smernice_kraja_identitete.pdf) zapisal:
Socialni inženiring je nabor tehnik napadalca za prepričevanje uporabnika ali administratorja sistema, da mu izda avtentikacijske podatke, s katerimi se nato nezakonito prijavi v sistem. Socialni inženiring temelji na t.i. imenovanih kognitivnih odklonih in izkorišča reagiranje ljudi v določenih situacijah (npr. pod pritiskom). Izvajalci socialnega inženiringa s pomočjo obvladovanja veščin prevzemanja identitete drugih ljudi lahko izjemno uspešno pridobijo pomembne podatke. Verjetno najbolj znani hacker, Kevin Mitnick, je slovel ravno po zmožnostih izvabljanja podatkov od ljudi. Pri socialnem inženiringu so lahko zelo koristna omrežja za spletno druženje (npr. Facebook), kjer ljudje sami od sebe objavljajo številne osebne podatke, ki napadalcu omogočijo boljše poznavanje žrtve in s tem predvidevanje njenega reagiranja.

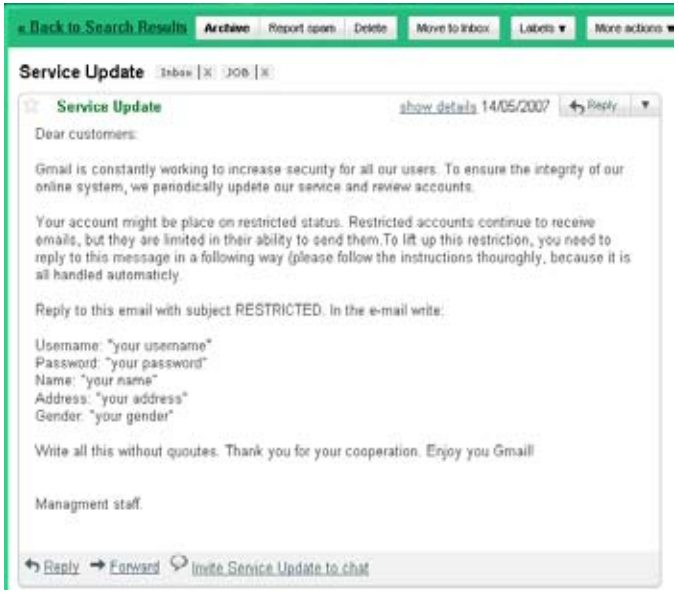
1.2 Klasični primeri socialnega inženiringa

V t. i. informacijski dobi je izmenjava informacij neverjetno dinamična, poteka ves čas in vsepovsod; za sodoben način življenja in delovanja ljudi je tako pomembna, da nekateri govorijo o sodobnem človeku kot o *homo informaticus*-u.

Vse to, povezano z naravnim nagnjenjem človeka k zaupanju (kot trdijo nekateri) ter po drugi strani z željo po hitrem zaslužku, lahko pripelje do nadvse raznolikih primerov socialnega inženiringa. V nadaljevanju opisujemo nekaj takih primerov.

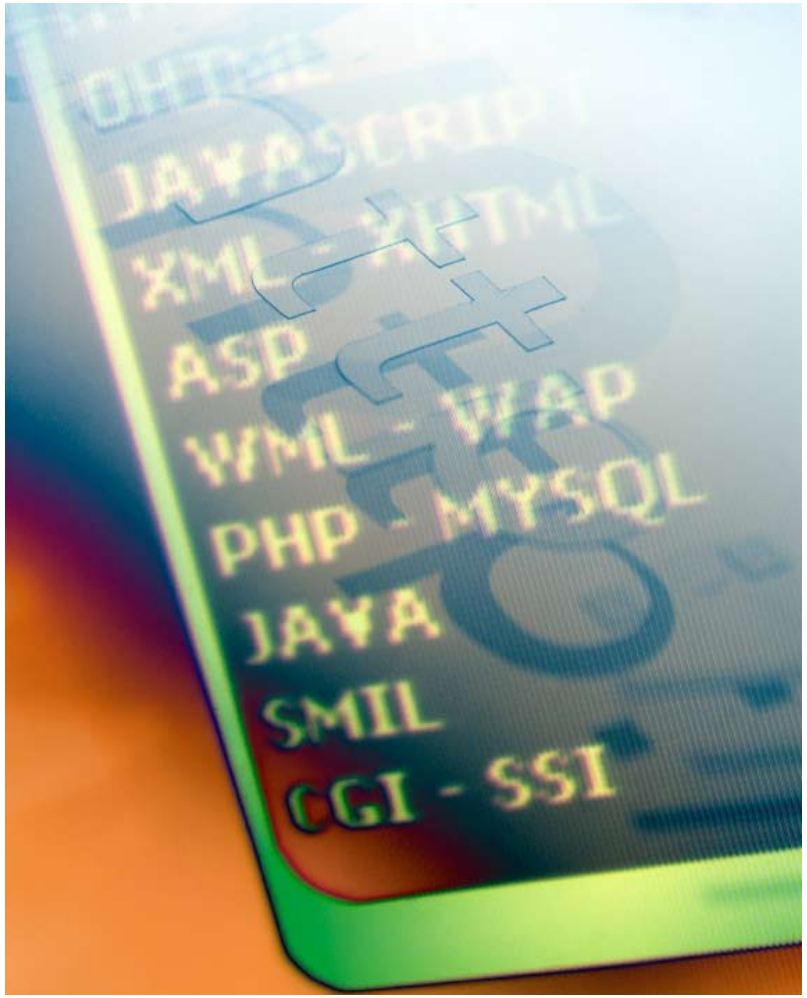
Izjemno pogost primer (poskusa) socialnega inženiringa se dogaja na področju uporabe elektronske pošte. Soočimo se lahko z različnimi tehnikami zlorabe našega zaupanja, predvsem kadar socialni inženirji "igrajo na karto" našega tehnološkega neznanja. Spodaj je prikazano elektronsko sporočilo, ki je s pomočjo t. i. **ribarjenja** (angl. ***phishing***) skušalo pridobiti naše uporabniško ime, geslo, ime, naslov in spol. Gre za klasično obliko socialnega inženiringa, saj se pošiljatelj izdaja za uslužbenca ponudnika storitve Gmail.

1 *"Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."* Vir: http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294530,00.html, dostop dne 28. 6. 2009.



Pogosta **tarča socialnega inženiringa so tudi uporabniki spletnih bančnih poslovalnic**. Poleg prejemanja elektronskih sporočil, kjer "upravitelji spletne poslovalnice" od posameznika "zaradi varnostnih razlogov" zahtevajo geslo za dostop do osebnega e-računa, se pogosto pojavijo tudi lažne spletne strani, ki zavedejo uporabnika, da vanje vnesejo svoje osebne podatke in s tem neposredno tvegajo izgubo finančnih sredstev na transakcijskem računu. Tudi v tem primeru gre za ribarjenje.

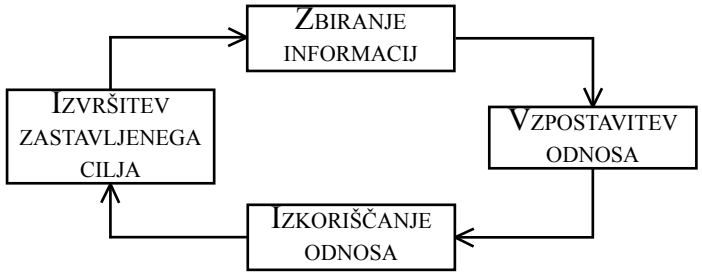
Vedno bolj navzoče pa so tudi prakse t. i. **varnostnega preverjanja** podjetja. V teh primerih sicer **ne gre za tehnike socialnega inženiringa**, temveč za **preverjanje dovzetnosti uslužbencev** nanje. Znano je, da podjetja ali organizacije neredko s telefonskimi klici preverijo, ali so njihovi zaposleni osebi na drugi strani (torej preverjevalcu) pripravljeni posredovati določene podatke; gesla ali druge avtorizacijske podatke, osebne podatke ali celo poslovne skrivnosti. Tovrstne prakse so seveda predvsem preventivne narave in so združene s kasnejšim izobraževanjem zaposlenih o pomenu previdnosti pri posredovanju podatkov neznanim osebam. Socialni inženiring kaže svojo nevarno podobo ravno v primerih, ko nas denimo v službo pokliče oseba, ki se predstavlja za tehnika, ki nudi pomoč in podporo sistemu, za računovodjo, ki potrebuje podatke za opravljanje dela za nas, za uslužbenca banke, ki izvršuje finančno transakcijo … V 5. poglavju bomo podrobneje prikazali tehnike, kako se pred takimi napadi ubraniti, seveda pa v prvo obrambno linijo sodita uporaba zdravega razuma ter razumna mera previdnosti.



2. Življenjski cikel socialnega inženiringa

Vsak napad s pomočjo socialnega inženiringa sestoji iz štirih korakov. Vse stopnje so med seboj povezane (oz. prehajajo druga v drugo) in odvisne druga od druge.

Življenjski krog napada s socialnim inženiringom:



Zbiranje informacij

Zbiranje informacij je prvi in verjetno najpomembnejši korak v življenjskem krogu. Uspeh socialnega inženirja je odvisen predvsem od količine in kakovosti pridobljenih podatkov. Ti podatki obsegajo bolj splošno znane podatke, kot so telefonske številke, elektronski naslovi ali poštni naslovi, pa tudi bolj osebne podatke, kot so rojstni datum, dekliški priimek, vzdevek ali kaj podobnega. **Podatki pa niso vezani samo na ljudi, temveč tudi na stvari** - npr. na arhitekturo informacijskega sistema, poznavanje organizacijskih postopkov v podjetju. Napadalec uporabi podatke za **vzpostavitev in razvoj odnosa z žrtvijo** (naslednji korak v življenjskem ciklu).

Vzpostavitev odnosa

Druga faza je odvisna predvsem od načina delovanja samega napadalca. Napadalec na tej stopnji vzpostavi ter razvija odnos z žrtvijo. Napadalec izkoristi pridobljene podatke iz prejšnje faze in glede na dano situacijo odigra določeno vlogo. Prepričljivost odigrane vloge napadalca je odvisna predvsem od kakovosti in količine pridobljenih podatkov ter njegovih "igralskih" spretnosti. Ljudje smo nagnjeni k temu, da zaupamo določene informacije tistemu, za katerega menimo, da je zaupanja vreden, to pa napadalec doseže predvsem s poznavanjem oz. posredovanjem podatkov nam. **Cilj te faze je prepričati žrtev**, da socialnemu inženirju lahko **zaupa** in zato tudi deli z njim podatke, ki so bolj ali manj zaupni.

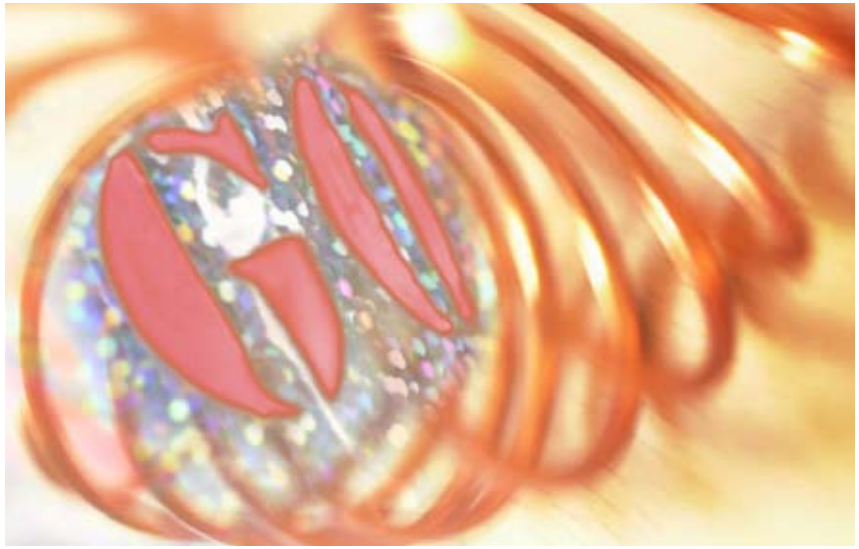
Izkoriščanje odnosa

Ko napadalec pridobi zaupanje in vzpostavi odnos z žrtvijo, sledi korak, v katerem izkorišča ta odnos oz. pridobljeno zaupanje. Če je napadalec v prejšnjem koraku uspešno prepričal žrtev, da je vreden zaupanja, mu žrtev velikokrat brez zadržkov izda podatke, ki jih želi.

Izvedba zastavljenega cilja

Izvedba zastavljenega cilja je zadnji korak v procesu. V tem koraku napadalec izkoristi pridobljene podatke za dosego zastavljenega cilja. Tako lahko že same informacije pripeljejo do zastavljenega cilja ali pa jih napadalec uporabi za pomoč pri vdiranju na tehnični način.

Pomembno je poudariti, da življenjski krog napada s socialnim inženiringom ni končan. Napadalec lahko tako nadalje zbira informacije in s tem ali razširi napad glede na informacijski sistem, uporabi podatke pri drugi žrtvi ali pridobi dodatne podatke, ki mu omogočajo izvesti drug napad. Ker je napadalec že vzpostavil odnos z žrtvijo, ga lahko s pridom izkorišča tudi v drugih situacijah.



3. Tehnike socialnega inženiringa

3.1 Zbiranje informacij s pomočjo interneta

3.1.1 Spletni iskalniki

Socialni inženiring velikokrat poteka po principu **izrabe že obstoječih informacij** o posamezniku za pridobitev še več in bolj ključnih podatkov. Glede na to, da se skoraj o vsakem izmed nas na internetu pojavljajo določeni podatki, socialni inženir lahko zlahka pridobi podatke o naši preteklosti (o naših hobijih, obiskovanih šolah, profesionalnemu življenju in ostalih aktivnosti). Nemalokrat se zgodi celo, da so na internetu objavljeni določeni osebni podatki (v obliki seznamov, tabel,…) pomotoma, saj za velikimi strežniki in računalniškimi ekrani seveda sedijo ljudje, uredniki spletnih strani, ki lahko objavijo na internetu nekaj, česar pravzaprav niso nameravali.

Tudi Informacijski pooblaščenec je že obravnaval primere, ko so bili na internetu pomotoma objavljeni domači naslovi in GSM številke zaposlenih v podjetju, davčne številke, itd. Informacije, ki so prosto objavljene na internetu, lahko napadalec uporabi najprej za izbiro najustreznejše žrtve in nato za nadaljnje pridobivanje podatkov od nje same s pomočjo psihološke manipulacije oz. uporabo ene od tehnik socialnega inženiringa. Če socialni inženir pridobi imena in priimke naročnikov revije o luksuznih avtomobilih, lahko naročnika pokliče, se izdaja za predstavnika revije ter z lažno anketo denimo pridobi podatke o tem, kakšno varnost namenja svojemu avtomobilu.

Druga možnost zlorabe interneta pa je **vzpostavitev t. i. lažnih spletnih strani**; v skrajnem primeru gre za lažne strani spletnih bančnih poslovalnic, pa tudi vseh ostalih strani, ki za vstop zahtevajo registracijo oz. prijavo. Napadalec pridobiva osebne podatke od obiskovalcev spletnih strani tako, da jih pravzaprav prelisiči, da vpišejo svoje podatke na spletno stran, za katero so prepričani, da je "prava" oz., da pripada osebi ali podjetju, ki so mu pripravljeni zaupati.

3.1.2 Socialna družabna omrežja

Iz leta v leto število uporabnikov spletnih družabnih omrežij, kot so na primer Facebook, MySpace, Twitter itd., neverjetno hitro raste. Samo število aktivnih uporabnikov omrežja Facebook je v juliju 2009 preseglo 250 milijonov in tako predstavlja okoli 30 % svetovnih uporabnikov spleta. Navedeni podatki pričajo o izjemni razširjenosti spletnih družabnih omrežij, ki temeljijo na ustvarjanju lastnega profila ter s tem na objavljanju lastnih osebnih podatkov. Spletna družabna omrežja tako predstavljajo pravo **zakladnico informacij** za socialne inženirje. Bistvo socialnega inženiringa so ravno informacije – več kot jih napadalec ima, lažje bo izvedel svoj napad.

3.1.3 Ribarjenje (phishing)

Izraz ribarjenje podatkov (*phishing*) izvira iz angleških besed za geslo (*password*) in ribarjenje (*fishing*). Gre za nezakonit način zavajanja uporabnikov, pri katerem poskuša prevarant s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnikov na takšen ali drugačen način izvabiti njihove osebne podatke, kot so: številke kreditnih kartic, uporabniška imena in gesla, digitalna potrdila in ostale osebne podatke. Pri tem uporabljajo različne tehnike, ki spadajo v domeno socialnega inženiringa. Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od vas z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti vaše podatke z vašim odgovorom na to sporočilo.

Gre za primer, ko storilec pošlje elektronsko sporočilo, ki je videti na primer kot pravo sporočilo banke. V sporočilu bo pošiljatelj navedel, da je prišlo do problemov z uporabnikovim bančnim računom, zaradi česar ga prosijo, da mu pošlje številko računa oz. uporabniško ime in geslo. V kolikor bi uporabnik na takšno sporočilo odgovoril, bi postal žrtev spletne prevare.

3.1.4 Pharming napadi

Napadi *pharming* (gre za skovanko med angleškima besedama *farming* in *pharmacy*, navezuje pa se na tehniko genetskega inženiringa,v svetu interneta bi lahko govorili o inženiringu naslovov spletnih mest), so za uporabnika zelo nevarni, saj jih je težko prepoznati.

Glavna razlika med phishing-om in pharming-om je v tem, da gre pri pharmingu bolj za tehnični napad kot za tehniko socialnega inženiringa, na katerem temelji ribarjenje podatkov. Praviloma gre bodisi za neposreden napad na DNS strežnike

bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika (gre za t.i. datoteko o gostiteljih oz. host file, kjer se nahajajo podatki o URL-jih in domenah). Uporabnik je v teh primerih prepričan, da se nahaja na pravi strani, saj je vtipkal pravi URL naslov strani, v resnici pa ga je eden od omenjenih načinov napada preusmeril na lažne strani, ne da bi se pri tem spremenil URL naslov v oknu brskalnika. Uporabnik je seveda v tem lažnem zaupanju dovolj samozavesten, da vnaša svoje osebne podatke v obrazce, ki se nahajajo na takšnih straneh.

3.1.5 Trojanski konji, virusi in črvi

Virusi so predstavniki škodljive kode, ki živijo znotraj datotek kot so npr. datoteke urejevalnika besedil Word, urejevalnika preglednic Excel in ostalih. Ob odprtju okužene datoteke se virus razširi in okuži ostale datoteke na računalniku. Črvi so ravno tako samorepliciraj̨oči se programi, ki pa so za razliko od virusov nekoliko bolj inteligentni, saj znajo samodejno iskati primerne tarče za okužbo. Tako črvi kakor tudi virusi prinašajo s seboj breme (*payload*), ki jim omogoča prevzem nadzora nad okuženim računalnikom, brisanje datotek ali tatvino osebnih podatkov. Bežen pregled tovrstnega področja nam pove, da se vsak teden pojavi okrog 500 novih virusov in črvov. Število virusov in črvov se vsako leto poveča za 400 %, pri čemer postajajo njihovi avtorji/kriminalci vse bolj inovativni. Tovrstni predstavniki zlonamerne kode so pogosto doma ravno v nezaželenih elektronskih sporočilih (*spam*), zato je potrebno biti pri odpiranju tovrstne pošte še posebno pazljiv.

Še ena kategorija škodljivcev pa so trojanski konji, ki se v računalnik pritihotapijo v preobleki legitimnega programa. Ko uporabnik namesti legitimni program, se hkrati namesti tudi trojanski konj, ki napadalcu omogoči prevzem nadzora nad računalnikom.

3.2 Socialni inženiring preko telefona

Izvedba socialnega inženiringa s pomočjo telefonskega klica je glede na svojo učinkovitost precej enostavna. Napadalec pokliče ciljno osebo z namenom, da od nje pridobi določene podatke; velikokrat so to administratorska prijavna imena in gesla. Tovrstnim napadom so podvrženi zlasti razni asistenti, tajnice in drugi zaposleni v sprejemnih pisarnah. Prav ti ljudje so namreč navadno slabše poučeni o varnostni politiki in morajo biti ustrežljivi in prijazni do vsakega klicatelja. Torej sprejemajo klic za klicem, ne pomišljajo na posledice, to pa predstavlja veliko varnostno luknjo. Takšen napad se najpogosteje izvede iz telefonske naprave, pri kateri ni potrebna nobena avtentikacija storilca.

3.3 Vishing

Vishing je novejši poltehnični pristop socialnega inženiringa, ki izkorišča telefonske sisteme vrste VoIP (*Voice over IP*). Tudi ta izraz je kombinacija dveh besed, in sicer “voice”, torej glas, in “phishing”, ribarjenje. Vishing se uporablja predvsem za krajo identitete in drugih zaupnih podatkov (npr. podatki o kreditnih karticah). Pri izvedbi klica napadalec **skrije pravo številko in jo zamenja s številko, ki jo žrtev pozna ali ji zaupa** (npr. operaterja). Tehniko je mogoče uporabiti v navezi z ribarjenjem, tako da je v elektronski pošti navedena številka namesto spletne povezave. Napad se izvede ob pomoči vnaprej posnetega govora, ki uporabnika opozori, da je z njegovim računom nekaj narobe. Nato ga ta posnetek vodi skozi procese, ki na koncu pripeljejo do želenega razkritja zaupnih informacij.

3.4 Neposredni pristop in ankete

Za metodo neposrednega napada s socialnim inženiringom velja, da je

najenostavnejša, vendar tudi nekoliko manj uspešna. Za izvedbo ni potrebna posebna priprava in načrtovanje. Osnovna oblika tega napada je, da **napadalec enostavno vpraša po želeni informaciji** osebo, za katero meni, da z informacijo razpolaga.

Ta metoda lahko vsebuje različne pristope napadalca:

- **Naključni obiskovalec**: Socialni inženir pod **pretvezo anketarja** (študenta, raziskovalca ipd.) spraševanje podjetje in zaposlene razna vprašanja, s pomočjo katerih lahko marsikaj izve o podjetju, kar mu pomaga pri nadaljnjem delu.
- **Pomembni uporabnik**: Socialni inženir se žrtvi predstavi kot eden pomembnih (hierarhično višjih) članov podjetja in mu na primer razloži, da mora nujno dokončati neko pomembno nalogo ter s tem žrtev prepriča, da mu posreduje želene informacije.
- **Nemočen uporabnik**: Socialni inženir se pretvarja, da je novo zaposleni v podjetju in da se še ne spozna na računalniško opremo ter prosi žrtev, naj mu pomaga, če je potrebno tudi z administratorskim uporabniškim geslom.
- **Oseba za tehnično pomoč**: Socialni inženir se pretvarja, da je eden od članov tehnične podpore (administrator) in da mora nekaj popraviti. Žrtvi enostavno reče, da potrebuje njeno uporabniško ime in geslo.

3.5 Gledanje čez ramo (shoulder surfing)

Socialni inženir opazuje čez žrtvino ramo podatke, ko se žrtev prijavlja v poslovni sistem. Podatke, ki pomenijo koristno informacijo, na primer uporabniško ime in geslo, si socialni inženir zapomni in se z njimi okoristi.

Do takšnega napada prihaja tudi v trgovinah pri **plačevanju s kreditnimi karticami** ali pri **dvigu gotovine na bankomatih**, ko napadalec sledi žrtvinim gibom, ko vtipka geslo. Če žrtev za več storitev uporablja isto geslo, je delo socialnega inženirja s tem še lažje.

3.6 Brskanje po smeteh (dumpster diving)

Veliko informacij lahko socialni inženir pridobi z **brskanjem po smeteh**, kar s tujko imenujemo tudi *dumpster diving* ali *trashing*. V smeteh lahko socialni inženir najde marsikaj »uporabnega«, kar mu koristi pri spoznavanju tarče, kot je na primer stara računalniška oprema, diski s podatki, zavrženi dokumenti z raznimi gesli, telefonski imeniki, naslovi zaposlenih, organizacijske sheme podjetij, koledarji ipd.

Vse naštete stvari lahko predstavljajo neprecenljive vire socialnemu inženirju. Telefonski imenik mu bo podal seznam zaposlenih, delovna mesta in številke, ponekod celo privatne številke. Organizacijske sheme bodo ponazorile pomembnost in položaj zaposlenih v podjetju. Kratka sporočila, zapiski bodo dodali svoj delček v mozaik o predstavi osebe, ki je odvrgla sporočilo. Odvrženi pravilniki in smernice podajo sliko o varnosti in organiziranosti podjetja. Koledarji nakažejo odsotnosti in čas, kdaj se socialni inženir lahko osredotoči na napad. Razna navodila, občutljivi podatki, gesla, sistemske nastavitve lahko predstavljajo vir tehničnih informacij in opremo, s katero podjetje posluje. Med dokumenti se lahko znajde tudi kakšna varnostna politika, s katero lahko socialni inženir ugotovi, s kako varovanim podjetjem ima opravka.

3.7 Nosilci podatkov (CD/DVD mediji, USB ključki, ipd.)

Male nosilce podatkov odlikuje praktičnost, so lahki in prenosni, hkrati pa glede na svojo velikost sprejmejo veliko količino podatkov. Ravno zaradi njihove popularnosti in vsesplošne uporabnosti lahko hitro postanejo način, kako izrabiti nepazljivost žrtve.

Socialni inženir napad s pomočjo USB ključka navadno izvede tako, da **ključek s škodljivo programsko kodo pusti na javnem kraju**, kjer ključek čaka na žrtev. Ker smo ljudje po naravi zvedavi, ključek nekdo pobere in ga pogosto brez pomisleka vtakne v računalnik. Ob tem se na računalniku zažene program, ki z računalnika pobere vsa shranjena gesla in jih pošlje na elektronski naslov napadalca. Lahko se celo zgodi, da se s ključka samodejno namesti trojanski konj ali podobna škodljiva programska oprema.

Leta 2006 je novica o takem napadu prenekaterega uporabnika predramila iz navidezne varnosti, saj skoraj nihče ni posumil, da je lahko navaden USB ključek zmožen tako prodornega napada. Podjetje s področja varnosti je dobilo nalogo, da analizira varnost neke banke, še posebej pa se je moralo osredotočiti na socialni inženiring. Varnostno podjetje je razvilo aplikacijo, ki so jo namestili na dvajset USB ključkov, te pa raztrosili v okolici banke. Aplikacija je bila prirejena tako, da je izgledala kot navadna slikovna datoteka (imeSlike.JPG.exe), in ko je žrtev kliknila nanjo, je aplikacija pregledala delovno postajo in preko elektronske pošte poslala uporabniška imena in gesla nazaj v varnostno podjetje. Od dvajsetih USB ključkov so jih uslužbenci banke našli petnajst in vseh petnajst je preko e-pošte poslalo informacije v varnostno podjetje.

3.8 Ostalo

Piškotki (cookies)

Piškotki so majhne tekstovne datoteke, ki se shranijo na uporabnikovem računalniku ob obisku spletne strani. Njihov namen je poenostavitev uporabnikovega dela. Nekatere spletne storitve zahtevajo uporabniško ime in geslo in da ob ponovnem obisku ni potrebno znova vpisovati teh podatkov, nam lahko ob pripadajoči izbiri pomagajo prav piškotki. Spletne trgovine nam tako kar same ponujajo že izbrane artikle, ki so bili izbrani ob zadnjih obiskih teh strani. Poznamo časovno omejene in trajne piškotke. Razlikujejo se po svoji obstojnosti, ki je določena od spletne aplikacije, ki jih je ustvarila. Nekateri poidejo že ob zaprtju brskalnika, nekateri po določenem času. Piškotki lahko tudi kršijo zasebnost, če posameznik o njih ni ustrezno obveščen in npr. lastniki spletnih strani zaznajo uporabnikovo nakupovalno obnašanje na spletu in tako sestavijo uporabniški profil.

Mobilni telefoni, dlančniki, tehnologija modri zob

Dnevi, ko so se mobilni telefoni uporabljali zgolj pogovorno, so prešli. Izpopolnjene funkcije kot so integrirana kamera, koledar sestankov, igre, multimedijski sporočilni sistem-MMS, infrardeča in modrozoba (*Bluetooth*) komunikacija, z možnostjo brskanja po spletnih straneh, pretvarjajo običajen mobilni telefon v majhno večpredstavnostno, multifunkcijsko napravico. Hkrati pa velja, da z več ponujenimi funkcijami in storitvami večamo ranljivost in šibimo varnost naprav.

Večina sodobnih mobilnih telefonov podpira modri zob komunikacijo in s tem lahko hitro pride do nepooblaščenega dostopa do koledarja, imenika, celo do shranjene pošte. Velikokrat se namreč zgodi, da z vključitvijo storitve modrega zoba na svojem telefonu zaznamo prisotnost drugih naprav. S par potezami bi lahko prišli celo do slik lastnikov teh naprav. Veliko varnostno luknjo pa predstavljajo ponujene možnosti snemanja multimedijske vsebine (slik, iger, tonov itd.) od nepreverjenih ponudnikov zabavne industrije.

Brezžična omrežja (WirelessLan)

WLAN kratica pomeni *Wireless Local Area Network*, v prevodu brezžično omrežje. S to tehnologijo komunicirajo različne naprave, notesniki, mobilni telefoni, tiskalniki, projektorji in druge naprave, ki imajo potrebo po mobilnosti. Delujejo na različnih frekvenčnih območjih in z različnimi razredi varnosti. S primerno nastavitvijo dosegajo tudi do 200 metrov pokritosti okrožja. Varnost oziroma ranljivost komunikacije je v odvisnosti od same konfiguracije naprav za brezžični pristop. Omogočeno je prestrezanje, saj je nosilec oz. medij zrak, in kljub enkripciji prometa obstaja možnost spremljanja prometa[2].

Najhujši primer je namestitev tujega brezžičnega usmerjevalnika direktno v omrežje podjetja. Obiskovalec namesti usmerjevalnik na prosto mrežno vtičnico in ga nekje skrije. Od zunaj na varnem, recimo na parkirišču, pa brez problema dostopa do zaupnih podatkov.

2 Šifriranje prometa z WEP in WPA je že bilo razbito, zato se priporoča uporaba AES šifriranja.

4. Kako se ubraniti pred socialnim inženiringom?

4.1 Varnostne politike

Dobra varnostna politika (varnostni pravilniki po posameznih področjih) v organizaciji je ključ do uspeha v boju proti odtekanju pomembnih informacij podjetja in pred napadi na celoten informacijski sistem v njem. To pomeni, da je potrebno vnaprej zagotoviti, da bodo **zaposleni seznanjeni** s tem, kateri podatki so bolj občutljive narave, in kako z njimi ravnati. Na področju osebnih podatkov Zakon o varstvu osebnih podatkov v 24. členu predvideva sprejem organizacijskih, tehničnih in logično-tehničnih postopkov in ukrepov, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov. Zaposleni v podjetju oz. organizaciji morajo biti s tovrstnimi postopki in ukrepi predhodno seznanjeni, pri tem pa naj ne bi šlo zgolj za dodatno breme delodajalca. S **predhodnim osveščanjem zaposlenih o pomembnosti pazljivega ravnanja s podatki** (osebnimi in drugimi pomembnimi podatki) in o natančnih "pravilih igre" v zvezi s tem, si namreč lahko delodajalec prihrani marsikatero nevšečnost, če ne celo izgube dobička ali sredstev. Pravilniki o varovanju (osebnih) podatkov, nameščanje ustrezne varnostne opreme, obveščanje in učenje zaposlenih o načinu uporabe delovnih sredstev in ostalih postopkih, pri katerih se obdeluje podatke, je torej izjemnega pomena za preprečevanje napadov socialnega inženiringa v podjetju oz. organizaciji.

Varnostne prakse, ki jih je smiselno uvesti za zaščito pred socialnim inženiringom, so sledeče:

- **Pravilnik o postopkih in ukrepih za zavarovanje osebnih podatkov**: Pravilnik mora določati organizacijske, tehnične in logično-tehnične postopke in ukrepe za zavarovanje osebnih podatkov z namenom, da se prepreči nepooblaščena obdelava osebnih podatkov (pridobivanje, shranjevanje, spreminjanje, priklicanje, vpogled, uporaba, razkritje, sporočanje, posredovanje,…).
- **Hramba podatkov**: Hramba podatkov mora biti jasno opredeljena.
- **Zamenjava gesel**: Varnostna politika bi morala zahtevati uporabo mešanih znakov (številk, velikih in malih črk) pri ustvarjanju gesel. Določiti bi morala tudi pogostost menjave in minimalno dolžino gesel.
- **Pomoč zaposlenim**: Varnostna politika mora **prepovedati kakršnokoli posredovanje gesel brez preverjanja istovetnosti osebe** s sledečimi metodami:
  - zaposlenega **pokličemo nazaj**, da preverimo lokacijo (če je res klical s svojega delovnega mesta),
  - z uporabo identifikacije klicatelja na telefonu,
  - pri e-pošti z uporabo elektronskega podpisa zaposlenega,
  - s tem, da vztrajamo, da morajo zaposleni sami prevzemati želene informacije.
- **Nadzor dostopa**: Varnostna politika bi morala določiti, ali je potrebno podpisati varnostni sporazum pred dovoljenim dostopom do omrežja in prostorov; kdo ima pravico dodeljevati dostop do sistema in kakšne pravice lahko dodeljuje; metode za ustvarjanje uporabniških računov in njihovo brisanje; postopke za ustvarjanje uporabniških računov in brisanje le-teh.
- **Fizično varovanje**: Ključne predele je treba označiti in primerno zaščititi dostop, sam dostop pa dovoliti samo upravičenim osebam. Ključev do varovanih mest se ne sme puščati na vidnih in dostopnih mestih. Katerikoli vstop v službene prostore je treba identificirati in kontrolirati.
- **ID zaposlenega**: Podjetje naj opredeli politiko razpoznavanja zaposlenih (ID kartica, ključ, koda,…), prav tako naj vsak gost ob prihodu dobi začasno kartico. Tovrstni ukrepi se lahko v manjših okoljih, kjer se vsi medsebojno poznajo, ustrezno prilagodijo (oz. omilijo), so pa toliko bolj pomembni v večjih sistemih, kjer se ljudje med seboj osebno ne poznajo. Zaposleni naj se navadijo identificirati vsakogar brez kartice in zahtevati, da se predstavi.
- **Uničevanje dokumentov**: Vsak pomemben dokument, ki ga ne potrebujemo več, je treba uničiti z rezalnikom dokumentov oz. ga kako drugače avtorizirano uničiti. Vsi magnetni mediji morajo biti pred zavrženjem očiščeni vseh podatkov ali fizično uničeni.
- **Modemi in brezžične dostopne točke**: Politika bi morala jasno opredeliti, da modemi in brezžične dostopne točke niso dovoljeni v omrežju podjetja, saj s tem ustvarjajo varnostno luknjo v omrežju in deloma izničujejo vlogo požarnega zidu. Če se že nameščajo, naj bodo nameščeni z vsemi varnostnimi ukrepi.

10 priporočil za varna gesla:

1. Gesla naj bodo dolga vsaj 6-7 znakov.
2. Vsebujejo naj alfanumerične znake (velike in male črke, simbole in številke).
3. Gesel ne zapisujemo na listke! Če se temu ne moremo izogniti, listkov nikakor ne hranimo v bližini računalnika (na monitorju, pod tipkovnico, pod telefonom, v lahko dosegljivih predalih ipd.)
4. Gesla redno menjujemo. Priporočljivo jih je menjati vsak mesec ali pa vsaj na vsake tri mesece.
5. Ne uporabljamo starih gesel in ne kombiniramo preteklih gesel z dodatnimi številkami (npr. janez1, janez2 itd.)
6. Ne uporabljamo zaporednih črk ali števil (npr. "abcdefg" ali "234567") in ne uporabljamo sosednjih tipk na tipkovnici (npr. "qwertz").
7. Ne uporabljamo besed, ki se nahajajo v slovarjih in ne uporabljamo gesel, ki jih je lahko uganiti ali njihovih običajnih kombinacij (imen hišnih ljubljenčkov, partnerjev, otrok, avtov, registrskih številk, letnic in datumov rojstev ipd.).
8. Dobro in varno geslo je takšno, ki ga vemo samo mi, obenem pa si ga je lahko zapomniti in ga ni potrebno nikjer zapisovati.
9. Kako torej sestaviti varno geslo, ki pa si ga je tudi lahko zapomniti in mi ga ni potrebno zapisovati? Dobro in varno geslo lahko enostavno sestavimo tako, da si npr. izberemo priljubljeno pesem in uporabimo recimo prve črke posamezne besede, npr.: **N**a **P**lanincah **S**ončece **S**ije, **N**a **P**lanincah **L**uštno **J**e. Če med prvim in drugim verzom dodamo še nekaj številk, recimo svojo težo, višino ali kaj podobnega, kar vemo bolj ali manj samo mi, dobimo geslo, ki si ga hitro zapomnimo, obenem pa je precej varno: **NPSS175nplj**. Pri zamenjavi gesla enostavno uporabimo drugo pesem in drugo številko. In seveda, ne uporabite ravno te pesmice.
10. Ne uporabljajte istega gesla za različne stvari (aplikacije, spletne strani ipd.)!

Tudi pri delu z računalnikom ali drugimi sredstvi doma lahko veliko naredimo z uporabo ustrezne politike gesel ter z nameščanjem in rednim posodabljanjem zaščitne programske opreme. Glede na to, da smo prikazali tudi nekatere druge tehnike socialnega inženiringa (recimo brskanje po smeteh, fizični vdor ipd.), se je vedno, ko imamo opravka z malce bolj občutljivimi osebnimi podatki (bančnimi izpiski, položnicami, različnimi potrdili,…), priporočljivo vesti skrbno in pomisliti, ali bi želeli, da tovrstni podatki pridejo v roke nepoklicanim osebam.

4.2 Izobraževanje in načelo previdnosti

Glede obrambnih mehanizmov, s katerimi se obranimo pred različnimi tehnikami socialnega inženiringa, se lahko **le deloma zanesemo na tehnične rešitve.** Protivirusni programi, programi za prepoznavanje škodljive programske kode, kot so vohunski programi in sledilniki, nas lahko obranijo določenih tehničnih prijemov socialnih inženirjev, ne morejo pa nas ubraniti pred tistimi napadi, ki temeljijo na ne-tehničnih pristopih. Pri slednjih, kot je recimo uporaba telefona, tehnikah pomembnega in nemočnega uporabnika in drugih, pa je predvsem pomembno poznavanje tematike in ozaveščenost zaposlenih. Študija ENISA[1] kot enega izmed hitrih ukrepov priporoča naslednji kontrolni seznam, s katerim preverimo, ali gre za legitimno zahtevo ali pa gre dejansko za poskus manipulacij in izvabljanja informacij:

Legitimnost	Ali se zdi zahteva legitimna in običajna? Npr., ali bi vas res nekdo smel spraševati za te informacije in ali je to tisti način, na katerega bi informacijo običajno predali?
Pomembnost	Kakšna je vrednost informacije, za katero vas sprašujejo, ali pa dejanja, ki naj bi ga izvršili, in kako oziroma za kaj bi lahko to bilo zlorabljeno?
Vir	Ali resnično lahko zaupate viru zahteve? Ali bi to lahko na kakšen način preverili?
Odzivnost	Ali morate odgovoriti takoj? Če imate še vedno dvome, si vzemite čas za dodatne poizvedbe ali poiščite pomoč.

1 »Social Engineering: Exploiting the Weakest Links«; http://www.enisa.europa.eu/doc/pdf/publications/enisa_whitepaper_social_engineering.pdf

Napaka, ki se pojavlja v mnogih podjetjih, je, **da upoštevajo zgolj možnost napada v fizičnem smislu, to pa zaposlene pušča povsem nepripravljene za primer družbeno-psiholoških vplivanj**. Podjetja morajo razumeti, da so vse investicije v programsko opremo popolna izguba, če ne upoštevamo ustreznih mehanizmov za zaščito pred socialnim inženiringom, ki temelji predvsem na psiholoških tehnikah.

Ni dovolj, da se uporabnikom zgolj pove, kako naj se obnašajo. Uporabniki morajo **razumeti in sprejeti razloge**, ki stojijo za varnostnimi pravili. Ena od metod personalizacije varnostnih pravil je, da zaposlenim pokažemo, da karkoli počnejo, vpliva na njih same, kakor tudi na podjetje v celoti; pojasniti pa jim je treba tudi potencialne **izgube in škodo, do katere lahko pripelje napačno ravnanje**. Program ozaveščanja zaposlenih naj služi za informiranje o varnostni politiki, z namenom povečanja dojemanja o morebitnih kritičnih situacijah in ključnih načinih socialnega inženiringa ter metodah za njegovo prepoznavo in obrambo. Uporabnike je priporočljivo obveščati o primerih iz resničnega sveta. Uporabniki morajo torej biti ne samo informirani o varnostnih pravilih, ampak morajo tudi vedeti kako ravnati in zakaj je potrebno tako ravnati.

Uporabniki modernih tehnologij se moramo poleg splošnega izobraževanja za preprečevanje poskusov manipulacij in izvabljanja informacij, **izobraževati tudi o samih tehničnih možnostih, ki jih omogočajo moderne tehnologije.** Osveščeni uporabnik modernih tehnologij ima seveda veliko manj možnosti, da bo postal tarča napada socialnega inženiringa.

Zaradi hitro razvijajoče se tehnologije in vsak dan novih možnosti, ki jih leta prinaša, je potrebno osnovno znanje, ki ga imamo domala vsi uporabniki modernih tehnologij, ves čas izpopolnjevati in prilagajati. Kar je včasih veljalo za neproblematično (varno) uporabo tehnologije ali pa ta sploh še ni bila v uporabi, je morda danes lahko vir tveganj, ki ga bodo napadalci zlahka uporabili proti nam. Glede na poplavo osebnih podatkov tako na internetu kot v različnih zbirkah osebnih podatkov, s katerimi upravlja javni in predvsem zasebni sektor, je pomembno, da se zavedamo, kje so ti potencialni viri tveganja in kako se z njimi spopadati in pred njimi zavarovati.

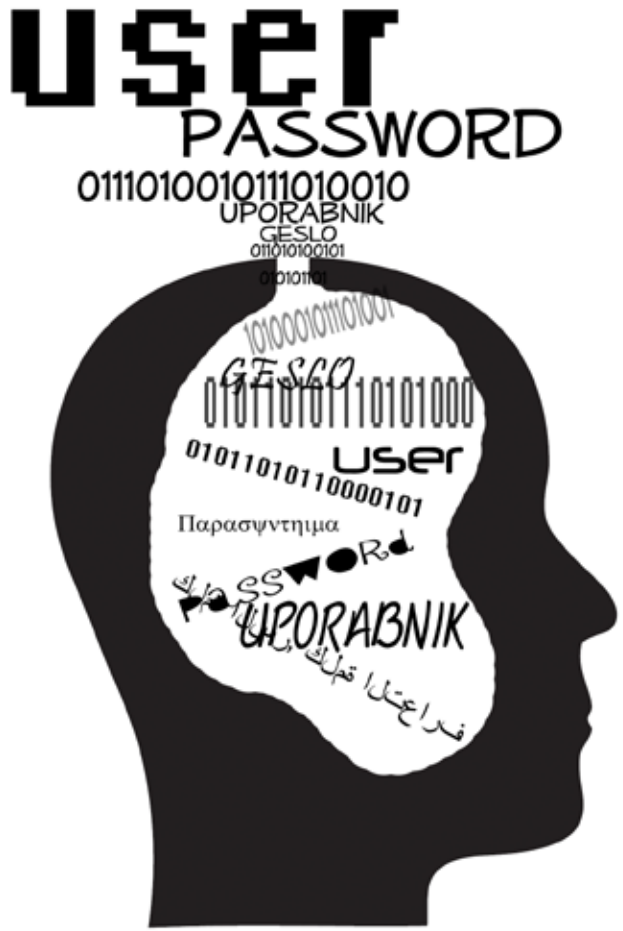
Končno pa se je treba zavedati, da zlorabe niso možne le na internetu (denimo z virusi, s katerimi se ubranimo s protivirusno zaščito), ampak tako rekoč povsod, kjer puščamo svoje osebne podatke; če vržemo dohodninsko napoved v smeti, izgubimo USB ključek z nekodiranimi pomembnimi podatki, nam ukradejo telefon,… Z **razumno mero previdnosti**, ki jo lahko poosebimo le, če se zavedamo možnosti zlorab s socialnim inženiringom in načinov, kako se pred njimi ubraniti, lahko mirno izvršujemo svojo pravico do varstva osebnih podatkov, osebnosti in zasebnosti ter finančnih interesov.

Nekaj običajnih taktik socialnega inženiringa in strategije njihovega preprečevanja:

Območje tveganja	Taktika socialnega inženirja	Strategije obrambe
telefon	hlinjenje in prepričevanje	izučiti zaposlene, da nikdar ne posredujejo gesel in ostalih zaupnosti preko telefona
telefon	hlinjenje in pretvarjanje ob klicu v sprejemno pisarno/«help desk«	vsakemu zaposlenemu naj bo dodeljena PIN koda, ki je specifična za podporo v »help desku«
telefon	kraja dostopa do omrežja in impulzov	kontrola časovno in krajevno oddaljenih klicev, izsleditev klicev, zavračanje prevezave
vstop v stavbo	neavtoriziran fizični dostop	nepropustna varnost z identifikacijskimi oznakami, urjenje zaposlenih in prisotnost varnostnikov
pisarna	»gledanje čez ramo«	Pri tipkanju gesel bodite pozorni, da vam ne »gledajo pod prste«
pisarna	kraja občutljivih dokumentov	označite občutljive dokumente kot zaupne in jih temu primerno hranite
pisarna	sprehajanje po hodnikih in iskanje odprtih pisarn	zahteva, da so vsi obiskovalci pospremljeni ves čas obiska
sistemska soba in telefonska govorilnica	poskus dostopa, odstranitev opreme in/ali priključitev dodatne opreme za prisvajanje podatkov	telefonske govorilnice, sistemske sobe ipd. morajo biti neprestano pod ključem, beležiti vsak vstop in izstop
odlagališča smeti	brskanje po smeteh	hraniti vse smeti v varovanih območjih, razrez vseh pomembnih odsluženih dokumentov ter ustrezno in dokončno uničenje vseh magnetnih medijev
sprejemna pisarna	vstavljanje ponarejenih pošiljk in drugih dokumentov	zaklenjeni prostori

Območje tveganja	Taktika socialnega inženirja	Strategije obrambe
internet	ustvarjanje lažne programske opreme z namenom vohunjenja in kraje gesel	neprestana pozornost glede sprememb sistema in omrežja, priporočila glede izbire v uporabi gesel
splošno - psihološko	pretvarjanje in prepričevanje	spodbujanje zaposlenih k neprestani previdnosti s pomočjo učinkovitih treningov

Vir: neVARNOST.org



5. Pravno varstvo

5.1 Zakonodaja

5.1.1 Ustava RS

V skladu z 38. členom Ustave RS je zagotovljeno varstvo osebnih podatkov ter prepovedana uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon, vsakdo pa se ima pravico seznaniti z zbranimi osebnimi podatki, ki se nanašajo nanj ter pravico do sodnega varstva ob njihovi zlorabi. To pomeni, da je v skladu z Ustavo RS dovoljena tista obdelava osebnih podatkov, ki je vnaprej predvidena in določno opredeljena v posameznem zakonu.

5.1.2 Kazenski zakonik

Kazenski zakonik Republike Slovenije (Uradni list RS, št. 55/08; KZ-1) opredeljuje kaznivo dejanje zlorabe osebnih podatkov določeno v 143. členu; le-ta določa:

1. Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.
2. Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.
3. Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.
4. Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.
5. Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let.

6. Pregon iz tretjega odstavka tega člena se začne na predlog.

5.1.3 Zakon o varstvu osebnih podatkov

ZVOP-1 kot temeljni in sistemski predpis s področja varstva osebnih podatkov v 1. točki 6. člena določa, da je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, pri čemer je posameznik določena ali določljiva fizična oseba, na katero se nanaša osebni podatek. Obdelava osebnih podatkov pomeni v skladu s 3. točko 6. člena ZVOP-1 kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje.

Poleg načela sorazmernosti iz 3. člena ZVOP-1 je osnovno načelo varstva osebnih podatkov načelo zakonitosti in poštenosti. 2. člen ZVOP-1 določa, da se osebni podatki obdelujejo zakonito in pošteno. **Pridobivanje osebnih podatkov s tehnikami socialnega inženiringa in zloraba pridobljenih osebnih podatkov za pridobivanje koristi** torej ne ustreza zahtevi po zakoniti in pošteni obdelavi osebnih podatkov in predstavlja **kršitev ZVOP-1**.

8. člen ZVOP-1 predpisuje obvezne pravne podlage za obdelavo osebnih podatkov in določa:

1. Osebni podatki se lahko obdelujejo le, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana osebna privolitev posameznika.
2. Namen obdelave osebnih podatkov mora biti določen v zakonu, v primeru obdelave na podlagi osebne privolitve posameznika pa mora biti posameznik predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov.

V primeru socialnega inženiringa je posameznik, torej »žrtev«, v nekaterih primerih podal svoje soglasje (recimo, ko je napadalcu sama posredovala osebne podatke), vendar to **soglasje nikakor ni bilo informirano**. Tako soglasje, pridobljeno z goljufijo ali prevaro, je torej nično in se šteje, kot da nikoli ni bilo podano. Socialni inženir (navadno so to fizične osebe ali osebe zasebnega sektorja) torej ni imel pravne podlage - osebne privolitve posameznika - za obdelavo njegovih osebnih podatkov in jih je obdeloval nezakonito. V vsakem primeru pa posameznik v slučaju, da je bil žrtev socialnega inženiringa, ni bil »predhodno pisno ali na drug ustrezen način seznanjen z namenom obdelave osebnih podatkov«. Še več; napadalec je **žrtev zavedel**, da se bodo osebni podatki uporabili za namene, ki bodo posamezniku morda celo koristili (obljubljeno popravilo strežnika, izvršeno naročilo, nagrada,…), v resnici pa gre za obdelovanje osebnih podatkov v nasprotju z namenom, za katerega so bili pridobljeni.

24. člen ZVOP-1 določa, da zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:

1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. **preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;**
4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov. Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.

Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so **dolžni varovati tajnost osebnih podatkov**, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.

Dolžnost zavarovanja osebnih podatkov je določena v 25. členu ZVOP-1. Upravljavci osebnih podatkov in pogodbeni obdelovalci so dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona. Upravljavci osebnih podatkov v svojih aktih predpišejo postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

Pri socialnem inženiringu je bistvenega pomena, da upravljavci zbirk osebnih podatkov **poleg tehničnih** ukrepov za zavarovanje osebnih podatkov poskrbijo tudi za ustrezne **organizacijske ukrepe**, pri katerih imamo v mislih predvsem **izobraževanje zaposlenih**. Zaposlenim je potrebno **predstaviti nevarnosti socialnega inženiringa, načine prepoznavanja** socialnega inženiringa in **mehanizme za obrambo** pred tovrstnimi napadi. Ustrezno izobraževanje zaposlenih je bistveno tudi z vidika odgovornosti upravljavcev zbirk osebnih podatkov, saj se ob odsotnosti ustreznega izobraževanja lahko ugotovi, da upravljavec osebnih podatkov ni v zadostni meri poskrbel za zavarovanje osebnih podatkov, s tem pa je podana njegova odgovornost za kršitev določb ZVOP-1 o zavarovanju.

5.2 Prijava kršitev

Vsak posameznik lahko Informacijskemu pooblaščencu vloži prijavo, če meni, da je nekdo kršil Zakon o varstvu osebnih podatkov. Pooblaščenec nato po uradni dolžnosti na podlagi Zakona o inšpekcijskem nadzoru izvede ustrezne inšpekcijske postopke. Če posameznik torej meni, da je t.i. socialni inženir obdeloval njegove osebne podatke brez njegove privolitve ali podlage v zakonu, ali pa je osebne podatke s prevaro izvedel ali pridobil s strani oseb, ki so obdelovale osebne podatke pri upravljavcu zbirk osebnih podatkov, lahko vloži prijavo Informacijskemu pooblaščencu.

Škodljive posledice kršitve varstva osebnih podatkov pa so lahko tudi hujše, če izpolnjujejo znake kaznivega dejanja zlorabe osebnih podatkov v skladu s 143. členom KZ-1. V teh primerih se žrtev kaznivega dejanja zlorabe osebnih podatkov lahko obrne na policijo ali tožilstvo ter poda kazensko ovadbo.

Zaključek

Dvigovanje ozaveščenosti ter stalno izobraževanje in izpopolnjevanje že mnogo let veljajo za mantro varnega in uspešnega delovanja v informacijski družbi. To seveda velja tudi ali še posebej pri ravnanju z osebnimi in drugimi podatki. Kaj kmalu se namreč lahko zgodi, da od naše pravice do informacijske samoodločbe (komu, zakaj in kakšne osebne podatke bomo posredovali) ostane le še oddaljen spomin in veliko težav, ki jih moramo reševati, ne da bi bili zanje krivi sami. S premeteno uporabo tehnik socialnega inženiringa se lahko, kot smo že opisali, zgodi, da ostanemo brez sredstev na transakcijskem računu, da utrpimo poslovno škodo ali s kopico drugih nevšečnosti. Preventivno delovanje v smislu učinkovite varnostne politike in uporabo ostalih previdnostnih ukrepov ter učinkovito izobraževanje zaposlenih, ki ravnajo s podatki v podjetju ali organizaciji, lahko prepreči veliko večino poskusov napada s pomočjo tehnik socialnega inženiringa. Seveda pa ima posameznik v primeru, ko se napad že zgodi in so tudi posledice očitne (ali tudi, če te še niso nastopile), možnost vložiti prijavo Informacijskemu pooblaščencu ali celo podati kazensko ovadbo, da bi zavaroval svojo ustavno zavarovano pravico do informacijske zasebnosti. Podatki kažejo, da so opisane možnosti zlorabe osebnih podatkov v porastu, vendar se jim lahko s proaktivnim delovanjem uspešno zoperstavimo.