VIŠJA STROKOVNA ŠOLA ACADEMIA MARIBOR

DIPLOMSKO DELO

Prepoznavanje in preprečevanje pridobivanja zaupnih informacij s pomočjo poslovne medijske komunikacije

Kandidat: Robert Bolko
Študent študija ob delu
Številka indeksa: 11190122557
Program: Multimediji
Mentor: Zlatko Mihaljčič, univ. dipl. soc.

Maribor, januar 2009

ZAHVALA

Iskreno se zahvaljujem vsem, ki ste verjeli vame in me ves čas študija vzpodbujali.

Za mentorstvo in strokovno pomoč pri svojem diplomskem delu se zahvaljujem mentorju Zlatku Mihaljčiču, univ. dipl. soc. Prav tako hvala celotnemu kolektivu VSŠ Academia.

Posebno zahvalo namenjam prof. Sabini Pinter, strokovni prevajalki, za lektoriranje moje diplomske naloge in za vso duhovno podporo.

IZJAVA O AVTORSTVU DIPLOMSKE NALOGE

Podpisani Robert Bolko, št. indeksa 11190122557, rojen dne 18. 5. 1972,

v kraju Maribor sem avtor diplomske naloge z naslovom

Prepoznavanje in preprečevanje pridobivanja zaupnih informacij s pomočjo poslovne medijske komunikacije,

ki sem jo napisal pod mentorstvom g. Zlatka Mihaljčiča, univ. dipl. soc..

S svojim podpisom zagotavljam, da:

- je predložena diplomska naloga izključno rezultat mojega dela.
- sem poskrbel/a, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navadena oz. citirana skladno s pravili Višje strokovne šole Academia.
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oz. misli, kot moje lastne – kaznivo po Zakonu o avtorskih in sorodnih pravicah; UL št. 16/2007; (v nadaljevanju ZASP), prekršek pa podleže tudi ukrepom VSŠ Academia skladno z njenimi pravili.
- Skladno z 32. členom ZASP dovoljujem VSŠ Academia objavo diplomske naloge na spletnem portalu šole.

Kraj in datum, Podpis študenta:

Maribor, 7. 1. 2009

POVZETEK

V diplomski nalogi najprej predstavim osnove komuniciranja. Vse od osnovnega pojma podatka do informacije kot nadgradnje in nazadnje oblikovanja sporočila. Kot manipulacijo in prepoznavanje ter preprečevanje pridobivanja zaupnih informacij, opredelim socialni inženiring v okviru informacijske varnosti in njegove specifične lastnosti kot največjo grožnjo našega časa. V zaključku nadgradim nalogo tako, da se soočim s pridobljenimi rezultati raziskovalne naloge in se z opravljeno analizo in predlogi nagibam k preprostemu stavku.
Korak za korakom k boljši informacijski varnosti.

Ključne besede: podatek, informacija, komuniciranje, manipulacija, socialni inženiring, varnost

ABSTRACT

Giving the introduction of my diploma work, I first start with the fundamentals of communication, going from the basic concept of data to the information as its upgrading and the formation of message in the end.

As manipulation with information and its identification and prevention from gathering confidential information, I define social engineering and its specifics regarding security of information as the greatest threat of our time.

In the closure my diploma work is upgraded with results of my research work and their analysis as well as with my proposals leaning towards the simple sentence.
Step by step to higher degree of information security.

Key words: data, information, communication, manipulation with information, social engineering, information security

KAZALO VSEBINE

SEZNAM SLIK

SEZNAM TABEL

SEZNAM GRAFIKONOV

1 UVOD

1.1 Opredelitev obravnavane zadeve

V času velikega tehnološkega napredka in podajanja multimedijskih vsebin s pomočjo vse hitrejšega razvoja komunikacijskih sredstev in strategij komuniciranja, dosegamo vse večjo povezljivost in smo pod vplivom vse večjega krajšanja osebnostnih relacij med ljudmi. Posledično pa prihaja do vse večjih možnosti manipulacije z informacijami, ki jih lahko v grobem delimo na namerne in nenamerne.

Kot primere namernih manipulacij z informacijami bi podal zlonamerno kodo, konkurenčno vohunjenje, odtekanje zaupnih poslovnih podatkov, sabotaže in podobno. Vse so v glavnem povzročene z določenim ciljem.

Nenamerne manipulacije ali interpretacije informacij, pa opredeljujem kot posledico neobveščenosti in neosveščenosti zaposlenih, bodisi uporabnikov, sodelavcev in navsezadnje odnosa samega vodstva podjetij.

V samem poslovnem komuniciranju v veliki meri varnost temelji na človeškem faktorju in ni popolne zaščite, ki bi to popolnoma eliminirala. Le od nas samih je odvisno, kako intenzivno in s kakšnimi načini, pravilniki in varnostnimi mehanizmi se bomo zaščitili pred tem.

Podatek oziroma informacija sta postala pomembno gibalo našega časa. Postala sta pomembno tržno blago, istočasno orodji za doseganje različnih poslovnih in osebnih ciljev in vse premalo se podjetja tega zavedajo.

Zaradi same narave svojega dela, že več let opravljam skrbništvo nad različnimi informacijskimi infrastrukturami različnih podjetij, katerih dejavnosti obsegajo različne poslovne segmente.

Podjetja komunicirajo v veliki meri na podoben način, razširjajo informacije, sporočajo, objavljajo ali celo oddajajo vsebino, pa naj si bo ta namenjena le delavcem podjetja ali širnemu svetu. Pri tem uporabljajo kombinacijo klasičnega načina komuniciranja
(pogovori, sestanki, poslovni dopisi, seznami ali navodila itd.) in elektronskega (stacionarna in mobilna telefonija, odzivniki, faksi itd.), oziroma spletnega komuniciranja.

Zaposleni uporabljajo spletno medosebno ali medpodjetniško poslovno komuniciranje, predvsem elektronsko pošto in komuniciranje v realnem času, takojšnje komuniciranje s pomočjo klepetalnic, skupinskih portalov, skupnih map in orodij za skupinsko delo.

Še vedno največji delež poslovnega komuniciranja lahko izpostavi telefonija, pa naj bo klasična ali mobilna ter osebni stik in sestankovanje.

Neposredna komunikacija (pogovori, sestanki, predstavitve, delavnice itd.) so del vsakdana, ljudje so fizično prisotni, so v pristnem stiku, ne prihaja do motenj, saj v bistvu ni posrednikov in ne prenašalcev, pa vseeno prihaja lahko do napačnega razumevanja (interpretacije) ali celo do odtekanja informacij.

1.2 Namen, cilji in osnovne trditve diplomskega dela

Namen

Sam namen raziskovalnega dela je osredotočenost na raziskovanje odtekanja, izgube in manipulacije informacij, povzročene s strani poslovne medijske komunikacije, kdo je pri tem v veliki meri udeležen, kaj do tega privede in kako lahko to prepoznamo in postavimo primerne varnostne mehanizme, pa naj bo to odtekanje posledica namerne lastne iniciative ali enostavno nezavednega podajanja zaupnih podatkov.

Namen raziskovalnega dela ni samo v določitvi komunikacijskih točk, možnih kritičnih točk odtekanja informacij in smeri komunikacijskih kanalov, temveč tudi ugotoviti vpliv človeških napak na delež varnostne pomanjkljivosti in zavedanje zaposlenih na teh delovnih mestih. S skupnim imenovalcem, namen mojega diplomskega dela je predstaviti stanje in področje informacijske varnosti in nujnost vzpostavitve sistema varovanja in ozaveščenosti.

Delež vzpostavljene varnostne politike v organizaciji, ki je podprta s strani najvišjega vodstva, je zagotovo ključni vzvod, ki povečuje zavedanje o skrbi za informacijsko varnost med zaposlenimi.

Cilji

Cilj raziskave je analizirati stanje informacijske varnosti in komunikacije v izbranih slovenskih organizacijah. S pomočjo anketnih vprašalnikov, s katerimi bom pridobil ustrezne informacije in s pomočjo analize le-teh, bom opozoril na kritične točke, izluščil raven in spodbudil misel ali dve na to problematiko. Podal bom predloge oziroma priporočila za izboljšanje stanja varnega komuniciranja, hkrati pa vse anketirance posredno s tem dejanjem opozoril na morebitne grožnje.

Osnovne trditve diplomskega dela

V svojem diplomskem delu izhajam iz trditve, da je raven informacijske varnosti in varnost poslovne komunikacije nizka. Največji problem predstavlja po moji predpostavki najšibkejši člen v verigi varnega komuniciranja – **človek**.

V veliki meri pozabljamo na uporabnika (kot ključno varnostno točko), stopnjo njegovega tehnološkega znanja in osveščenosti, navkljub njegovi tehnološki opremljenosti. To bom skušal dokazati z analizo anketnih vprašalnikov, s pomočjo izbranih kriterijev in izbranih organizacij.

1. 3 Predpostavke in omejitve

Predpostavljam, da lahko z več vprašalniki (anketami), ki vsebujejo vsebinsko različna vprašanja, postavljena in namenjena posameznem segmentu anketirancev, določim stanje in odnos do informacijske varnosti.

Predpostavke in omejitve, ki bodo upoštevane v diplomskem delu:

1. Pri raziskovanju je zaradi vsebine vprašalnikov nujno segmentirati anketirance.
   Ciljne skupine:
   - **zaposleni na komunikacijskih točkah** (kritične točke),
   - **informatika** (odgovornost za varnost pretoka informacij),
   - **vodstvo organizacije** (najvišja raven podjetja) .
2. Skrbna izbira vprašanj za posamezni segment anketirancev.
3. Izbrana vprašanja so ključno izbrana iz množice vprašanj standardov informacijskih varnosti, ki so vpeljani v tujini in tam predstavljajo stalno prakso ter vprašanja, ki so izšla iz same raziskovalne naloge.
4. Raziskava se nanaša samo na določen del informacijske varnosti, osredotočenost je na medijsko komuniciranje in tveganje človeškega faktorja.
5. Podatki, ki bodo uporabljeni v diplomskem delu, so poslovna skrivnost posameznega podjetja, zato imena podjetij in posamezne fizične osebe ne bodo razkrite.
6. Podatki se bodo uporabili izključno za analitični in statistični pregled.
7. V anketo bo zajetih najmanj 100 anketirancev iz več kot 25 podjetij.

Zbiranje in dostop do podatkov je otežen, saj se loteva varnostnih in osebnih podatkov. Zahteva soglasje vodstva, seveda v vsakem pogledu sodelovanje in pripravljenost samih zaposlenih. Verjamem, da je zanimanje za pridobljene rezultate veliko, ne dvomim pa, da je za posamezno podjetje v začetku lahko že dovolj, da se zave svojih kritičnih informacijskih točk in temu primerno lahko ukrepa.

1. 4 Predvidene metode raziskovanja

Pri izdelavi raziskovalnega dela bi uporabil naslednje metode preučevanja:

1. Teoretično raziskovanje, ki zajema zbiranje in urejanje obstoječe literature in znanj.
2. Deskriptivni pristop v smislu podrobnega opisa izpostavljenega problema, vpliva človeškega faktorja, manipulacije, odtekanja informacij v poslovnem medijskem komuniciranju, od podatka kot najmanjše enote do informacije oziroma sporočila. Opisal bom uporabo instrumentov, varnostnih mehanizmov, ki so na voljo uporabnikom komunikacijskih sredstev, in opreme.
3. Analitični pristop v smislu priprave vprašalnikov in izvedbe v določenem terminu, pri čemer bom uporabil metodi kompilacije in komparacije.

Iz izbrane literature in pridobljenih znanj, bi najprej predstavil različne vrste medijskega komuniciranja in kot rdečo nit podrobneje področje manipulacije in izkoriščanja človeške zaupljivosti in ranljivosti, v tujini označenega s terminom »**Social Engineering**«.
Nato bi se osredotočil na varnost poslovnega sistema, pomen revizije in standardov.
Z rezultati ankete bi pridobil primerjalne vrednosti, jih analiziral ,podal zaključke in dosežen cilj.

2 OSNOVE KOMUNICIRANJA

2.1 Podatek in informacija

Vse pogosteje sta izraza podatek in informacija uporabljena kot sinonima, čeprav obstaja med njima precejšnja pomenska razlika.
Razlog tiči morebiti v času vse večjega zbliževanja in enačenja procesov v človeški glavi s procesi v računalniku. Navsezadnje je človek snovalec programov, ki vodijo vsestransko komunikacijo s strojno opremo, v vsej možni interakciji med človekom in računalnikom (angl. *human computer interaction*).

2.2 Podatek

V Slovarju slovenskega knjižnega jezika je podatek opredeljen kot dejstvo, ki o določeni stvari nekaj pove ali se nanjo nanaša (SSKJ, 2008).

Iz povzetka definicije iz standarda ISO/IEC2382, *Information Technology Vocabulary*, je podatek predstavljen kot predstavitev informacije na formaliziran način, ki je primeren za komunikacijo, interpretacijo ali obdelavo (s strani človeka ali stroja).
Definicija pravi, da mora biti predstavitev izvedena na formaliziran način, kar pomeni, da mora obstajati nek predpis - konvencija, po katerem simbole ali vrednosti analognih veličin zapisujemo oziroma beremo. [http://dmst.aueb.gr/dds/bib/isostd.htm].
Nekoliko starejša definicija iz istega vira pa pravi, da je podatek poljubna predstavitev s pomočjo simbolov ali analognih veličin, ki ji je pripisan ali se ji lahko pripiše nek pomen.

Iz definicije lahko izluščimo, da je podatek lahko diskreten, če se pri predstavitvi uporabljajo simboli ali podatki, ki jih dobimo s štetjem (npr. vrednost temperature, stran v knjigi, dan v mesecu, število oseb v avtobusu itd.), ali pa analogen, če se za predstavitev uporablja kakšna fizikalna veličina (npr. dolžina živosrebrnega stolpca, čas v peščeni uri, hitrost avtomobila na tahometru s kazalcem, dolžina elastične vrvice, količina vode v posodi itd.).
Obema definicijama je skupno to, da se podatku lahko pripiše nek pomen na osnovi določenega predpisa oziroma znotraj nekega konteksta. V svoji zasnovi je podatek vedno opis ali zapis nekega pojava ali dejstva in je lahko predstavljen v številčni, tekstovni ali grafični obliki.
[http://dmst.aueb.gr/dds/bib/isostd.htm]
Medtem, ko je podatek nek surov, nepovezan, kvaliteten ali kvantiteten element, je informacija povezana z odgovori na vprašanja, situacije ali dejstva in tako predstavlja končni proizvod. [http://www.academia.si/clanek/1-tiho-znanje-pridobljeno-z/stran-2.html]

Podatek je zgolj zabeležen element brez prave smiselne vsebine. Podatek preide v informacijo takrat, ko ga lahko povežemo z nekim drugim podatkom in vsebinsko zaključimo. Ko tako smiselno povežemo več podatkov med seboj, dobimo novo, vsebinsko zaključeno in jasno sporočilo, ki se imenuje informacija. (Ivanuša, 2008, 1; povz. po Eppler, 2003, 18).

2.3 Informacija

Z vsako informacijo lahko izveš nekaj, česar pred tem še nisi vedel, širiš obzorje, znanje, vendar le pod pogojem, da je bila prejeta informacija razumljena. Informacija lahko predstavlja nekaj nejasnega, nekaj kar prejmeš šele takrat, ko se v tvojih možganih zbudi določena predstava.

Če je količina podatkov prevelika, se lahko zgodi, da s podatki ni posredovana nobena informacija. Ponavljajoča informacija pa lahko vodi k zmanjšanju negotovosti in k lažjemu odločanju.

Osnovne dimenzije informacije so količina, kakovost in vrednost.

Definicija pomena besede informacija je v standardu ISO/IEC2382*, Information Technology Vocabulary*, opisana kot: »Informacija je znanje, ki se nanaša na objekte kot so dejstva, dogodki, stvari, procesi ali ideje, vključno s koncepti, ki imajo v okviru nekega konteksta določen pomen.«

Informacija je pomen, ki ga človek lahko pripiše podatkom s pomočjo znanih konvencij, ki so uporabljene pri njihovi predstavitvi.« Informacija so ovrednoteni podatki v specifični situaciji«, to definicijo je zapisal G.C. Everest leta 1986, malo drugače, a se po pomenu vsekakor ujema s predhodnico. Avtor ene izmed zelo znanih definicij informacije je Börje Langefors,leta 1980. (Mohorič, 1999, 446).

Definicija je znana tudi pod imenom informacijska enačba. Informacija je novo spoznanje, ki ga človek doda svojemu poznavanju sveta. Odnos med informacijo, podatki, časom in interpretatorjevim znanjem predstavlja informacijska enačba: **I = i (D, S, t)**:

I - informacija, ki jo posredujejo podatki, **i - informacijska funkcija**, **D - podatki**, **S - prejemnikovo znanje**, **t - čas**, ki je na voljo prejemniku za interpretacijo podatkov.

Zaključki, ki jih je povzel Langefors iz omenjene definicije, pa so na kratko naslednji:

- podatki niso informacija,
- podatki ne vsebujejo informacije,
- podatki posredujejo informacijo prejemniku, katerega znanje je konsistentno z izbrano predstavitvijo podatkov in modelom sveta, na katerega se nanašajo,
- če je količina podatkov tako velika, da se jih v času, ki je na voljo za ukrepanje na njihovi osnovi, ne da interpretirati, se lahko zgodi, da s podatki ni posredovana nobena informacija.

Langeforsovo definicijo je zanimivo primerjati z definicijo informacije, ki se uporablja v informacijski teoriji. Informacija je v tem primeru definirana kot:

»znanje, ki zmanjša negotovost, povezano s pojavom določenega dogodka iz končne množice možnih dogodkov.«

Informacija je takšno zaporedje znakov v danem znakovnem sistemu, ki :

- je sintaktično pravilo,
- ima nedvoumno semantično vsebino,
- ima za upravljavca pragmatično vrednost (Mohorič, 1999, 447).

Informacijo lahko obravnavamo na več načinov, ima več dimenzij (Gradišar, 1998, 508), te so:

- informacijska vsebina - semantična vrednost informacije
- pragmatična lastnost informacije - informacijska vrednost
- informacijska količina
- sintaktična vrednost

Informacijska vsebina je karakteristika, ki loči podatek od informacij. Izraža se z uporabno vrednostjo informacije.

Pragmatičnost informacije pomeni vrednost in korist informacije v odvisnosti od časa.

Informacijska količina pove, da informacijo lahko merimo. Enota za merjenje količine informacije je bit.

Sintaktična vrednost pomeni, da mora biti informacija podana formalno pravilno. Sintaktična razsežnost opredeljuje formalno pravilnost zapisa v določenem znakovnem sistemu. Nanaša se torej le na izbrani znakovni sistem, ki pa mora biti takšen, da je z njim mogoče izraziti želeno sliko, pojav. Sintaktična razsežnost obsega torej celoto odnosov med znaki v določenem znakovnem sistemu. Sintaksa danega znakovnega sistema določa, kako v množici znakov oblikujemo in preoblikujemo formalno pravilna sporočila, npr. v slovenskem jeziku iz besed pravilne stavke. (Gradišar, 1998, 509)

Po definiciji iz knjige *Teorija informacij* , avtorja (Shannon, 1948), predstavlja informacija novo spoznanje, ki ga človek doda svojemu poznavanju sveta.

Prejeta informacija spremeni naše znanje, vpliva na naše odločitve in ravnanje.

Informacija predstavlja neko novo znanje , zmanjša negotovost, ki je posledica pomanjkanja informacije. Tako mora biti naslovljena na konkretnega uporabnika.

Kakovost informacij je lahko definirana takole:

- dostopnost
- točnost
- pravočasnost
- popolnost
- zgoščenost
- ustreznost
- razumljivost
- objektivnost

Relacija podatek- informacija

Karakteristika, ki loči podatek od informacije, je informacijska vsebina; izraža se z uporabno vrednostjo informacije.

Relacija informacija- sporočilo

Z informacijo odpravljamo neko nedoločenost, pove nam nekaj, česar še nismo vedeli.
Sporočilo pa nastane, ko podatke komu sporočimo, posredujemo, lahko pa sporoča nekaj, kar prejemnik že ve (v tem primeru ne zmanjša nedoločenosti, negotovosti).

Kdaj nastane informacija sporočilo?

Takrat, ko je sporočilo v danem znakovnem sistemu pravilno (sintaktična pravilnost), ima nedvoumen pomen (vsebinska ali semantična pravilnost) in ima za prejemnika uporabno vrednost (pragmatičnost).

2.4 Sporočilo

Sporočilo so podatki, ki jih s posredovanjem medija odpošlje pošiljatelj prejemniku. Pošiljatelj mora svoje koncepcije najprej predstaviti s pomočjo jezika in simbolov, šele nato na določenem mediju posredovati prejemniku. Na drugi strani pa mora prejemnik seveda poznati jezik in tudi simbole, s katerimi je sporočilo zapisano. Sporočila še vedno ne bomo znali interpretirati, če ne poznamo koncepcij, šele če razumemo jezik in poznamo simbole s katerimi je sporočilo zapisano, bomo vedeli, kaj nam sporočilo sporoča. Sporočilo torej znamo prebrati in ga razumemo v tem primeru.
V informacijskem slovarju je sporočilo definirano kot strnjen, smiseln niz simbolov in signalov, ki jih pošiljatelj, oddajnik usmerja k naslovniku, sprejemniku na določen način in z določenim namenom. [http://www.islovar.org].
Poznamo več oblik sporočil, nam najbolj znano je elektronsko sporočilo, signalizacijsko ali opozorilno sporočilo in celo lažno sporočilo (*Hoax).* Pri komunikaciji med ljudmi pa lahko ločimo sporočila na verbalna in neverbalna.

2.5 Komuniciranje

Beseda komunikacija izvira iz latinske besede *communicare*, kar pomeni posvetovati se, razpravljati o nečem, vprašati za nasvet. Ko komuniciramo, prenašamo sporočila s pomočjo različnih simbolov (besed, kretenj, govorice telesa, slik, svetlobnih in zvočnih simbolov…). Komuniciranje je sestavni del našega življenja.
(Mihaljčič, 2006, 12)

Strokovni izraz »komuniciranje« se uporablja tako v družboslovju kot humanistiki in tehničnih znanostih, na primer v računalništvu, elektrotehniki ipd.

Komunikacija je torej proces, v katerem vsi udeleženci sprejemajo, pošiljajo in interpretirajo sporočila oz. simbole, ki so povezani z določenim pomenom. Je vedno dvosmeren proces, saj je povezana s sočasno medsebojno zaznavo in hkratno medsebojno izmenjavo sporočil.

Komunikacija nam omogoča usklajevanje mnenj, doseganje različnih ciljev, pa tudi vzpostavljanje, vzdrževanje in spreminjanje medosebnih odnosov. Čeprav je veščina komuniciranja najpomembnejša izmed vseh, ki jih ljudje sploh imamo, se je le malokdaj načrtno učimo.

Učinkovito komuniciranje oziroma pošiljanje sporočil: sporočilo mora biti razumljivo, pošiljatelj mora biti zaupanja vreden, pomembna je tudi povratna informacija (*feedback*) o tem, kako je sporočilo vplivalo na prejemnika.

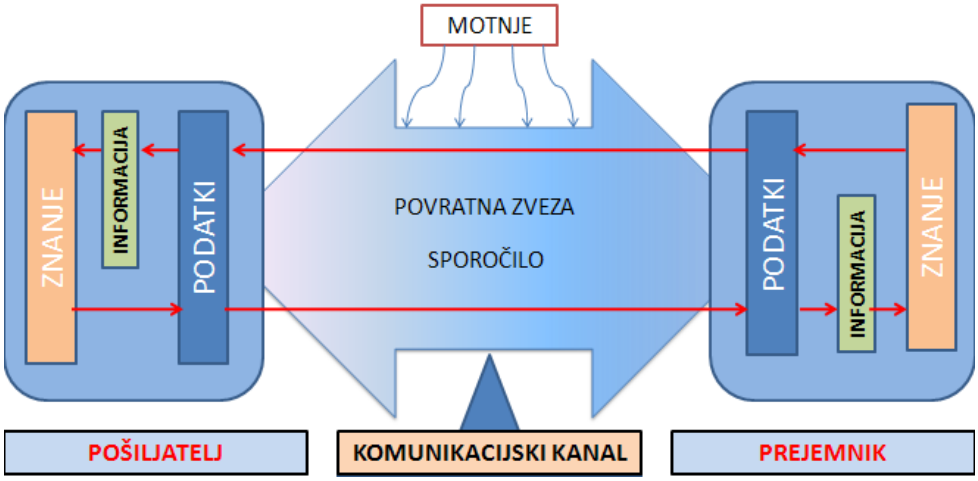
Ker je komuniciranje zelo pomembno, ga želimo vedno izvesti brez motenj oziroma težav. Svoj namen želimo doseči s čim manj napora in v čim krajšem času. Če le-ta poteka brez motenj, lahko govorimo o kakovostnem komuniciranju.

Podatke posredujemo prejemniku vedno na kakšnem sredstvu ali mediju, ki nam služi za njihov prenos. Transport se vrši preko tako imenovanega komunikacijskega kanala. Sam medij lahko predstavlja list papirja, slika na platnu, posneta glasba na zgoščenko itd.

Če je bila prejeta informacija posredovana preko več medijev, je njen učinek še večji in komuniciranje še bolj kakovostno.

Uporabimo lahko termin *multimedijsko* komuniciranje, ki pomeni komuniciranje preko več medijev, večji del s pomočjo računalnika in različnih komunikacijskih sredstev.

Slika 1: Komunikacijski kanal



Vir: lasten

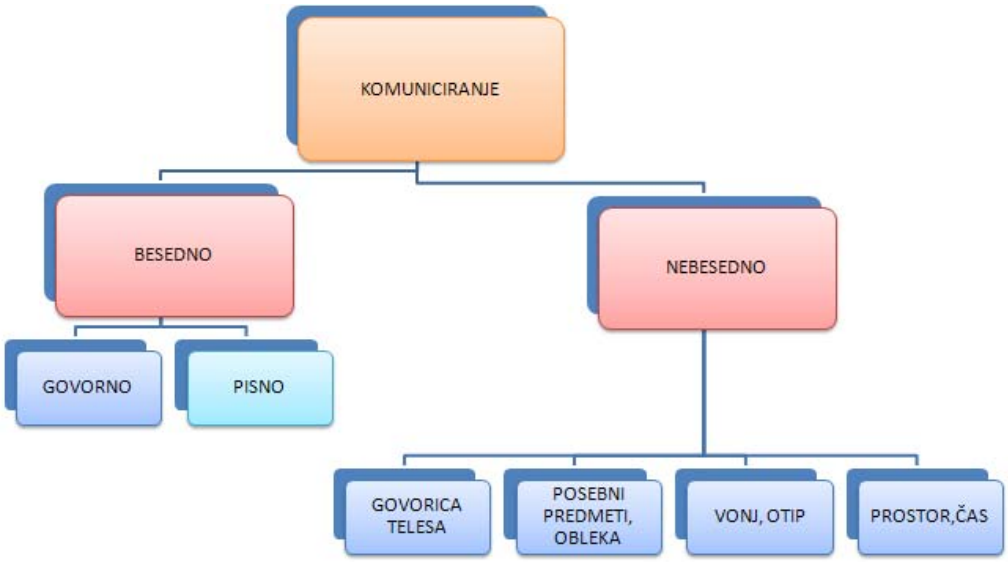
Najbolj preprost komunikacijski sistem predstavljajo štiri sestavine:
pošiljatelj, prejemnik, sporočilo in komunikacijska pot, kanal.
Pošiljatelj je oseba, ki sporočilo tvori in oddaja. Prejemnik je oseba, ki ji je sporočilo namenjeno in ki sporočilo sprejme, razume. Sporočilo vsebuje dejstvo, mnenje, željo, skratka informacije, ki jih želi pošiljatelj prenesti prejemniku. Komunikacijska pot je kanal, po katerem potuje sporočilo od pošiljatelja k prejemniku. Glede na komunikacijsko pot pa lahko razlikujemo neposredno in posredno komuniciranje. Za neposredno komuniciranje je značilno, da ne vključuje tehničnih vmesnikov med pošiljatelji in prejemniki, ampak samo človekove oddajne komunikacijske organe (za govor, kretnje, mimiko) in sprejemna čutila (sluh, vid, tip), posredno komuniciranje pa temelji na specifičnih tehničnih nosilcih slike, zvoka in podatkov (papir, žični in brezžični aparati za prenos avdio in video signala, elektronskih podatkov) in na ustreznih tehničnih aparatih za prepoznavo jezika komuniciranja (kodiranje, dekodiranje). Posredno komuniciranje običajno označujemo kot komuniciranje preko »medijev«. (Mihaljčič, 2006, 16)
Medium, latinsko, je srednji del ali prostor, lahko bi ga označili kot »nosilec« v našem primeru.

Sestavine komunikacijskega sistema

Besedno komuniciranje : neposredno ali z uporabo tehničnih sredstev (telefon, radio ipd.).
Pisno komuniciranje: za prenos besed uporabljamo pisavo in temu ustrezna sredstva (pisma, časopisi, revije, oglasne plošče ipd.).
Elektronsko komuniciranje: pri tem za prenos glasu ali pisave uporabljamo elektronska sredstva (računalnike, mreže ipd).
Vse tri vrste komuniciranja pa imajo svoje prednosti in slabosti.

Načini komuniciranja

Slika 2: Načini komuniciranja



Vir: lasten

Govorno komuniciranje ima vrsto prednosti. Je hitro, običajno zajema tudi povratno informacijo ter omogoča sočasno komuniciranje z več ljudmi. Govorno sporočilo lahko oddamo v trenutku, ko smo ga v mislih izoblikovali. Prav tako hitro ga lahko tudi preoblikujemo, dopolnimo, spremenimo. Pomembno je, da lahko med pogovorom zlahka preverimo ali je bilo sporočilo pravilno razumljeno ali ne, ali je doseglo želeni cilj. Napako lahko takoj popravimo. Slabosti govornega sporočanja pa se pokažejo takrat, kadar pri prenašanju takega sporočila sodeluje več ljudi. Čim več ljudi sodeluje pri prenašanju sporočila, tem več je možnosti, da se bo sporočilo, ki doseže sprejemnika, bistveno razlikovalo od poslanega sporočila (Možina, Tavčar, Zupan in Kneževič, 2004, 54).

Prednost pisnega komuniciranja so jasnost, nazornost, trajnost. Pošiljatelj in sprejemnik posedujeta dokumentiran zapis sporočila kot dokaz in kot dokument za arhiviranje. Pisne komunikacije so ponavadi bolj dodelane, logične in jasne. Slabosti pisnega komuniciranja pa se kažejo predvsem v porabljenem času za njegovo snovanje. Veliko težje in zamudno je tudi preverjanje ustreznosti razumevanja nekega pisnega sporočila (Hribar, 2001, 16).

Prednosti elektronskega komuniciranja so , da so informacije hitro posredovane, so točne in natančne. Slabosti pa so, da ni vedno znano ali je prejemnik sporočilo razumel kot je bilo mišljeno in če je sporočilo videl ta pravi prejemnik, kateremu je bilo sporočilo namenjeno.
(Treven in Sriča, 2001, 198)

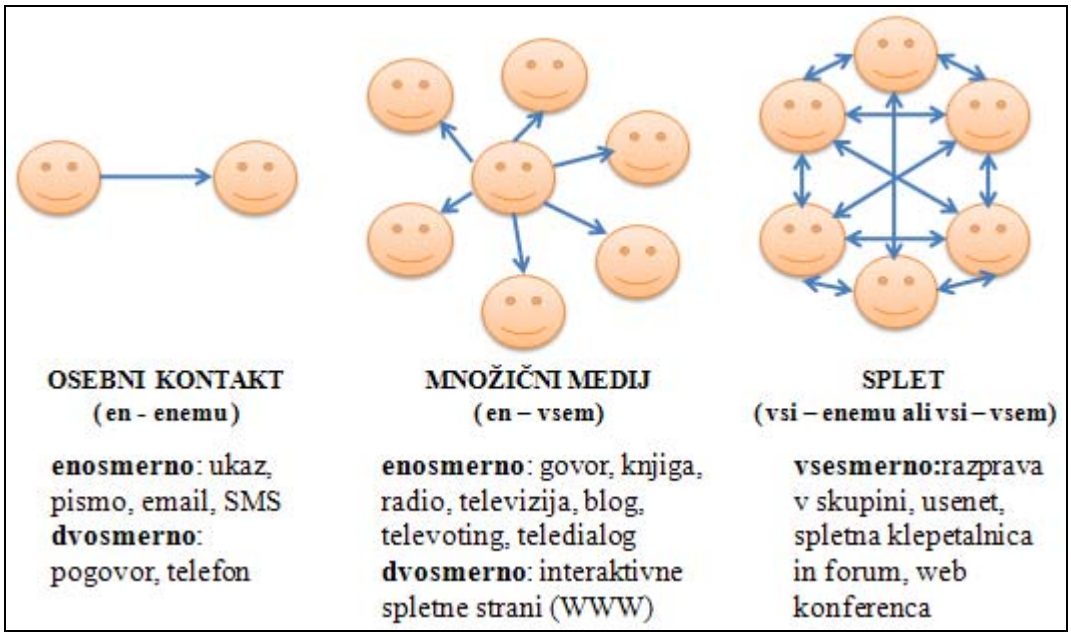
Nebesedna komunikacija

Nebesedna komunikacija je v bistvu komuniciranje brez besed. Nebesedno komunikacijo sestavljajo govorica telesa (mimika, gestika, telesna drža, hoja in podobno),
prostor (temperatura, razsvetljava, oprema), zunanji videz (obleka, pričeska, brada, nakit), vonjave (prijetne, neprijetne, blage, močne in podobno) in otip.
(Mihaljčič, 2006, 17).
Nebesedna sporočila nikoli niso samo zamenjava za jezik. Besedna komunikacija ne more enostavno nadomestiti nebesedne in obratno. Običajno se obe komunikaciji med seboj dopolnjujeta. (Mihaljčič, 2006, 27).

3 MEDIJSKO KOMUNICIRANJE – RAZLIČNE VRSTE

Čisto preprosta stvar, ki povsem razlikuje tradicionalno poslovno komuniciranje in elektronsko poslovno komuniciranje, je ravno tehnologija, s katero je podprto samo poslovanje in komunikacija podjetja. Že sam pomen besede elektronsko poslovno komuniciranje nam pove, da je osnova komuniciranja na elektronski izmenjavi podatkov v informacijskem omrežju. Brez omrežne podpore je torej obstoj elektronsko poslovnega komuniciranja povsem nemogoč. Uporaba tehnologije doprinese ogromen vpliv na sam potek oziroma smer poslovne komunikacije, bodisi med zaposlenimi ali navsezadnje s strankami. Poslovni komunikacijski model je kategoriziran v tri različne tipe elektronskega poslovanja. (Schneider, 2006, 56)

Slika 3: Različne vrste kontaktov



Vir: lasten

Osebni kontakt (eden - eden)

Ta tip komunikacijskega modela, ki se v sami organizaciji komunikacije ponaša v ospredju z osebnim kontaktom in komuniciranjem, lahko označimo kot tradicionalno, klasično komuniciranje.

Množični medij (eden – vsem)

Sam pristop omogoča organizacijam vsestransko komunikacijo, vendar le iz ene izhodiščne točke, razpršitev oglaševalskega in promocijskega materiala, ključna točka v podjetju je samo ena. Prav gotovo predstavlja primer široko sprejetega tradicionalnega poslovnega komuniciranja in poslovanja.

Splet (vsi – enemu ali vsi – vsem)

Splet hkrati združuje vse sestavine pristopa množičnih medijev, osebnega kontakta, hkrati pa nudi interaktivnost, sodelovanje in povratne informacije v zelo kratkem času. In še več. Pa vendar se osebni kontakt vse bolj izgublja v primerjavi s povsem tradicionalnim, klasičnim nivojem komuniciranja in poslovanja. Ta tip lahko označimo kot povsem elektronsko komuniciranje in poslovanje.

Visoka ali nizka raven zaupanja?

Zanimivo je ugotovljeno dejstvo, da pri primerjavi vseh vrst komuniciranja prihaja v začetku poslovnega komuniciranja, kot tudi poslovnega sodelovanja podjetij, vedno, ne oziraje se na tip in tehnologijo komunikacije, do nizke ravni zaupanja. V določeni kontinuiteti se sčasoma dviguje raven zaupanja in na koncu lahko celo preide v monotono in neučinkovito preverjanje zaupanja. Sploh če prištejemo, da so ljudje neosveščeni o morebitnih zlorabah in živijo v zmotnem prepričanju, da je tako in tako vse varno in se ne more nič pripetiti. Sama pristnost komunikatorja, ki komunicira na drugi strani, je težje preverljiva v primerjavi s tradicionalnim, klasičnim komuniciranjem.

Poslovno komuniciranje se je v zadnjih desetletjih v podjetjih krepko spremenilo. Nezadržen je razvoj poslovne komunikacije z uvedbo e–poslovanja in uporabe omrežij, predvsem spleta, tako za komunikacijo podjetja s kupci, dobavitelji, podizvajalci, zastopniki, partnerji kot z zaposlenimi, ki imajo do internih informacij dostop od zunaj. Vse to podjetjem prinaša velike prednosti in nove izzive ter tudi odgovornosti.

Glede na časovno premico in primerjavo s preteklostjo, bi lahko takšno komuniciranje v grobem razdelili glede na uporabljeno tehnologijo in komunikacijski kanal (neposredno in posredno), na vse bolj razširjeno elektronsko in na klasično tradicionalno komuniciranje.

3.1 Elektronsko komuniciranje v poslovnem odnosu

Sama tehnologija temelji na elektronski izmenjavi podatkov, kot medij je uporabljen informacijski omrežni sistem (brezžični, žični). Preko ponudnika internetnih storitev je omogočeno komuniciranje navzven oziroma nudenje vstopne točke v splet. Vse skupaj pa sloni na tehnologiji, ki takšen prenos podpira.

Osnova elektronskega komuniciranja je splet (*World Wide Web*), največ pa se pri elektronskem poslovanju uporablja elektronska pošta, faks in telefon, izvaja pa se preko zasebnih ali javnih informacijskih sistemov.

E-poslovanje in poslovno komuniciranje

Glavni predstavnik elektronskega poslovnega komuniciranja je e-poslovanje.

Elektronsko poslovanje se nanaša na izvajanje poslovnih transakcij, na upravljanje odnosov s strankami in na komuniciranje tako znotraj podjetja, kot med različnimi podjetji, kupci in državno upravo.

Osredotočil bi se na poslovno komuniciranje in vpliv interakcije človeškega faktorja nanj.

Slika 4: Poslovno komuniciranje

Vir:lasten

Elektronska pošta

Angleško imenovana *electronic mail* ali skrajšano *e-mail*,
je ena najpogosteje uporabljanih storitev, ki jih omogoča svetovni splet. Elektronska pošta omogoča, da si lahko ljudje, ki niso v neposrednem stiku, s pomočjo računalnika izmenjujejo sporočila. Elektronsko pošto uporabljamo tako, da na računalniku poženemo program, ki se imenuje odpravnik pošte (angl. *mailer*). Isto sporočilo lahko naenkrat pošljemo več prejemnikom. Elektronska pošta ne zahteva, tako kot telefon, da so na različnih koncih omrežja hkrati navzoči vsi, ki jim je sporočilo namenjeno. Sprejeto sporočilo se ohrani in se lahko prebere kadarkoli. (Mihaljčič, 45, 2006)
Prednosti in slabosti elektronske pošte:

- velika hitrost izmenjave pošte
- ni potrebna prisotnost naslovnika
- pošljemo lahko hkrati več naslovnikom
- dokaz ali verodostojnost
- sporočilo lahko poleg besedila vsebuje tudi priponke
- za izmenjavo pošte je potrebna tehnologija (odjemalec pošte)
- strah in odvračanje nekaterih ljudi pred takšno vrsto komunikacije
- bonton in etika
- zgubljanje osebnega stika

Telefax

Faks oz. *fax*, krajšava za *facsimile*, latinsko *fac simile* , naredi podobno, napravi kopijo, pomeni pa telekomunikacijsko tehnologijo, ki se uporablja v namen posredovanja kopij dokumentov in pri tem uporablja naprave, ki posredovane podatke preoblikujejo in posredujejo v pisni obliki. [http://www.wikipedia.org/]

S faksi lahko poslujemo v obliki računalniškega programja, kjer s pomočjo treh najvažnejših komponent (računalnik, skener, modem) dosežemo enak, a varnejši učinek.

V preteklosti je uporaba faksa pomenila precejšno prednost v primerjavi s pošiljanjem sporočil v klasični pisemski obliki. V današnjem času, pa uporaba faksa izgublja glede kvalitete obstojnosti v primerjavi z elektronsko pošto, a je še vedno priznana oblika prenosa dokumentov v (elektronski) papirni obliki.

Telefon

Izhaja iz dveh sestavljenih grških besed *tele*, v prevodu daleč in *phone, v* prevodu glas.

Predstavlja pa telekomunikacijsko napravo, ki se uporablja za prenos in sprejem govora (v večini primerov), po navadi med dvema osebama, včasih pa tudi tremi ali več.

Je najbolj razširjeno komunikacijsko sredstvo na svetu v današnjem času. Skorajda ni gospodinjstva, ki ga ne premore. Vpliva na družbene aktivnosti ljudi. Večina telefonov deluje na način prenosa električnih signalov preko telefonskega omrežja, kar pa omogoča splošno neomejeno povezanost. Telefonu sicer vedno bolj konkurirajo druga komunikacijska sredstva, kot sta na primer telefax in elektronska pošta, kljub temu pa ostaja telefon še naprej najpogostejši nadomestek za osebne poslovne stike in pisno sporazumevanje.

(Mihaljčič, 2006, 33).

Tehnološki napredek je opazen pri sami povezljivosti in nudenju storitev, prehod iz analognega signala v digitalni, prenos podatkov, mobilnost in dosegljivost ter pri samih napravah. Slabosti telefonskega sporazumevanja:

- odpade neverbalna komunikacija
- teže se vživimo v sogovornika
- teže se oceni resnost, njegovi pošteni nameni
- možnost vplivanja na poslušalca je večja
- stalna dosegljivost in možnost komuniciranja z nezaželenimi osebami in še to po možnosti ob nepravem času

Samo telefonijo lahko ločimo na stacionarno in mobilno telefonijo.
V zadnjem času zasledimo zelo hiter tehnološki napredek, ki odpravlja določene slabosti in vodi h konvergenci (sovpadanje različnih tehnologij) posameznih tehnoloških naprav, glede na želje in povpraševanja. Konvergenca posameznih tehnoloških naprav pa omogoča predvajanje interaktivnih vsebin, kupovanje, obveščanje, rezervacije, navigacije in še bi lahko našteval, to je le začetek svetle prihodnosti, ki nam jo napovedujejo te aktivnosti.

Večji kot je tehnološki napredek, več možnosti nam ponujajo naprave in bolj so dostopne širši množici. Le za peščico ljudi lahko trdimo, da je seznanjena z vsemi možnostmi, ki ji te naprave nudijo in jih popolnoma izkoristijo. Ravno zaradi preobilice možnosti in nastavitev, bodisi pravilnih ali ne, je vprašljiva varnost komunikacije. Včasih se zaradi sledenja modnim in tehničnim trendom rado pozablja na varnost in zaščito posameznika. Na srečo že proizvajalci ali ponudniki tehnoloških rešitev v standardu ponujajo zaščito, za katero pa ne moremo trditi, da je najboljša, saj je še vedno posrednik človeški dejavnik.

Slabost elektronskega poslovanja, človeški dejavnik, je najbolj očitna pri samem uvajanju, saj primanjkuje dovolj usposobljenega in izobraženega kadra. Na elektronsko poslovanje je potrebno pripraviti vse ali vsaj večino zaposlenih. Le-ti pa imajo različno stopnjo znanja poznavanja sodobnih tehnologij in različen interes za priučitev novosti oziroma za udeležbo na dodatnih usposabljanjih. (Kastelic, 12, 2008)

Internet – Svetovni splet (WWW) - komunikacija

Internet, imenovan tudi medmrežje, skrajšano iz angl. besede *inter-network*, je v splošnem smislu računalniško omrežje, ki povezuje več omrežij. Kot lastno ime je Internet javno razpoložljiv, mednarodno povezan sistem računalnikov skupaj z informacijami in uslugami za uporabnike. Sistem uporablja način paketno preklopljivih komunikacijskih protokolov. Tako se največje medmrežje enostavno imenuje Internet. Spretnost povezovanja omrežij na ta način se imenuje internetno delovanje. V razširjenem izražanju se internet velikokrat nanaša na usluge kot so svetovni splet (WWW), elektronska pošta in neposredni klepet. [http://www.wikipedia.org/]

World Wide Web

Veliko ljudi uporablja termin *Internet* in *World Wide Web*, v nadaljevanju *Web* in ju med seboj zamenjuje, vendar ta dva termina nista sinonima.
Internet označuje globalno podatkovni komunikacijski sistem. Pomeni pa strojno in programsko infrastrukturo, ki omogoča povezljivost med računalniki. V kontrastu, *Web* je samo eden izmed komunikacijskih storitev preko Interneta. Je zbir med seboj povezanih dokumentov in drugih virov. Sama povezava je omogočena z navigatorji (*Hyperlinks*) in spletnimi naslovi z opisom lokacije in načina pristopa (URL). [http://www.wikipedia.org]

Splet, svetovni splet ali z angleško kratico *WWW* (World Wide Web) je porazdeljen nadbesedilni (hipertekstni) sistem, ki deluje v medmrežju. Hipertekstne dokumente pregledujemo s programom imenovanim brskalnik (*Internet Browser, Explorer*), ki s spletnega strežnika dokument prenese in ga prikaže, navadno na računalniškem zaslonu. Besedilnim spletnim dokumentom pravimo spletna stran, smiselno povezanim spletnim mestom pa spletišče. V spletnih straneh so lahko povezave, ki kažejo na druge spletne strani ali celo pošljejo povratno informacijo spletnemu strežniku. Za sprehajanje po spletnih straneh se uporablja izraz deskanje (*surfing*).
HTTP (*Hypertext Transfer Protocol*) je danes eden izmed najbolj prepoznavnih komunikacijskih protokolov oziroma storitev na internetu.
Razvili so ga v *CERN-u* (Evropska organizacija za jedrske zadeve), točneje predstavlja izum g. Tim Berners Lee – ja, z namenom omogočiti znanstvenikom po vsem svetu kar se da hiter oziroma preprost dostop do podatkov in raziskav, ki so jih izvajali takrat in še danes.
Popularna brskalnika sta Internet Explorer in Firefox. Spletni dokumenti lahko vsebujejo skoraj vsako kombinacijo računalniških podatkov, ki lahko združujejo grafiko, zvoke, tekste, video, multimedijo in interaktivne vsebine, kot so igre, pisarniške aplikacije in znanstvene predstavitve. [http://www.wikipedia.org/]

3.2 Klasično tradicionalno komuniciranje v poslovnem svetu

Temeljilo je predvsem na osebni verbalni komunikaciji, res klasični analogni telefoniji in papirno podprtih poslovnih procesih. Zapiski, papirna sporočila, klasična pisma, so še vedno predmet komuniciranja. Prav tako sprejem gostov in organizacija srečanj. Papirno podprte poslovne procese bo zamenjalo povsem elektronsko poslovanje. Poslovno komuniciranje in druženje na povsem elektronski ravni pa čaka bodoče generacije.

Lahko trdimo, da se je v zadnjih letih precej spremenilo in dopolnilo, kar preobrazilo, nekatere osnove pa so vseeno ostale, saj pristna človeška komunikacija še vedno predstavlja srce poslovnih odnosov.

3.3 Točke in varnost komuniciranja

Ob predpostavki, da se osredotočimo predvsem na komunikacijo podjetja in zaposlene, lahko kot točke poslovnega komuniciranja označimo vse vsakodnevno vzpostavljene kontakte in relacije med zaposlenimi, predvsem pa z zunanjim svetom z vsemi razpoložljivimi tehničnimi sredstvi. V odvisnosti posamezne funkcije delovnega mesta, smeri in frekventnosti potekanja (pretočnosti) poslovne komunikacije, lahko posamezne točke iz varnostnega vidika označimo kot pomembnejše od ostalih točk.

Atributi teh točk v odvisnosti od zaposlenih na teh delovnih mestih, so zelo pomembni pri vzpostavitvi poslovnega stika in navsezadnje dajejo informacijo in sliko podjetja. Na žalost pa lahko tudi vse ostalo, kar pa v današnjem času zlahka izkoristijo konkurenčna podjetja in še kdo drug. Odvisno od organizacije podjetja, je še vedno v večini podjetij v ospredju sprejemnica, recepcija. Sprejemnica ali recepcija je okno in ogledalo podjetja. Za podjetja pomeni lahko sprejemnica ali recepcija manifestacijo njihovih poslovnih odličnosti. Večji del se odvija poslovna komunikacija po elektronski poti, a ostaja še vedno pristen kontakt in ponavadi predstavlja vstopno točko vsakogar, ki si želi stikov s podjetjem. Označimo jo lahko kot najpomembnejšo točko.

V ospredju so v glavnem točke, kjer na delovnih mestih poteka vsakodnevna komunikacija, kjer zaposleni razpolagajo ali so v stiku z določenimi pomembnimi informacijami in na drugi strani sogovorniki, ki vzpostavljajo poslovni kontakt ali pridobivajo običajne informacije.

Ne smemo zanemariti dejstva, da se lahko pri vsakem navezovanju poslovnega komuniciranja ustvari točka, ki predstavlja varnostno vrzel.

Podjetja se lahko zavarujejo z določenimi akti, pravilniki, ki zaposlene zavezujejo k upoštevanju poslovne tajnosti in osebnih podatkov.

3.4 Zakonodaja in predpisi

Eden od ciljev uvajanja elektronskega poslovanja med podjetji je zmanjševanje števila pisnih dokumentov pri poslovanju, ki onemogočajo hitro poslovanje ter zmanjševanje nepotrebnega dela zaradi ročnega vnašanja podatkov. Vendar so za poslovno elektronsko komuniciranje v širšem obsegu do sedaj oviro predstavljali zakonski predpisi, ki urejajo pisno obliko dokumentov, predložitev izvirnikov, podpisanih dokumentov in za zagotavljanje pravnega

učinka elektronskih podatkov pravni status elektronskega podpisa. S sprejetjem zakona o elektronskem poslovanju in elektronskem podpisu so odpravljene tudi te ovire.
Razvoj e-poslovanja temelji v veliki meri na zaupanju in varnosti, ki ju čutijo uporabniki do elektronskih komunikacij. Z načinom izmenjave podatkov se spreminja tudi način varovanja teh podatkov. Varna elektronska pošta, elektronsko poslovanje, dostop do baz podatkov zahtevajo visoko stopnjo varnosti, ki mora zagotavljati: zaupnost, overjanje uporabnikov, kontrolo dostopa, neokrnjenost podatkov in nezmožnost zanikanja. Obstajajo številne aplikacije, ki so povezane z elektronskimi podpisi oziroma le-tega potrebujejo za delovanje. Na tak način potekajo plačila, sklepanje pogodb, dostop do različnih storitev podjetij ali državne administracije, varne komunikacije med različnimi subjekti, nabava in podobno. Zato se uporaba digitalnih potrdil, elektronsko podpisovanje in šifriranje z javnimi ključi pojavljajo kot najpogostejši način uvajanja visoke stopnje varnosti. [http://www.gov.si/cvi/]

Podpisan dokument je osnova vsake poslovne komunikacije. Prehod na brezpapirno elektronsko poslovanje je dobil pravno podlago z *Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP)*, ki v svojem 15. členu določa, da ima elektronski podpis pravno veljavo, če je overjen s t.i. kvalificiranim digitalnim potrdilom. Digitalna potrdila so sestavni del tehnoloških rešitev, ki nudijo dve osnovni možnosti za zasebnost v elektronskem poslovanju in komuniciranju. Gre za šifriranje podatkov, ki zagotavlja zaupnost, in digitalni podpis, ki je digitalna alternativa klasičnemu podpisu. Digitalni podpis zagotavlja nedvoumno identiteto imetnika digitalnega potrdila, očitno lastništvo podpisanih e-podatkov in celovitost e-podatkov, kar pomeni, da ni mogoče spremeniti ali drugače popraviti brez (vednosti) podpisnika. [http://www.gzs.si/slo/]

Razvoj e-poslovanja oziroma e-komuniciranja temelji v veliki meri na zaupanju in varnosti, ki ju čutijo uporabniki do elektronskih komunikacij in izdajateljev digitalnih potrdil. Obstajajo številne aplikacije, ki so povezane z elektronskimi podpisi oziroma jih potrebujejo za varno in legitimno delovanje, ali pa vsebujejo zaupne podatke, ki jih je potrebno zaščititi pred nepooblaščenimi osebami. Pomembno je, da storitve, ki se vršijo na elektronski način, zagotovijo vsaj enak oz. celo višji nivo varnosti in zaupanja kot storitve, ki se opravljajo na klasičen način. [http://www.gov.si/cvi/]

Na tak način poteka elektronska izmenjava podatkov, varen in avtenticiran (pooblaščen) dostop do podatkovnih baz, sklepanje pogodb, plačila, dostop do različnih storitev podjetij ali uprave, nabava, e-arhivi in podobno. Prehod na elektronski način opravljanja storitev po eni strani prinaša veliko prednosti, npr. enostavnost, dostopnost, ipd., po drugi strani pa ima lahko velik vpliv na delovanje in organizacijo znotraj same institucije.

V Sloveniji je Državni zbor Republike Slovenije na seji dne 1. februarja 2007 potrdil uradno prečiščeno besedilo Zakona o elektronskih komunikacijah, ki obsega:

- *Zakon o elektronskih komunikacijah*,
- *Zakon o varstvu osebnih podatkov*,
- *Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah*.

Prav tako se e-poslovanje v podjetjih nanaša na Zakon o spremembah in dopolnitvah »*Zakona o elektronskem poslovanju in elektronskem podpisu«* [http://zakonodaja.gov.si/]

Zakonodaja in predpisi urejajo regulativo v odnosu ponudnika in odjemnika storitev. Lahko je to pravna ali fizična oseba, izobraževalna ustanova itd. Vsekakor se Slovenija z vstopom v EU približa z zakonodajo in predpisi ostalim evropskim državam v uniji.

Od samega podjetja pa je odvisno, v kakšni meri z določenimi pravilniki in smernicami, ki jih sprejme, zaščiti svoje poslovanje in zaposlene. Nekateri pravilniki so zakonsko določeni, lahko pa si podjetje pomaga z določenimi priporočili oziroma standardi, ki bodo v bližnji prihodnosti predstavljali kar zakonsko nujo v poslovanju podjetja.

Priporočila za pripravo informacijske varnostne politike so usklajena s standardom BS 7799 in veljavno slovensko zakonodajo. Zasnovana so tako, da obsegajo vsa pomembna področja informacijske varnosti ter poskušajo identificirati vsa morebitna tveganja ter hkrati ponuditi praktične in hitro izvedljive pravne, organizacijske in tehnološke ukrepe za zmanjševanje teh tveganj.

Priporočila vključujejo naslednja področja:

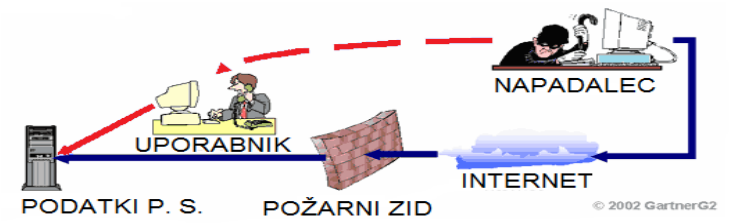
- sistem upravljanja z varnostjo
- človeške vire
- zagotavljanje varnega okolja
- upravljanje z informacijskimi sistemi
- obvladovanje dostopov
- razvijanje, naročanje, prevzemanje in vzdrževanje programske opreme
- načrtovanje neprekinjenega poslovanja
- naročanje storitev pri zunanjih izvajalcih
- usklajenost

4. ČLOVEŠKI FAKTOR KOT NAJŠIBKEJŠI ČLEN »SOCIALNI INŽENIRING«

4.1 Kaj je socialni inženiring?

Podjetja se premalokrat zavedajo, da je človek in človeški faktor odločilnega pomena v varnem poslovanju podjetja. Dogaja se, da podjetja zapravijo ogromno časa in denarja za zaščito svojega poslovanja, svoje informacijske infrastrukture, omrežij z raznimi nadgradnjami, popravki, varnostnimi paketi in enkripcijskimi algoritmi.
V resnici pa je najšibkejši člen prav človeški dejavnik, torej človek.
Obstaja sistem, ki vse te zaščite enostavno preskoči in tega poimenujemo socialni inženiring (angl. *Social Engineering*).

Slika 5: Socialni inženiring



Vir : Gartner , Edvard Šilc, predavanje Forum Varna tajnica, 2008

Pojem socialnega inženiringa je poznan že zelo dolgo, vendar ne pri nas.
Opredelimo ga lahko kot zunanje zavajanje zaposlenih pri pridobivanju internih informacij ali nezakonit dostop do virov (angl. *resources*). Pri tem se nanaša na najšibkejši člen v varnostni politiki poslovanja in komunikaciji podjetja.
»Oseba ali skupina, ki izkorišča človeške pomanjkljivosti v smislu neizobraženosti, naivnosti in posameznikove želje, da bi pomagal nekomu, se okorišča s pomočjo socialnega inženiringa«, je opredeljeno v Wikipediji.
Varnostni analitik Rich Mogull iz podjetja Gartner, podaja možnost, da poteka socialni inženiring tipično v treh conah oziroma dejavnikih:

- notranje (*internal*)
- zaupljivost (*trusted*)
- zunanje (*external*)

Notranje

Grožnje prihajajo iz vrst zaposlenih, ki skušajo manipulirati druge zaposlene in tako priti do občutljivih informacij in dostopov do poslovnega sistema. Notranje storilce lahko predstavljajo nezadovoljni zaposleni, po organizacijski shemi najnižje postavljeni zaposleni, zaposleni s kriminalni preteklostjo ter pomožne službe, kot so čistilni servisi in vzdrževanje. S slednjimi je poslovodstvo na neki določeni ravni zaupanja, kar pa pomeni še več možnosti in lažjih načinov izvedbe aktivnosti socialnega inženiringa.

Zaupljivost

Grožnje prihajajo iz smeri posameznikov ali skupin, ki so na formalni način povezane z organizacijo, na povsem običajni ravni in niso na plačilni listi. Med te ljudi lahko štejemo pogodbene delavce, svetovalce, navsezadnje tudi partnerje organizacije. Pogosto uživajo ti posamezniki ali skupina zelo visoko raven zaupanja in včasih ravno ta vrednota nudi dostop do občutljivih podatkov in sistemov. Zelo redko so ti potencialno nevarni dejavniki vključeni v varnostne pravilnike.

Zunanje

Zunanje grožnje prihajajo od ljudi, ki niso povezani s podjetjem. V to kategorijo lahko spadajo rekreacijski napadalci (*hackers*), posamezniki konkurenčnih podjetij čakajoč na kakšno zaupno informacijo ali ostali kriminalci, ki želijo kaj odtujiti in se okoristiti.
Ti ljudje nimajo vzpostavljenega zaupanja s samo organizacijo, zato si prizadevajo te kratkoročne povezave vzpostaviti.
Temeljijo na kratkoročni zaupljivosti z uporabo različnih tehnik socialnega inženiringa.
[http://www.enisa.europa.eu/doc/pdf/deliverables/WGAR/guide_sl.pdf]

V zunanje bi lahko prišteli še bivše zaposlene, katerim status zaposlenega je potekel, a še vedno imajo vezi z zaposlenimi, določeno zaupanje in informacije, s katerimi so razpolagali ali si jih tako ali drugače pridobili. Veže jih lahko motiv nezadovoljstva, tako da lahko poskušajo na nek način s tem povzročiti škodo podjetju ali direktno nekaterim posameznikom. [http://articles.techrepublic.com.com/5100-10878_11-1047991.html]

Socialni inženiring je metoda, s katero se pridobivajo informacije, ki bi jih bilo drugače težko pridobiti ter izkoriščajo človekova naravna nagnjenja, da zaupa in pomaga drugim. Večina ljudi je prepričana, da ne bi nihče namerno poskusil prevarati in manipulirati z javnostjo, vendar pa je socialni inženiring dejansko ena od najpogosteje uporabljenih oblik napada. Napadalci pogosto izberejo to metodo, ker je presenetljivo preprosta in ne zahteva časa. Zakaj bi napadalci zapravljali ure in ure za dekodiranje gesla, če lahko neposredno navežejo stik z osebo, se izdajajo za službo za pomoč uporabnikom banke ali druge institucije in nato preslepijo lahkoverno osebo, da jim posreduje občutljive informacije.
Nekatere najpogostejše metode socialnega inženiringa vključujejo zamenjavo identitete, dobrikanje in ustvarjanje občutka nujnosti ter pooblastilo tretjega. Zato je nujno potrebno razviti in izvajati izobraževalno strategijo, ki posebej obravnava to vprašanje.

4.2 Kdo je socialni inženir ?

Nekdo, ki je vešč takšne manipulacije, lahko prevzame kontrolo nad kakršnimkoli sistemom, ne ozirajoč se na platformo, strojno opremo ali nameščene programe.
Prav zaradi tega se je takšne vrste napadov najtežje ubraniti.
Socialni inženirji so ljudje, ki s pomočjo prevare pripravijo ljudi do tega, da izdajo (zaupne) informacije. Dober socialni inženir mora zbrati veliko informacij o tarči in podjetju, kjer je tarča zaposlena. Informacije lahko pridobi s pomočjo interneta, telefonskih imenikov, obiskov podjetja, itd.
»V bistvu socialni inženiring temelji na medsebojnem komuniciranju, a se velikokrat zgodi, da se socialni inženir (posameznik ali skupina) le malokrat sreča ali pa sploh ne, z izbrano osebo napada. Sam stik ali celo direkten nagovor pa je dovršeno izpeljan, kjer sta govor in neverbalna komunikacija usklajena«, je povedal Edvard Šilc na predavanju Forum Varna tajnica 2008, ki je potekal letošnje leto.
Kot komunikacijsko sredstvo uporablja socialni inženir v večini primerov telefon, faks, SMS, MMS, internet, klepetalnice (*chat rooms*) ter elektronsko pošto. Vse bolj pa se s tehnološkim napredkom in z medsebojnim omreževanjem z različnimi tehnikami socialnega inženiringa prepletajo razne spletne goljufije in internetna zavajanja. Vrednost informacije je vprašljiva, če ni informacija transparentna in povratno preverljiva.
Zanimivost socialnega inženiringa pa je tudi možnost, da je žrtev lahko vsak zaposlen, tudi tisti, ki ne dela z računalnikom, a zaradi neznanja, nepazljivosti ali zaupanja pomaga pri vdoru.

Hekerji (*Hackers*)

Beseda označuje posameznike ali skupino, ki skuša na vsak način prevzeti nadzor nad uporabniškimi napravami, osebnimi računalniki, strežniki, usmerjevalniki, napravami, s katerimi ljudje opravljajo različne poslovne ali osebne dejavnosti. Iščejo možnosti za vdor z različnimi orodji in pripomočki, ki jih uporabljajo in namestijo s pomočjo socialnega inženiringa. Velikokrat uporabijo napaden računalnik v neposrednem smislu, preko tega računalnika strateško izvršijo napad na druge in s tem zakrivajo sledi. Predvsem pa je njihovo početje povezano s kriminalno dejavnostjo, zlorabo, izsiljevanjem in okoriščanjem.

4.3 Definicija socialnega inženiringa

Definicija socialnega inženiringa je predstavljena v varnostnem in psihološkem smislu različnih ljudi in organizacij. *High Tech Dictionary* , ga recimo definira kot

vdor v varnost poslovne organizacije s pomočjo človeške interakcije. [http://www.computeruser.com/resources/dictionary/]

Kevin Mitnick, najbolj znan socialni inženir, je nekoč opisal socialni inženiring kot

»izkoristiti človeško naivnosti, s pomočjo vpliva, prepričevanja in manipulacije, z namenom pridobitve ključnih informacij«. (Mitnick, 2008, 19)

Drugače povedano, prepričati zaupanja vrednega uslužbenca podjetja, da razkrije občutljive informacije ali izvede kakršnokoli dejanje, od katerega ima korist napadalec.

V krogu poznavalcev je socialni inženiring označen kot umetnost in znanost, pripeljati ljudi do izpolnitve interesov socialnih inženirjev.

CISSP (*The Certified Information Systems, Security Professionals study guide*) pa ga označuje kot spretnost, pri kateri neznana oseba pridobi zaupanje nekoga znotraj same organizacije, ga vzpodbudi (angl. *encourage*), da napravi spremembo v informacijskem sistemu v smislu omogočenega pristopa. (Tittel, Chapple, Stewart, 2003, 16)

Wikipedia pa definira socialni inženiring kot način pridobivanja zaupnih informacij, s pomočjo manipuliranja legitimnih uporabnikov.

V realnem svetu je lahko socialni inženiring vsako od naštetih definicij, odvisno s katere perspektive ga gledamo.

Če pa poiščemo skupno točko, s katero se večji del vsi strinjamo, je pomen socialnega inženiringa ravno v tem, da se s pametno komunikacijo v psihološkem smislu da izvedeti marsikaj in izvesti manipulacijo, ki jo podpira človeška tendenca k zaupanju.

Varnost sloni na zaupanju.

Človeški člen predstavlja najšibkejši člen v varnostni verigi.
Veliko izkušenih strokovnjakov na področju varnosti opozarja na to problematiko. Ne glede na število izdanih časopisnih prispevkov in publikacij na temo mrežnih varnostnih lukenj (*network holes*), obližev (*patches*), popravkov (*updates*) ter uporabljene metode zaščite oziroma orodij, kot so požarni zidovi (*Firewalls*) in odstranjevalci škodljive zalege (*Antivirus, Antiworms, Antispy, Rootkits*) ter ostalih zaščitnih programov, prihaja do vsakodnevnih groženj in ne obstaja popolnoma zaščiten sistem. Ranljivost, kakor tudi grožnje te vrste, se dajo zmanjšati z osveščanjem in izobraževanjem ljudi.

4.4 Najbolj znani uporabniki socialnega inženiringa

Kevin Mitnick

Rojen 6. avgusta 1963 v Los Angelesu, je z 12. leti odkril socialno inženirstvo takšne vrste. Izkoristil je takratni avtobusni sistem potrjevanja kartic in se brezplačno vozil po vseh linijah Los Angelesa. S 13. leti je pričel manipulacijo telefonskih sistemov in svoje takratno početje, hobi, poimenoval »*phreaking*«. V bistvu pa je to pomenilo predhodnico računalniškega vdiranja (*hacking*).
S 16. leti ga je pričelo zanimati računalništvo in tehnologija in je svoje vrhunsko znanje manipulacije in vdorov v telefonski sistem samo izpopolnil. S prehodom telefonskega sistema na računalniški, stikalno podprti sistem, je samo sledil trendu in se izpopolnil tudi v teh veščinah. Znano je bilo, da je bilo vse njegovo početje namenjeno bolj intelektualnemu izzivu in radovednosti, kot pa povzročanju škode, uničevanju informacij ali okoriščanju.
Dolgo se je upiral roki pravici, a so ge vendarle prijeli in postavili pred sodišče, kjer je leta 1999 priznal krivdo za neupravičen dostop v računalniške sisteme in nepooblaščeno kopiranje programov in njihovih izvornih kod. Obsojen je bil na zaporno kazen in jo v nekaj letih tudi odslužil.
Danes je Kevin Mitnick svetovno znani svetovalec na področju varnosti, vdorov in socialnega inženiringa. Vodi svoje podjetje *Mitnick Security Consulting*, kjer s svojimi sodelavci opravlja projekte na področju varnosti in je udeležen skorajda pri vseh večjih korporacijskih in državnih in notranjih službah na tem področju. Opravlja preizkuse varnostnih sistemov in lukenj, predstavitve in izobraževanja ter je pisec mnogih člankov in knjig na temo socialnega inženiringa in varnega komuniciranja.
[http://www.wikipedia.org/]

Bratje Badir

Rojeni v Izraelu, od rojstva slepi, so razvili tako izostren sluh, da so lahko preko zvokov in izjemnega spomina prebijali zaščite telefonskih sistemov, odtujevali impulze, si organizirali celotno mrežo manipulacije s pomočjo socialnega inženiringa, prihajali do zaupnih podatkov in informacij. Leta 1999 so jih kriminalisti privedli k preiskovalnemu sodniku, ki je hkrati odredil tudi hišno preiskavo, v kateri pa žal niso našli obremenilnih dokazov, le denar in nekaj brezkoristnih dokumentov. Roki pravice so se uspešno upirali 6 let in v tem času nabrali 44 obtožb in kaznivih dejanj, izmed teh najodmevnejše telekomunikacijske prevare, kraje računalniških podatkov in številk kreditnih kartic, lažna predstavljanja, podkupovanja, izsiljevanja, vdor v izraelski vojni radijski sistem itd. Danes se je za njimi izgubila vsaka sled. [http://www.wikipedia.org/]

Frank William Abagnale, Jr.

Rojen 27. aprila 1948, je še do nedavnega opravljal službo ameriškega varnostnega svetovalca. Uvedel je sistem preverjanja, *Confidence trick* , trikov zaupanja, katerih poskus je goljufati ljudi ali skupine s pomočjo pridobitve njihovega zaupanja (angl. *gaffle, grift, scam, scheme, swindle*). Poneverba (*forgery*), je ena izmed tehnik goljufanja, vključno s krajo identitete in ena izmed varnostnih groženj, ki je uspešno zastopana v socialnem inženiringu.
Samozvanec (*impostor)*, pa je oseba, ki se predstavlja, da je nekdo drug. Pogosto je razlog finančne in socialne narave, torej okoriščanja s pomočjo socialnega inženiringa.
V 60. letih je Abagnel »zaslovel« s posredovanjem ponarejenih čekov, v 26. državah v obdobju 5. let in pri tem uporabljal tehnike socialnega inženiringa in poneverbe. V tem času se je predstavljal v različnih službah kot: letalski pilot, univerzitetni asistent, zdravnik, odvetnik itd.
Kriminalisti so ga prijeli v Franciji, uspelo mu je pobegniti, vendar je kasneje kazen odslužil v ameriških in švedskih zaporih. Pogojno je bi izpuščen in vse do letošnjega leta opravljal službo svetovalca v preiskovalnem biroju, FBI in notranjem ministrstvu.
V letu 2002 je Abagnale napisal knjigo *The Art of the Steal*, kjer v vsebini razkriva zaupne trike in poti, s katerimi se lahko uporabniki zaščitijo pred goljufijami in socialnim inženiringom. Knjiga po vsebini obsega tudi področje kraje identitete in pojav internetnega *skiminga* (*Internet scamming*), kar s tujko označujemo kot sofisticiran način kraje bančnih kartic in njihovih podatkov kar preko interneta.

Z letom 2008 je pričel voditi svojo družbo *Abagnale and Associates*, finančno protigoljufijsko svetovalno družbo. [http://www.wikipedia.org/]

4.5 Zgodovina in nastanek

Socialni inženiring nas obkroža v različnih oblikah, že od nastanka našega časa. Iz biblijskih časov lahko zasledimo podobna dejanja in prevare, najbolj poznan primer še iz antičnih časov iz Troje. Že mnogo let pred dobo računalnikov so obstajali ljudje, ki bi jih danes lahko poimenovali vdiralci (*hackers*). Uporabljali so vse zaznane tehnike in s tem pospeševali napredek tehnike zaznave in preprečevanja.

V današnjem času lahko podatke posredujemo s pomočjo opreme na drugo stran sveta, ampak jih na drugi strani lahko sprejme nekdo, ki jih bo znal sprejeti in uporabiti.

Nekateri vidijo varnost samo s stališča informacijske infrastrukture in naprav, vendar nam ostanejo še zapiski, dokumenti v papirni obliki, potrdila, vstopi, gesla in reči, ki niso shranjene v računalnikih. Tukaj pa pride na plan vsa umetnost socialnega inženiringa.

Veliko knjig je bilo napisanih, ki so nekako povezane s to metodo ali pa imajo kaj skupnega in že opisanega. [http://packetstorm.decepticons.org/docs/social-engineering/socintro.html]

- Zgodbe Sherlock Holmes-a, *The Bohemian Scandal*, Conan Doyle 1887
- *How to Make Friends and Influence People*, Dale Carnegie 1936
- *Dyadic communication section*, knjige ki temeljijo na psihologiji človeka , *Dyadic communication*, razlaga proces direktne komunikacije med dvema osebama ali skupine, npr. prodajalec in kupec.
- *Interpersonal Communication*, Joseph Devito: *Interpersonal communication* predvideva trende v načinu kako ljudje komunicirajo. Zanimivo je videti, kakšni so vsi načini in koliko je obstoječih vzorcev.

4.6 Razvrstitev in usmerjenost napadov

Glede na napad, lahko socialni inženiring razvrstimo na 2 ravni: fizično in psihološko raven.

Pri fizični ravni bo vsa usmeritev in aktivnost usmerjena na fizične priprave in stvari za pripravo napada: delovno mesto, telefon, koš, lahko tudi direkten pristop.

Sam napad se lahko vrši na način, da se socialni inženir pretvarja, da je vzdrževalec in si na ta način pridobi informacije na samem delovnem mestu, iz ležečih, nalepljenih listov, napisanih gesel, seznamov, opravil. Lahko pa samo opazuje delo zaposlenega in z opazovanjem ali seveda s pretvarjanjem, pridobi geslo.

Kasneje doma pregleda pridobljene informacije in izdela strateški plan napada. Je najbolj učinkovit način in se kombinira s fizičnim nastopom.
Psihološka raven pa poteka kot komunikacija in pretvarjanje, s skupno besedo **manipulacija**.
[http://www.securityfocus.com/infocus/1527]

Napadalci najprej opravijo poizvedbo, ki je odvisna od njihovega cilja. Opravijo raziskavo podjetja in njegovih zaposlenih.
Poznamo 4 osnovne korake napada s socialnim inženiringom:
1. socialni inženirji najprej ugotovijo, kdo razpolaga z informacijami, ki jih želijo
2. nato ugotovijo, kdo ima dostop do njih in
3. kateri so pogoji, da ta oseba izda informacije, na primer prodajalcu ali nekomu, ki je na pomembnem položaju v podjetju
4. korak napada je ponavadi uspešen, ko napadalec ustvari te pogoje. Napad lahko traja od 60 sekund do 2 leti. Odvisno, če želi napadalec opraviti res sofisticiran napad.
(Mitnick, 2008, 19)

Usmerjenost napada

Socialni inženiring lahko razvrstimo v dve večji skupini, napadi s strani človeka in računalniški napadi. Socialni inženiring, ki temelji na računalniškem napadu, se nanaša predvsem na tehnologijo za pridobivanje nepooblaščenih informacij.
Primer: pojavi se pojavno okno, kjer se uporabniku sporoči, da se je prekinila omrežna povezava, da mora vnesti uporabniško ime in geslo, če želi vzpostaviti omrežno povezavo. Tako se lahko podatki pošljejo po spletni pošti na nek oddaljen računalnik in s tem napadalec pridobi podatke. Seveda se tukaj predpostavlja, da je napadalec že prej nekako namestil pričujoči program (pojavno okno) na računalnik, bodisi preko spletne pošte (zlonamerno programsko kodo), CD-ja, USB ključa, osebno ipd.

Najbolj enostavna in tudi najučinkovitejša oblika socialnega inženiringa je še vedno človek. Zanaša se na medosebne odnose in zavajanje, kjer lahko z laskanjem, zastraševanjem, avtoritativnim pristopom in omalovaževanjem, doseže marsikaj. V ta namen lahko napadalec uporabi katerikoli komunikacijski medij; ena na ena, pogovor z osebo, telefon, spletno pošto.

4.7 Tehnike socialnega inženiringa

Socialni inženir si pri svoji dejavnosti pomaga z različnimi tehnikami. Vse uporabljene tehnike imajo skupen imenovalec, imenovan angleško *Pretexting*. Definicija ga razlaga kot dejanje stvaritve in uporabe izmišljenega scenarija, s katerim svojo tarčo pripravijo do želenih dejanj. Predvsem je izvedba tega dejanja poznana organom za notranje zadeve, privatnim preiskovalcem in na žalost tudi socialnim inženirjem.
[www.wikipedia.org]

Socialni inženiring preko telefona

Štejemo ga za enega izmed najbolj prevladujočih tehnik socialnega inženiringa. Socialni inženir bo s klicem in z imitacijo nekoga drugega, ki razpolaga z določeno ravnijo avtoritete, pomembnosti in postopno pridobljenih informacij, ki mu jih nevede daje zaposleni, uspel zaobiti vsak informacijski varnostni sistem. V prvi vrsti so temu podvrženi centri za pomoč uporabnikov, sprejemnice, tajništva oziroma poslovni sekretariat. Pri tem se lahko predstavi kot notranji sodelavec ali celo kot nov sodelavec v telefonski sprejemnici, kot vzdrževalec na telefonskem omrežju, varnostnik. V večini primerov je v korporacijah lažje, saj se vsi zaposleni ne poznajo med seboj. Telefonski prikaz oziroma ID pa ni vedno zanesljivi vir klicatelja, saj si je socialni inženir že pridobil dostop v PBX centralo:
Pozdravljeni, kličem iz vaše telefonske centrale in nastavljam ponovno enumeracijo.
Ali lahko prosim pritisnete nekaj gumbov zame (iz *Computer Security Institute*).
Centri za pomoč uporabnikom (*help desk*) ali sprejemnice (*reception*) so veliko bolj ranljive, ravno zaradi namena pomagati in so vsakodnevno izpostavljeni ljudem, ki želijo informacije. Zaposlenim na teh točkah nalaga že poslovni bonton, da so prijazni in dajejo informacije. Predstavljajo pa največji cilj socialnih inženirjev.
[http://www.securityfocus.com/infocus/1527]

Veliko zaposlenih v centrih za pomoč uporabnikom in na sprejemnih mestih je v veliki meri neinformiranih, neizobraženih kar se tiče področja varnosti in ponavadi nezadovoljnih, premalo plačanih. Torej sprejemajo klic za klicem, ne pomišljajo na posledice, to pa predstavlja veliko varnostno luknjo.

Brskanje po smeteh (*dumpster diving)*

S tujko imenovano tudi *trashing*, smetarjenje. Veliko informacij lahko socialni inženirji pridobijo z brskanjem po smeteh. Lahko pa tudi z enostavno položenimi stvarmi na mizah ali obešenih na stenah. Primer: neuničeni dokumenti, telefonski imeniki, naslovi zaposlenih, organizacijske sheme, kratka sporočila, koledarji , pravilniki, navodila, celo gesla, zgoščenke itd. Celo stara računalniška oprema/diski s podatki se lahko znajde v smeteh. V poštev pride tudi odpisana računalniška oprema ali celo informacija, da koga ne bo kar nekaj časa, zaradi koriščenja dopusta ali zaradi bolezni.

Vse naštete stvari lahko predstavljajo neprecenljive vire socialnemu inženirju. Telefonski imenik jim 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 nam povedo, odsotnost in čas, kdaj se lahko osredotočijo na napad. Razna navodila, občutljivi podatki, gesla, sistemske nastavitve lahko predstavljajo vir tehničnih informacij in opremo s katero podjetje posluje. Nazadnje odpisana ali odvržena oprema, pretežno diskovne naprave, arhivske kasete, pri restavriranju pomenijo veliko izbiro uporabnih informacij.

Gledanje čez ramo (*shoulder surfing)*

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

[http://www.klemen.fraj.net/?p=1742]

Internet

Internet predstavlja središče oziroma glavno komunikacijsko središče moderne dobe. Na žalost pa predstavlja tudi na široko odprta vrata vsemu internetnemu kriminalu oziroma socialnim inženirjem. Na spletu se puščajo različne stvari, od osebnih podatkov, poštnih naslovov in celo gesel. Primarna napaka, ki jo lahko večkrat opazimo pri uporabnikih je, da uporabljajo preprosto geslo in enako uporabniško ime (poštni naslov), skorajda na vseh spletnih računih enako. Primeri so spletne strani; *Yahoo*, *Gmail*, *Facebook*, udejstvovanje in prijava v novičarske skupine (*forums)*, puščanje podatkov v obliki prijav itd.

Včasih celo s prednastavljenim internetnim brskalnikom na avtomatsko beleženje uporabniških imen in gesel. Torej, posledično napadalec s pridobitvijo pravilnega gesla pridobi ključ, ki odpira še več vrat. Eden izmed poznanih načinov je, da si napadalec pridobi podatke s pomočjo on-line obrazca (*formular*). Obrazec primerno opremi, nastavi vabo, po vsej verjetnosti je to kakšna nagrada. Uporabnik z izpolnitvijo obrazca ne poda samo svoj internetni naslov, tudi svoje geslo, je celo pozvan, da se s svojo odobritvijo namesti kakšen pritajen program. Lahko se celo zgodi, da poda osebni račun, ki ga uporablja v podjetju, saj je ta edini s katerim razpolaga. Obrazec je posredovan lahko preko spletne strani, kot okno, ki izskoči (*pop-up*) ali poštno sporočilo, pripet k podatkom, ki jih lahko snamemo itd. Poštna sporočila se masovno pošiljajo širši množici, spletne strani nastajajo s tem namenom ali celo najbolj obiskane spreminjajo. http://www.securityfocus.com/infocus/1527

Ribarjenje (*phishing)*

Sama beseda *phishing* je sestavljena iz treh angleških besed: *password* (geslo), *harvesting* (trgatev) in besede *fishing* (ribarjenje). Z metodo tako imenovanega ribarjenja poskušajo napadalci priti do zaupnih podatkov, ki jim jih nič hudega sluteči internetni uporabniki posredujejo. Pri tem lahko gre za ribarjenje kontnih informacij , na primer on-line licitacijske hiše (*eBay*) ali nič manj pomembne pristopne podatke internetnega bančništva. Napadalci izkoriščajo zaupljivost in pripravljenost ljudi k pomoči, pri tem uporabijo spletno pošto, ki je pogosto opremljena z napačnim naslovom pošiljatelja in shemo ali celo enakim izgledom, kot uradno sporočilo. V spletni pošti je žrtev prijazno obveščena, da je njen kontni račun ali račun internetnega bančnega predala, žal potekel. Spletna pošta vsebuje povezavo (*link*), kjer si lahko žrtev spremeni uporabniško ime in geslo. Žal pa povezava ne vodi na pristno stran ponudnika storitev (npr. banke), ampak na identično stran, ki jo je postavil napadalec. S pridobljenimi podatki napadalec upravlja v imenu žrtve in koristi njene finančne in osebne vire. [http://www.melani.admin.ch/themen/00103/00203/index.html?lang=de]

Socialni inženir postavi spletno stran identično spletni strani katere od bank in nato žrtev prepriča o pristnosti strani - stran zbira informacije ali pa celo na računalnik namesti programsko opremo za vdor. [http://www.klemen.fraj.net/?p=1742]

Strokovnjaki že nekaj časa opozarjajo, da so socialna omrežja največkrat izvor ribarjenja za osebnimi podatki. Napadalci spreminjajo tehniko in za žrtve izbirajo brskalnike in ne spletnih mest, saj lahko z uporabo tako imenovanega socialnega inženiringa laže prepričajo

uporabnike, da si naložijo škodljive programe, čeprav verjamejo, da so si pravkar naložili koristen pripomoček. [http://www.dnevnik.si/novice/znanost 17.4.2008]

Precej enostavno je urediti posnetek spletne strani legitimne organizacije. S pomočjo HTML kode, prevarant računa, da bodo ljudje resnično mislili, da kontaktirajo z legitimno stranjo. Socialni inženirji pri svojem početju uporabljajo celo princip nezaželene pošte *(spamming*), ki jo pošiljajo veliki skupini ljudi, ki je že opravila kak nakup oziroma pustila občutljive podatke pri ponudnikih storitev in že zaupa temu načinu poslovanja. Za občutljive podatke štejemo: osebne podatke, številke kreditnih kartic, številke računov, kontnih računov, prijavna uporabniška imena in gesla itd. [www.wikipedia.org]
Primer: [http://www.arnes.si/si-cert/obvestila/2004-06.html]

***Pharming* napadi**

Pharming napadi (gre za skovanko med angleškima besedama *farming* in *pharmacy*, navezuje pa se na tehniko genetskega inženiringa, v svetu interneta pa bi lahko govorili o inženiringu naslovov spletnih mest) so verjetno bolj nevarni za uporabnika, saj jih je nekoliko težje prepoznati. Glavna razlika je v tem, da gre pri *pharming-u* za bolj tehnični napad kot za tehniko socialnega inženiringa, na katerem temelji ribarjenje podatkov oziroma *phishing.* Praviloma gre pri *pharming* napadih bodisi za neposreden napad na DNS strežnike, bodisi za napad na določeno datoteko, ki se nahaja na računalniku uporabnika (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. [www.wikipedia.org]

Če so *phishing* napadi temeljili predvsem na ponarejenih e-sporočilih, ki so na lažne spletne strani privabljali uporabnike z namenom, da si na protipraven način pridobijo njihove številke kreditnih kartic in ostale zaupne podatke, pa napadalci sedaj vse bolj uporabljajo napade brez vabe. Posledica *pharming* napada je, da je uporabnik brez njegove vednosti preusmerjen na lažno stran, ki je popolna kopija originalne, vendar posebej narejena za zbiranje zaupnih podatkov z namenom njihove kasnejše zlorabe. [http://www.nasvet.com/pharming-napadi/]

Spletna pošta *(E-mail)*

Precej razširjena oblika, z direktnim dostopom do uporabnika in poslovnega sistema. Navsezadnje predstavlja spletna pošta vodilo glavne komunikacije v podjetju in je na splošno najpogosteje uporabljena. Priponke v spletni pošti lahko vsebujejo oziroma nosijo viruse, črve in »trojanske konje«, izvajalne skripte in v glavnem vso škodljivo internetno zalego. Dokumentiran je primer vdora v ponudnika storitev AOL (*America on line*). Napadalec je večkrat klical AOL tehnično podporo in se nazadnje pogovarjal s tehnikom podpore skorajda eno uro. V času konverzacije je napadalec omenil, da prodaja avtomobil in to po zelo nizki ceni, kar je v tehniku podpore spodbudilo zanimanje, posredoval je svoj spletni naslov in prejel pošto s priponko slike avtomobila. Namesto »slike avtomobila« je odprtje spletne pošte izvedlo izvajanje programa imenovanega angl. *Backdoor Exploit*, ki je odprl navzven stranska vrata skozi AOL požarni zid. Tako je bil pristop v AOL varnostni sistem omogočen. [http://www.vigilante.com]

Nevarnosti spletne pošte

- okužena pripeta datoteka
- nevaren *JavaScript*
- zlonamerni spletni naslovi - vdor preko ranljivega brskalnika
- ribarjenje *phishing* in kraja identitete

Anketiranje (*mail-outs)*

Socialni inženir pod pretvezo anketarja (študenta, raziskovalca ipd.) sprašuje podjetje in zaposlene razna vprašanja, s pomočjo katerih lahko marsikaj izve o podjetju, kar mu pomaga pri nadaljnjem delu. [http://www.klemen.fraj.net/?p=1742]

Intranet *(technical support)*

Drug način napada takšne vrste je, da se napadalec lažno predstavlja kot mrežni skrbnik, ki pošlje uporabnikom zahtevo po njihovih geslih. V vseh primerih takšna vrsta napada socialnega inženiringa ne uspeva, saj vseeno uporabniki postanejo pozorni in se ponavadi odzovejo. Naslednji način napada je z okni, ki izskočijo (*pop-up*), zahtevajo pozornost, izgledajo kot del omrežnega sistema in zahtevajo, da uporabnik ponovno vnese svojo uporabniško ime in geslo. Ponavadi se nanašajo na kakšen navidezni problem, ki ga

uporabnik lahko pomaga rešiti. S te točke bi se morali uporabniki zavedati, da ne pošiljajo gesel naokrog, tudi sistemskim skrbnikom ne.

Prepričevanje *(persuasion)*

Socialni inženirji pri svojem delu uporabljajo veščine, ki temeljijo na psihološkem pogledu ljudi, zanimivo je kako ustvarijo popolnoma psihološko okolje za izvedbo svojih ciljev. Osnovna metoda prepričevanja vsebuje: laganje, dvorjenje, skladnost, razpršitev odgovornosti in vzpostavitev enostranskih prijateljskih vezi. Ne glede na uporabljeno metodo, je osrednji del, prepričati osebo s pripadajočo informacijo oziroma predstavo, da je socialni inženir v resnici oseba, ki ji lahko zaupa vse občutljive podatke. Drug pomemben ključ prepričevanja je, da se nikoli ne vprašuje po več informacijah hkrati, ampak v majhnih in jasno namenjenih vprašanjih določeni osebi, z namenom ohranitve pristnega odnosa.

Pomemben uporabnik *(important user)*

Socialni inženir se žrtvi predstavi kot eden izmed pomembnih članov podjetja (višje kot žrtev) in da mora nujno dokončati neko pomembno nalogo ter lahko s tem žrtev prepriča, da mu posreduje informacije za dostop na daljavo ter vse potrebne podatke; reče, da je pozabil geslo in da želi novega.

Nemočen uporabnik *(helpless user)*

Socialni inženir se pretvarja, da je nov v podjetju in da nima pojma o računalnikih ter prosi tarčo, naj mu pomaga - če je potrebno tudi s kakšnim uporabniškim imenom/geslom.

Neposreden pristop (*direct approach*)

Precej neučinkovita in najlažja metoda - žrtev preprosto vprašamo za geslo.

Nasprotni socialni inženiring *(reverse social engineering - RSE)*

Štejemo ga v naprednejšo metodo pridobitve nedovoljenih informacij. Ta metoda pride v poštev, ko se napadalec predstavi kot oseba s poslovno avtoriteto in je po lestvici pomembnosti v podjetju višje kot žrtev. V primeru problemov, nedelovanja ali zakasnitev v delovnih procesih se raje žrtev obrne k osebi takšne vrste poslovne avtoritete. Nasprotni socialni inženiring je sestavljen iz raziskovanja, načrtovanja in izvedbe.

V primeru uspešnega obratnega socialnega inženiringa ima napadalec veliko več možnosti pridobiti si informacije. Vsekakor zahteva velik del priprav, raziskav, načrtovanja in tipanja (*sniffing*) za izvedbo.

Po opisu v članku *Methods of Hacking: Social Engineering*, Rick Nelsona, lahko razdelimo obratni socialni inženiring na tri med sabo prepletajoče se korake:

Sabotaža

Napadalec sabotira omrežje ali napravo, povzroči nastanek problema oziroma situacije.

Oglaševanje

Napadalec oglašuje oziroma ustvarja s svojo podobo zaupanja vredno osebo, ki bo rešila to situacijo in na katero se bo žrtev obrnila.

Pomoč

Ko pride do pomoči, odprave napake, pa napadalec zahteva določene informacije od zaposlenih in doseže, kar je tudi bil njegov cilj. Žrtev se ne zaveda ali gre za napadalca ali ne, saj je njen problem odpravljen (omrežje ali naprava). Vsi so srečni ob normalnem poteku delovnega procesa, saj je s tem tudi njihovo delo opravljeno.

Tipičen primer te tehnike je ta, da napadalec sabotira določen del sistema, žrtev opazi napako in išče nekoga, ki bi jo popravil - tukaj spet nastopi socialni inženir, ki napako popravi, obenem pa pridobi razne podatke, ki »naj bi mu bili potrebni« za odpravo napake. [http://www.klemen.fraj.net/?p=1742]

Trojanski konj *(Trojan)*

Izkoristi žrtvino radovednost ali pohlepnost in enostavno dostavi zlonamerno programsko kodo (*malware)*. Primer »Trojanarja« je lahko spletna pošta z obetajočo vsebino, zanimivega, sexy ohranjevalnika zaslona, pomembna antivirusna in sistemska nadgradnja, popravki ali celo zadnje rumene novice popularnih oseb. Najpomembnejša stvar pa je v priponki, kjer se skriva trojanski konj, v obliki zlonamerne kode. Žrtve z odprtjem priponke ali celo predogleda spletne pošte, aktivirajo dejanje. Ker uporabnika vedno žene določena naivnost, je ta tehnika kar precej učinkovita.

Podobna tehnika trojanskega konja je program, ki daje napadalcu vstop in vsebuje v sami programski kodi skrito, pritajeno zlonamerno kodo (npr. *spyware*) ali se pretvarja da je nekaj, kar ni, npr. snemljiva datoteka brezplačnega novega programja, se pa v resnici obnaša kot znani konj iz Troje, ki omogoča napad kar znotraj računalniškega sistema.

Za samo razpršitev okuženih spletnih sporočil so odgovorne metode socialnega inženiringa, na ta način, da se naslov spletne pošte, vsebine ali priponke nanaša na kakšno znano osebo, znan iskan program, zanimivo sliko itd. Svetovno znan primer je *ILOVEYOU* virus in *Ana Kurnikova* trojanski konj.

Stranska vrata *(backdoor)*

Je računalniški sistem, bodisi kriptiran ali v algoritmu, metoda, s katero lahko označimo več aktivnosti, ki ostanejo neopažene uporabniku računalnika. Z njo zaobidemo normalno avtentikacijo, opravimo varen pristop v računalnik, pridobimo dostop do podatkov. Pojavlja se lahko v obliki nameščenega programa (npr. *Back Orifice*) ali pa modificira že kak nameščen program ali napravo. [www.wikipedia.org]

Virusi (*viruses*)

Širijo se preko »gostiteljev«, to so predvsem datoteke, tako izvršljive (.exe,.com itd.), kot tudi podatkovne, ki vsebujejo skripte ali makroje (.doc, .xls). Poženejo oziroma aktivirajo se takoj, ko okuženo datoteko odpremo. Virus lahko v računalniškem sistemu povzroči veliko škodo, izvede pa lahko skorajda vsako interakcijo v računalniku. V prvi vrsti je lahko samo nadaljnja širitev virusov, lahko popolni zastoj ali izguba podatkov.

Črvi *(worms)*

Po zadnjih podatkih so črvi še bolj nevarni kot virusi. Širijo se podobno kot virusi samodejno preko spleta. Izkoriščajo socialni inženiring za svojo širitev in povzročajo veliko omrežnega prometa. Računalniki in računalniška omrežja, ki vsebujejo črve, delujejo zelo počasi ali včasih povsem neizogibno zastanejo. Hkrati pa so črvi nosilci raznovrstnih zlonamernih programov, jih pa nekateri protivirusni programi sploh ne odkrijejo, saj vsebujejo drugačne specifike kot virusi.

Zlonamerne spletne strani

Obstajajo s točno določenim namenom: izkoristiti varnostne napake oziroma luknje v brskalnikih za pridobivanje podatkov, navsezadnje tudi za vdor v računalnik.
Omenjeni podatki so lahko osebne narave, zraven tega se lahko zbirajo poštni naslovi, za kasnejše masovno pošiljanje pošte (*spam*) in ribarjenja (*phishing*).

Vohunski in oglaševalski programi so *Spyware* in *Adware*; v bistvu zastopajo vso spremljanje uporabnikove dejavnosti na spletu in zbir in razpošiljanje teh podatkov na določene naslove, k temu prištevamo recimo beleženje pritisnjenih tipk (*keyloggers)*, prisluškovanje omrežnemu prometu (*sniffers*) in zajemanje zaslonskih slik (*print screens*). *Adware* termin je nastal iz dveh angleških besed, *advertising* in *software*. Povsem jasna razlika v definiciji *Spyware* in *Adware* ne obstaja in ju je stežka ločiti. *Adware* se velikokrat uporablja v reklamne namene, izkorišča uporabnikove navade deskanja po spletu in največkrat obiskane spletne strani. Oglašuje določene produkte, strani in storitve. Skozi spletne naslove kar enostavno vsiljivo nameša uporabnikovo pot do želene strani. Lahko celo spremeni začetno stran v brskalniku. Programom te vrste uspeva širitev in nameščanje ravno preko uporabnikov samih, preko različnih programov, ki so bili sneti s spleta.
[http://www.melani.admin.ch/themen/00103/00201/index.html?lang=de]

Zlonamerna koda (*Malware)*

Škodljive kode (*Malware*) so programi, dokumenti ali sporočila, ki lahko negativno vplivajo na uporabnike računalniških sistemov in jim povzročajo škodo in težave. [http://www.safe.si]
Zlonamerno programje (angl. ***malicious software; mal +ware= malware*****)** so vsi zlonamerni programi, npr. virusi, črvi, stranska vrata, trojanski konji, vohunsko programje
[http://www.islovar.org]

Korenski uporabniški komplet (*Rootkits)*

Tako poimenujemo zlonamerno kodo, ki je sestavljena iz programa ali celo kombinacije skupine programov, izvorno narejenih z namenom prevzeti osnovno oblast nad računalniškim sistemom, brez dovoljene avtorizacije lastnikov in legitimnih upravljalcev.
[www.wikipedia.org]
Termin izhaja iz angl. besede *root*, kar pomeni koren, oziroma jedrni del operacijskega sistema in *kit* , v kompletu. Ime izhaja iz operacijskega sistema *Unix*, kjer *root* predstavlja skrbniški dostop. Zelo težko ga je odkriti, saj je v jedrnem delu zaščiten ali celo skrit v različnih oblikah, navsezadnje v strojni opremi oziroma v *Biosu*. Prisotnost *Rootkitov* je bilo zaznati na vseh večjih znanih operacijskih sistemih, kot so Microsoft Windows, Linux, Mac OS, Solaris in Unix. Njihovo delovanje je pogosto v obliki modifikacije posameznih delov

operacijskega sistema in lastna namestitev v obliki gonilnikov in posameznih modulov, zbirnikov ukazov jedra.

Napadalci uporabljajo pri svojih napadih socialni inženiring, kjer so omejeni izključno s svojo domišljijo in iznajdljivostjo. Pretentati skušajo končne uporabnike, ki so pogosto najšibkejši člen v varnostni verigi, da poženejo "trojanskega konja", ki okuži njihov sistem. [http://www.krneki.net/rootkits/Rootkits.pdf]

Odstranjevanje *Rootkitov* je mogoče samo z za to prirejenimi orodji za odkrivanje in eliminiranje te zlonamerne kode, samo preprečevanje pa sloni na preventivi oziroma ozaveščanju uporabnikov in skrbnikov.

Vzpostavljalci in usmerjevalci zvez (*Dialers*)

V preteklosti velikokrat popularni ravno zaradi načina pristopa k spletu, ki so ga nudili ponudniki internetnih storitev. Njihova nevarnost je tičala v samodejni vzpostavitvi telefonske zveze in klicanja preko uporabnikovega računa. Usmerjenost predvsem na oglaševalske strani, velikokrat na pornografske strani. Ta nevarnost je delno eliminirana vsaj v državah, kjer je ponudba internetnih storitev na ravni naprednejših tehnologij in neomejenega dostopa in ne preko klicne povezave.

Je pogosto uporabljeno orodje vdiralcev in socialnih inženirjev. V obdobju zadnjih let so se tako imenovani *Dialersi* obdržali z izvedbo zlonamerne kode, ki usmerja promet v brskalnikih na njihove določene spletne strani.

Izbrani cilji in sredstva

Nevarna zalega si prizadeva spremeniti v naših osebnih računalnikih varnostne nastavitve, omejiti funkcionalnost, se okoristiti z našimi podatki in informacijami, pridobiti informacije, za katere še sami ne vemo, da obstajajo.

To lahko počnejo npr.:

- s spreminjanjem tekstovne datoteke *host*, ki se nahaja natančno v (c:\windows\system32\drivers\ect)
- z upravljanjem z dodatki za brskalnik (*HBO, BrowserHelperObjects*)
- s spreminjanjem nastavitev v brskalniku
- z vnosi in spremembami v registru
- z izvajanjem okuženih programov, sredstev in storitev

- s preusmeritvami in oteževanjem delovanja osnovnih funkcij operacijskih sistemov
- v generiranju prometa z razpošiljanjem in širjenjem v omrežju

Potegavščine (*Hoax)*

Sporočila spletne pošte, ki vsebujejo informacije o posodobitvah ali novih nevarnostih, nesrečah, ki krožijo po spletu, so tako imenovana zavajajoča sporočila (angl. *Hoax*). Vsa zavajajoča sporočila uporabljajo enak vzorec in pozivajo, da jih pošljemo naprej, pri čemer ljudje celo puščajo za seboj svoje poštne naslove. Prištevamo jih lahko tudi med verižna pisma. To so pisma, ki se pošiljajo od uporabnika k drugim uporabnikom in ponavadi ne spreminjajo vsebine. Za uporabnika so zavajajoča, povzročajo promet in obremenitev v poštnem sistemu.

Verižna pisma *(Spam*)

Spam označujemo kot krovni pojem nezaželenega oglaševanja in verižnih pisem. Osebo, ki pošilja sporočila na več naslovov in vsa sporočila v njih usmerja za lastno promocijo ter brez dovoljenja, imenujemo *Spamer*. Različne raziskave potrjujejo, da je delež nezaželene pošte že okrog 60% globalnega poštnega prometa ter še v porastu. Nezaželena pošta postaja vse večji problem uporabnikov, podjetij in upraviteljev poštne infrastrukture. [http://www.melani.admin.ch/themen/00103/00206/index.html?lang=en]

Piškotki (*Cookies*)

Piškotki so majhne tekstovne datoteke, shranjene na uporabnikovem računalniku pri obisku spletne strani. Njihov namen je poenostavitev uporabnikovega dela. Nekatere on-line spletne storitve zahtevajo uporabniško ime in geslo. Da ob ponovnem obisku ni potrebno znova vpisovati teh podatkov, nam lahko ob pripadajoči izbiri pomagajo prav piškotki. Spletne trgovine kar same ponujajo že izbrane artikle, ki so bili izbrani ob zadnjih obiskih teh strani. Poznamo kratkoročne in dolgoročne piškotke. Razlikujejo se po svoji obstojnosti, ki je določena od spletne aplikacije, ki jih je ustvarila.
Nekateri poidejo že ob zaprtju brskalnika, nekateri ob določenem času. Hkrati pa piškotki na nek način kršijo zasebnost, tako da lahko lastniki spletnih strani izluščijo in zaznajo

uporabnikovo nakupovalno obnašanje na spletu in lahko sestavijo uporabniški profil. [http://www.melani.admin.ch/themen/00103/00207/index.html?lang=en]

Klepetalnice in takojšnje sporočanje (*Chats, Instant Messaging*)

Klepetalnica je oblika komunikacije ljudi preko spleta v realnem času. Precej je podobna telefonski komunikaciji, le da pogovor ne teče govorno, temveč pisno. Odvisno od teme, so odprti različni komunikacijski kanali, imenovani klepetalniške sobe (*chat rooms*). Uporabnik lahko participira z vsemi uporabniki hkrati, lahko samo s specifičnim uporabnikom, se seli v privatne sobe oziroma kanale. Podobna ponudba je s komunikacijo preko sporočilnih storitev (npr. *AOL, MSN, ICQ, Yahoo*), s katerimi so povezani milijoni ljudi. Slaba stran teh storitev je, da se preko njih izvajajo različna kriminalna dejanja, npr.: pedofilija, virusi, črvi, Trojanci itd.[http://www.melani.admin.ch/themen/00103/00208/index.html?lang=en]

Mobilni telefoni, dlančniki, tehnologija modri zob (*Mobile phones, PDA, Bluetooth*)

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 (*infrared)* 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. Nekatere implementacije danes ne dosegajo varnostnih meril, predvsem pri tehnologiji modrega zoba pri posameznih proizvajalcih teh naprav. Večina dlančnikov podpira modri zob komunikacijo. Odprt je nepooblaščen dostop do koledarja, imenika, celo do shranjene pošte. Velikokrat se zgodi, da zaznamo prisotnost naprav z vključitvijo storitve modrega zoba na našem telefonu ali dlančniku. 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 in različna pozivanja h klicanju številk 0900. [http://www.melani.admin.ch/themen/00103/00209/index.html?lang=en]

Brezžična omrežja (*WirelessLan*)

WLAN kratica pomeni *Wireless Local Area Network*, v prevodu brezžično omrežje. S to tehnologijo komunicirajo različne naprave, notesniki, dlančniki, tiskalniki, projektorji in

druge naprave, ki imajo potrebo po mobilnosti, premičnosti in svobodi premikanja, navkljub povezanosti. Delujejo na različnih frekvenčnih območjih in z različnimi razredi varnosti. S primerno nastavitvijo dosegajo tudi do 200 metrov pokritosti okrožja. V odvisnosti od same konfiguracije naprav za brezžični pristop je varnost oziroma ranljivost komunikacije. Omogočeno je prestrezanje, saj je nosilec oz. medij, zrak , in kljub enkripciji prometa obstaja možnost spremljanja prometa.
[http://www.melani.admin.ch/themen/00103/00210/index.html?lang=en]

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

Varnostne luknje (*Security holes*)

Programske aplikacije so sestavljene iz inštrukcij, ukazov, ki računalniku povedo, katere aktivnosti bodo izvedene in na kak način. Aplikacije so pogosto iz preko milijona programskih vrstic takšnih inštrukcij. Upoštevajoč številčnost teh vrstic in hitrost priprave teh aplikacij, ni presenetljivo, da prihaja do napak. Skoraj dnevno se ustvarijo ali odkrijejo napake v razširjenih programih in se zato posledično pišejo popravki. Vendar te napake same po sebi ne predstavljajo varnostnih lukenj. Če pa pride do napak v aplikaciji, ki nekako onemogočijo varnost in odprejo vrata nepooblaščenemu pristopu, potem govorimo o varnostni luknji (*security hole*) in ranljivosti (*vulnerability*).
[http://www.melani.admin.ch/themen/00103/00211/index.html?lang=en]

Različni pristopi zlonamerne kode (*Malware)*

V večini primerov izkoriščajo socialni inženiring kot vzvod oziroma se širijo s pomočjo človeške nagnjenosti k zaupljivosti in nevednosti.
S pomočjo socialnega inženiringa se širijo preko nekaj naštetih možnosti:

- priponk v spletni pošti
- z izvedbo skript, pritajenih in skritih v spletnih straneh
- programov, ki so na voljo za snet s spleta, za aktualno in zanimivo širšo množico
- izmenjave datotek v različnih socialnih mrežah (*P2P, Facebook* itd.)
- nepravih in zavajajočih spletnih strani
- dodatkov in obližev za vzdrževanje operacijskih sistemov, programov, predvajalnikov

- varnostnih lukenj v operacijskih sistemih, programih, brskalnikih, komunikacijskih programih
- nepravilno nastavljenih varnostnih zaščit in odprtih računalnikov
- zunanjih medijev, nosilcev zapisov
- ponudnikov internetnih storitev in globalnega marketinga
- nevednosti in zaupljivosti ljudi.

V nevarnosti niso samo naprave, za katere mislimo, da so najbolj ogrožene (osebni računalniki, strežniki), ob tem mislimo tudi na mobilne naprave (GSM, dlančniki, GPS itd.) in elektronske naprave, katerih logika dopušča komunikacijo in upravljanje na daljavo. Vse zgoraj naštete možnosti napadov združuje internet in človeški dejavnik, vse skupaj se gradi na bistvu obstoja. Medij predstavljata tako internet kot splet.

Nosilci podatkov - mediji

Ljudje vse prevečkrat nasedejo lastni radovednosti in podležejo skušnjavi.
Predvsem v zadnjih letih so postali nosilci podatkov USB ključki, zelo popularni. Odlikuje jih praktičnost, so lahki in prenosni, hkrati pa kapacitetno razpoložljivi. Izkušen socialni inženir bi z lahkoto izvedel svoj namen s prirejenimi USB ključi ali CD mediji ter s pomočjo radovednosti ljudi zlonamerno kodo na podatkovnem nosilcu uspešno impliciral v informacijski sistem.

Napake uporabnikov

Napake uporabnikov so najbolj pogost vzrok nepravilnega delovanja informacijskih sistemov. Vzrokov za nastanek teh napak je mnogo. Najpogosteje uporabniki ne upoštevajo navodil, organizacijskih predpisov ali so pri delu površni (Gradišar, 2003, 56). Večina informacijskih sistemov ima vgrajenih veliko varoval, ki napake preprečujejo oziroma nanje opozarjajo. A še vedno lahko uporabnik po nekem naključju izvede operacijo, ki v fazi testiranja ni bila predvidena. Ne glede na kakovost informacijskih sistemov, bodo ti vedno ostali občutljivi na napake uporabnikov. (Rakovec, 2005, 65)

4.8 Varnostni trendi in analize v letu 2008 in naprej

Varnostni strokovnjaki iz podjetja AVG (varnostni in zaščitni produkti) in svetovno znani varnostni strateg Bridwell, so izdali analizo 10. najpogostejših nevarnosti na spletu in trend gibanja nevarnosti in zaščite na svetovnem spletu v prihodnjih letih.
Spletni trgovci, iskalniki, socialne mreže in plačljive iskalne kampanje ter razna podjetja, so označeni kot najbolj ranljiva področja.
Po navedbi so v letu 2007 in s predpostavkami o varnostnih grožnjah iz leta 2006, virusi predstavljali le 15 % groženj v spletu v primerjavi z ostalo nevarno spletno zalego.
Kot nevarno spletno zalego lahko štejemo razna ribarjenja (*phishing*), črve (*backdoor worms*), trojanske konje (*Trojans*), beležnike tipk (*Keyloggers*), vohunske programe (*Spyware*), oglaševalske programe (*Adware*) in ostale spletne izvajalne skripte in grožnje.
[http://www.avg.com/press-releases-news]

Virusne grožnje v letu 2007, razvrščene po pomembnosti

(*Global Security Strategist, Larry Bridwell*)

1. W32/Detnat 2. W32/Netsky
3. W32/Mytob 4. W32/Bagle
5. W32/MyWife 6. W32/Virut
7. W32/Zafi 8. W32/MyDoom
9. W32/Lovegate 10. W32/Bagz

Protivirusna industrija se je v obdobju zadnjih dveh ali treh let srečevala z zlonamerno kodo, ki se je preoblikovala iz preprostega virusa v kompleksno zlonamerno spletno grožnjo. Kompleksna zlonamerna koda je podprta z dejavniki zlonamerne kode, orodij, odprtih kodnih napisanih programov in socialnega inženiringa ter uprta v nič hudega slutečega uporabnika.
[http://www.avg.com/66551]
Z razliko od klasične zlonamerne kode, ki je bila ponavadi sestavljena iz trojanskih konjev, ki so bili napisani z namenom iskanja, povzročanja zmešnjave in dajanja občutka pomembnosti, je v porastu posebna kategorija kriminalno podprtih programov (*Crimeware*). S samim imenom *Crimeware* je povezana kriminalna (*cyber)* kiber-združba, ki se okorišča s krajo identifikacij in podatkov in deluje z namenom povzročanja škode podjetjem in finančnim doprinosom.

Pričakovati je razmah različnih visoko razvitih orodij in pripomočkov zlonamerne kode v prihodnosti. Cilj napadalcev in resnična nevarnost so napadi usmerjeni na iskalnike in socialne mreže (*social network service*).
[http://www.idc.com/events/emea/emea_sp_bridwel_larry.jsp]

Aktivnosti zlonamerne kode v letu 2007 (*Global Security Strategist, Larry Bridwell*)

1. S*uper Bowl/Dolphins* spletna stran, opremljena z zlonamerno kodo! (February)
2. Google storitev *AdWords o*kuži in preusmerja! (April)
3. Google lažno oglašuje z že napadenimi strežniki (*Bait & Switch)*! (July)
4. Spletna stran *Bank of _India* okuži obiskovalce! (August)
5. S*torm Trojan* predstavi lažne *YouTube* poti! (August)
6. *.Gov* uspe vdreti v vladno spletno stran (ZDA)! (September)
7. *Facebook* vstavljena pasica distribuira zlonamerno kodo*!* (September)
8. *V*dor v *Alicia Keys/MySpace behind the scenes!* (November)
9. *MLB in NHL.com* okužena pasica *(benner)!* (November)
10. *Monster.com* okuži iskalce zaposlitve*!* (November)

[http://explabs.blogspot.com/2007_07_01_archive.html]

Iz napadov na *Facebook* in spletno stran *Major League Baseball*, do *Alicia Keys* spletne strani je jasno, da se je pospešeno povečala preteča nevarnost, ki prihaja naravnost iz spleta (*on-line*).
V letu 2008 smo priča še bolj izpopolnjenim in organiziranim kiber-kriminalnim vdorom oziroma napadom s pomočjo vse večjega tehnološkega napredka, ki je predvsem naperjen v storitve socialnih mrež. Storitve socialnih mrež so najbolj ranljive, ker slonijo na obsežni in povezani vsebini, deljenju informacij in zaupanja njenih udeležencev.

4*.9 Pričakovane grožnje v naslednjem letu in v prihodnosti*

1. **Spletni napadi in spletno podprti napadi s pomočjo socialnega inženiringa**
   »Virusi bodo kontinuirano predstavljali grožnjo, priča bomo hitremu porastu napadov s pomočjo socialnega inženiringa in napadov na Splet 2.0 (Web 2.0)«, pravi Thompson, svetovalec pri podjetju AVG.

2. ***Storm Worm*** **je črv na obzorju** »*Tukaj bo ostal v različnih oblikah in intenziteti. Pričakujemo ga lahko v orkestralnih napadih v kombinaciji z ostalimi, po vseh različnih osnovah« ,* pravi Obluk, svetovalec pri podjetju AVG.
3. **S spletno pošto razširjeni virusi**
   Marsikateri novinec bo nasedel prevari in se ne bo zavedal, da je z odprtjem priponke ali s klikom na lažno pot nasedel prevari.
4. **Spletni napadi na zaupanja vredne strani** »Današnji kiber-kriminalni trend je usmerjen na »dolgo viseče sadeže«. Če uspejo vdreti v kakšno popularno spletno stran, lahko zelo hitro poberejo vse zasluge in izginejo, hitreje kot so se pojavili« , pravi Thompson.
5. **Povečanje števila Windows Vista napadov**
   S prehodom vse večjega števila uporabnikov na zadnji Microsoftov operacijski sistem, predstavlja Microsoftova Vista, veliko in poželjivo tarčo napadalcev.
   [http://www.avg.com/press-releases-news]
6. Strokovnjaki za informacijsko varnost pozivajo mednarodno pravo, da se s sprejetjem ustreznih zakonov pobližje spoprime s kiber-kriminalom v letu 2008.
   »*Majhna je verjetnost, da bo sprejetje kakšnega zakona zajezilo porast kiber-kriminala, saj je v tem krogu enostavno preveč denarja*« , pravi Thompson.
   [http://www.avg.com/press-releases-news.ndi-82050]

Storitve socialnih mrež in socialne mreže

Osredotočene so na graditev spletnih skupin oziroma komun na ljudi, ki delijo skupne interese in aktivnosti, ali na tiste, katerih interes je radovedno raziskovati te interese in dejavnosti. Večina teh storitev temelji na spletu in ponuja različne načine interakcije med ljudmi, kot je na primer spletna pošta, klepetalnice in *»instant«* sporočanje.

Primer 1: 12.4.2008

V *Panda Security* laboratorijih za odkrivanje in analizo škodljivih programov, so odkrili *YTFakeCreator*, program, ki ga kiber-kriminalci uporabljajo za ustvarjanje lažnih *YouTube* internetnih strani. Z njimi želijo okužiti računalnike uporabnikov s škodljivimi kodami.
Metoda okužbe je naslednja: kiber-kriminalci pošljejo elektronsko sporočilo, ki vsebuje video z domnevno mamljivo, senzacionalno vsebino (erotične vsebine, smrt slavnih oseb itd.) in

s tem spodbudijo uporabnika h kliku na povezavo za ogled videa. Ta metoda je poznana kot socialni inženiring. Ko uporabnik enkrat vstopi na lažno stran, ki je zelo podobna pravi strani *YouTube*, se prikaže okno s poročilom o napaki, ki obvešča uporabnika, da si video vsebine ne mora ogledati zaradi manjkajoče komponente (kode, *Adobe Flash* posodobitev itd.) in predlaga njeno takojšnjo namestitev. Če uporabnik temu navodilu sledi, si na računalnik namesti škodljivi program. [http://www.flickr.com/photos/panda_security/2840011688/]
YTFakeCreator omogoča kiber-kriminalcem, da z lahkoto ustvarijo lažne *YouTube* strani. Te lahko vstopijo preko besedila za poročilo o napaki, ki se prikaže na internetni strani. Definira se, koliko časa potrebuje sporočilo za svoj prikaz, vstopi preko povezave do okužene datoteke, ki si jo uporabnik namesti na svoj računalnik in ustvari lažen profil enak tistemu na strani *YouTube*, pod pretvezo, da je bil video naložen preko pravega uporabnika. Vse to s pomočjo enega samega programa. Kiber-kriminalec lahko izbere različne vrste škodljivih kod (viruse, črve, trojance…) za njihovo distribucijo preko teh lažnih internetnih strani. [www.pandalabs.com]

Primer 2: 16.11.2008

Uporabnike *Facebooka* in *Myspace* napada črv *Boface.G*

Omenjeni črv pripne povezavo na profil okuženega uporabnika ali pa ponuja povezavo na lažen *YouTube* video. Lahko pa tudi pošlje kontaktnim osebam okuženega uporabnika, sporočila s povezavo. Ko si uporabniki skušajo ogledati video (ki naj bi jim ga posredoval eden izmed prijateljev), jih povezava odpelje na internetno stran, ki jih želi prepričati v prenos nadgradnje oz. posodobitve programa *Flash Player*, da bi si lahko ogledali želeni video. V primeru, da uporabnik sledi in si omenjeno posodobitev naloži, dovoli kopiji črva vstop v računalnik in poleg gostujočega okuži tudi vse ostale osebe s kontaktnega seznama.
Eno izmed ogroženih socialnih omrežij je že reagiralo in privzelo nekatere varnostne ukrepe, da bi tako zaščitilo svoje uporabnike.

Slika 6: Namestitev okuženega dodatka

Vir: [www.adobe.com]

Socialna omrežja privlačijo kiber-kriminalce

»Socialna omrežja privlačijo na milijone uporabnikov in so postala ena izmed najbolj priljubljenih načinov kiber-kriminalcev za razpošiljanje škodljivih kod«, pojasnjuje tehnični direktor Pandinih laboratorijev, Luis Corrons.

Svarilo pred neprevidnostjo

Uporabniki socialnih omrežij morajo zato po njegovih besedah preveriti izvor teh sporočil, preden sledijo povezavi ali prenašajo karkoli na svoj računalnik.
[http://www.mojmikro.si/news/crvi_postali_glavna_groznja]

Požarni zid (*Firewall*)

Glavna namembnost požarnega zidu je, da dovoljuje oziroma omejuje vstop iz interneta in v internet le določenim programom. Omejevanje se definira z odprtostjo vrat (*ports*) in programov, ki dostopajo skozi njih. Problem se pokaže ob nepravilni konfiguraciji požarnega zidu ali celo ob njegovi neuporabi, izklopitvi. Dogaja se, da požarni zidovi celo ovirajo uporabo legalnih programov, so pogosto vir težav pri nameščanju novih programov in storitev, navsezadnje kot večina varnostnih programov, upočasnijo delovanje računalnika.
[http://www.fg.uni-mb.si/dokument.aspx?id=1377]

5 VARNOST POSLOVNEGA SISTEMA

5.1 Osnovni pojmi revizije

- Revizija – pregled, katerega namen je, prepričati se, da je pregledovano urejeno v skladu z zakoni, s pravili in standardi ter *dobrimi navadami*.
- Informacijski sistem – sistem zbiranja, urejanja, obdelovanja, hranjenja in prikazovanja podatkov ter njihovega preoblikovanja v informacije, največkrat s pomočjo računalniške tehnologije.

Revizija informacijskih sistemov je torej pregled sestavin in povezav zbiranja, urejanja, obdelovanja, hranjenja podatkov in njihovega preoblikovanja v informacije z namenom prepričati se, da so pregledovani informacijski sistemi urejeni v skladu s pravili (zakoni, predpisi, standardi itd.) in dobrimi navadami na področju informatike in informacijske tehnologije. [http://www.si-revizija.si/isaca/revizija_IS.php]

5.2 Pomen revizije informacijskih sistemov

Revizija informacijskih sistemov lahko vodstvu poslovnih sistemov odgovori na vprašanja, ali uporaba računalniške tehnologije zagotavlja:

- rešitve, ki podpirajo dolgoročne poslovne cilje,
- učinkovitost razvojnih projektov in prenov informacijskih sistemov,
- funkcionalnost računalniških rešitev za izvajanje in upravljanje poslovnih procesov,
- ustreznost izrabe računalniške tehnologije,
- delovanje računalniške podpore brez prekinitev oziroma vzpostavitve ponovnega delovanja brez izgub podatkov v primernem času,
- preprečevanje zlorab, poneverb, kraj in razkritij poslovnih skrivnosti.

Vodstva poslovnih sistemov lahko naročijo revizije informacijskih sistemov kot sestavni del revizije računovodskih izkazov ali kot samostojno revizijo.
[http://www.si-revizija.si/isaca/revizija_IS.php]

5.3 Smernice revizije

Cilj vsake revizije je povečati uspešnost le-te in zmanjšati motnje zaradi procesa revizije. Organizacije naj točno in sporazumno izvajajo presoje informacijskih sistemov bodisi samostojno ali v obsegu finančnih revizij in s tem zmanjšajo nevarnost prekinitve poslovnih procesov. Načrti za presojo naj bodo dokumentirani in potrjeni s strani vodstva. Orodja, uporabljena pri presoji, morajo biti uradno potrjena. Presoje naj bodo dokumentirane skupaj z rezultati, neskladnostmi in nadaljnjimi ukrepi. (Rakovec, 2005, 15)

6 INFORMACIJSKI STANDARDI

6.1 BS 7799

Zaradi kompleksnosti področja se je varovanja informacij smiselno lotiti sistematično in sicer na nivoju celotne organizacije. Celovit način upravljanja varovanja informacij obravnava standard *BS7799*. Je mednarodno veljaven standard, namenjen vodstvenemu osebju ter predstavlja model za učinkovit sistem upravljanja varovanja informacij *(SUVI)*. Trenutno aktualen je *ISO/IEC27001*.

Standard *ISO/IEC27001* je soroden s standardi *ISO 9000*, *ISO1400* ter *ISO18000*, kar organizacijam, ki te standarde že imajo, poenostavi in poceni uvedbo.

6.2 SUVI (sistem za upravljanje varovanja informacij)

Vodstveni sistem, ki v organizaciji skrbi za vpeljavo, vzdrževanje in nenehno izboljševanje na področju informacijske varnosti.

Za uspešno delovanje sistema *SUVI* je nujna ustrezna razporeditev vlog in odgovornosti od vodstva organizacije na najvišjem nivoju, do vseh zaposlenih na najnižjem nivoju.

(Gradišar, 2003, 51)

6.3 ISO/IEC 27001

Standard, ki je v tem trenutku v večini sveta temeljni okvir za varovanje informacij.

Tudi na slovenskih tleh se uvaja kot aktualni standard in skupaj z dobrimi praksami vodi k izdelavi in pripravi varnostnih pravilnikov. Standard je zelo splošen in napisan tako, da ustreza potrebam različnih organizacij.

[www.wikipedia.org]

7 PREPREČEVANJE ODTEKANJA INFORMACIJ

7.1 Varnostne politike

Dobra varnostna politika je osnova vsakega varnostnega načrta v podjetju. Napisana mora biti z mislijo na končne uporabnike, z drugimi besedami, jasno in enostavno, da jo bodo tudi nevešči uporabniki razumeli. Vsebovati mora čim manj IT žargona. V njej mora biti tudi zapisano, kaj se pričakuje in na koga se obrniti z morebitnimi vprašanji.

Varnostna politika je definirana z varnostnimi pravilniki po posameznih področjih, ki jih je potrebno ciklično pregledovati in obnavljati. Ko celotno varnostno politiko spravimo v okvir, jo zapišemo v obliki dokumenta, podjetja jo lahko objavijo na intranetu, skupaj z različico dokumenta in datumom, tako da je trenutna različica vedno dosegljiva zaposlenim.

Varnostne politike, katere je smiselno uvesti za zaščito pred socialnim inženiringom, so sledeče:

- Posredovanje podatkov: varnostna politika mora opredeliti, kdo lahko posreduje podatke v javnost in pod kakšnimi pogoji.
- Nadzor dostopa: določiti, ali je potrebno podpisati varnostni sporazum pred dovoljenim dostopom do omrežja in/ali prostorov.
- Pravica dodeljevanja dostopov do sistema in kakšne pravice se lahko dodeljujejo: kdo ima pravico in kaj lahko dodeljuje.
- Uvedba metodologije za ustvarjanje uporabniških računov in njihovo brisanje.
- Razvoj postopkov za ustvarjanje uporabniških računov in brisanje le-teh za preprečevanje zmede in zmanjševanje števila napak.

Gesla

- Zamenjava gesel: varnostna politika bi morala zahtevati uporabo posebnih znakov, števil, velikih in malih črk pri ustvarjanju gesel. Določiti bi morala pogostost menjave gesel – ne preveč pogosto, sicer bodo zaposleni začeli gesla pisati na listke.
- Posredovanje gesel: vsako posredovanje gesel preko Centra za pomoč (*Help Desk*), tajništva, IT oddelka, brez preverjanja istovetnosti osebe s sledečimi metodami:
    - zaposlenega pokličemo nazaj, da preverimo lokacijo (če je res klical s svojega delovnega mesta),
    - z uporabo identitete klicatelja na telefonu,
    - z uporabo digitalnega podpisa zaposlenega (el. sporočilo) ali
    - osebni dvig želene informacije.

Pristopne točke

Modemi in brezžične dostopne točke.

Varnostna politika mora jasno opredeliti, da modemi in brezžične dostopne točke niso dovoljeni v omrežju podjetja, ker s tem ustvarjajo varnostno luknjo v omrežju in izničujejo vlogo požarnega zidu. Če pa se nameščajo, naj bodo nameščeni z vsemi varnostnimi ukrepi in merili. Podjetje naj da strokovno namestiti to infrastrukturo, v nasprotnem primeru jo bodo sami zaposleni kot laiki.

ID zaposlenega

Razpoznava zaposlenih, identifikacija (ID kartica, ključ, koda itd.), prav tako bi moral vsak gost dobiti svojo začasno kartico ob prihodu. Zaposleni bi morali v vsakem primeru identificirati vsakogar brez kartice in zahtevati naj se predstavi.

Uničevanje dokumentov

Vsak pomemben dokument, ki ga več ne potrebujemo in bi ga želeli zavreči, bi bilo potrebno uničiti v uničevalcu dokumentov, s tem preprečimo brskanje po smeteh (*dumpster diving*).

Fizično varovanje

Ključne predele je potrebno označiti in primerno zaščititi dostop, sam dostop pa dovoliti samo upravičencem.

Kršitve

Obstajati mora enostaven in jasen postopek prijav kršitev pravil oziroma sumljivih dejanj.

Hramba podatkov

Življenjska doba podatkov, hrambe in strojne opreme ter z njimi povezane politike, morajo biti jasno napisane.[http://www.sans.org/reading_room/whitepapers/engineering/]

7.2 Program varnostnega ozaveščanja zaposlenih

Če želimo, da nam napadalci v obliki socialnega inženiringa ne bodo škodovali, moramo veliko vlagati v stalno izobraževanje in ozaveščanje zaposlenih.

Varnostna politika podjetja je dokumentirana in objavljena na intranetu. Vodjem posameznih oddelkov mora biti poslano elektronsko sporočilo, v katerem je navedeno, kje lahko dobijo nov pravilnik, katerega morajo prebrati vsi zaposleni in podpisati izjavo, da so seznanjeni z novo varnostno politiko. Najbolj nevarna situacija je takšna, ko nadrejeni mislijo, da je varnostna politika na mestu samo zato, ker je zapisana v nekem dokumentu, potrebne so stalne kontrole.

Obstaja veliko načinov za preverjanje varnostne ozaveščenosti zaposlenih, vendar so vsi le deloma uspešni. Med njimi so vsekakor: video izobraževalni posnetki, novičarska pisma, brošure, priročniki, označbe, plakati, kemični svinčniki, podloge za miško, ohranjevalniki zaslona, majice, itd.. Težava večine naštetih načinov ozaveščanja je v tem, da jih je potrebno redno posodabljati, spreminjati, drugače je njihov učinek zelo majhen in kratkotrajen.

Program ozaveščanja zaposlenih lahko služi za informiranje zaposlenih o varnostni politiki podjetja, da se poveča dojemanje zaposlenih o morebitnih kritičnih situacijah in ključnih načinih socialnega inženiringa ter seveda kako le-te prepoznati in preprečiti. Vendar ni dovolj, da uporabnikom povemo, kako naj se obnašajo, dojeti in sprejemati morajo razloge za temi pravili. Ena od metod je personalizacija varnostnih zadev, s tem jim pokažemo, da karkoli počnejo, se tiče njih samih, kakor tudi podjetja v celoti, potrebno jim je pojasniti, kakšne so lahko izgube, če bodo ravnali napačno.

Čeprav je izobraževanje zaposlenih ključen dejavnik pri preprečevanju socialnega inženiringa, se včasih izkaže za zelo težko nalogo. Vsakdo je ranljiv za napade socialnega inženiringa, zaposlenim je potrebno pravilno sporočiti, kako ravnati. Ena izmed najbolj učinkovitih metod izobraževanja zaposlenih, je podajanje primerov iz resničnega sveta preko Intraneta oziroma podajanje novic in varnostnih napotkov preko elektronskih sporočil. Takšni primeri, zgodbice delujejo in jih je mogoče vključiti v izobraževalne seminarje za zaposlene, s tem povečamo odpor do takšnih napadov na uporabnikom prijazen in prijeten način.[http://www.securityfocus.com/infocus/1860/2]

Dober program varnostnega ozaveščanja zaposlenih mora biti večplasten. Kdor skrbi zanj, mora izrabiti vsako priložnost in orodje za njegovo zagotavljanje.
Zaposleni morajo biti ne samo informirani o varnostnih pravilih, ampak morajo tudi vedeti, kako ravnati in zakaj je potrebno tako ravnati. (Rakovec, 2005, 16)

Izobraževanje uporabnikov

Zagotoviti je treba, da se uporabniki zavedajo pomembnosti in groženj, ki ogrožajo varnost informacij, da so opremljeni tako, da lahko med delom podpirajo varnostno politiko podjetja.
Organizira se usposabljanje za osnovno varnostno ozaveščanje za vse zaposlene. Vsi udeleženci naj bodo seznanjeni z varnostno politiko, cilji in okviri, v katerih naj bi delali. Redno morajo biti seznanjeni tudi z njenimi spremembami in dopolnitvami. Zraven splošnega usposabljanja, naj se določijo kritične točke, označijo delovna mesta, ki so najbolj komunikacijsko obremenjena in predstavljajo varnostno nišo.
Zaposlenim na teh delovnih mestih oziroma kritičnih točkah naj se pripravi individualni način usposabljanja, v skladu z njegovim znanjem in delovnim mestom. (Rakovec, 2005, 34)

Kontrole proti zlonamerni kodi

Ob samem ozaveščanju in usposabljanju ljudi naj se sprotno vršijo kontrole oziroma preverjanje izvajanja organizacijskih navodil, smernic, pravilnikov. Zaposlene se o pojavu pomembnejših virusov in nadaljnjem ravnanju obvešča po elektronski pošti. Postopek obveščanja naj bo v naprej dogovorjenih predlogah. Preprečiti je potrebno nasedanje potegavščinam, kjer uporabniki brišejo pomembne ali nameščajo nepotrebne dele sistema, upoštevati se morajo izključno le navodila administratorja sistema. Postopki za odpravo posledic zlonamerne kode naj se vključijo v načrt za neprekinjeno poslovanje.
(Rakovec, 2005, 77)

Ravnanje z informacijami

Uvedejo naj se postopki glede ravnanja z informacijami. Informacije naj se razvrstijo v smiselne skupine. Če je mogoče, naj posamezne tipe določijo kontrole, ki skupaj z ustreznim vodenjem in zapisi skrbijo za varno ravnanje z vsemi oblikami informacij. Vedno naj bo določeno, kdo je v danem trenutku za neko informacijo odgovoren. (Rakovec, 2005, 78)

7.3 Smernice in pravilniki

Preprečevanje zlorab

Organizacije različno nadzirajo zlonamerno uporabo informacijskih sredstev. Področje elektronske pošte in interneta mora biti dobro nadzorovano. Tedensko naj se avtomatsko izdelujejo pregledi uporabe elektronske pošte. Prav tako mora biti uvedena politika preprečevanja pošiljanja in prejemanja datotek avdio in video formata in izvršilnih datotek. Nadzira naj se tudi internetni promet. Ti pregledi se pošiljajo vodjem, ki na posamezne kršitve primerno reagirajo. O pravilih dela z elektronsko pošto in internetom ter o nadzoru se uporabnike obvesti preko organizacijskega predpisa (pravilnika ali smernic) za posamezno področje.

Organizacija naj izdela pravila uporabe informacijskih sredstev za vsa področja. Sestavi naj izjavo o varovanju informacij. S podpisom izjave se uporabniki zavežejo zgolj k uporabi v službene namene. Zlorabe naj se temu primerno obravnavajo z disciplinskimi ukrepi.

(Rakovec, 2005, 78)

Varovanje elektronskih sistemov

Organizacije v večini primerov nimajo politike varovanja elektronskih poslovnih sistemov, niti za to področje nimajo izdelane analize tveganj. Večina režijskih delavcev ima dostop do elektronskih poslovnih sistemov, a se tveganj, katerim s svojim delom izpostavljajo informacije, v večini ne zavedajo.

Organizacije naj pripravijo politiko varovanja elektronskih poslovnih sistemov, ki naj poleg pravil obnašanja vsebuje tudi smernice za nadzor poslovnih in varnostnih tveganj. Preveri naj se način hrambe informacij. Opredeli se tudi način, pogostost in dolžina hrambe informacij, ki se ustvarjajo, prenašajo in spreminjajo v toku poslovnih sistemov. Posebna pozornost pa naj se posveti sistemom, ki so dostopni preko javnih omrežij, kot je internet oziroma splet.

(Rakovec, 2005, 79)

V prilogi primeri smernic.

8 RAZISKOVALNO DELO - ANKETA

8.1 Priprava in analiza ankete

Raziskovalni del diplomske naloge obsega anketni vprašalnik.

Vprašalnik segmentno pokriva vsebino informacijske varnosti, ključne dejavnike in točke, opravil je bil anonimno in je služil izključno samo izdelavi diplomskega dela.

Pridobljeni podatki in analize zbirnih poročil so potrdile veljavnost trditve in pokazale raven stanja med slovenskimi podjetji.

Za lažjo in praktično izvedbo ankete sem uporabil orodje, ki je prosto dostopno na spletnem naslovu http://www.surveygizmo.com/ in že v osnovni različici omogoča izvedbo vseh potrebnih aktivnosti. Z dnem 14.11.2008 sem preko svoje uporabniške konzole objavil vse tri pristopne spletne naslove.

Zaradi lažjega in pravilnega pridobivanja informacij sem vprašalnik razdelil na 3 segmente. Vprašalniki obsegajo 49 vprašanj.

1 Segment - Komunikacijska točka (poslovni sekretariat, recepcija, sprejemnica, finance, logistika itd.) Število vprašanj 15.

[http://www.surveygizmo.com/s/67393/anketa-komunikacij-podjetja-nizja-raven-2008]

2 Segment - Informatika (vodja IT, varnostni inženir, IT strokovnjak, IT podpora, IT outsourcing, informatik itd.) Število vprašanj 16.

[http://www.surveygizmo.com/s/82546/anketa-informatika-vi-ja-raven-2008]

3 Segment - Uprava, Vodstvo (predsednik uprave, član uprave, direktor podjetja, lastnik itd.) Število vprašanj 18.

[http://www.surveygizmo.com/s/82547/anketa-uprava-podjetja-srednja-raven-2008]

Vprašanja so bila skrbno in načrtno izbrana po posameznih področjih, dodatna vprašanja pa so predstavljala mozaik k dopolnitvi slike na to temo.

Še preden sem objavil spletne naslove, sem si pripravili načrt vseh aktivnosti.

Za razliko od ostalih anket, ki se ponavadi kar same odvijajo v spletnih krogih, sem se najprej dogovoril s ciljnimi podjetji. V okviru poslovne komunikacije in predhodnega dogovora s predstavniki podjetja, s privolitvijo k dejanju ankete, sem pripravili seznam podjetij in ljudi, ki bodo pomagali pri izvedbi. Vsako podjetje, predstavnike vodstva in izbrane ljudi, sem osebno kontaktiral, jim razložil cilj in bistvo ter način izvedbe anketnega vprašalnika. S tem sem hkrati zmanjšal možnost napak, pripomogel k pravilnejši izvedbi in pritegnil v vsakem podjetju ključne ljudi za izvedbo dejanja.

V roku 14 dni sem uspel pridobiti več kot 123 odgovorjenih vprašalnikov, nekaj tudi nepopolno in prekinjeno zajetih vprašalnikov. Prekinjene ali prazne vprašalnike nisem upošteval pri analizi. V nepopolnih sem upošteval vsa odgovorjena vprašanja. Za vsako vprašanje bom pokazal statistiko in z njeno pomočjo opravil analizo ozaveščenost o varni poslovni komunikaciji, socialnem inženiringu, informacijski varnosti in njeni ravni med slovenskimi podjetji.

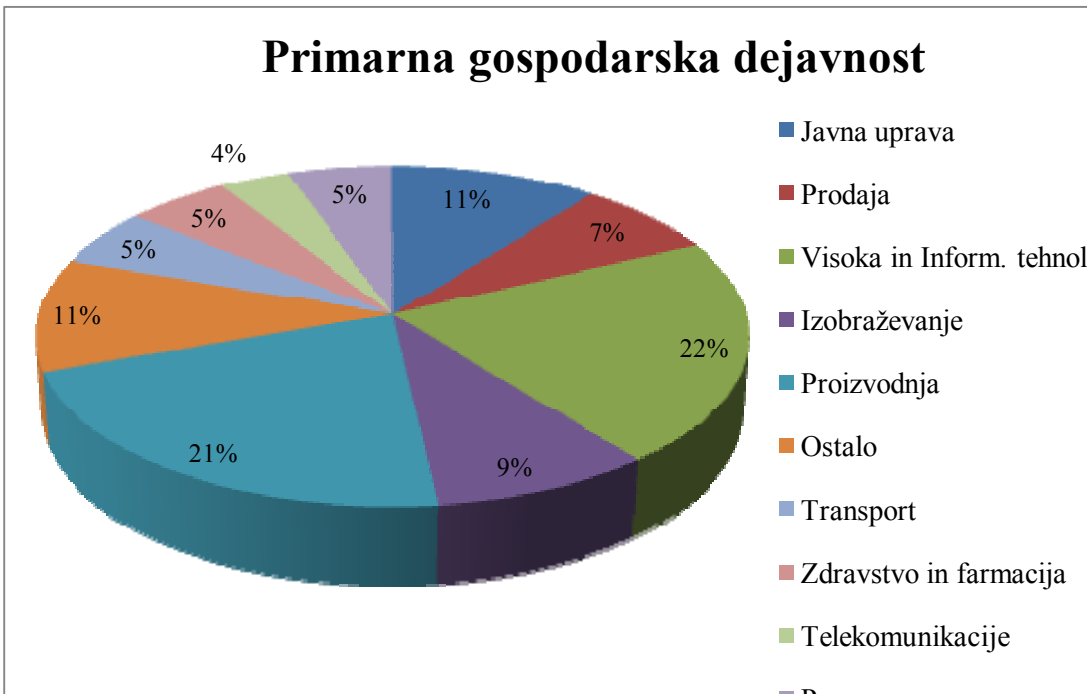
Gospodarska dejavnost

Primarna gospodarska dejavnost anketirancev je obsegala naslednja področja:

Tabela 1: Primarna gospodarska dejavnost

PRIMARNA GOSPODARSKA DEJAVNOST	št	%
Javna uprava	6	11%
Prodaja	4	7%
Visoka tehnologija in informacijska tehnologija	12	22%
Izobraževanje	5	9%
Proizvodnja	11	21%
Ostalo	6	11%
Transport	3	5%
Zdravstvo in farmacija	3	5%
Telekomunikacije	2	4%
Pravo	3	5%

Vir: lastna raziskava



Grafikon 1: Primarna gospodarska dejavnost Vir: lastna raziskava

Spol

Razmerje anketirancev glede na spol je po posameznih segmentih kazalo takole:

Komunikacijska točka je obsegala sledeče razmerje glede na spol;

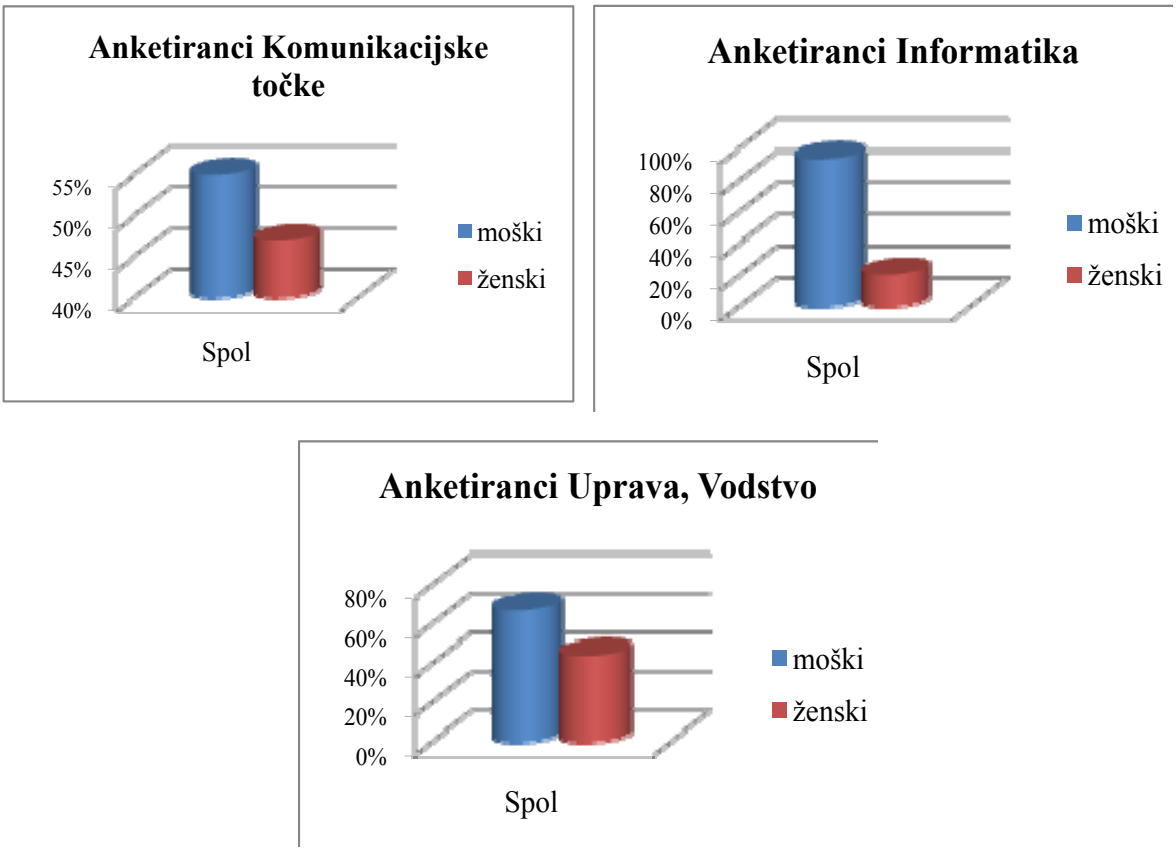
moški del anketirancev 46% in ženski del 54%.

Informatika ciljna skupina, je ponazorila sledeče razmerje v prid moških;

moški del anketirancev 87% in ženski del 13%. To še vedno priča, da je informatika v domeni moških.

Uprava, Vodstvo v razmerju;

moški del anketirancev 61% in ženski del 39%.



Grafikon 2: Razmerje anketiranih glede na spol Vir: lastna raziskava

Starost

Anketiranci so se razvrščali po kriterijih: 18-30 let, 30-40 let, 40-50 let ali več.

Komunikacijska točka je prevladovala v starostni skupini 30-40 let z 38%, sledila je 40-50 let s 33%, 18-30 z 18% in najmanj v skupini več kot 50 let, 11%.

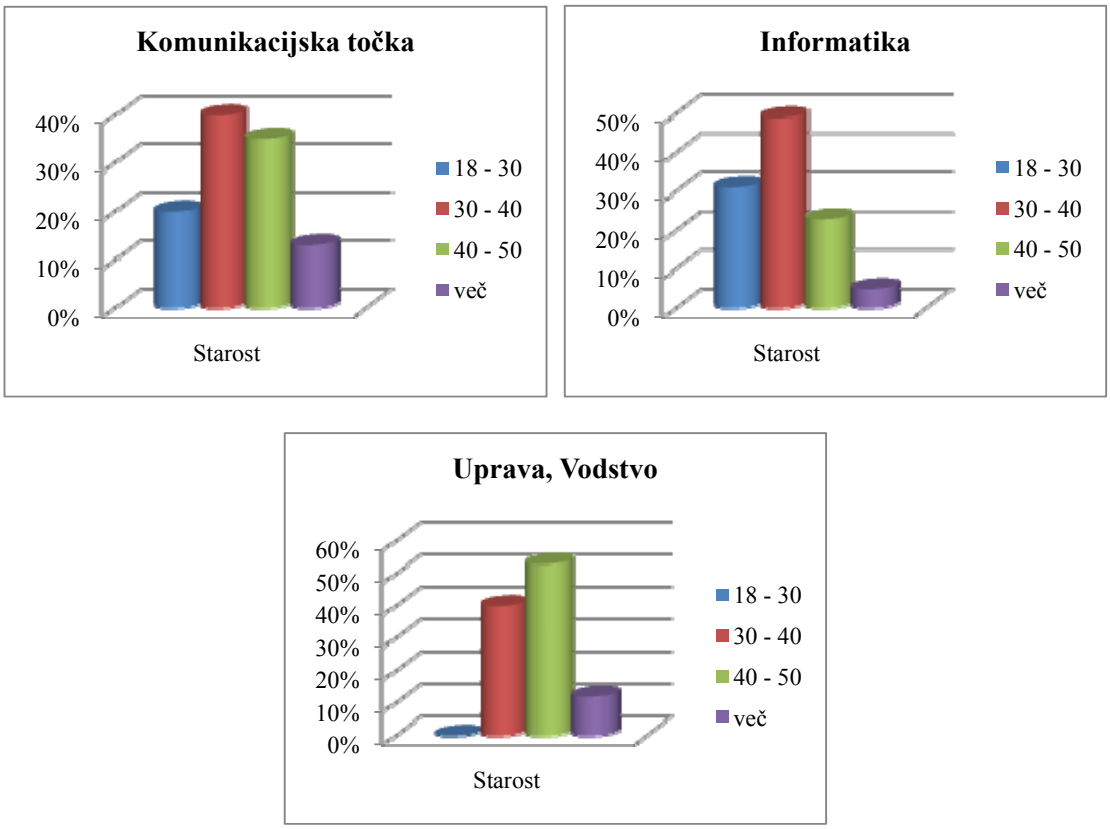
Informatika je prevladovala v starostni skupini 30-40 let s 47%, sledila je 18-30 let z 29%, 40-50 z 21% in najmanj v skupini več kot 50 let, 3%.

Uprava, Vodstvo je prevladovala v starostni skupini 40-50 let s 50%, sledila je 30-40 let z 39% in nato skupina več kot 50 let, 11%. V skupini 18-30 let ni bilo oddanega vprašalnika.

Tabela 2: Starostna skupina

STAROST	Komunikacijska točka		Informatika		Uprava, Vodstvo	
	št.	%	št.	%	št.	%
18 - 30	7	18%	11	29%	0	0%
30 - 40	15	38%	18	47%	5	38%
40 - 50	13	33%	8	21%	7	54%
več	4	11%	1	3%	1	8%

Vir: lastna raziskava



Grafikon 3: Razmerje anketiranih glede na starost Vir: lastna raziskava

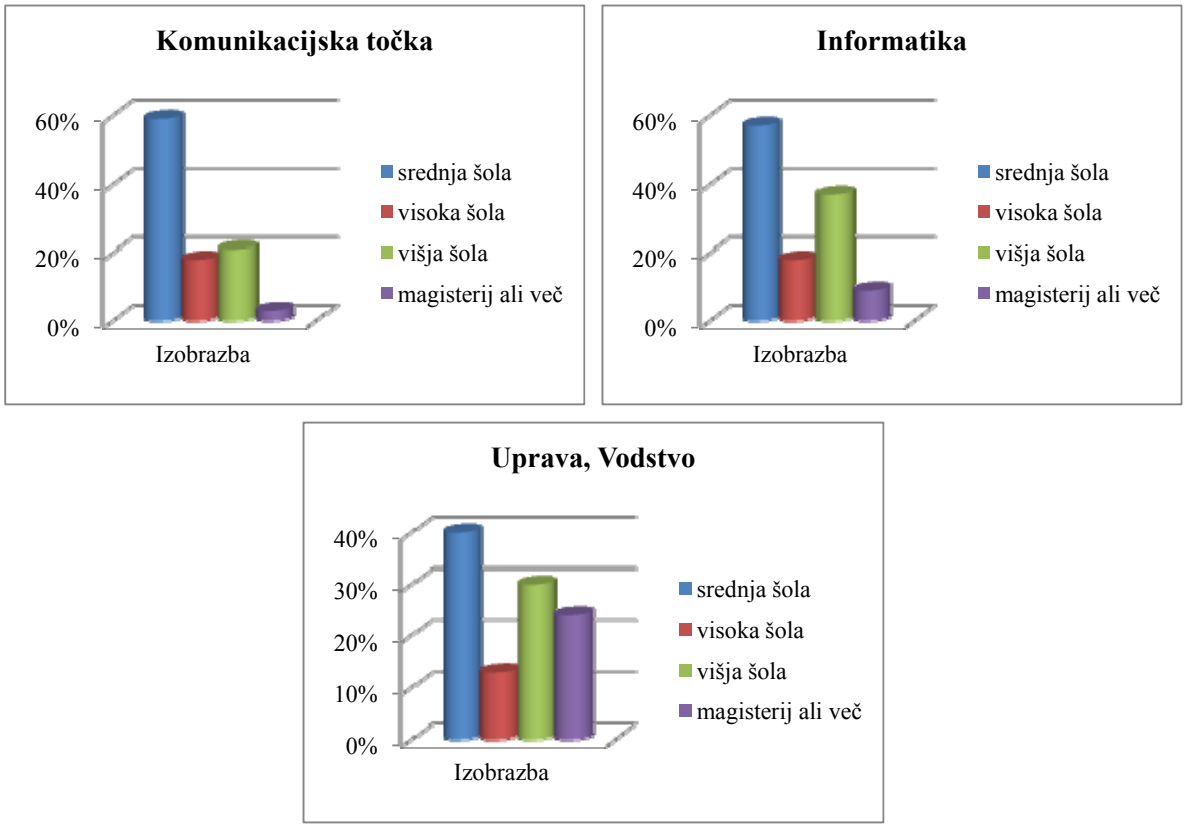
Izobrazbena struktura

Anketiranci so se razvrščali po kriterijih: srednja šola, višja šola, visoka šola, magisterij ali več. Po rezultatih sodeč, je bila v vseh treh segmentih izobrazbena udeležba predvsem srednješolska, vendar je tudi ostalo razmerje zelo dobro.

Tabela 3: Izobrazbena struktura

IZOBRAZBA	Komunikacijska točka		Informatika		Uprava, Vodstvo	
	št.	%	št.	%	št.	%
srednja šola	23	59%	19	50%	7	39%
višja šola	7	18%	5	13%	2	11%
visoka šola	8	21%	12	32%	5	28%
magisterij ali več	1	3%	2	5%	4	22%

Vir: lastna raziskava



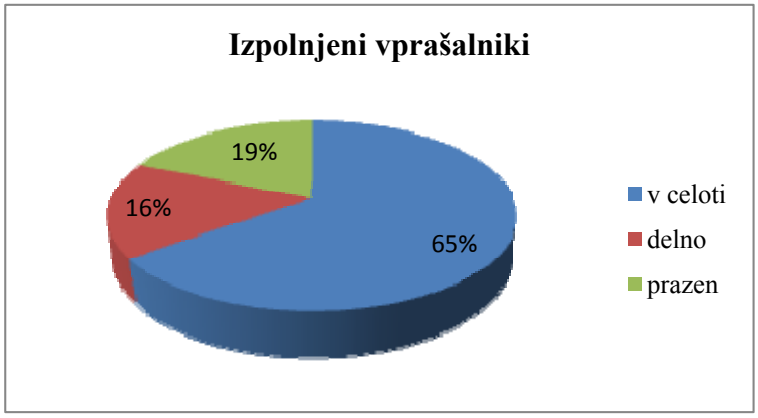
Grafikon 4: Razmerje anketiranih glede na izobrazbo Vir: lastna raziskava

Udeležba

Tabela 4: Izpolnjeni vprašalniki

VPRAŠALNIKI	št.	%
v celoti	80	65%
delno	20	16%
prazen	23	19%

Vir: lastna raziskava



Grafikon 5: Razmerje izpolnjenih vprašalnikov Vir: lastna raziskava

Komunikacijska točka

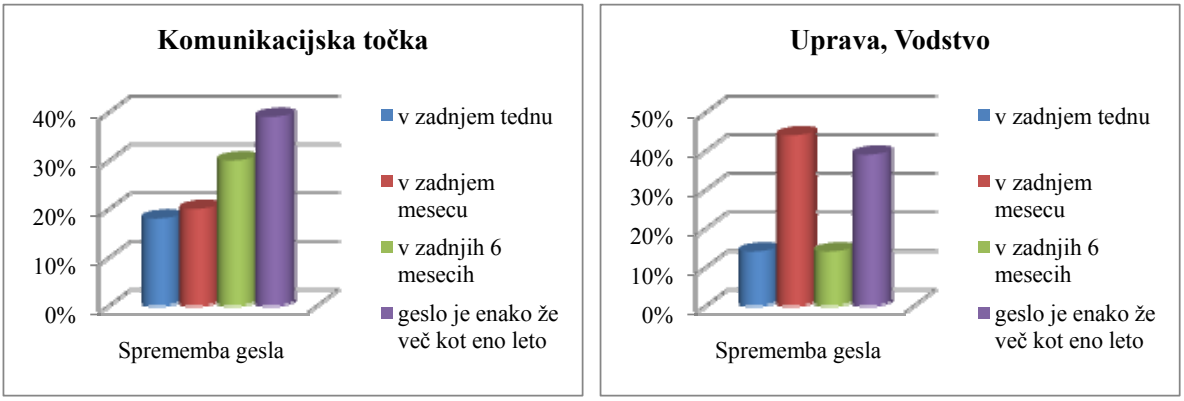
Vprašanje:

Kdaj ste nazadnje spremenili geslo?

Tabela 5: Sprememba gesla

SPREMEMBA GESLA	Komunikacijska točka		Uprava, Vodstvo	
	št	%	št	%
v zadnjem tednu	6	16%	2	12%
v zadnjem mesecu	7	18%	7	41%
v zadnjih 6 mesecih	11	29%	2	12%
geslo je enako že več kot eno leto	14	37%	6	35%

Vir: lastna raziskava



Grafikon 6: Sprememba gesla v določenem času Vir: lastna raziskava

Kot sem pričakoval in napovedal , je na **komunikacijski točki**, tako imenovani kritični točki , prav tako v **upravi, vodstvu** velika varnostna vrzel, kjer po rezultatih sodeč prednjači: **geslo je enako že več kot leto dni** oziroma **v zadnjih 6 mesecih**. Pomeni, da se lahko socialni inženir ali vsakdo, ki je vešč ali ima določen cilj pridobitve gesla, okoristi z njim in povzroči zelo veliko škodo v podjetju. Predlog: menjava gesla naj poteka vsak teden, uporabnika pa se seznani z odgovornostjo in varnostno ozaveščenostjo.

Ugotovljeno stanje ni zadovoljujoče v smislu informacijske varnosti.

Komunikacijska točka, Informatika, Uprava, Vodstvo

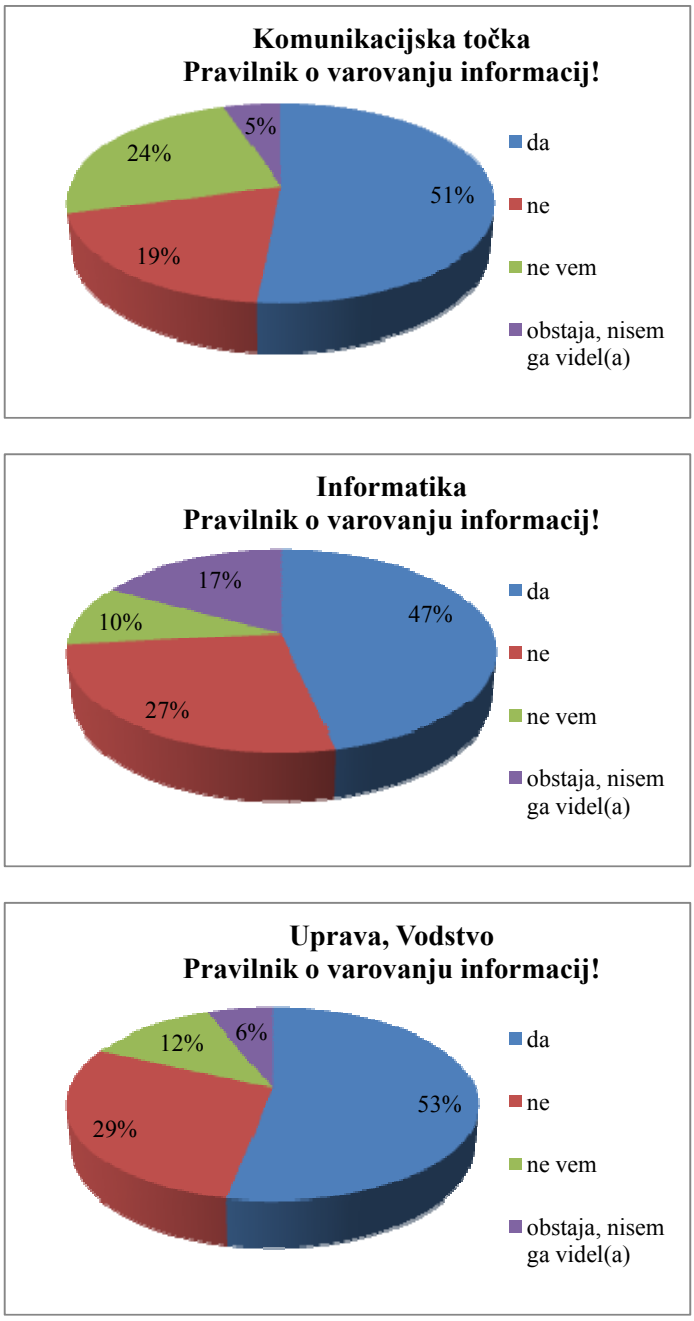
Vprašanje:

Ali imate napisan pravilnik o varovanju informacij in ste z njim seznanjeni?

Tabela 6: Pravilnik

PRAVILNIK	Komunikacijska točka		Informatika		Uprava, Vodstvo	
	št.	%	št.	%	št.	%
da	19	51%	14	47%	7	53%
ne	7	19%	8	27%	2	29%
ne vem	9	24%	5	17%	5	12%
obstaja, nisem ga videl(a)	2	5%	3	10%	4	6%

Vir: lastna raziskava



Grafikon 7: Napisan pravilnik in seznanitev z njim Vir: lastna raziskava

Dobljeni rezultati so zelo zanimivi, saj prav kažejo na vprašanje, kaj si predstavljajo anketiranci pod »**Pravilnik o varovanju informacij**«. Dejstvo, da jih vseeno več kot **49%** na **komunikacijski točki**, preko **informatike 53%**, pa vse do **61%** v **upravi**, **vodstvu**, ne more zagotoviti, da ga ima in da so seznanjeni z njim. Predlog: apel na upravo, vodstvo in posredno na informatiko, da je nujno potrebno pripraviti pravilnik o varovanju informacij in z njim seznaniti obvezno vse zaposlene.

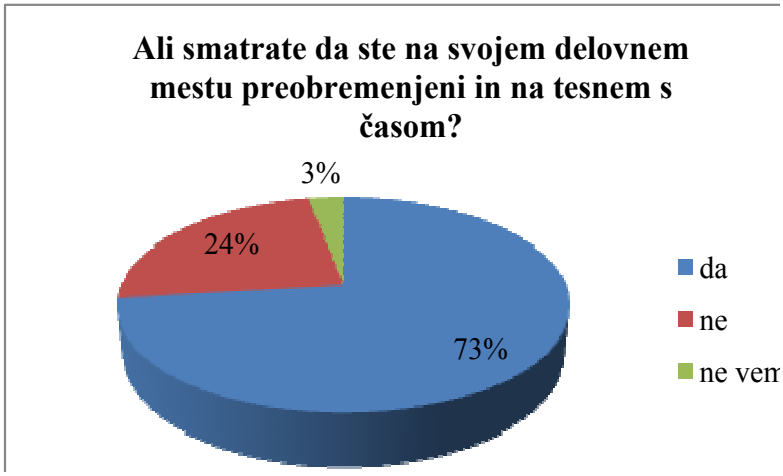
Komunikacijska točka

Vprašanje: **Ali smatrate, da ste na svojem delovnem mestu preobremenjeni in na tesnem s časom?**

Tabela 7: Preobremenjenost na delovnem mestu

PREOBREMENJENOST	št	%
da	27	73%
ne	9	24%
ne vem	1	3%

Vir: lastna raziskava



Grafikon 8: Preobremenjeni na delovnem mestu Vir: lastna raziskava

Dobljeni rezultati na komunikacijski točki lepo ponazorijo, da so zaposleni preobremenjeni in na tesnem s časom, kar pa pomeni priložnost socialnega inženirja, da preko pravih prijemov izkoristi časovno stisko zaposlenega in pridobi informacije, ki jih v urejenem poslovnem okolju ne bi mogel. Predlog: preučiti delovno okolje zaposlenih in njihove poslovne procese. Le-te je mogoče s pomočjo primerne poslovne organizacije optimizirati.

Komunikacijska točka

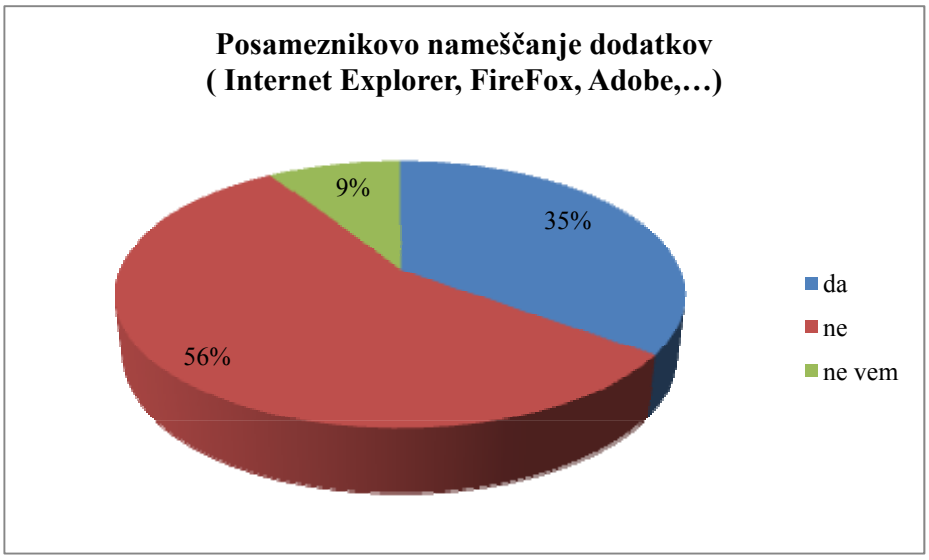
Vprašanje:

Ali sami nameščate potrebne dodatke v Brskalnik (Internet Explorer, FireFox, ..), če ste k temu pozvani?

Tabela 8: Nameščanje dodatkov

NAMEŠČANJE	št	%
da	12	35%
ne	19	56%
ne vem	3	9%

Vir: lastna raziskava



Grafikon 9: Posameznikovo nameščanje dodatkov Vir: lastna raziskava

V večini primerov zaposleni sami dodatkov ne nameščajo, odgovarja 56%, vseeno pa ostaja odprto vprašanje pri številu, malenkost manjšem od polovice, ki **pa namešča dodatke** ali pa celo **ne ve**, če jih prištejemo zraven. Predlog: s pomočjo pravilnika o varovanju informacij in opredelitve varnostnih mehanizmov za zaščito informacijskega sistema, se onemogoči uporabnikov poseg v delovanje operacijskega sistema,v nameščanje orodij itd.

Vsak nepooblaščeno nameščen dodatek ali sprememba lahko povzroči nalaganje zlonamernega programja ali izvedbo skript, ki vodijo k okuženju sistema in k nepravilnemu delovanju, nazadnje tudi k odpovedi sistema.

Komunikacijska točka !

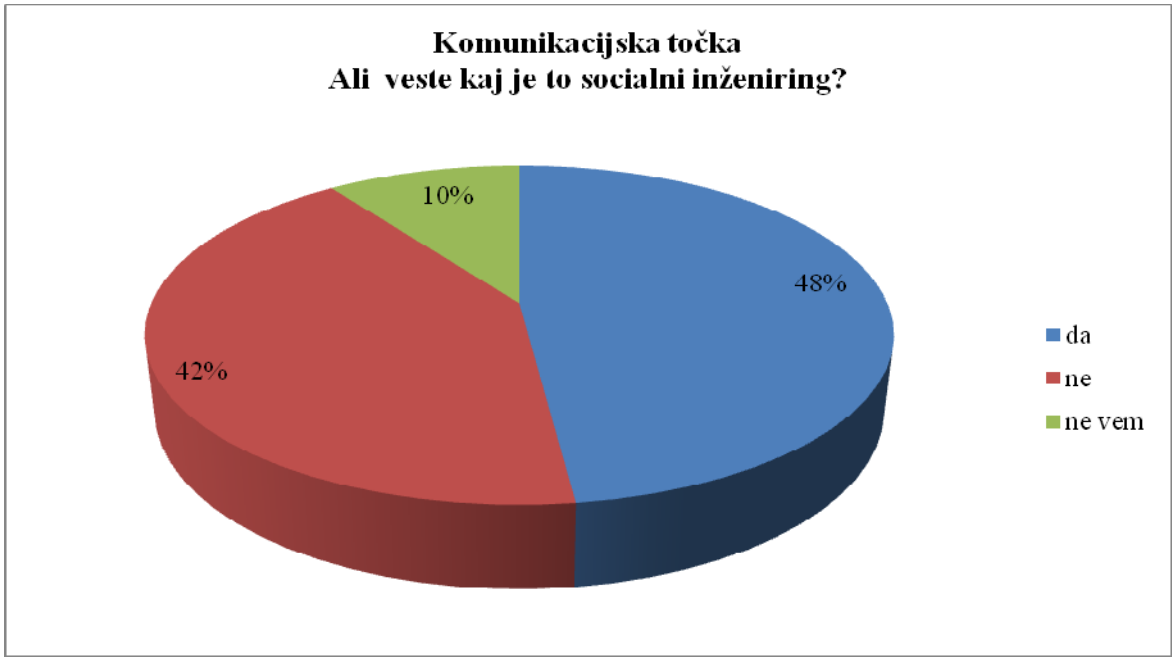
Vprašanje

Ali veste kaj je to socialni inženiring in kaj je manipulacija ljudi z namenom pridobitve informacij?

Tabela 9: Socialni inženiring

POZNAVANJE	št	%
da	16	48%
ne	14	42%
ne vem	3	10%

Vir: lastna raziskava



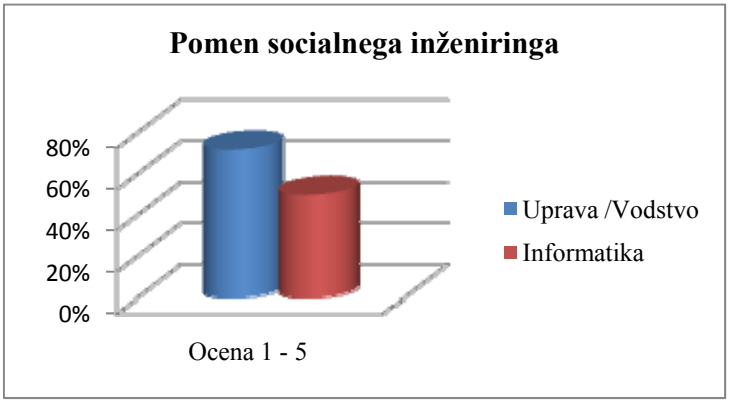
Grafikon 10: Prepoznavanje socialnega inženiringa Vir: lastna raziskava

Osveščenost o nevarnosti socialnega inženiringa je v največjem odstotku prisotna pri **Upravi, Vodstvu,** kjer je **64 %** vprašanih ocenilo velik pomen; manjša pri **Informatiki,** le **37%** jih je tako ocenilo. Še slabšo sliko kažejo rezultati **komunikacijske točke**, kjer je kljub temu, da smo v vprašanje dodali **Kaj je manipulacija ljudi z namenom pridobitve informacij?** odgovorila slaba polovica, da to pozna, vendar odgovarja druga polovica, da tega ne ve, torej imamo polovico nevednih in neosveščenih. Predlog: potrebno je organizirati izobraževanje, ga podkrepiti s primeri, vse zaposlene opozoriti na šibke točke in možnosti napadov, izobraževanja kontinuirano osveževati in predpisati kot stalnico.Vse to pogosteje pri zaposlenih na kritičnih točkah.

Tabela 10: Pomen socialnega inženiringa

POMEN SOC.INŽENIRINGA	Informatika	Uprava, Vodstvo
Povprečna ocena	43%	64%

Vir: lastna raziskava



Grafikon 11: Razmerje socialnega inženiringa Vir: lastna raziskava

Komunikacijska točka

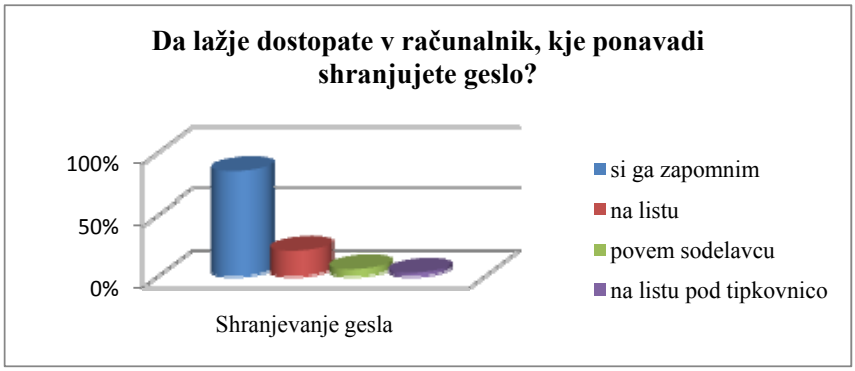
Vprašanje

Da lažje dostopate v računalnik, kje ponavadi shranjujete geslo?

Tabela 11: Shranjevanje gesla

SHRANJEVANJE GESLA	št.	%
si ga zapomnim	29	85%
na listu	7	21%
povem sodelavcu	2	6%
na listu pod tipkovnico	1	3%

Vir: lastna raziskava



Grafikon 12: Shranjevanje gesla Vir: lastna raziskava

Rezultat je deležen pohvale, od 34 odgovorov na vprašanje v komunikacijski točki, daje zadovoljiv odgovor 85% - **si ga zapomnim.** Le 2 oziroma 1 odgovor ne ravnata v skladu informacijske varnosti in predstavljata varnostno vrzel.

Informacijska točka

Vprašanje

Katerega od spodaj naštetih prosite, da se identificira in ga evidentirate?

Hkratni odgovori, število odgovorov 33 .

Tabela 12: Identificiranje

IDENTIFIKACIJA	št.	%
ne preverjam	13	39%
novi zaposlen	11	33%
serviser/ vzdrževalec	11	33%
stranka	10	30%
poslovni partner	9	29%
sorodnik zaposlenega	4	12%

Vir: lastna raziskava

Grafikon 13: Identifikacija in evidentiranje Vir: lastna raziskava

Na komunikacijski točki na žalost v veliki meri **ne preverja** identifikacije ljudi , ki prihajajo v podjetje ali v bistvu predstavljajo poslovno sodelovanje, **39%**. Pa tudi če jo preverjajo, ni varnostnega mehanizma, ki bi istovetil osebo, ki se je identificirala z dokumentom, s tem, kdo v resnici je. Nevarnost se predstavlja ne samo z vidika informacijske varnosti, ampak tudi z vidika fizičnega varovanja lastnine in ljudi. Predlog: preveriti identiteto, opraviti evidentiranje, obvezno preveriti povezanost z zaposlenim, če za obisk obstaja domenek z obeh strani ali celo poklicati v matično podjetje obiskovalca.

Informacijska točka

Vprašanje

Zaradi ugotavljanja kompleksnosti (če je dovolj varno) vašega gesla, mi prosim napišite svoje geslo.

Vprašanje je bilo namenoma postavljeno na konec in označeno kot obvezno. Prav tako se ni uporabil prikriti način, kar bi že lahko predstavljal dodaten sum anketirancu. Uporabljeno tehniko lahko štejemo med direktne metode socialnega inženiringa. Anketiranec je moral pod pritiskom časa, samo da se reši obveznosti in pod pretvezo, da je dovolj varno, vpisati svoje geslo. Ni bilo zahtevano specifično geslo.

V vprašalniku komunikacijske točke je bilo na vprašanje podanih 33 odgovorov.

Vsega 7 jih je odgovorilo na način **ne , ne dam, ne zaupam, ne bom povedal, morda še številko čevljev**, 9 jih je prestavljalo namige za uporabniška gesla, iz ostalih se ni dalo razbrati podobnosti geslu, verjetnost pa še vedno obstaja. Iz stališča varnosti so rezultati na meji zadovoljivega, vendar niso preverljivi.

Uporabniki se morajo zavedati, da je geslo osebno (službeno), zato je prepovedano zaupanje ali deljenje njihovega gesla s tretjo osebo.Vsako kršenje te politike lahko povzroči hude posledice informacijske varnosti v podjetju in uporabniku samemu (kraja identitete).

Informatika

Vprašanje

Katere zunanje smernice ali strokovno znanje je uporabilo lani vaše podjetje?

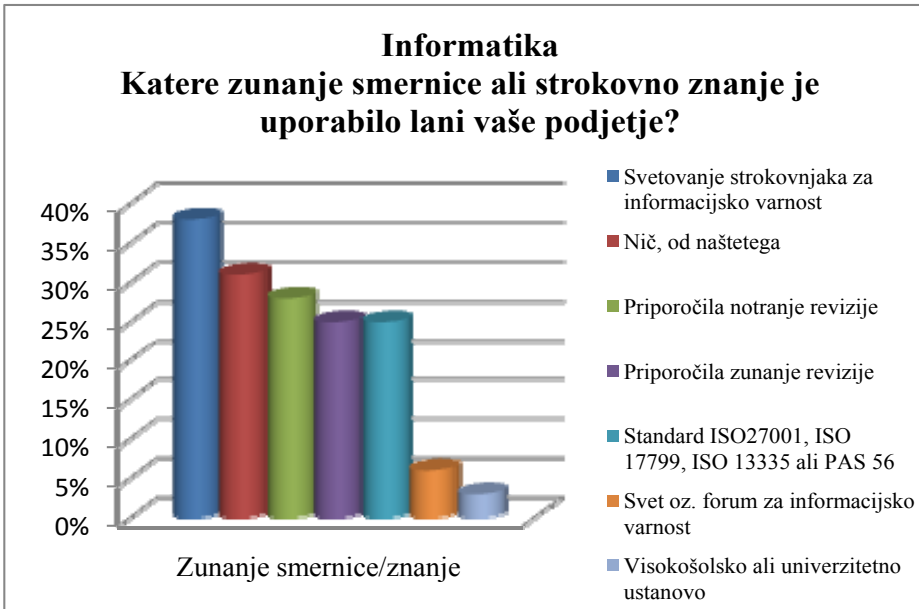
Vprašanje je zadevalo vprašalnik informatikov, ki so ocenjevali, na koga se poleg lastnega znanja v organizaciji ob izvedbi in delovanju poslovnega sistema še opirajo. Od skupno 32 hkratnih odgovorjenih izbir, se informatiki odločajo v največjem številu, kar predstavlja **38%**, za **svetovanje strokovnjaka za informacijsko varnost** in za **notranje in zunanje revizije** (predvsem javne ustanove, prosveto, koncernska podjetja itd.). Ker pa je pomoč odvisna tudi od finančnih sredstev in od posluha uprave, vodstva, se je pokazalo, da se jih vsaj **31%** ne odloči za **nič naštetega**. Lahko sklepamo, da se ti lahko potem oprejo ali samo na lastno znanje ali pa v resnici na nič, kar pa je zaskrbljujoče.

Vsekakor je potrebno skozi neko obdobje pritegniti strokovna mnenja tretjih oseb, si postaviti varnostno politiko ter tudi cilj izobraževanja in svetovanja.

Tabela 13: Zunanje smernice/ znanja

ZUNANJE SMERNICE/ZNANJE	Informatika	
	št.	%
Svetovanje strokovnjaka za informacijsko varnost	12	38%
Nič od naštetega	10	31%
Priporočila notranje revizije	9	28%
Priporočila zunanje revizije	8	25%
Standard ISO27001, ISO 17799, ISO 13335 ali PAS 56	8	25%
Svet oz. forum za informacijsko varnost	2	6%
Visokošolsko ali univerzitetno ustanovo	1	3%

Vir: lastna raziskava



Grafikon 14: Zunanje smernice/znanje Vir: lastna raziskava

Informatika

Vprašanje

Kakšne metode uporabljate za avtentikacijo uporabnika?

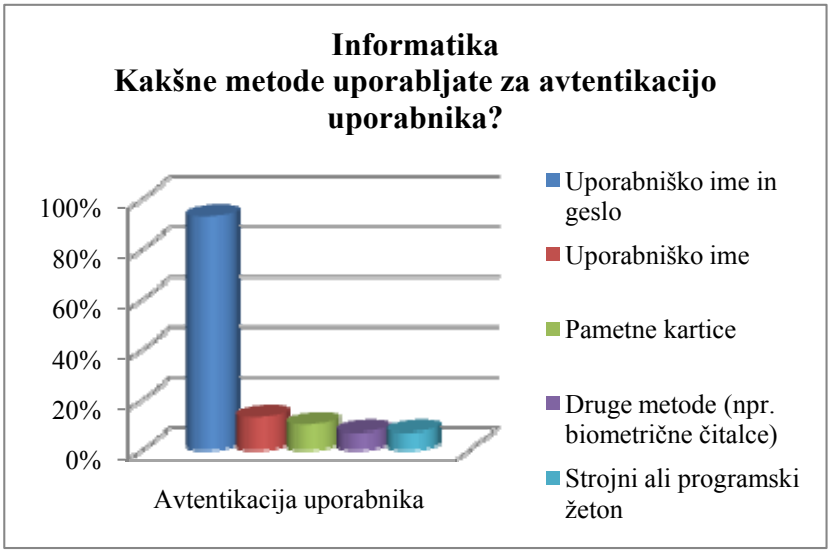
Vprašanje je zadevalo informatiko in je glede na zbrane podatke postavilo zadovoljiv rezultat. Avtentikacija se preverja, nasproten odgovor ni bil podan , vendar spet izstopa en odgovor. Najslabše v tej lestvici je postavljen odgovor **Uporabniško ime**, s 13%. Pomeni, da 4 anketiranci za prijavo uporabljajo samo uporabniško ime brez gesla in predstavljajo grožnjo sistemu varnosti v organizaciji.

Najmanj, kar lahko pričakujemo pri avtentikaciji, je Uporabniško ime in geslo, seveda ob predpostavki, da nista enaka in da ne predstavljata imena uporabnika in delovnega mesta.

Tabela 14: Avtentikacija uporabnika

AVTENTIKACIJA UPORABNIKA	Informatika	
	št.	%
Uporabniško ime in geslo	28	93%
Uporabniško ime	4	13%
Pametne kartice	3	10%
Druge metode (npr. biometrične čitalce)	2	7%
Strojni ali programski žeton	2	7%

Vir: lastna raziskava



Grafikon 15: Zunanje smernice/znanje Vir: lastna raziskava

Informatika

Vprašanji

Kakšne varnostne kontrole izvaja vaša organizacija pri pošiljanju/sprejemu elektronske pošte?

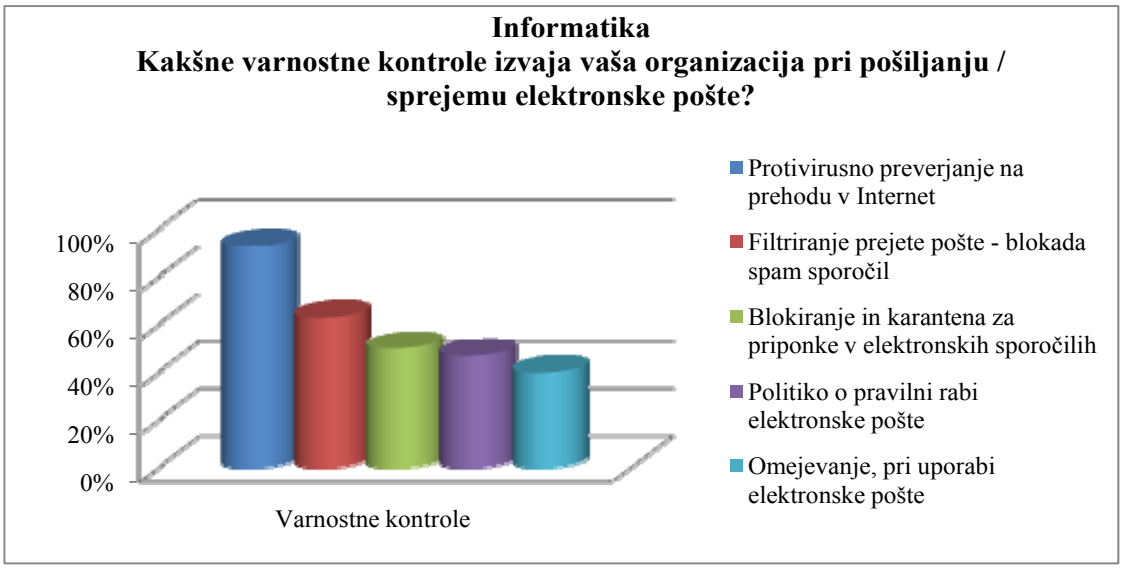
Kakšne varnostne kontrole izvaja vaša organizacija pri dostopu do svetovnega spleta?

Vprašanji sta bili 30 -krat izpolnjeni in ustrezno potrjeni po naštetih varnostnih mehanizmih. Sodeč po rezultatih, informatiki dobro čuvajo področje pošte in dostopa do spleta. Pridobljeni podatki so za oba področja precej podobni. Zavedati se moramo, da je v varnostnem sistemu še vedno največja grožnja prav človek sam in bi se morala tudi na tem področju dvigniti raven.

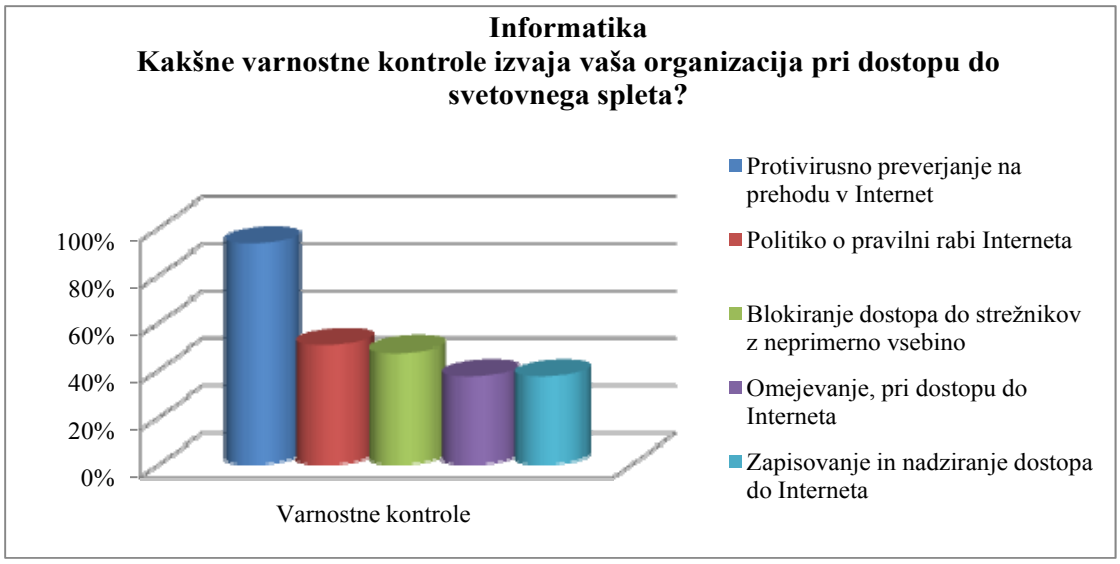
Tabela 15: Varnostni mehanizmi

VARNOSTNI MEHANIZMI	Informatika	
SPLETNA POŠTA	št.	%
Protivirusno preverjanje na prehodu v Internet	28	93%
Filtriranje prejete pošte - blokada spam sporočil	19	63%
Blokiranje in karantena za priponke v elektronskih sporočilih	15	50%
Politiko o pravilni rabi elektronske pošte	14	47%
Omejevanje pri uporabi elektronske pošte	12	40%
INTERNET		
Protivirusno preverjanje na prehodu v Internet	28	93%
Politiko o pravilni rabi Interneta	15	50%
Blokiranje dostopa do strežnikov z neprimerno vsebino	14	47%
Omejevanje pri dostopu do Interneta	11	37%
Zapisovanje in nadziranje dostopa do Interneta	11	37%

Vir: lastna raziskava



Grafikon 16: Varnostni mehanizmi pošte Vir: lastna raziskava



Grafikon 17: Varnostni mehanizmi internetne povezave Vir: lastna raziskava

Informatika

Vprašanje

Kolikšen odstotek proračuna za informatiko je bil namenjen za varovanje informacij, če sploh?

Situacija je v izbranih slovenskih podjetjih naslednja: **31%** odgovarja, da se za varovanje informacij iz proračuna nameni le **1% ali manj**, prav tako **31% ne ve** koliko.

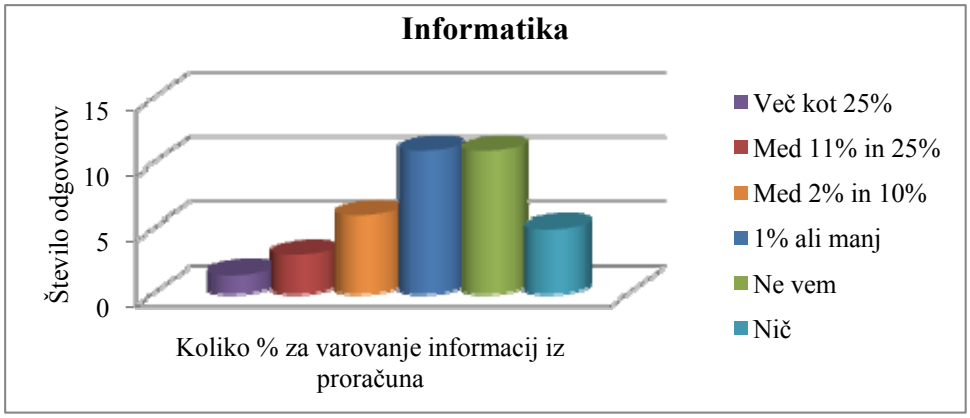
16% anketirancev odgovarja, da **med 2% in 10%** ter **6%** anketirancev, da **med 11% in 25% .** Izjema je le eden z **več kot 25%**. Zaskrbljujoč je podatek **Nič,** odgovorjen štirikrat, kar pomeni, da podjetja pač ne vlagajo v informacijsko varnost in se ne zavedajo nevarnosti, torej ne vlagajo namerno v informacijsko varnost. Na nek način so zaščiteni samo od privzetih možnosti, ki jih poslovni sistemi ponujajo ali od iznajdljivosti informacijske podpore.

Predlog: podjetja se bodo morala sprijazniti z dejstvom, da je informacijska varnost še kako pomembna v poslovanju in določiti delež, ki bo namenjen pripadajočim aktivnostim.

Tabela 16: Informacijska varnost

INFORMACIJSKA VARNOST V PRORAČUNU (%)	Informatika	
	št.	%
1% ali manj	10	31%
Ne vem	10	31%
Med 2% in 10%	5	16%
Nič	4	13%
Med 11% in 25%	2	6%
Več kot 25%	1	3%

Vir: lastna raziskava

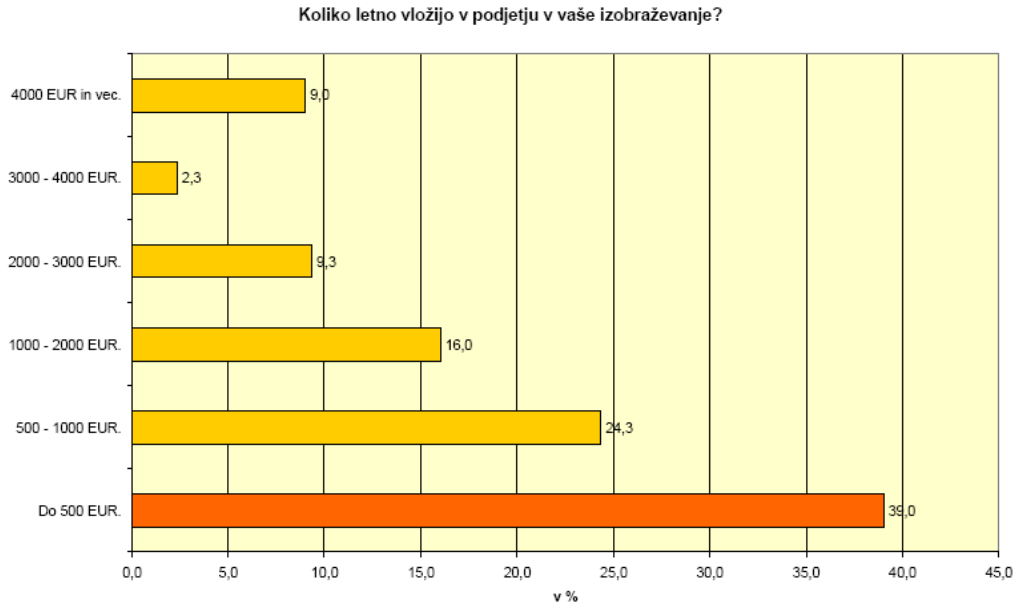


Grafikon 18: Informacijska varnost (%) iz proračuna Vir: lastna raziskava

Izobraževanje

Kot poslednjo temo v analizi štejem izobraževanje, ki v anketnem vprašalniku ni bilo zajeto. Razlog tiči v tem, daj bil v času zasnove vprašanj za diplomsko nalogo v pripravi kompleten vprašalnik v okviru slovenske izobraževalne ustanove. Del je zajemal tudi področje izobraževanja. K anonimni raziskavi je bilo sredi oktobra 2008 povabljenih blizu 6000 zaposlenih. Ugotovitve raziskave so bile objavljene z dne 13.11.2008 v vseh pomembnih strokovnih revijah, kot tudi na spletni strani.
[http://www.housing.si/docs/Novice/Raziskava_Housing_2008.pdf]
Zanimiv je podatek, koliko denarja so pripravljena podjetja vložiti v svoj zaposlitveni kader, še posebej, če ta podatek vključuje tudi informatiko, kjer je stalno izobraževanje neizbežno in potrebno.

Slika 7: Koliko letno vložijo v podjetju v vaše izobraževanje?



Vir: [http://www.housing.si/docs/Novice/Raziskava_Housing_2008.pdf]

Misel, ki se poraja ob prebiranju teh rezultatov je, da si želimo napredka in razmisleka ob teh podatkih ter morda »rahlih« popravkov proračunov ter ciljev v naslednjih letih, povezanih z zaposlenimi, delom z njimi, vodenjem, motiviranjem in nagrajevanjem.

8.2 Rezultati ankete

Rezultati ankete potrdijo prvotno stališče o informacijski varnosti v podjetjih, ki pa žal ni na zavidljivi ravni. Komunikacijske točke, ki so hkrati tudi najbolj kritične točke in predstavljajo povezavo z ostalim poslovnim svetom, so najbolj ogrožene in hkrati najmanj ozaveščene o prežečih nevarnostih ter izgubah informacij. Informatiki lahko do določene ravni zaščitijo uporabnika in informacijski sistem, vendar so brez podpore uprave oziroma vodstva brez moči. Razbrati je tudi, da poslovna komunikacija med Uprava, Vodstvo, Informatiki in Komunikacijskimi točkami ne poteka po pričakovanih smernicah, da včasih potrebne informacije ne dosežejo cilja oziroma namena. Razmeroma v kratkem času pa se bodo morala podjetja zavedati, da pomeni vlaganje v izobraževanje zaposlenih največje bogastvo in ključ do uspeha v vseh poslovnih procesih.

9 SKLEP

Trditi, da imate popolnoma varen informacijski sistem, je v današnjem času zelo smela izjava, ki jo lahko izreče le nekdo, ki ne premore niti trohice znanja o varovanju informacij ali pa se sploh ne zaveda nevarnosti, ki prežijo na vsakem koncu. Podatek in informacija, sta ključni komponenti in predstavljata vodilo napredka oziroma gibalo našega časa. Predstavljata lahko našo največjo dobrino oziroma tržno blago, ki jo moramo varovati in si venomer postavljati vprašanja ali je bilo postorjeno dovolj, da tako tudi ostane. Na varnost je potrebno gledati kot na proces, ki je dinamičen in je vedno v teku, ne sme postati stanje, saj nikoli ne smemo biti prepričani, da bomo varni tudi v prihodnje, če smo varni danes. Vsa nadaljnja razmišljanja o varnosti nas privedejo do spoznanja, da je potrebno od primera do primera oceniti tveganje za izgubo ali zlorabo podatkov. Se zavedamo vrednosti naših podatkov ali pač živimo v prepričanju, da nas kaj zlega ne more doleteti?

Najpogostejše primere lahko združim skupaj in jih povežem v dva glavna dejavnika, upoštevajoč napake oziroma defekte strojne opreme. Glavna dejavnika sta zlonamerna programska koda in najšibkejši člen v verigi varnosti podatkov, to je človek sam. Na eni strani lahko k temu navaja sam pridobitni namen, na drugi strani pa človek sam s svojo naravo pripomore in nevede ponudi vse potrebne informacije in podatke kar na dlani. Okoriščanje s človekovo zaupljivostjo in s psihološkim nagnjenjem pomagati bližnjemu, z namenom pridobitve informacij in koristi, imenujemo socialni inženiring.

V slovenskem prostoru je kar precej nepoznan in kot je pokazal vprašalnik, več kot polovica ljudi ne verjame, da so lahko na poklicni (profesionalni) način zavedeni od temu primerno usposobljenih ljudi. Zavedajmo se, da lahko kar hitro podležemo manipulaciji.

Sama informacija je zgolj del mozaika in je sama po sebi nekoristna, ničvredna, če ni podprta z znanjem, ki ji predstavlja odločilni pomembnostni faktor. Izkušnje poročevalca, uporabna možnost, primerno komunikacijsko orodje oziroma komunikacijski kanal, poskrbijo, da prejemnik prejme informacijo v pravi obliki in ob pravem času. Strojna oprema s pomočjo vnaprej določenih komunikacijskih protokolov, izvede brezhibno transakcijo informacij in služi le namenu, kateremu je bila zasnovana. Za zadovoljivo varovanje našega informacijskega premoženja pa žal ni dovolj samo tehnologija. Potrebni so v prvi vrsti ljudje, procesi in postopki, kot osnova pa sprejeta varnostna politika, ki določa, kaj in kako varovati, predvidevati posledice izgub in določiti ukrepe za sankcioniranje.

Kaj pa človek?

Središče dogajanja mora biti vedno človek, ki se mora zavedati, da je varnost informacijskega premoženja danes na prvem mestu . Informacijska varnost ne zadeva samo poslovni svet, ampak tudi slehernega posameznika. Prepričan sem, da se bodo podjetja soočila z vsemi varnostnimi vprašanji v prihodnosti, ko bodo na nek način prisiljena z zakonsko regulativo, zagotoviti pričakovano raven informacijske varnosti.

Glavno vodilo mora biti ponavljajoče se izobraževanje in ozaveščanje ljudi, ki skupaj z vpeljanimi postopki, procesi in pravilniki v podjetjih, tudi z oglaševanjem v medijih, seveda ob primerni tehnični podpori, zadovolji ustrezno raven informacijske varnosti.

Skozi razgrnitev problematike, raziskovalnega dela in zaključkov na to temo, skuša diplomsko delo spodbuditi zavest in miselnost ter hkrati marsikatero vprašanje, recimo,

« **V kolikšni meri pa ste varni vi?«**

10 LITERATURA

1. Bratuša, T., Egan, M., Mather, T.: *Varovanje informacij + Hekerski vdori in zaščita, druga izdaja*, Pasadena, 2007
2. Gradišar, M.: *Uvod v informatiko*, Ekonomska fakulteta, Ljubljana, 2003
3. Gradišar, M., Resinovič, G.: *Informatika v poslovnem okolju*, Ekonomska fakulteta , Ljubljana, 2001
4. Hribar, B.: *Poslovno komuniciranje in vodenje*, Lesarska šola Maribor-Višja strokovna šola, Maribor, 2001
5. Kastelic, T.: *Varovanje informacij - izkušnje policije*, Varnostni Forum, Palsit, maj 2008, 12 - 14
6. Mihaljčič, Z.: *Poslovno komuniciranje*, Jutro, Ljubljana, 2006
7. Mitnick, K.: *Lahko me postaviš pred vrata pekla, vendar se ne bom uklonil*, Varnostni Forum, Palsit, maj 2008, 18 – 19
8. Mitnick, K: *Art of deception, second release*, Willey Publishing, 2003
9. Mitnick, K: *Art of intrusion*, Willey Publishing, 2005
10. Mohorič, T.: *O podatku in informaciji*, Organizacija, oktober 1999, 446-448, 1999
11. Možina, S., Tavčar, M., Zupan, N., Kneževič, A.: *Poslovno komuniciranje*, Obzorja, založništvo in izobraževanje, Maribor, 2004
12. Rakovec, S.: *Obvladovanje informacijske varnosti*, Varnostni Forum, Palsit, februar 2005, 29 - 30
13. Ruth, A., Hudson, K.: *Security+ Certification Training Kit* , Microsoft Corporation, 2007
14. Schneider, G.P.: *Electronic Business 7th Ed*, Thompson Learning, Cambridge, 2006
15. Shannon, C.E.: *A Mathematical Theory of Communication*, Bell System Technical, 1948
16. Tittel, E., Chapple, M., Stewart, J. M.: CISSP: Certified Information Systems Security Professional Study Guide, Sybex, 2003
17. Treven, S., Sriča, V.: *Mednarodno organizacijsko vedenje*, GV Založba, Ljubljana, 2001
18. Ur.l.RS, št 43/04, *Zakon o elektronskih komunikacijah*, 2004
19. Ur.l.RS, št 25/04, *Zakon o spremembah in dopolnitvah Zakona o elektronskem poslovanju in elektronskem podpisu*, 2004

20. Ur.l.RS, št 129/06, *Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah*, 2006
21. Ur.l.RS, št 86/04, *Zakon o varstvu osebnih podatkov*, 2004

11 VIRI

1 http://articles.techrepublic.com.com/5100-10878_11-1047991.html, dne 6.12. 2008
2 http://books.google.si, dne 25.11. 2008
3 http://dmst.aueb.gr/dds/bib/isostd.htm, dne 26.11. 2008
4 http://packetstorm.decepticons.org/docs/social-engineering/socintro.html, dne 26.11. 2008
5 http://pandalabs.pandasecurity.com/, dne 6.12. 2008
6 http://www.klemen.fraj.net/?p=1742, dne 16.11. 2008
7 http://www.academia.si/clanek/1-tiho-znanje-pridobljeno-z/info.html, dne 10.11. 2008
8 http://www.arnes.si/si-cert/obvestila/2004-06.html, dne 7.12. 2008
9 http://www.avg.com/, dne 7. 12.2008
10 http://www.computeruser.com/resources/dictionary/, dne 6. 12.2008
11 http://www.dnevnik.si/novice/znanost 17.4.2008, dne 17.4. 2008
12 http://www.enisa.europa.eu/doc/pdf/deliverables/WGAR/guide_sl.pdf, dne 6.12. 2008
13 http://www.fg.uni-mb.si/dokument.aspx?id=1377, dne 5.12. 2008
14 http://www.flickr.com/photos/panda_security/2840011688/, dne 26.11. 2008
15 http://www.gov.si/cvi/, dne 7.12. 2008
16 http://www.gzs.si/slo/, dne 7.12. 2008
17 http://www.housing.si/docs/Novice/Raziskava_Housing_2008.pdf, dne 16.11. 2008
18 http://www.idc.com/events/emea/emea_sp_bridwel_larry.jsp, dne 6.12. 2008
19 http://www.islovar.org, dne 5.11. 2008
20 http://www.krneki.net/rootkits/Rootkits.pdf, dne 3.12. 2008
21 http://www.melani.admin.ch/themen/, dne 4.11. 2008
22 http://www.mojmikro.si/news/crvi_postali_glavna_groznja, dne 13.11. 2008
23 http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt, dne 6.11. 2008
24 http://www.nasvet.com/pharming-napadi/, dne 6.12. 2008
25 http://www.sans.org/reading_room/whitepapers/engineering/, dne 29.10. 2008
26 http://www.securityfocus.com/infocus/, dne 7.12. 2008
27 http://www.si-revizija.si/isaca/revizija_IS.php, dne 6.12.2008
28 http://www.surveygizmo.com/, dne 6.12.2008
29 http://www.vigilante.com, dne 6.12.2008
30 http://www.wikipedia.org/, dne 6.12.2008

12 PRILOGA

* V prilogi na CD mediju

- Anketni vprašalniki in rezultati,
- Primeri smernic in pravilnika uporabe elektronskega in komunikacijskega sistema,
- Izjava o varovanju informacij,
- Komunikacija v primeru varnostnega incidenta.