UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

DIPLOMSKO DELO

TRŽENJE STORITVE COMPANY ON NET

Ljubljana, avgust 2010 SABA RESNIK

IZJAVA

Študentka Saba Resnik izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom _____, in da dovolim njegovo objavo na fakultetnih spletnih straneh.

V Ljubljani, dne_____ Podpis: _____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Po podatkih Statističnega urada republike Slovenije je svetovni splet (v nadaljevanju splet) v prvem četrtletju 2009 uporabljalo skoraj 1.100.000 oseb oz. 64 % vseh oseb v starosti 10–74 let (redni uporabniki spleta), to je za 6 odstotnih točk več kot v enakem obdobju 2008. Tudi slovenska podjetja pogosto uporabljajo splet, saj je v prvem četrtletju 2009 imelo dostop do spleta 96 % opazovanih podjetij. Če opazovana podjetja razdelimo po velikosti, so vsa srednje velika in vsa velika podjetja (100 %) imela dostop do spleta. Pri svojem delu je 43 % zaposlenih vsaj enkrat na teden uporabljalo računalnik z dostopom do spleta (Statistični urad Republike Slovenije, 2009). Navedeni podatki pričajo o pomembnosti spleta tako za podjetja kot za posameznike, zato je zagotavljanje varnosti toliko pomembnejše.

Uporabnike spleta poleg raznih računalniških virusov ogrožajo tudi spletne goljufije. Spletnih goljufij obstaja več vrst, podrobneje bom v nalogi opisala zgolj dve, in sicer lažno predstavljanje in zvabljanje. Uporabniki spleta danes uporabljajo najrazličnejše zaščite, vendar so le-te pogosto neučinkovite. Problem se največkrat pojavi, ko uporabnik spleta ne ve, kdo je lastnik spletne strani, katero obišče. Tako ob porastu spletnega kriminala vedno večjo vlogo pri spletni predstavitvi podjetja igra zaupanje, ki ga ustvari spletna stran. Eno od rešitev ponuja storitev Company on Net, podjetja CONNET, d. o. o., za katerega sem izvedla trženjsko raziskavo, predstavljeno v diplomskem delu.

Namen diplomskega dela je s pomočjo znanja, pridobljenega iz domače in tuje literature, ter s pomočjo primarnih podatkov, pridobljenih s pomočjo trženjske raziskave, pomagati podjetju CONNET, d. o. o., pri trženju njihove nove storitve Company on Net. Primarni podatki so pridobljeni s pomočjo trženjske raziskave.

Cilj diplomskega dela je s pomočjo pridobljenih primarnih podatkov ugotoviti, kakšne mehanizme zaščite uporabljajo podjetja, v kolikšni meri jih skrbi varnost na spletu in koliko so pripravljeni odšteti za storitev, ki bi jih varovala pred spletnimi goljufijami. S pomočjo zbranih podatkov bom kasneje podjetju CONNET, d. o. o., lahko predlagala, kako čim bolj učinkovito tržiti njihovo storitev.

Diplomsko delo je sestavljeno iz osmih vsebinskih sklopov. V prvem poglavju je s pomočjo domače in tuje literature opisano trženje storitev, značilnosti storitev, trženjski splet P8, sestavine storitev, razvrščanje le-teh, življenjski ciklus storitev, nove storitve, načrtovanje trženja storitev, izvajanje le-teh in zadovoljstvo porabnikov storitev. Drugo poglavje predstavlja uvod v tretje in četrto poglavje, saj govori o socialnemu inženiringu, ki ima za posledico številne spletne goljufije. Dve izmed spletnih goljufij sta podrobneje opisani v nadaljevanju: v tretjem poglavju lažno predstavljanje oz. ribarjenje (angl. *phishing*) in v četrtem poglavju zvabljanje (angl. *pharming*). Peto poglavje je namenjeno predstavitvi podjetja CONNET, d. o. o., temu sledi poglavje s podrobnim opisom storitve podjetja CONNET, d. o. o., ki se imenuje Company on

Net. V sedmem poglavju so določeni cilji trženjske raziskave, njena izvedba ter postavljene domneve. Sledi poglavje, ki vsebuje rezultate raziskave. V tem poglavju je opisan vzorec anketiranih podjetij, analize nekaterih posameznih vprašanj in na koncu tudi preverjanje postavljenih domnev. Diplomsko delo se zaključi s sklepom kot zadnjim poglavjem.

1 TRŽENJE STORITEV

Potočnik (1998, str. 2–5) opredeli trženje kot dejavnost, ki zagotavlja podjetju prodajo izdelka in vsebuje vse procese, ki so potrebni, da izdelek pride od podjetja do porabnika. »Trženje storitev je težje kot trženje izdelkov. Značilnosti izdelkov lahko zaznavamo s svojimi čutili, pri storitvah to ni mogoče. Porabniki storitev so praviloma aktivno vključeni v oblikovanje in izvedbo storitve, zato je trženje storitev interaktivni proces med izvajalcem in porabnikom, ki zahteva oblikovanje trženja na podlagi medsebojnih odnosov« (Potočnik, 2004, str. 178).

Za lažje razumevanje trženja storitev moramo najprej razumeti, kaj storitev je, kaj spada pod storitev itd., zato bo v naslednjih podpoglavjih nekaj več napisnega o sami storitvi, njenih sestavinah, izvajanju storitev in življenjskemu ciklu. V podpoglavju 1.2 bo opisan trženjski splet storitev in kasneje opis lastnosti novih storitev ter načrtovanje trženja storitev.

1.1 Storitev

»Storitev je aktivnost ali serija aktivnosti (bolj ali manj) neotipljive narave, ki se običajno izvaja v sodelovanju med potrošnikom, zaposlenim v storitveni dejavnosti, fizičnimi viri in elementi za izvedbo same storitve pod pogojem, da le-ti predstavljajo odgovor na potrošnikove potrebe« (Grönroos, 2000, str. 27).

Storitev lahko opišemo tudi kot rezultat celovitega trženjskega napora podjetja, da ustreže zahtevam in potrebam potrošnikov. Je integralni del poslovne in razvojne politike podjetja. Koriščenje storitev predstavlja zadovoljevanje družbenih potreb, istočasno pa se s prodajo ustvarja dobiček. Storitev je vse, kar lahko podjetja ponudijo trgu in kar vzbudi pozornost, povpraševanje, nabavo in koriščenje (Devetak, 2000, str. 27).

Podjetje lahko ponudi izdelek ali storitev. Glede na to, koliko storitev je vključenih v ponudbo podjetja, pa jo razdelimo v pet vrst ponudbe (Potočnik, 2004, str. 30):

- samo izdelek,
- izdelek s storitvami, ki naredijo ta izdelek bolj privlačen za kupca,
- izdelek in storitev sta enakovredno zastopana v ponudbi,
- storitev, ki jo spremljajo manj pomembni izdelki, in
- sama storitev.

Kot je zapisno že v uvodu, se bom v diplomskem delu osredotočila na trženje storitve Company on Net (v nadaljevanju CON) podjetja CONNET, d. o. o. Če se oprem na zgoraj naštete vrste ponudbe, storitve ne morem umestiti v nobeno izmed ponudb. Glede na zastavljeno strategijo podjetja in vklop nekaterih dodatnih storitev ne morem umestiti podjetja zgolj v sklop: samo storitev. Ena izmed ustanoviteljic podjetja, Anka Lipičnik, je ponudbo podjetja opisala kot »storitev, ki jo spremljajo dodatne storitve«.

1.1.1 Značilnosti storitev

Za samo razumevanje storitev je poleg definicije pomembno upoštevati tudi značilnosti storitev. Za storitve veljajo naslednje značilnosti (Kotler, Armstrong, Starr, R.G., Wong, 1996, str. 466–468):

- neopredmetenost,
- neločljivost,
- spremenljivost in
- minljivost.

Storitve so večinoma neopredmetene, kar pomeni, da jih ne moremo okusiti, otipati, občutiti, slišati ali vonjati. Prav zaradi neopredmetenosti so za kupce toliko bolj pomembna fizična dokazila o kakovosti storitve, kot so gradiva, prospekti, dokumenti, ustno izročilo itd. Ena izmed najbolj pomembnih značilnosti je neločljivost, kar pomeni, da storitve nastanejo in se porabijo hkrati. V takem primeru je porabnik prisoten in zato pride do interakcije med podjetjem (kot ponudnikom) in porabnikom. Spremenljivost storitve je lahko precejšnja, odvisno od tega, kdo, kje in kdaj storitev izvaja. Tukaj je zelo pomembno ustno sporočilo, saj se porabniki predhodno pozanimajo o kakovosti določene storitve. Storitev ni možno skladiščiti, saj so minljive, prav zato so storitve še toliko bolj občutljive na nihanja v povpraševanju. Kadar povpraševanje po določeni storitvi zelo niha, ima podjetje lahko problem zaposlovanja izvajalcev. Prav tako nihanje v povpraševanju povzroči problem zaradi relativno kratke življenjske dobe storitve, saj storitev obstaja le, dokler traja proces (Potočnik, 1998, str. 14).

Porabniki storitev pri nakupu občutijo več tveganja kot pri nakupu izdelka in v primeru pozitivne izkušnje lahko ostanejo veliko bolj zvesti ponudniku. Zato je pri storitvah zelo pomembna pozitivna izkušnja in zaupanje porabnika v izvajalca. Podjetja imajo pri trženju storitev tri naloge: povečati diferenciacijo storitev v primerjavi z drugimi ponudniki iste storitve, povečati produktivnost (intenzivnejše delo in povečan obseg storitev) in izboljšati kakovost storitev (Potočnik, 1998, str. 15).

Značilnosti storitev pa je možno razdeliti tudi na: generične (procesnost, nesnovnost in neobstojnost) in izvedbene značilnosti storitev. Med slednje sodijo: nezmožnost prevoza storitve, neločljivost od izvajalca, sočasnost izvajanja in uporabe, neposredni odnos med izvajalci in uporabniki (sodelovanje uporabnikov pri izvajanju in variabilnost izvajanja storitev). Posledice

zaradi slabe izvedbe storitve lahko podjetje ublaži z nekaterimi metodami, kot so: načrtovanje izvajanja storitve (angl. *blueprinting*), standardizacija, trženje na podlagi pozitivnih odnosov (angl. *relationship management*) itd. (Potočnik, 1998, str. 19).

Vse zgoraj omenjene značilnosti pa za trženje storitev predstavljajo problem, ki ga je potrebno premostiti. Pri oblikovanju storitvene ponudbe se je zato potrebno osredotočiti na pet elementov (Žabot, 2005, str. 17):

- storitev je treba narediti oprijemljivo,
- prav tako je treba preiti mejo neločljivosti, zato morajo biti vsi v podjetju obrnjeni k potrošniku,
- treba je uravnavati spremenljivost, tako da določimo in nadziramo kakovost,
- uravnavati minljivost in
- uravnavati ponudbo in povpraševanje.

Z naraščanjem deleža storitev v strukturi gospodarstva nastaja vse večja potreba po razvrščanju, zato lahko storitve razvrstimo na različne načine. Sprva se storitve delijo na storitve, ki temeljijo na opremi, in tiste, ki temeljijo na ljudeh. Storitev CON spada v slednjo. Prav tako je pri storitvi porabnik prisoten ali pa ne. Anka Lipičnik opiše storitev podjetja CONNET, d. o. o., takole: »Storitev CON je večplastna. Podjetje CONNET, d. o. o., jamči in zagotavlja vse za tehnično izvajanje storitve. Matično podjetje ostaja vezano na tehnološko plat. Od zastopnikov prejemamo pripombe in konstruktivne predloge za izboljšave, ki jim tehnologija skuša kar najhitreje slediti. Od podjetja CONNET, d. o. o., zastopniki kupijo storitev, ki jo nato prodajo končnemu kupcu, pri čemer končni kupec ni edini in končni uporabnik, pač pa se storitev izvede vsakič znova ob obisku na kupčevi spletni strani.«

1.2 Trženjski splet 8P za trženje storitev

Če povzamem nekatere definicije, je trženjski splet niz instrumentov, ki jih podjetja uporabljajo z namenom slediti postavljenim trženjskim ciljem na ciljnem trgu. Najbolj osnoven trženjski splet vsebuje štiri sestavine (4P), ker pa se trženje storitve precej razlikuje od trženja izdelkov, moramo koncept 4P: izdelek oz. storitev, cena, tržna pot in trženjsko komuniciranje (angl. *product, price, place, promotion*) prilagoditi še s 4P: ljudje, izvajanje storitev in fizično okolje ter produktivnost in kvaliteta (angl. *people, process, physical evidences, productivity and quality*). Tako nastane trženjski splet 8P, ki vsebuje zgoraj naštete elemente. Ti elementi predstavljajo ključne sestavine za nastanek strategij za zadovoljevanje potrošnikovih potreb (Lovelock, 2007, str. 22).

»Koncept storitve pogosto opredelimo kot storitveni izdelek, ki vsebuje vse sestavine storitve, pretekle izkušnje porabnikov in rezultate izvajanja. Opisani koncept razširja pojmovanje 7P storitev z dodatnim P, torej 8P, ki določajo storitveni izdelek, to je produktivnost in kakovost« (Potočnik, 2004, str. 38).

Devetak (2000, str. 32–36) elemente trženjskega spleta opiše:

1. Izdelek oz. storitev: tu najpogosteje obravnavamo kakovost, funkcionalnost, značilnosti, blagovno znamko, servis in garancijo itd.
2. Na oblikovanje cene vpliva predvsem konkurenca. Cena storitve se lahko razlikuje glede na prodajna območja, kupce, sezono, namen uporabe itd.
3. Tržna pot oz. distribucija se pri storitvah obravnava drugače kot pri izdelkih, tako govorimo o prostoru ali kraju izvajanja storitve (in ne o organiziranem prevozu kot pri izdelkih). Kraj izvajanja storitve je lahko pri proizvajalcu, pri naročniku ali na tretjem kraju, ki je dogovorjen med izvajalcem in naročnikom storitve.
4. Promocija je vsakršno komuniciranje s porabniki z namenom pospeševanja in povečevanja prodaje. Načinov, kako promoviramo storitev, je več: demonstracija storitev, tehnična svetovanja, oglaševanje v sredstvih javnega obveščanja itd.
5. Ljudje imajo vlogo kupcev na eni in vlogo izvajalcev storitev na drugi strani. Poleg strokovne podkovanosti izvajalcev je pomembna tudi hitrost in kakovost storitev, ki jih izvajalci opravljajo. Pri prodaji ima pomembno vlogo tudi videz in urejenost izvajalca.
6. Izvajanje storitev (angl. *processing*) predstavlja bistvo storitve. Pri izvajanju storitev mora biti poskrbljeno za varnost, kakovost, ustrezno hitrost, strokovnost izvajalcev, za primerno komunikacijo s porabniki, sodelovanje in timsko delo med strokovnjaki in trženjskim sektorjem ter izvajalci, kulturo in etiko. Zaposlene v storitveni organizaciji delimo v štiri skupine: kontaktno osebje, pomožno osebje, vplivneži in drugi zaposleni.
7. Fizični dokazi predstavljajo vse, kar porabnik vidi, sliši ali občuti.

1.3 Sestavine storitev

Sedaj, ko imamo boljšo predstavo o tem, kaj storitev je in v kolikšni meri se razlikuje od izdelka, bo v nadaljevanju zapisano nekaj več o glavnih sestavinah storitev, ki so s trženjskega vidika po Potočniku (1998, str. 16–18) naslednje: storitvena organizacija, porabnik storitev in kakovost storitev. Podrobneje sem sestavine opisala v nadaljevanju.

1.3.1 Storitvena organizacija

Storitvena organizacija vsebuje fizično podporo, kontaktno osebje in notranje organiziranje. Fizično podporo predstavljajo sredstva, ki se uporabljajo pri izvajanju storitev, in fizično okolje. Poleg fizične podpore storitvena organizacija vsebuje še kontaktno osebje, ki predstavlja podjetje. To so osebe, ki prihajajo v stik s ponudniki pri ponudbi in izvajanju storitev. Notranje organiziranje pa je pomembno predvsem zato, ker je od tega odvisna učinkovitost tako fizične podpore kot tudi kontaktnega osebja (Potočnik, 1998, str. 16–18).

Zgoraj napisano teoretično razlago sestavin storitev bom sedaj predstavila na praktičnem primeru. Kaj vse morajo vsebovati organizacije, katerih storitev so elektronske komunikacije? Na trg storitev elektronskih komunikacij spada tudi podjetje CONNET, d. o. o. Anka Lipičnik pojasnjuje: »Za potrebe marsikaterega razpisa so elektronske vsebine in elektronske storitve definirane kot vsebine in storitve informacijske družbe, ki se zagotavljajo na daljavo, z elektronskimi sredstvi in na posamezno zahtevo uporabnika storitev. Pri tem 'na daljavo' pomeni, da se storitev zagotavlja, ne da bi bili strani navzoči sočasno. 'Z elektronskimi sredstvi' pomeni, da se storitev na začetku pošlje in v namembnem kraju sprejme z elektronsko opremo za obdelavo, vključno z digitalnim stiskanjem, in za shranjevanje podatkov ter v celoti pošlje, prenese in sprejme po žici, radiu, optičnih ali drugih elektromagnetnih sredstvih. 'Na posamezno zahtevo prejemnika storitev' pa pomeni, da se storitev zagotavlja s prenosom podatkov na posamezno zahtevo. Storitve informacijske družbe v splošnem zajemajo široko področje gospodarskih in negospodarskih dejavnosti, ki potekajo na spletu in drugih globalno dostopnih omrežjih (npr. omrežje mobilne telefonije). Storitve informacijske družbe vključujejo tako plačljive kot tudi neplačljive, prosto dostopne storitve. Storitve informacijske družbe vključujejo tudi prenos podatkov po komunikacijskem omrežju, dostop do komunikacijskega omrežja ali shranjevanje podatkov, ki jih zagotovi prejemnik storitve.«

1.3.2 Porabnik storitev

Porabniki storitev imajo različne osebnostne značilnosti, želje, pričakovanja, vrednote, življenjski slog itd. Zato je porabnikovo storitev težko nadzorovati in podjetja so primorana raziskovati motivacije in osebnostne značilnosti porabnikov storitev (npr. kdo so dejanski in kateri potencialni porabniki, njihove demografske, psihografske, vedenjske značilnosti, katere storitve že uporabljajo oz. bi jih uporabljali pri zadovoljevanju svojih potreb in kako ocenjujejo konkurenčne storitve) (Potočnik, 2004, str. 69).

1.3.3 Kakovost storitve

Podjetje se mora nenehno ukvarjati z vrzeljo med pričakovanji stranke in njeno oceno dejansko opravljene storitve. Za zmanjšanje te vrzeli mora podjetje dobro poznati pričakovanja strank. V ta namen je potrebno definirati kakovost storitev. To lahko storimo s konceptom »storitvenega srečanja«, z drugimi besedami tudi »trenutka resnice«. Koncept »storitveno srečanje« je vsaka direktna interakcija med ponudnikom storitve in stranko. »Če se zgodi, da so pričakovanja stranke višja od opravljene storitve, to še ne pomeni, da je storitev v očeh kupca opravljena nekakovostno. Kakovost je relativna in odvisna od osebnih pričakovanj. Kakovost storitve je potemtakem funkcija vrzeli med strankinimi pričakovanji in dejansko opravljeno storitvijo« (Kač, 2004, str. 1).

1.4 Razvrščanje storitev

Zaradi naraščanja deleža storitev v strukturi gospodarstva nastaja težnja po razvrščanju storitvenega sektorja. Potočnik (2004, str. 48) jih razdeli v naslednje skupine:

- Storitve glede na tehnološko opremljenost
  Tukaj razlikujemo storitve, ki temeljijo na opremi (npr. avtomatske pralnice avtomobilov), ali storitve, ki temeljijo predvsem na ljudeh (npr. ročne pralnice avtomobilov).
- Pri storitvah glede na porabnike razlikujemo: porabniške storitve (končno povpraševanje) in podjetniške storitve (medorganizacijsko povpraševanje).
- Tradicionalne storitve (npr. transport, turizem) in nove storitve (temeljijo predvsem na razvoju informacijske tehnologije).
- Storitve v proizvodnem procesu
  V tem sklopu ločimo storitve glede na potek proizvodnje, torej: storitve, ki jih moramo opraviti pred proizvodnim procesom, storitve, ki so povezane s proizvodnim procesom, storitve, ki potekajo hkrati s proizvodnim procesom.
- Inovativne storitve (storitve na podlagi znanja, npr. zdravstvene in izobraževalne storitve) in rutinske storitve (večinoma standardizirane).
- Formalne storitve (formalni sektor storitev, ki je v celoti registriran) in neformalne storitve (neformalni sektor storitev, kjer so storitve le delno ali pa sploh niso registrirane).

1.5 Življenjski ciklus storitve

Uspešne storitve so tiste, ki se jim uspe najbolj približati porabniku in v največji meri zadovoljiti njihove potrebe. Da bi bilo podjetje pri tem uspešno, mora dobro poznati osnovne trženjske metode in ena izmed teh je tudi koncept življenjskega ciklusa storitve (Urych, 2004, str. 1).

Vsaka storitev ima tako kot živa bitja omejeno življenjsko dobo. Ideja življenjskega ciklusa izvira iz biologije, vendar je bila uspešno prenesena tudi v trženje. Življenjska zgodba večine storitev oz. izdelkov je prehajanje skozi različne stopnje, za katere je značilen različen obseg prodaje, naraščanje ali upadanje dobička in ravno zato posamezne stopnje zahtevajo različne trženjske pristope in aktivnosti (Ulrych, 2004, st. 2).

Faze življenjskega ciklusa storitve, kot jih navaja Devetak (2000, str. 98), pa so naslednje:

- uvajanje na trgu,
- rast prodaje,
- zrelost,
- zasičenost trga in
- odmiranje in upadanje prodaje.

Storitev CON se nahaja v fazi uvajanja na trgu. Ta faza je ena izmed najtežjih in najbolj

občutljivih, saj morajo biti pri prodaji poleg tržnikov vključeni tudi strokovnjaki, ki kupce informirajo o delovanju storitve, tehničnih značilnostih in načinu uporabe. Obenem se storitev tudi glede na odzive trga v določeni meri prilagaja in spreminja. CONNET, d. o. o., zato v tej fazi svojo storitev največkrat nudi brezplačno (za obdobje treh mesecev), saj je to najboljši način, kako kupcu in uporabnikom predstaviti storitev. To je eden izmed načinov, kako podjetje informira trg o uvajanju nove storitve. Stroški v fazi uvajanja so precejšnji, dobiček pa zelo majhen. Uspeh storitve je odvisen od več dejavnikov, med drugimi: kako hitro se bo trg zavedal, da takšno storitev potrebuje; od konkurence; od plačilne sposobnosti itd. To fazo lahko podjetje tudi skrajša, vendar le, če razpolaga z ustreznim strokovnim kadrom in dovolj sredstvi za uvajanje storitve (Devetak, 2000, str. 100).

1.6 Nove storitve

Glede na to, da moja raziskava, katere opis in rezultati sledijo v 7. poglavju, temelji na storitvi CON, ki je relativno nova storitev, bom v tem poglavju na kratko opisala nove storitve in značilnosti le-teh.

Če povzamem številne definicije, lahko zapišem, da poznamo popolnoma nove storitve (v svetovnem merilu), zgolj preoblikovane storitve (delno nove storitve) in izpopolnjene storitve. Storitve lahko obravnavamo kot nove tudi z vidika podjetja, države ali svetovnega merila.

Za storitev CON lahko rečemo, da je nova storitev, saj na edinstven način zagotavlja varnost na spletu. Tako pri razvoju novih storitev poznamo več faz (Jeran, 2006, str. 5), ki so:

- snovanje ali pregled poslovne strategije (v tej fazi podjetje izoblikuje vizijo in določi cilje),
- strategija razvoja nove storitve,
- iskanje in ocenjevanje idej,
- oblikovanje in testiranje koncepta,
- poslovna analiza,
- testiranje storitve na trgu,
- komercializacija in
- ocena po dokončni uvedbi.

Na kakšen način je nastajala storitev CON, mi razloži Anka Lipičnik. V fazi snovanja, leta 2005, se je vodstvo odločilo za delovanje podjetja zgolj na spletu in tako se je začela postavljati nova vizija in novi cilji. Fazo strategije razvoja pa Anka Lipičnik opiše: »Najprej sva se z Alešem Lipičnikom (ustanovitelj podjetja CONNET, d. o. o.) odločila izpiliti idejo, nato se je izdelal prototip. Ideje se išče in ocenjuje vsakodnevno. V glavnem so moja skrb. Tudi če sem fizično odsotna, sem vedno vključena v te procese. Skuša se spodbujati kreativnost, saj včasih kaka preprosta ideja reši mnogo težav. Za ta del smo potrebovali kar eno leto, saj sva z Alešem imela zgolj enega programerja. Ko je bil prototip dokončan, se je lahko pričelo dogovarjanje za zaokroženje storitve – konkretno smo potrebovali Gospodarsko zbornico Slovenije (v

nadaljevanju GZS) v vlogi verifikatorja. GZS je projekt dala v oceno mnogim, ki so ga potrdili, in posledično se je podpisala pogodba. Inštitut Jožefa Stefana je proizvod sprejel z odprtimi rokami in tako se je v nadaljevanju sestavila nova ekipa programerjev, ki sedaj skrbi, za tehnično plat storitve.«

1.7 Načrtovanje trženja storitev

Podjetja, ki tržijo storitve, se največkrat poslužujejo strateškega načrta trženja, ki ga po Potočniku (1998, str. 29) sestavljajo naslednje stopnje:

- opredelitev strateških izhodišč,
- analiza položaja,
- oblikovanje strategije trženja,
- trženjski program in nadzor izvajanja.

Podjetje opredeli strateška izhodišča s pomočjo določitve poslanstva podjetja, njegove vizije in ciljev. Slednji morajo biti opredeljeni precej natančno količinsko in časovno in ne zgolj opisno, kakor se opredelita poslanstvo in vizija. Podjetje ima za en trg in eno storitev zgolj en strateški načrt, v primeru več storitev na različnih trgih pa za vsako storitev in trg svoj strateški načrt (Potočnik, 1998, str. 29).

V analizo položaja spadata pregled (revizija) dosedanjega načina trženja in SWOT-analiza (prednosti, slabosti, priložnosti, nevarnosti), pri kateri podjetje uporabi podatke iz pregleda dosedanjega trženja, da ugotovi prednosti in slabosti ter priložnosti in nevarnosti za storitev (Potočnik, 1998, str. 30).

Oblikovanje trženjskih strategij podjetja poteka prek naslednjih stopenj: opredelitev ciljnih trgov, opredelitev ciljev trženja (npr. obseg prodaje, tržni delež) in oblikovanje trženjskih strategij. Pri oblikovanju trženjskih strategij se uporabljajo tri vrste trženjskih strategij: ofenzivne, defenzivne in usmerjene na donosne storitve. Pri trženju storitev se čedalje pogosteje srečujemo z defenzivnim trženjem, ki temelji na ohranjanju dosedanjih uporabnikov in dosedanjega tržnega deleža. Za ofenzivne strategije pa je značilen prodor na nove trge, uvajanje novosti, pridobivanje novih kupcev, agresivno oglaševanje in pospeševanje prodaje itd. Pri tem načinu trženja poizkuša podjetje z oglaševanjem, oblikovanjem cen in pospeševanjem prodaje povečati svoj tržni delež (Potočnik, 2004, str. 188).

S programi delovanja poskuša podjetje odgovoriti na vprašanja, kot so: kaj bo narejeno, kdaj bo narejeno, kdo bo naredil in koliko bo stalo. Pri nadzorovanju pa mora podjetje opredeliti, kako bo spremljalo in izpolnjevalo načrt (Dimec, 2004, str. 11).

1.8 Izvajanje storitev

Storitve podjetje uspešno izvaja (poseduje) z upoštevanjem naslednjih dejavnikov: zanesljivost, pripravljenost zaposlenih (za pomoč uporabnikom in izvajanje storitev), strokovnost, dostopnost, vljudnost in prijaznost ter spoštovanje kontaktnih oseb, komuniciranje (obveščanje porabnikov povratne informacije itd.) in fizična podpora (npr. oprema za izvajanje storitev). Pri izvajanju storitev pa je podjetje podvrženo številnim vrzelim (Potočnik, 1998, str. 35). Model po Parasuramanu, Zeithamlu in Berryu opredeli pet vrzeli (Kotler, Armstrong, Starr, R.G., Wong 1996, str. 474–476):

1. Vrzel med pričakovanji porabnikov in zaznavanjem teh pričakovanj pri poslovodstvu
   Vodstvo podjetja ne zazna vedno prav, kaj porabniki želijo. Npr.: vodstvo v podjetju Company on Net, d. o. o., zazna, da si porabniki želijo novo obliko pečata, v resnici pa si želijo dodatne statistične obdelave prikazov pečata.
2. Vrzel med zaznavanjem pričakovanj pri poslovodstvu in natančno opredelitvijo kakovosti storitve
   Vodstvo pravilno zazna porabnikove želje, vendar določi napačen izvedbeni standard. Npr.: porabniki si želijo, da bi se certifikat na verificirani strani nalagal hitreje, poslovodstvo to željo pravilno zazna, vendar pri izvedbi tega postopka pride do ostalih sprememb, ki nato upočasnijo ostale postopke.
3. Vrzel med specifikacijo kakovosti storitve in izvajanjem storitve
   Osebje ni dovolj izobraženo ali sposobno ali pa veljajo nasprotujoči si standardi. Npr.: trenutno je ekipa, ki je zadolžena za CON, premajhna, zato včasih pride do preobremenitve.
4. Vrzel med izvajanjem storitve in zunanjimi komunikacijami
   Npr.: stranka je prepričana, da se bodo s storitvijo CON rešili vseh problemov v smislu varnosti njihove spletne strani, ne računajo pa na človeški faktor (socialni inženiring[1]), pred katerim je varnostni sistem nemočen.
5. Vrzel med zaznano in pričakovano storitvijo
   Ta vrzel se pojavi, kadar porabnik oceni delovanje podjetja drugače in napačno zazna kakovost storitve. Npr.: morda si uporabnik storitve CON predstavlja, da mu bo podjetje poročalo o neuspelih napadih na njegovo spletno stran.

1.9 Zadovoljstvo porabnikov s storitvijo in kakovost storitve

Najpomembnejši za storitveno podjetje so zvesti porabniki in njihovo zadovoljstvo, ki je odvisno od njihovega dojemanja storitve ter čustvenega odziva in ni v takšni meri objektivno kot pri izdelkih. Zadovoljstvo porabnikov pa je odvisno tudi od cene storitve oziroma razmerja med kakovostjo in ceno storitve (Potočnik, 1998, str. 37).

[1] Pojem socialni inženiring opišem na 13. strani diplomskega dela.

Porabnik storitve zaznava njeno kakovost racionalno, ravno nasprotno pa zadovoljstvo s storitvijo ocenjuje emocionalno. Na zadovoljstvo uporabnika v največji meri vplivajo njegova pričakovanja, ki jih lahko zaznamujejo naslednji najpomembnejši dejavniki (Potočnik, 2004, str. 132):

- cena (višja cena storitve zviša pričakovanja),
- razpoložljivost alternativne storitve (porabniki pri nakupu profesionalne storitve želijo pridobiti drugo mnenje – angl. *second opinion*),
- trženjske aktivnosti v veliki meri vplivajo na pričakovanja porabnika (ustno sporočanje v večji meri kot oglaševanje in druge trženjske aktivnosti storitvenega podjetja),
- prejšnje izkušnje.

Na zaznano kakovost storitve vplivajo motnje pričakovanj, ki jih razložimo kot vrzeli med zaznano in pričakovano kakovostjo storitve, te vrzeli so tako pozitivne kot tudi negativne (Potočnik, 1998, str. 37–39).

Da bi ublažili negativne učinke zgoraj omenjenih dejavnikov podjetja uvajajo garancije, ki pa jih je za storitev precej težje ponuditi kot za izdelek (garancija za izdelke zagotavlja zamenjavo, popravilo izdelka itd.). Storitvena podjetja ponujajo vračilo denarja ali izvršitev storitve v prihodnosti in mnoge druge oblike kombinacij med njima kot obljubo, da bo podjetje nadomestilo škodo, če storitev ne bo uspešna. Za podjetje je pomembna dobra garancija in njeno oglaševanje, saj s tem daje vtis kakovostne storitve in zmanjšuje tveganje porabnikov, to pa pripelje do večjega dobička zaradi večje prodaje in ugleda podjetja (Potočnik, 2004, str. 112–114).

Storitveno podjetje mora izvesti raziskavo zadovoljstva porabnikov, da se lahko osredotoči na izboljšanje kakovosti svoje storitve, da dobi povratne informacije o različnih ukrepih in odkrije svoje prednosti in slabosti. Pri organiziranosti tržne raziskave sta običajno prisotni dve stopnji: pripravljalna in izvajalna stopnja raziskave. Pripravljalna stopnja raziskave zajema opredelitev tržne raziskave in plan (opredelitev ciljev, določitev temeljnih virov informacij, izbor metod in tehnik zbiranja podatkov ter obdelave dobljenih informacij, organizacija izvajanja raziskave, časovna in stroškovna ocena …). Pri izvajalni stopnji raziskave pa podjetje zbira, ureja in obdeluje informacije, oblikuje sklepe in priporočila ter zaključno poročilo. Postopek raziskave je po Jacksonu Haugeu možno razdeliti na: opredelitev problema, načrtovanje, zbiranje informacij in podatkov, analizo informacij in podatkov, predstavitev rezultatov in njihovo interpretacija in nazadnje še na trženjske odločitve (v Devetak, 2000, str. 63–64).

Kadar govorimo o kakovosti izdelkov, imamo v mislih kakovost v proizvodnji, usklajenost izdelkov z vzorci, standardi ipd., kadar pa govorimo o kakovosti storitev, imamo v mislih predvsem maksimiranje zadovoljstva porabnikov, ki pa je odvisno od številnih najpogosteje neoprijemljivih in težko merljivih dejavnikov. Visoka kakovost storitve še ne zagotavlja visokih dobičkov, še zlasti v primeru, ko porabnik ne pričakuje tako visoke kakovosti. Stroški kakovosti

storitve pa nastajajo največkrat zaradi preprečevanja napak med procesom, kontrole kakovosti po končanem procesu, popravila napak med samim procesom, vračila denarja in popravila napak (Potočnik, 1998, str. 50–51). Pri popravilu napak med samim procesom v CONNET, d. o. o., beležijo največ stroškov.

Pri storitvi CON določena prednost lahko hitro postane napaka, saj nekatere spremembe na trgu (npr. spremembe v brskalnikih) narekujejo nova prilagajanja. Kakovost storitve je dejansko glede na potrebe večine kupcev že precej visoka, vendar jo skušajo v podjetju ohraniti na tem (višjem) nivoju zaradi prodora na trg.

S tem poglavjem zaključujem teoretični del o trženju storitev. V nadaljevanju se posvečam socialnemu inženiringu, ki predstavlja uvod v predstavitev spletnih goljufij in kasneje podrobno opisala dve vrsti spletnih goljufij.

2 SOCIALNI INŽENIRING

Prvo poglavje zajema splošno teorijo o trženju storitev, v drugem poglavju pa predstavim pojem socialnega inženiringa, z namenom boljšega razumevanja spletnih goljufij, o katerih pišem kasneje v tretjem in četrtem poglavju.

Socialni inženiring se je uporabljal že v času hladne vojne, sedaj pa se je prenesel tudi v sodobno okolje, v dobo računalnikov. Tudi v tej dobi pa ni nekaj novega, saj ga na področju informacijske varnosti poznamo že dobrih 20 let. Bistvo socialnega inženiringa je v tem, da goljufi ne iščejo lukenj v računalniških sistemih ali programih, s pomočjo katerih nato vdrejo v računalnik in tako pridejo do želenih informacij, temveč se poslužujejo metode, nad katero noben protivirusni program, sistem nadzora, požarni zid, itd. nima nadzora oz. moči. Ta metoda je prevara človeka (npr. zaposlenega v podjetju) (Fraj, 2007).

Na spletni strani Zveze potrošnikov Slovenije (v nadaljevanju ZPS) Bojan Radulj socialni inženiring opiše kot tehniko, s katero ciljne osebe z uporabo poznavanja psihologije ljudi, delovanja računalniških sistemov in z uporabo majhnih in verjetnih laži pripravimo do tega, da ravnajo tako, kakor v običajnih okoliščinah, ko imajo opravka s tujci oz. nepoznanimi osebami, ne bi nikoli (Zveza potrošnikov Slovenije, v nadaljevanju ZPS, 2009).

Tehnike za pridobivanje podatkov s pomočjo socialnega inženiringa so vedno bolj napredne in na žalost se bodoče žrtve pred takšno goljufijo težko zaščitijo s tehnično opremo. Najboljša rešitev je ozaveščanje in previdnost uporabnikov, saj je glavni cilj socialnega inženiringa prav uporabnik in njegova naivnost, nepremišljenost in nepazljivost. Uspešnost socialnega inženiringa je odvisna od vrste dejavnikov, predvsem pa od kakovosti zbiranja podatkov o žrtvi in prvega stika z žrtvijo. Cikel socialnega inženiringa lahko razdelimo na več faz. Prva je raziskovanje

(zbiranje podatkov o žrtvi), nato sledi pridobivanje zaupanja in kot zadnja nastopi izkoriščanje pridobljenega zaupanja, ki je najtežja in najbolj pomembna faza za napadalca. Zadnja faza vključuje pridobitev občutljivih podatkov od žrtve in nato uporabo le-teh (ZPS, 2009).

Obstajajo različni načini pridobivanja podatkov s pomočjo socialnega inženiringa. Med njimi so najpogostejši napadi s pomočjo informacijskih tehnologij, kot so lažno predstavljanje (angl. *phishing*) oziroma pošiljanje lažnih e-poštnih sporočil, neposredni napadi na DNS-strežnike[2], zvabljanje (angl. *pharming*) in mnogo drugih (ZPS, 2009). V diplomskem delu se omejim zgolj na lažno predstavljanje in zvabljanje.

Več o lažnem predstavljanju in zvabljanju sledi v naslednjih poglavjih, kjer goljufijo oz. napade opišem bolj podrobno in ju tudi grafično ponazorim.

3 LAŽNO PREDSTAVLJANJE – RIBARJENJE (ANGL. *PHISHING*)

Lažno predstavljanje ali ribarjenje (angl. *phishing*) je nezakonit način zavajanja uporabnikov spleta. Izraz ribarjenje (angl. *phishing*) izvira iz angleških besed za geslo (angl. *password*) in ribarjenje (angl. *phishing*). Spletni goljufi želijo s pomočjo lažnih spletnih strani in elektronskih sporočil od uporabnika izvabiti osebne podatke, kot so: številke kreditnih kartic, uporabniška imena in gesla (npr. spletnih bančnih računov), digitalna potrdila in ostale osebne podatke. Vse te podatke pridobijo na način, da pod pretvezo prepričajo žrtev o potrebi po posredovanju teh podatkov. Praviloma najprej postavijo lažno spletno stran, ki je zelo podobna pravi, nato pa od porabnika z lažnim elektronskim sporočilom poskušajo izvabiti bodisi obisk te strani ali kar takoj pridobiti podatke z odgovorom na to sporočilo (Informacijski pooblaščenec, 2009).

Eden izmed primerov lažnega predstavljanja je tudi ta, zapisan v reviji Delo (Forstnerič, 2009, str. 28): »Pred olimpijskimi igrami (2008) v Pekingu je neka spletna stran nekaj časa prodajala vstopnice, nato pa izginila, kupci pa kart nikoli niso dobili. Po nekaterih podatkih naj bi upravniki strani protipravno pridobili več kot 30 tisoč britanskih funtov.«

Število poizkusov prevar s pomočjo neželene oglasne pošte (angl. *spam*) v kombinaciji s ponarejenimi spletnimi stranmi se iz leta v leto strmo povzpenja. Najpogostejša oblika te prevare je, ko elektronsko pismo ali spletna stran od uporabnika zahteva, da vanjo vnese svoje finančne podatke ali gesla. Tako goljufiva spletna stran kot elektronsko pismo sta lahko na pogled popolnoma enaka spletni strani ali pismu legitimnega podjetja (npr. banke ali podjetja, ki izdaja kreditne kartice), vendar pa bosta finančne podatke žrtve posredovala tretjim osebam, ki se bodo z njimi okoristile (Informacijski pooblaščenec, 2009).

Da bi bila ta e-poštna sporočila videti še bolj avtentična, lahko njihov avtor priloži povezavo, ki

[2] Razlaga strežnika DNS je na 23. strani diplomskega dela.

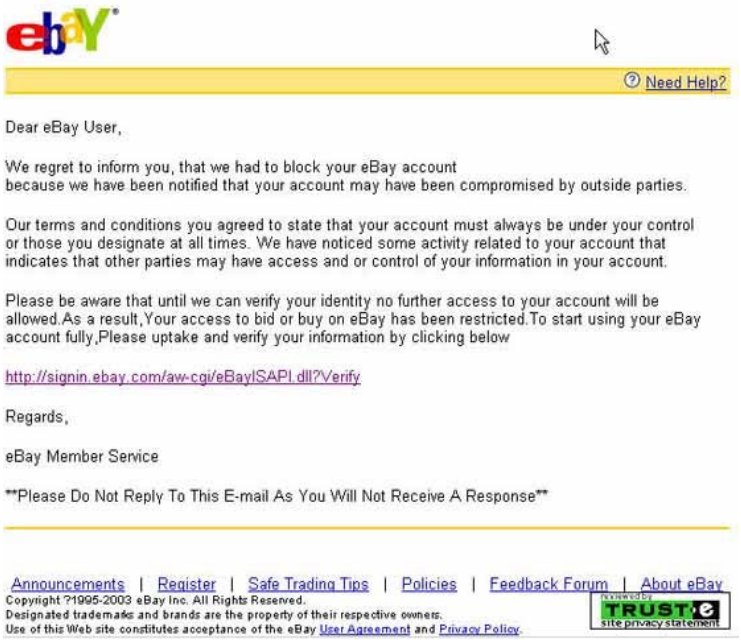
je videti, kot da vodi do pravega spletnega mesta podjetja (npr. banke), v resnici pa vodi do nepravega, ki je videti natanko tako kot pravo. Tem kopijam pogosto pravimo lažna spletna mesta. Ko obiščete eno od teh lažnih mest, lahko nevede vnesete osebne podatke, številke bančnih računov, gesla itd., ki se nato prenesejo neposredno do osebe, ki je spletno mesto ustvarila, ta pa jih lahko uporabi za nakupovanje izdelkov, naroči novo kreditno kartico ali ukrade identiteto žrtve (Informacijski pooblaščenec, 2009).

Vedno bolj pogosti napadi s pomočjo lažnega predstavljanja na uporabnike spletnih bančnih storitev in ostalih spletnih storitev dokazujejo, da so napadi resen varnostni izziv tako za ponudnike storitev na spletu kot tudi za uporabnike teh storitev (Informacijski pooblaščenec, 2009).

3.1 Napad z lažnim predstavljanjem

V prvem koraku prejme žrtev napada z lažnim predstavljanjem elektronsko sporočilo, kot ga lahko vidimo na sliki 1 (Nasvet, 2004).

Slika 1: Lažno elektronsko sporočilo



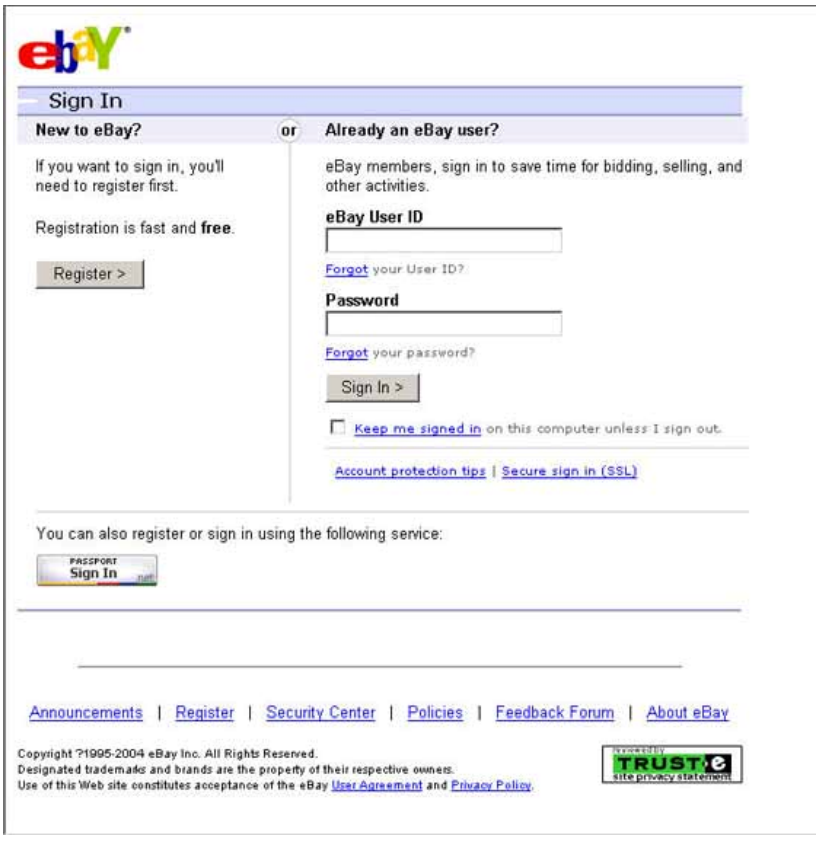
Vir: Akademska in raziskovalna mreža Slovenije (v nadaljevanju ARNES), 2009.

Sporočilo je videti popolnoma pristno, poleg tega pa je vsebina napisana tako, da takoj pritegne uporabnikovo pozornost in mu da vedeti, da gre za izjemno pomembno sporočilo (npr. prejemnik

je tako obveščen, da je njegov bančni račun zaklenjen in da je nujno potrebna potrditev njegove identitete preko spletne strani ali pa da je zaradi vse pogostejših zlorab nujno potrebna zamenjava gesel). Skupna lastnost vseh takšnih prejetih sporočil je, da vsebujejo povezavo do lažne spletne strani, preko katere bi uporabnik posredoval goljufom zaupne podatke (Nasvet, 2004).

V naslednjem koraku (glej sliko 2) goljufi naredijo popolne kopije spletnih strani nekega znanega podjetja (npr. banke ali druge finančne ustanove), s pomočjo skript zagotovijo, da se v naslovni vrstici uporabnikovega brskalnika prikaže nepravi URL-naslov, ki je podoben pravemu naslovu podjetja (npr. www.banka.com/xyz/ in nepozoren uporabnik ne bo opazil, da se nahaja na lažnih straneh), nato pa uporabnika s sporočilom, ki mu ga pošljejo na elektronski naslov, pozovejo k spremembi njegovih podatkov na lažni spletni strani (Nasvet, 2004).

Slika 2: Primer popolne kopije znane spletne strani, ki jo uporablja Ebay



Vir: ARNES, 2009.

Obstajajo primeri, ko elektronsko pismo, ki ga uporabnik prejme, že vsebuje vnosna polja. Tu preusmeritev na ponarejene spletne strani niti ni potrebna. Vneseni podatki bi bili namesto k podjetju "Visa" poslani na nek poštni predal pri podjetju "halfpricehosting.com".

3.2 Zaščita pred napadi z lažni predstavljanjem

Pred goljufijami z lažnim predstavljanjem obstaja nekaj načinov zaščite.

Na različnih spletnih straneh, kot so: ZPS, Microsoft, Nasvet.com, Gambit itd., najdemo veliko opozoril, kako se izogniti goljufiji z lažnim predstavljanjem:

- Nikoli ne odgovarjajte na elektronska pisma, ki od vas zahtevajo osebne in finančne podatke. Prav tako ne sledite povezavam do takšnih spletnih strani. Legitimna podjetja vam takšnih zahtev nikoli ne bodo pošiljala po elektronski pošti ali preko spleta.
- Obiskujte spletna mesta tako, da naslov vnesete URL[3] (npr. www.nlb.si/klik) v naslovno vrstico (in ne preko spletnega brskalnika).
- Osebnih in finančnih podatkov nikoli ne pošiljajte s pomočjo elektronske pošte, saj takšno pošiljanje podatkov ni varno.
- Redno preverjajte izpiske bančnih računov in kreditnih kartic.
- Na računalniku imejte nameščene najnovejše popravke operacijskega sistema in posodobljen protivirusni program.
- Prijavite sumljive zlorabe svojih osebnih podatkov ustreznim uradom.

Cilj vseh spletnih goljufij je kraja denarja (tako posameznikom kot tudi podjetjem). V takšnih primerih poleg izgubljenega denarja posameznikov verodostojnost in ugled izgubijo tudi podjetja, katerih spletne strani so bile ponarejene. To je še posebej škodljivo za spletne storitve finančnega sektorja, saj so te še v začetni fazi in je ena najbolj pomembnih lastnosti zaupanje porabnika v storitev (Nasvet, 2004).

Na številnih spletnih straneh (ena izmed teh je tudi Si-cert) prav tako najdemo mnogo nasvetov, kako se lahko podjetja zavarujejo proti goljufiji z lažnim predstavljanjem:

- Podjetje mora poskrbeti, da bodo stranke natančno vedele, kako jih bo podjetje kontaktiralo in katere informacije bo zahtevalo od njih (tudi preko spleta). Priporočljivo je, da so stranke obveščene, katerih podatkov podjetje od njih ne bo nikoli zahtevalo.
- Podjetja težav z računi strank ne smejo reševati preko elektronske pošte, zlasti če pri tem zahtevajo podatke z računa, številke računov, gesla itd. Pri tovrstnih težavah je obvezen osebni stik podjetja s stranko ali pa kak drug način zanesljive verifikacije.

Prav zaradi neučinkovitosti trenutnih tehnologij za zaščito proti zvabljanju (angl. *pharming*) in lažnemu predstavljanju so v podjetju CONNET, d. o. o., na tem področju odkrili novo tržno nišo in začeli ponujati izboljšano storitev na področju varnosti na spletu.

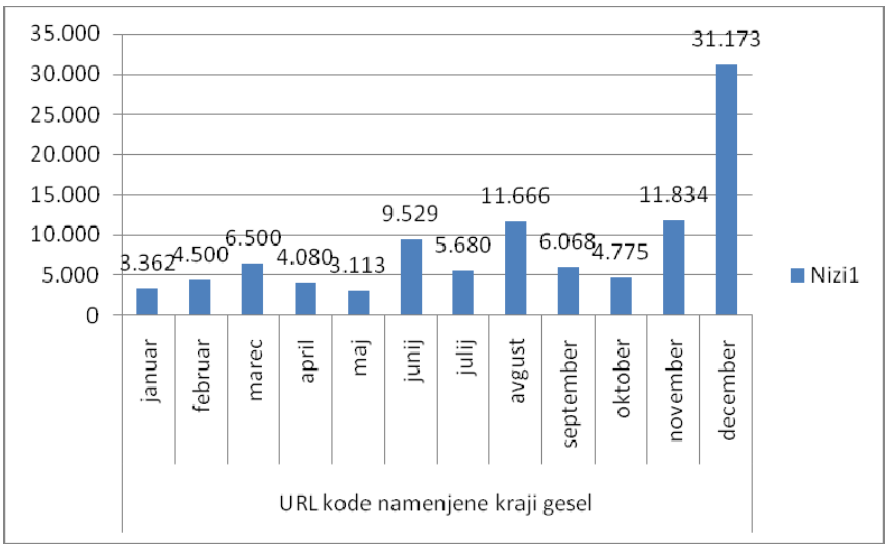
[3] URL – enolični krajevnik vira (angl. *Uniform Resource Locator*) je naslov spletnih strani v svetovnem spletu.

3.3 Lažno predstavljanje v številkah

V letu 2008 je bilo 275.000 prijav spletnega kriminala po svetu, kar je za tretjino več kot leto prej. Tudi slovenska policija opozarja pred goljufi, ki preko spleta ponujajo velik zaslužek. Organizacija Internet Crime Complaint Center, ki deluje v okviru ameriške FBI, je objavila podatke o spletnem kriminalu v letu 2008. V celotnem lanskem letu je bilo globalno približno 275.000 različnih prijav, povezanih s spletnim kriminalom, v letu 2007 pa približno 207.000. Skupno škodo zaradi različnih goljufij se globalno ocenjuje na več kot 260 milijonov dolarjev. Tretjina prijav se je nanašala na spletno nakupovanje, kjer naročniki niso dobili naročenega blaga oziroma je bilo to drugačno od naročenega. Druge prijave so se nanašale predvsem na prevare s kreditnimi karticami (24ur.com, 2009).

V nadaljevanju predstavljam nekaj podatkov o napadih na podjetja, o kraji identitet podjetij, lažnih spletnih straneh in podobnem v drugi polovici leta 2008. Podatke so pridobljeni na spletni strani Anti-Phishing Working Group (krajše APWG). Podatki na sliki 3 se nanašajo na vse države sveta, za katere je APWG pridobil podatke.

Slika 3: Število goljufivih spletnih strani, namenjenih pridobivanju gesel za leto 2008



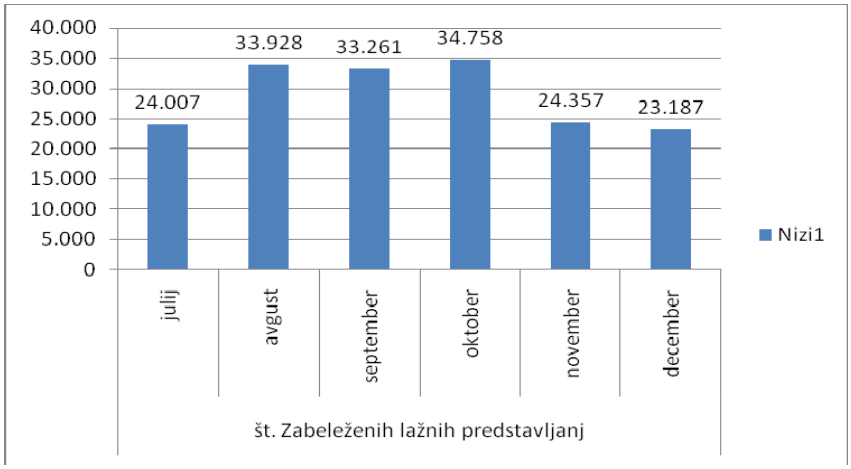
Vir: Anti-Phishing Working Group (v nadaljevanju APWG), 2009.

Število goljufivih spletnih strani, katerih namen je pridobiti gesla in ostale osebne podatke žrtev, je doseglo svoj vrhunec z 31.173 stranmi decembra 2008, kar je za 827 % več kot januarja 2008, ponazorjeno na zgornjem grafu (APWG, 2009).

Na Sliki 4 je prikazano število prejetih poročil o lažnih predstavljanjih za obdobje od julija do

decembra leta 2008. Število prejetih lažnih sporočil je sicer konec leta rahlo upadlo, vendar to ne prikazuje trenda upadanja.

Slika 4: Prejeta poročila na APWG o lažnem predstavljanju za obdobje od julija do decembra 2008



Vir: APWG, 2009.

Poročilo APWG oktobra 2009 poroča o naslednjih zaključkih pri goljufijah z lažnim predstavljanjem (vse države sveta, za katere je APWG pridobil podatke):

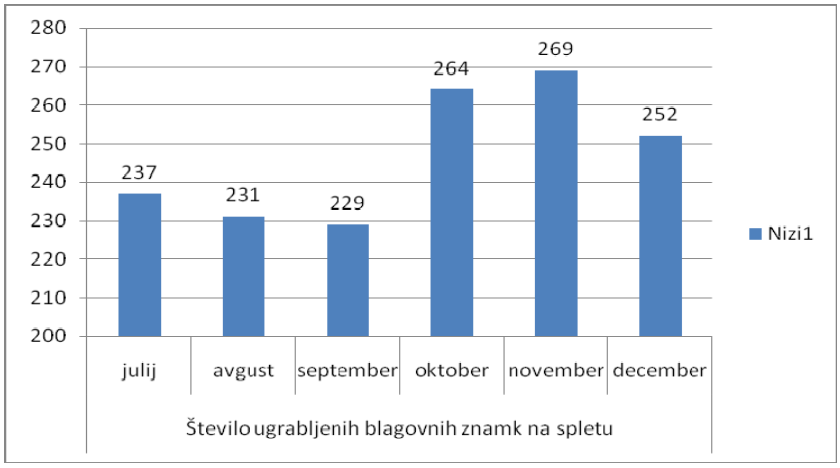
V prvi polovici leta 2009 se je povprečen čas delovanja (angl. *uptime*) posameznih spletnih strani, namenjenih lažnemu predstavljanju, skrajšal v primerjavi z drugo polovico leta 2008. V povprečju se največ napadov z lažnim predstavljanjem pripeti petim domenskim končnicam: .com (50,3 %), .net (8,5 %), .org (5,6 %), .eu (2,9 %) in .ru (2,4 %).

V prvi polovici leta 2009 je bilo prijavljenih 55.698 napadov z lažnim predstavljanjem, kar je zgolj malenkost manj kot v drugi polovici leta 2008, ko je bilo prijavljenih 56.959 tovrstnih napadov. Podatki se nanašajo na vse države sveta, za katere je APWG pridobil podatke (APWG, 2009).

V Sloveniji smo do konca marca 2009 imeli registriranih 67.207 domen. V prvi polovici leta 2009 smo imeli prijavljenih 23 napadov z lažnim predstavljanjem. V tem obdobju je bil povprečen čas delovanja posameznih spletnih strani, namenjenih lažnemu predstavljanju, 56 ur in 31 min (APWG, 2009).

Slika 5 prikazuje krajo identitete podjetjem. Število prijavljenih ukradenih identitet je bilo v obdobju od julija do decembra leta 2008 v povprečju 247 na mesec.

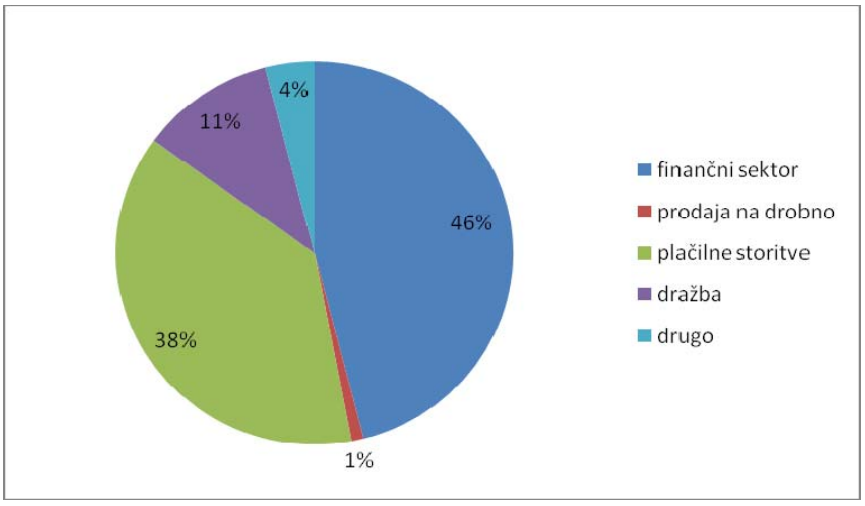
Slika 5: Število kraj identitet blagovnih znamk na mesec za drugo polovico leta 2008



Vir: APWG, 2008.

Na splošno velja, da so žrtve napadov največkrat podjetja iz finančnega sektorja in plačilnih storitev, kar je razvidno iz slike 6.

Slika 6: Največkrat napadeni gospodarski sektorji s strani spletnih goljufov za zadnjo četrtino leta 2008



Vir: APWG, 2009.

Septembra leta 2008 se je prvič zgodilo, da ZDA niso bile država, ki gostuje največ lažnih spletnih strani, povezanih z napadi z lažnim predstavljanjem. Za kratek čas septembra je to bila Švedska, kar je razvidno iz tabele 1.

Tabela 1: Statistični podatki o spletnih goljufijah za drugo polovico leta 2008 na globalni ravni

	JULIJ	AVG.	SEPT.	OKT.	NOV.	DEC.
Število elektronskih sporočil, namenjenih lažnemu predstavljanju (prijave, posredovane od strank APWG)	24.007	33.928	33.261	34.758	24.357	23.187
Število odkritih spletnih strani, namenjenih lažnemu predstavljanju	21.507	26.303	27.209	27.739	19.480	15.709
Število blagovnih znamk, ki jim je bila ukradena identiteta (lažno predstavljanje)	237	231	229	264	269	252
Država,ki gostuje največ spletnih strani, namenjenih lažnemu predstavljanju	ZDA	ZDA	Švedska	ZDA	ZDA	ZDA

Vir: APWG, 2009.

4 ZVABLJANJE (ANGL. *PHARMING*)

Poleg goljufij z lažnim predstavljanjem poznamo tudi obliko napadov, ki ji pravimo zvabljanje (angl. *pharming*). V tem poglavju bo delovanje le-teh podrobneje opisano, zato je treba pred tem razložiti nekaj izrazov:

- **Domena** je niz znakov, ki je registriran na določeno osebo (lastnika) v registru domen in predstavlja spletni naslov, ki se ga uporabi za prikaz določenih spletnih strani. Vsaka domena je unikat v svetovnem merilu, kar pomeni, da je lahko registrirana samo enkrat. Ko podjetje ali fizična oseba registrira domeno, postane njen lastnik in si pridobi ekskluzivno pravico do razpolaganja z domeno. »Končnice domen, kot so: .si, .com, .net, itd. so vrhnje domene v registru domen. Za vsako končnico obstaja register, kjer so zabeležene vse oblike domene, npr. domena1.si, domena2.si, v registru pa je za vsako domeno zapisan tudi lastnik domene ter administrativni in tehnični kontakt. Vsaka domena je usmerjena na strežnike DNS, ki so prav tako vpisani v registru (Domovanje.com).
- **IP-naslov** je številka, ki natančno določa računalnik na spletu. Kratica IP pomeni spletni protokol (angl. *Internet Protocol*). Število je običajno zapisano v (desetiški) obliki, npr. 193.95.198.35 (Microsoft Tech Net, Chapter 3, 2010).
- **URL**-kratica predstavlja enolični krajevnik vira (angl. *Uniform Resource Locators*) in je naslov spletnih strani v svetovnem spletu. Vsaka spletna stran ima edinstven naslov, ki jo določa, prav tako kot enolično določa telefonska številka telefonskega naročnika (Baza znanja Presentia, 2010).
- **Spletni strežnik** (angl. *Web server*) je računalnik za vzdrževanje spletnega mesta na spletu. Ko nekdo obišče spletno mesto in zahteva dokument, nam oddaljeni strežnik začne pošiljati

spletni dokument (How Web Servers Work, 2010).

- **DNS-strežnik** je kratica za sistem domenskih imen (angl. *Domain Name System*). DNS-strežniki služijo za usmerjanje domene na pravi strežnik, kjer se nahaja spletna stran. DNS-strežniki so npr. ns1.domovanje.com, ns2.domovanje.com, ..., ki so prav tako registrirani nazivi v registru in povezujejo ta naziv z IP-naslovom DNS-strežnika. Vsak računalnik na spletu ima lasten naslov, to je IP-številka, ki je sestavljena iz numeričnega niza (npr. www.imedomene.com = 1.1.1.1.). Preko DNS-zapisov na DNS-strežnikih za domeno (npr. domena1.si) spletni brskalnik najde strežnik, na katerem teče spletna stran pod to domeno (Microsoft Tech Net, Chapter 8, 15/3/10).

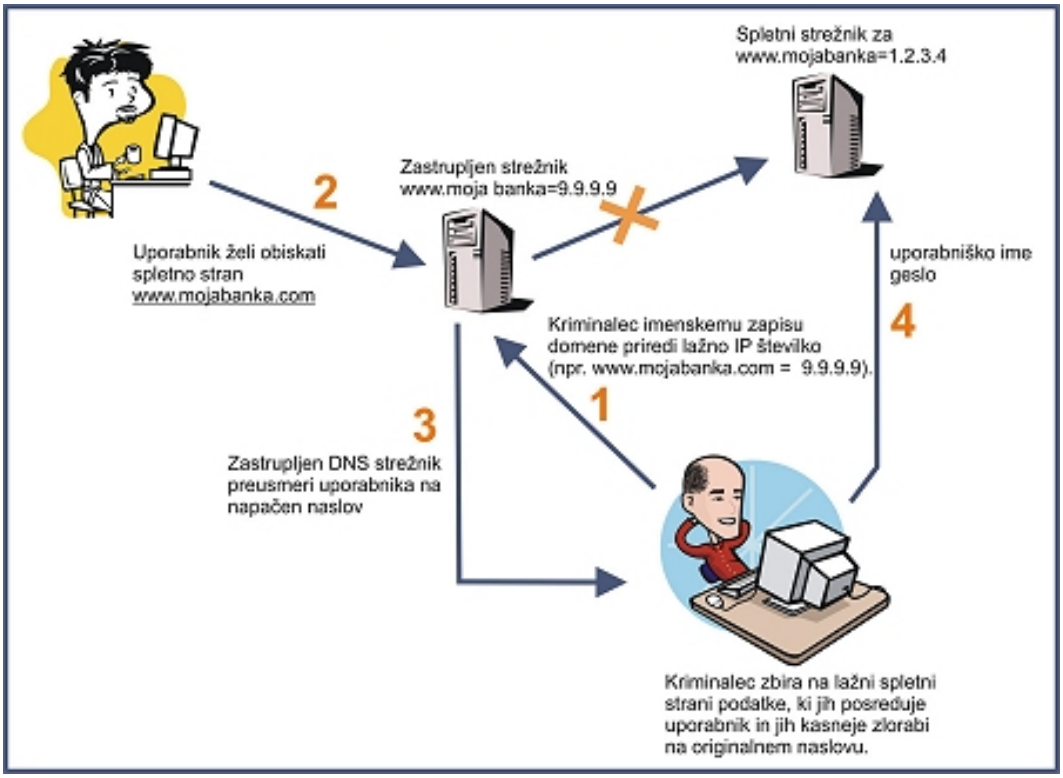
4.1 Delovanje strežnikov DNS

V nadaljevanju bo podrobneje opisano delovanje DNS-strežnikov, saj je le-to pomembno za lažje razumevanje napadov z zvabljanjem. »Ko želi uporabnik obiskati določeno spletno stran, se zahteva po obisku posreduje od njegovega računalnika do najbližjega DNS-strežnika, ki poskrbi za prevod spletnega naslova v ustrezen IP-naslov. Na podlagi uporabnikove zahteve po ogledu določene strani DNS-strežnik preusmeri uporabnika na stran, ki jo želi obiskati. Če strežnik zahtevka ne more razrešiti, ker nima ustreznega zapisa v pretvorbeni tabeli, posreduje zahtevo do drugega strežnika. Zahtevki potujejo naprej tako dolgo, dokler ne dobijo pravega odgovora in dokler računalnik ne dobi nazaj odgovarjajočega IP-naslova za spletno stran, ki jo želimo obiskati. DNS-sistem je bil uveden predvsem zaradi tega, ker si ljudje lažje zapomnimo spletna imena (npr. companyonnet.si), kot pa IP-naslove (npr. 193.77.122.36)« (Nasvet, 2005).

4.2 Delovanje zvabljanja

V prejšnjem poglavju sem podrobneje opisala napade lažnega predstavljanja, ki temeljijo predvsem na ponarejenih e-sporočilih, v primeru zvabljanja pa gre za neposredne napade (brez vabe) na DNS-strežnike ali pa na datoteko o gostiteljih (angl. *hosts file*), ki se nahaja na uporabnikovem računalniku. Posledica takšnih napadov je ta, da so uporabniki preusmerjeni na zlonamerne spletne strani (ne da bi to sploh vedeli), četudi v naslovno vrstico brskalnika pravilno vnesejo URL-naslov strani, ki bi jo radi obiskali. Lažna spletna stran, na kateri se uporabnik znajde, je največkrat popolna kopija originalne, zato uporabnik sploh ne opazi, da se nahaja na lažnem naslovu (goljufi nato brez problemov izvabijo zaupne podatke, kot npr. številke kreditnih kartic, gesla itd.) Slika 7 prikazuje potek napada zvabljanja (Nasvet, 2005).

Slika 7: Prikaz delovanja napada z izvabljanjem



Vir: Pharming napadi, 2009.

Pharming napadi se lahko izvajajo lokalno (na posameznemu računalniku) ali pa neposredno na DNS-strežnikih (v kratkem času lahko doseže veliko število žrtev). Lokalni napadi so veliko bolj nevarni in učinkovitejši od neposrednih, saj bo uporabnik tudi v primeru pravilnega vnosa URL-naslova preusmerjen na lažno stran, ki jo je ustvaril napadalec. V primeru lokalnega napada mora napadalec spremeniti tako imenovano host datoteko[4], ki se nahaja na uporabnikovemu računalniku (v direktoriju C:\WINDOWS\system32\drivers\etc) in ustvariti lažno spletno stran, na katero bo uporabnik preusmerjen. Napadalci pridejo do host datoteke na daljavo ali pa jo prepišejo s pomočjo različnih virusov ali trojancev (kot npr. Bancos, Banker ali Banbra), ki jih največkrat dobimo prek e-pošte (Nasvet, 2005).

4.3 Zaščita pred spletnimi goljufijami

Protivirusni programi so lahko zelo učinkovito sredstvo v boju proti napadom zvabljanja, saj lahko preprečijo okužbo računalnika z virusi, ki lahko spremenijo host datoteko. Žal pa tudi to ni popolna zaščita, saj se ustrezna orodja za odstranitev običajno pojavijo šele takrat, ko so virusi že nekaj časa v računalniku (Nasvet, 2005).

[4] Host datoteka je datoteka brez končnice, ki varuje računalnik pred nezaželenimi spletnimi stranmi.

»Strokovnjaki z varnostnega področja pravijo, da bi se lahko proti napadom lažnega predstavljanja obvarovali tudi tako, da bi spletni brskalniki podali avtentikacijo za identiteto spletne strani, ki jo želimo obiskati. Velik korak naprej na tem področju so naredili pri podjetju Netcraft, kjer so za Internet Explorer izdelali orodno vrstico Netcraft Toolbar (http://toolbar.netcraft.com), ki opozarja uporabnike na potencialno nevarnost napadov in goljufij tako, da prikaže, kdo je lastnik strežnika, na katerem se nahaja obiskana spletna stran in v kateri državi se strežnik nahaja. Če bi npr. želeli opraviti določeno transakcijo v vaši spletni banki, bi verjetno dvakrat premislili, preden bi vtipkali uporabniško ime in geslo, če bi se vam na zaslonu prikazal podatek, da spletna stran banke gostuje na strežniku, ki se nahaja v Rusiji« (Nasvet, 2005).

Peter Lamut, tehnični direktor NiteoWeb, d. o. o., zgoraj omenjeno orodje Netcraft Toolbar,komentira: »Orodna vrstica Netcraft Toolbar lahko pomaga pri odkrivanju goljufij z lažnim predstavljanjem in napadom zvabljanja, žal pa to ni nekaj, kar ta problem tudi rešuje. Na primer: jaz kot ruski goljuf se lahko odločim, da ponaredim neko spletno trgovino. Ker si ne želim, da obiskovalec spletne strani ugotovi, da se lažna spletna stran nahaja v Rusiji, enostavno v Sloveniji zakupim strežnik, na katerega se obiskovalci povezujejo. Ta slovenski strežnik pa nato, v ozadju, dejanske podatke pridobiva iz strežnika v Rusiji. Netcraft Toolbar bo mislil, da se uporabnik povezuje na slovenski strežnik (saj v resnici tudi se), ne bo pa vedel, da se ta slovenski strežnik v ozadju v resnici povezuje v Rusijo.«

5 PODJETJE CONNET, D. O. O.

V nadaljevanju bo predstavljeno podjetje CONNET, d. o. o., in tudi podjetje NiteoWeb, d. o. o., saj je slednje zastopnik za slovenski trg in se tako v veliki meri ukvarja s trženjem storitve CON.

Podjetje CONNET, d. o. o., je bilo ustanovljeno leta 2008 in trenutno nima redno zaposlenih delavcev, temveč se delo opravlja na podlagi drugih pogodb. Sedež podjetja se nahaja v Ljubljani, Tehnološki park 21. Glavna dejavnost podjetja je informacijska varnost, ustanovitelji podjetja pa so: Aleš Lipičnik, Anka Lipičnik, NiteoWeb, d. o. o., Jovica Petković, Marko Vene, Rok Lipičnik, Bojan Črnologar, Miha Kerčmar, Arceres, Razvojne storitve, d. o. o..

Storitev CON je tržno zanimiva, saj prihaja kot unikatna rešitev v času, ko so potrebe po takšni storitvi v svetu vedno večje. Storitev, ki jo je podjetje CONNET, d. o. o., razvilo, odgovarja zakonodaji s področja varovanja osebnih podatkov in varstva potrošnikov – v celotni Evropski skupnosti in čedalje bolj tudi v ZDA.

Kupci storitve CON so podjetja, ki jih skrbi za njihovo varnost in varnost obiskovalcev njihove spletne strani. Koliko kupcev bo storitev dosegla, načrtuje vsak zastopnik sam, pri čemer podjetje CONNET, d. o. o., določi minimalno količino, ki mora biti na trgu prisotna. Anka

Lipičnik dodaja: »Minimalno količino končnih kupcev, ki jih bo storitev dosegla, določimo s pomočjo podatkov o razvitosti spleta v neki državi, številu podjetij, številu uporabnikov spleta ipd.«

5.1 Prednosti in morebitne slabosti

Podjetje je bilo v letu 2008 ustanovljeno, glavna storitev se je takrat šele razvijala in hkrati s tem tudi modeli trženja. Posledica tega je tudi ta, da v tem letu ni bilo prometa.

Ena izmed prednosti podjetja je nagrada na konferenci ISSE (Information Security Solutions Europe) in TeleTrusT nagrada za inovacijo leta. Prav tako je prednost za podjetje CONNET, d. o. o., sprejem v Tehnološki park Ljubljana in dejstvo, da je proizvod informacijskega značaja, s čimer odpade logistika transporta. Podjetje ima lahko sedež kjer koli v državi ali na svetu, tudi na manj razvitih območjih, v kolikor so telekomunikacijska sredstva na voljo. Proizvod ne obremenjuje okolja, je globalen in nosi velik potencial tudi za samo državo Slovenijo.

Slabosti podjetja so nezadostne količine kapitala, ki bi pripomogel k hitrejšemu razvoju. Prav tako je slabost storitve, ki zagotavlja varnost, ta, da večino podjetij razmišlja predvsem o donosu, torej koliko jim določena investicija povrne. Storitev, ki ponuja varnost, pa ne zagotavlja nikakršnega donosa, temveč zgolj zmanjšuje potencialno izgubo donosa. To je slabost, saj je veliko teže prodati storitev, ki zgolj zmanjšuje izgubo, kot pa storitev, ki prinaša donos.

5.2 Konkurenca

Glavni konkurenti podjetja CONNET, d. o. o., so podjetja, ki se ukvarjajo z varnostjo na spletu. To so podjetja, ki prodajajo oz. izdajajo SSL-certifikate: Verisign, Thawte, Geotrust, Comodo in ostali izdajatelji SSL-certifikatov.

Kaj SSL-certifikat sploh je? To je digitalno potrdilo, ki omogoča kodiranje podatkov med strežnikom in odjemalcem preko SSL-protokola. Praktično gledano je potrdilo datoteka, ki prebiva na strežniku. Potrdilo vsebuje informacije o njegovemu imetniku in izdajatelju (Neoserv, 2009).

Storitev CON najbolj izstopa po kakovosti informacij, ki jih dobi obiskovalec. Večina podobnih storitev temelji na tem, da podjetja sama preverjajo informacije o podjetjih, za katera nato izdajajo certifikate. Slabost takšnega preverjanja je, da obiskovalec ne ve, kako natančno oz. površno so bile informacije preverjene. Pri storitvi CON pa informacije preverja zunanja lokalna ustanova, na področju Slovenije je to GZS.

Storitev CON je trenutno edina storitev v svetovnem merilu, ki obiskovalcu nedvoumno zagotavlja verificirano identiteto lastnika spletne strani.

6 PODROBEN OPIS STORITVE COMPANY ON NET (CON)

Osnovni elementi verifikacijskega sistema so trije (Company on Net, 2009):

- pečat na komercialni strani podjetja,
- certifikat,
- verificirana spletna stran na verificirani domeni.

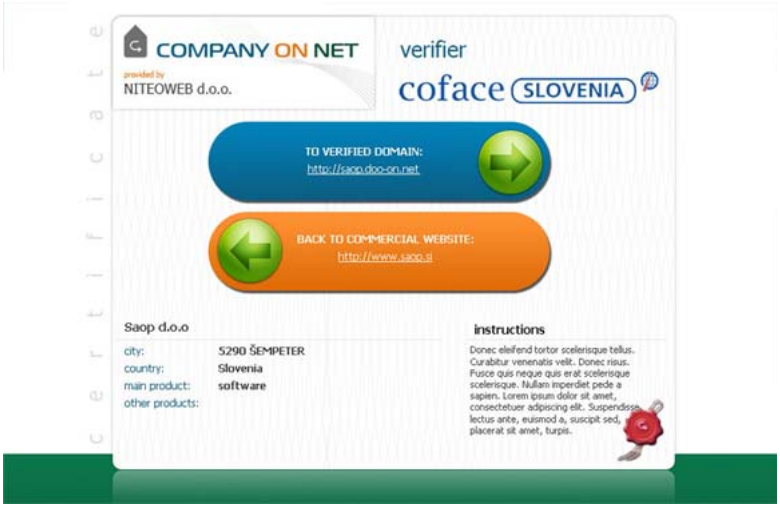
Kakšen je videti pečat oz. kako lahko uporabnik prepozna: v pečatu je naveden isti www naslov strani kot v brskalniku, v pečatu sta navedena trenutna ura in datum, pečat vodi na certifikat, kjer se avtentičnost pečata znova preveri, in nazadnje se zgoraj desno pod napisom Company on Net nahaja še štirimestna koda, ki mora biti identična kodi na certifikatu, ki se odpre ob kliku na pečat. Na sliki 8 je prikazan omenjeni pečat.

Slika 8: Pečat na komercialni strani

Vir: Podroben opis delovanja sistema, 2009.

Ob kliku na pečat lahko uporabnik preveri identiteto podjetja oz. lastnika spletne strani. Klik vodi na certifikat, ki ga prikazuje slika 9.

Slika 9: Odprt pečat na komercialni strani

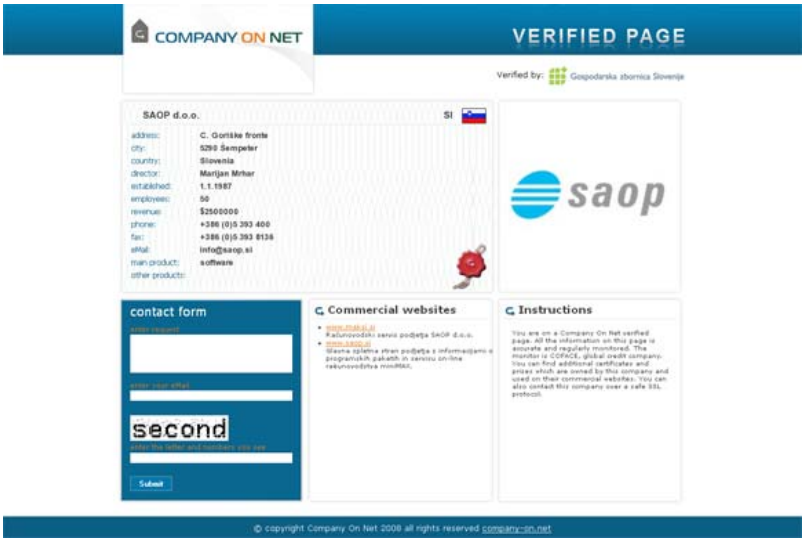


Vir: Podroben opis delovanja sistema, 2009

Certifikat je spletna stran, varovana z SSL-protokolom. Vsak pečat ima prirejeno svojo stran s certifikatom, na kateri se nahajata dve povezavi. Prva povezava kaže nazaj na stran, kjer se nahaja pečat, in druga naprej na verificirano stran podjetja. Zgoraj desno se nahaja tudi štirimestna koda, ki se ujema s kodo na pečatu, omenjeno pri sliki 8.

Na certifikatu so zapisani tudi osnovni podatki o podjetju, ki uporablja storitev (glej sliko 10). Podjetje s tem svoje uporabnike zaščiti pred napadi lažnega predstavljanja, saj s certifikata obe povezavi uporabnika usmerita na prave strani, ki so resnično v lasti tega podjetja. V primeru, da obiskovalec preko povezave na certifikatu pride na drugo komercialno stran in ne nazaj na tisto, s katere je prišel, mora zaupa povezavi s certifikata.

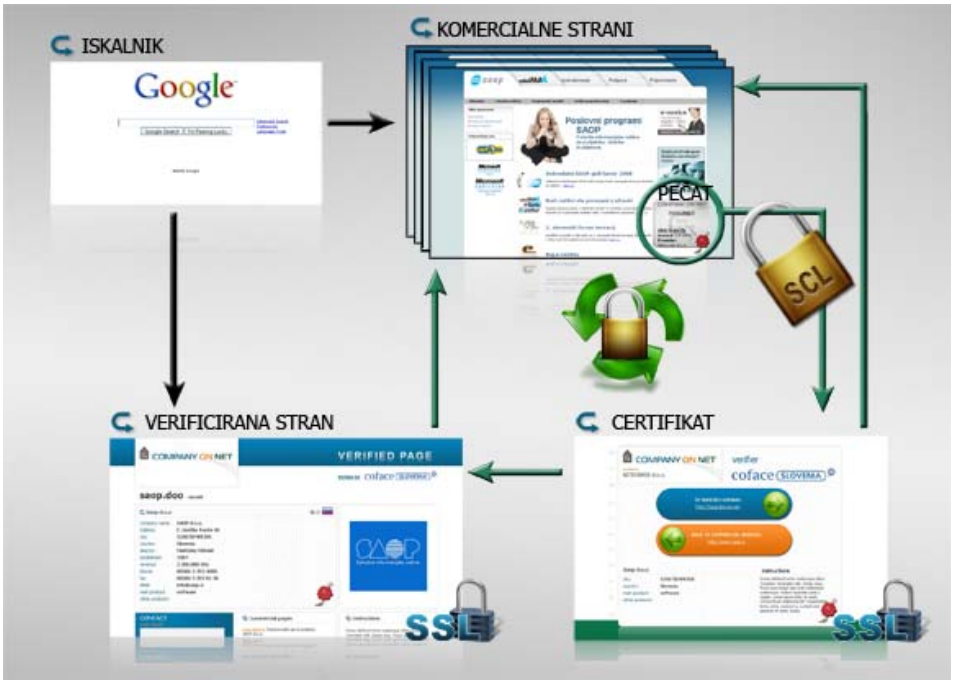
Slika 10: Verificirana spletna stran na verificirani domeni



Vir: Podroben opis delovanja sistema, 2009.

Povezava s certifikata obiskovalca vodi tudi na verificirano spletno stran, ki se nahaja na verificirani domeni. Tukaj se nahajajo zanesljivi in točni podatki o podjetju ter komercialnih domenah, ki jih podjetje uporablja. Prav tako se na tej strani nahajajo in so dodatno preverjeni vsi pečati in zunanji certifikati, ki jih podjetje uporablja na svojih spletnih straneh. Namen verificirane spletne strani je, da lahko obiskovalec po varni poti komunicira s podjetjem, lastnikom verificirane domene.

Slika 11: Celoten zaključen krog preverjanja certifikata



Vir: Podroben opis delovanja sistema, 2009.

Slika 11 prikazuje celoten ciklus: v iskalniku na ključne besede imena podjetja ali dejavnosti najdemo komercialne spletne strani podjetja. Na komercialnih straneh se nahaja pečat CON in ob kliku na pečat se uporabniku odpre certifikat tega podjetja. S certifikata pa v nadaljevanju lahko pride nazaj na komercialno stran ali pa nadaljuje na verificirano stran podjetja.

Storitev CON vsebuje varen kontaktni obrazec, ki ščiti prenos podatkov med stranko in podjetjem tako, da tretja oseba ne more prenesenih podatkov izrabiti v svoje namene. Zunanji verifikator, to je GZS, poskrbi za kredibilno predstavitev uporabnikovega podjetja na verificirani spletni strani. Osnovna storitev na letni ravni stane 197 EUR. Ob porastu spletnega kriminala vedno večjo vlogo pri spletni predstavitvi podjetja igra zaupanje, za katerega mora podjetje, ki je lastnik spletne strani, poskrbeti tako ali drugače. Sistem CON zavaruje uporabnikovo podjetje in obiskovalce teh spletnih strani pred različnimi oblikami spletnega kriminala. Največji vzrok za hitro širitev spletnega kriminala je prosta komercialnost domen (vsakdo lahko kupi domeno in jo poimenuje po lastni izbiri, npr.: ljubljanska_banka.si) in možnost popolne anonimnosti ob lastništvu le-teh.

7 TRŽENJSKA RAZISKAVA ZA PODJETJE CONNET, D. O. O.

V tem poglavju bodo najprej opredeljeni cilji raziskave, nato bo opisan postopek njene izvedbe in na koncu bodo oblikovane domneve.

Za dobro poslovanje podjetja so zelo pomembne informacije, ki jih podjetje pridobi s trženjskimi raziskavami, in ker se v podjetju CONNET, d. o. o., zavedajo pomembnosti takšnih informacij, so se odločili za raziskavo, ki sem jo izvedla po njihovem naročilu.

Kotler (1998, str. 130) definira trženjsko raziskavo, kot »sistematično načrtovanje, zbiranje in analizo podatkov, ki se nanašajo na določene za podjetje pomembne trženjske razmere ter poročanje o rezultatih.« Pri raziskavi za podjetje CONNET, d. o. o., sem si pomagala s procesom učinkovitega trženjskega raziskovanja, ki po Kotlerju (1998, str.131-140) zajema pet stopenj:

1. opredelitev problema in ciljev raziskave,
2. načrtovanje raziskave,
3. zbiranje informacij,
4. analiza informacij,
5. predstavitev informacij.

7.1 Cilji raziskave

Prva stopnja pri trženjski raziskavi je opredelitev problema in ciljev raziskave (Kotler, 1998, str. 131). Glavni cilj raziskave je ugotoviti, koliko se slovenska podjetja zavedajo nevarnosti na spletu in kakšno je zanimanje za nakup storitve CON. Podjetje CONNET, d. o. o., naročnika raziskave, zanima:

- Kako varno se počutijo slovenska podjetja na spletu?
- Koliko so v podjetjih pripravljeni plačati za pečat, ki bi jih v veliki meri ščitil pred spletnimi goljufijami?
- Ali v podjetjih zaposleni vedo, kakšne nevarnosti obstajajo na spletu?
- V kakšne namene podjetja uporabljajo spletne strani?
- V kolikšni meri zaupajo elektronskim sporočilom?
- Kdo v podjetju odloča o nakupu storitev za zaščito na spletu?

S pomočjo raziskave bom poizkušala odgovoriti na zgoraj zastavljena vprašanja.

7.2 Izvedba raziskave

Pri drugi stopnji trženjske raziskave je treba sestaviti načrt za pridobivanje podatkov. Zasnovo druge stopnje predstavljajo: viri podatkov, raziskovalne metode, raziskovalni instrumenti, načrt

vzorčenja in oblike komuniciranja (Kotler, 1998, str. 133).

7.2.1 Čas izvedbe raziskave

V začetnem delu raziskave sem se sestala z razvojnima vodjema Petrom Lamutom in Nejcem Zupanom in se z njima dogovorila o ciljih raziskave. Kasneje sem se sestala še z ustanoviteljico podjetja CONNET d. o. o., Anko Lipičnik, ki mi je bolj podrobno predstavila storitev CON in podjetje CONNET, d. o. o.. Zbiranje podatkov preko elektronske pošte je potekalo od konca oktobra 2009 do začetka decembra 2009, celotna izvedba raziskave pa od sredine septembra 2009 do februarja 2010.

7.2.2 Viri podatkov pri izvedbi raziskave

Pri raziskavi je smiselno najprej preveriti sekundarne podatke. Pod ta termin spadajo že obstoječi podatki, zbrani z nekim drugim namenom. Če sekundarni podatki raziskovalcu ne zadostujejo, se loti zbiranja primarnih podatkov, ki jih pridobi s pomočjo intervjujev, anket, poizkusov in ostalimi metodami (Kotler, 1998, str. 133–135).

Pri izvedbi trženjske raziskave sem si v veliki meri pomagala s primarnimi podatki, saj na temo spletnih goljufij v Sloveniji nisem našla veliko literature, prav tako na to temo v zadnjem času ni bilo izvedenih veliko raziskav, do katerih bi imela dostop. Največ informacij sem dobila preko spleta in časopisov. Na področju spletnih goljufij še ne obstaja dovolj sekundarnih podatkov, ki bi mi pomagali pri raziskavi.

S pomočjo neformalnih pogovorov z vodilnimi v podjetju sem prišla do koristnih informacij, s pomočjo katerih sem kasneje postavila cilje raziskave in domneve ter sestavila vprašalnik za anketiranje. Primarne podatke sem dobila s pomočjo anketiranja preko elektronske pošte in s pomočjo pogovorov z vodstvom podjetja CONNET, d. o. o. Pri zbiranju podatkov s pomočjo anketiranja preko elektronske pošte sem si pomagala z vprašalnikom (glej prilogo 2).

7.2.3 Vsebina vprašalnika

Vprašalnik je pogost raziskovalni instrument zaradi možnosti oblikovanja vprašanj na najrazličnejše načine, kar poveča fleksibilnost raziskovalnega instrumenta (Kotler, 1998, str. 136).

Vprašalnik je sestavljen iz šestnajstih vprašanj zaprtega tipa (vprašanja z več možnimi odgovori, Likertova lestvica itd.) in je razdeljen na štiri sklope. Prvi sklop je sestavljen iz vprašanj o obstoju spletne strani pri posameznih podjetjih, številu obiskovalcev na spletnih straneh podjetij in o namembnosti teh spletnih strani. V drugem sklopu so vprašanja o poznavanju spletnih

goljufij, o varnosti na spletu itd. S tretjim sklopom sem poizkušala ugotoviti, ali so v podjetju pripravljeni investirati v pečat, ki bi podjetje v veliki meri zaščitil pred spletnimi goljufijami, in o primernosti cene takšnega pečata. V zadnjem sklopu vprašalnika pa se nahajajo demografska vprašanja o velikosti podjetja, o delovnem mestu anketiranca in nazadnje še o dejavnosti podjetja (priloga 2).

7.2.4 Vzorec

Zaradi nizkih stroškov, hitrega odziva in velike geografske pokritosti sem se odločila za zbiranje podatkov preko elektronske pošte. Vprašalnik sem razposlala na 706 naslovov podjetij, ki mi jih je priskrbelo podjetje CONNET, d. o. o., in dodatnih 62 naslovov podjetij, ki imajo spletno trgovino, in sem jih poiskala preko spletnih brskalnikov. Podjetje CONNET, d. o. o., mi je priskrbelo podatke s pomočjo baze podatkov iPIS Marketing Manager. Končno število poslanih elektronskih sporočil je bilo 768. Pri načrtu raziskave sem upoštevala bazo podatkov, ki mi jo je posredovalo podjetje CONNET, d. o. o., in je vsebovala imena in elektronske naslove podjetij, ki so bila razvrščena po slovenskih regijah (gorenjska, goriška, koroška, kraška, ljubljanska, dravska, obalna, pomurska, savinjska, vzhodna in zasavska). Zaradi velikega števila majhnih podjetij in majhnega števila podjetij s spletno trgovino v omenjeni bazi sem naknadno zbrala še nekaj elektronskih naslovov podjetij, ki imajo spletno trgovino registrirano v Sloveniji, in tako prišla do že omenjenih 768 poslanih elektronskih sporočil. Sporočila sem pošiljala na splošne elektronske naslove oz. *info maile* in na naslove informacijskih oddelkov v podjetjih (v primerih, kjer sem imela podatek na voljo). Odzivnost je bila 9 %, kar pomeni, da sem imela v vzorec zajetih zgolj 85 podjetij.

7.2.5 Postavitev domnev

Spodaj navedene domneve sem postavila v skladu s predhodno omenjenimi cilji raziskave:

- H1a: Večja podjetja uporabljajo več mehanizmov za zaščito proti spletnemu kriminalu.
- H1b: Večjim podjetjem se zdi cena 200 EUR na leto za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, bolj primerna kot manjšim podjetjem.
- H1c: Velikost podjetja vpliva na ozaveščenost v podjetju glede različnih vrst spletnih goljufij.

Po pogovoru s tehničnim direktorjem Nejcem Zupanom sem prišla do zaključka, da podjetja težko investirajo v kakršno koli vrsto zaščite, saj tovrstne storitve podjetju ne prinašajo neposrednega dobička. Predpostavljam, da je večjim podjetjem laže investirati 200 EUR letno kot manjšim podjetjem. Prav zaradi tega predpostavljam tudi to, da večja podjetja uporabljajo več zaščit proti spletnemu kriminalu kot manjša podjetja. Pri zadnjem, tretjem delu domneve predpostavljam, da v kolikor se v podjetju zanimajo za investicije v spletno zaščito, potemtakem obveščajo svoje delavce o možnih nevarnostih in goljufijah na spletu.

- H2a: Podjetja, ki nimajo spletne strani, menijo, da je cena 200 EUR na leto manj primerna za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami.
- H2b: Podjetja, ki nimajo spletne strani, slabše poznajo spletne goljufije kot podjetja, ki imajo spletno stran.
- H2c: V podjetjih, kjer nimajo spletne strani, zaposlene manj skrbi, da bi njihovo podjetje postalo žrtev spletne goljufije.

Predpostavljam, da v podjetju, kjer nimajo spletne strani, ne bodo pripravljeni investirati v pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, saj ga pravzaprav ne potrebujejo. Prav tako predpostavljam, da podjetja, ki nimajo spletne strani, slabo poznajo spletne goljufije. Kljub temu da v podjetju nimajo spletne strani, lahko podjetje kaj hitro postane žrtev goljufije z lažnim predstavljanjem (ali katere izmed ostalih spletnih goljufij), saj podjetje vseeno sodeluje s partnerji in zunanjimi sodelavci preko elektronske pošte. Kljub temu predpostavljam, da bo zaposlene v podjetju, kjer nimajo spletne strani, manj skrbelo, da bi njihovo podjetje postalo žrtev spletne goljufije.

- H3a: Večje število obiskovalcev na spletni strani podjetja vpliva na to, da podjetja bolj skrbi, da bi postali žrtev katere izmed spletnih goljufij.
- H3b: Večje število obiskovalcev na spletni strani podjetja vpliva na večjo ozaveščenost zaposlenih o vrstah spletnih goljufij.
- H3c: Večje število obiskovalcev na spletni strani podjetja vpliva na to, da so v podjetju mnenja, da je cena 200 EUR na leto bolj primerna za pečat, ki bi podjetje v veliki meri zaščitil pred spletnimi goljufijami.

Podjetja, ki beležijo večje število obiskovalcev na svoji spletni strani, so bolj podvržena morebitnemu slabemu imenu zaradi spletnega kriminala vandalizma ali goljufij. Predvidevam, da takšna podjetja bolj skrbi, da bi postali žrtev katere izmed spletnih goljufij. Predpostavljam, da večje število obiskovalcev na spletni strani podjetja vpliva na večjo ozaveščenost zaposlenih o vrstah spletnih goljufij. Prav tako predpostavljam, da v primeru, ko ima podjetje večje število obiskovalcev na svoji spletni strani, vpliva na to, da so v podjetju mnenja, da je cena 200 EUR na leto primerna za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami.

8 REZULTATI RAZISKAVE

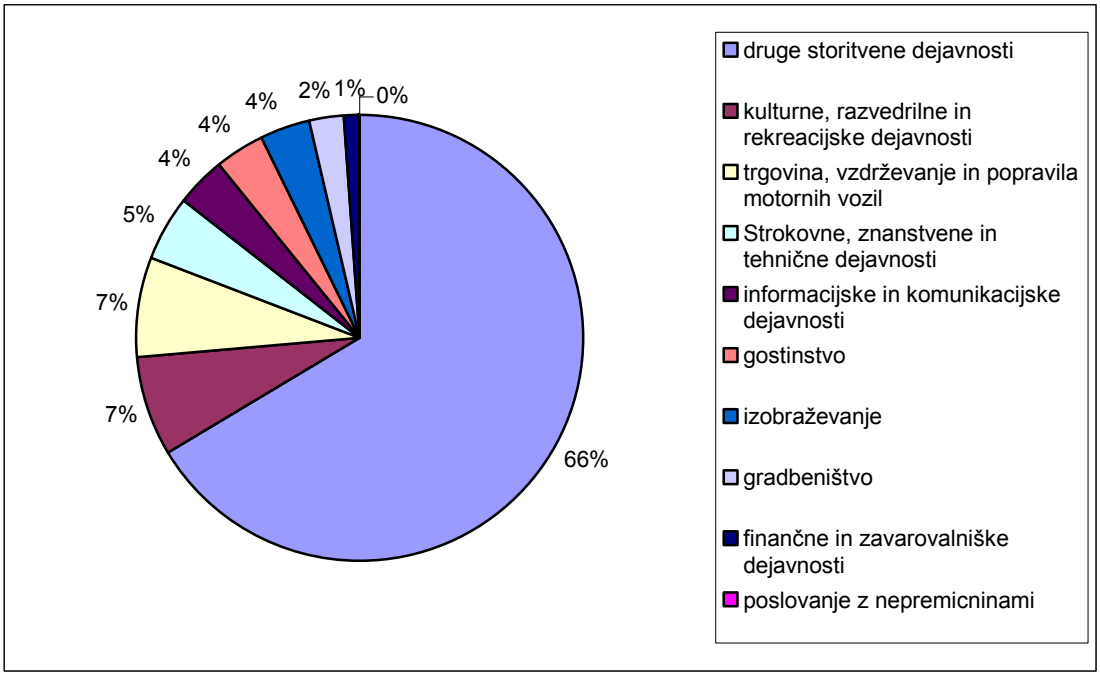
Podatke, ki sem jih pridobila z anketiranjem, sem obdelala s programom SPSS for Windows 15 in s programom Microsoft Office Excel 2007. Pri predstavitvi rezultatov bom najprej opisala vzorec, nato bom predstavila vprašanja, ki so dala najbolj zanimive rezultate, sledilo bo preizkušanje domnev in na koncu še povzetek najpomembnejših ugotovitev.

8.1 Vzorec

V anketi je sodelovalo 85 podjetij. Vzorec je zajemal 72 (85 %) podjetij, ki imajo vsaj eno spletno stran in 13 (15 %) podjetij, ki nimajo svojih spletnih strani (glej prilogo 3.1).

Vzorec je zajemal kar 66 % podjetij, ki so se opredelila kot druge storitvene dejavnosti, sledila so podjetja, ki so se opredelila kot dejavnosti trgovine, vzdrževanja in popravil motornih vozil (7 %), in podjetja v kulturnih, razvedrilnih in rekreacijskih dejavnostih s 7 %. Strukturo vzorca po dejavnostih podjetij kaže slika 12.

Slika 12: Dejavnost podjetja

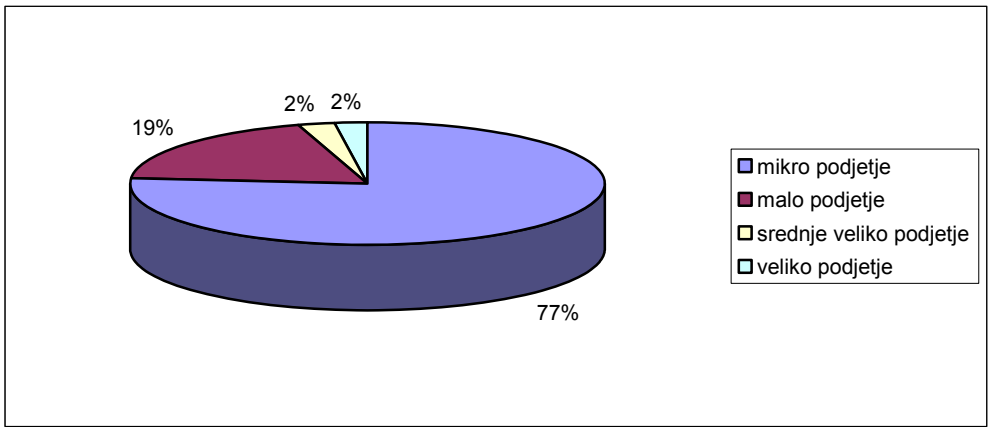


Vir: Podatki iz ankete, 2009.

Na vprašalnik so v večini odgovarjali direktorji podjetij (43,5 %), vodje (15,3 %) in zaposleni v informacijski službi (12,9 %). Vzorec je zajemal tudi zaposlene v oddelku za trženje (11,8 %), zaposlene v drugih oddelkih (11,8 %), v finančni službi (2,3 %) in zaposlene v računovodstvu (2,3 %) (glej prilogo 3.2).

Največ podjetij v vzorcu, kar 76,5 %, je bilo mikro podjetij, ki štejejo do 9 zaposlenih, sledijo jim mala podjetja (18,9 %) s številom zaposlenih od 10 do 49. Vzorec je zajemal zgolj 2,3 % srednje velikih podjetij s številom zaposlenih od 50 do 249 in prav tolikšen odstotek velikih podjetij. Strukturo vzorca po velikosti podjetij prikazuje slika 13.

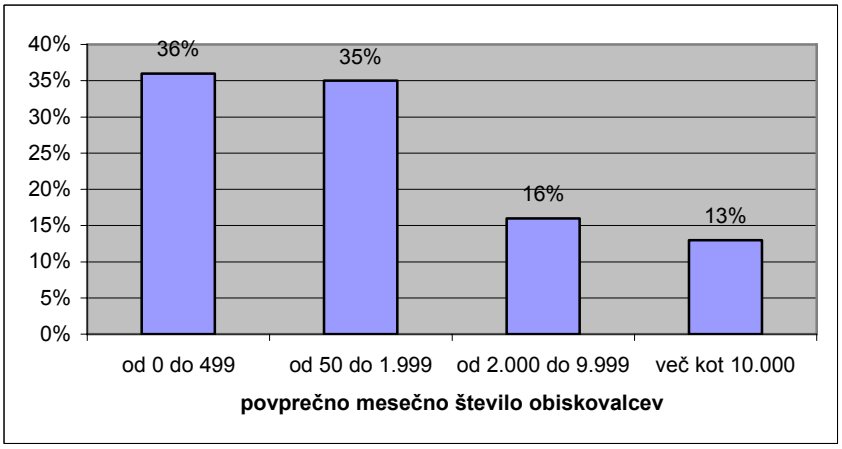
Slika 13: Velikost podjetij po številu zaposlenih



Vir: Podatki iz ankete, 2009.

Podjetij, ki na vprašanje, koliko obiskovalcev v povprečju zabeležijo na svoji spletni strani na mesečni ravni, ni znalo odgovoriti, je bilo 35,3 %. 23,5 % podjetij se je razvrstilo v prvi razred, 22,3 % v drugi, 10,6 % v tretji in 8,2 % v četrti razred. Prvi razred predstavlja od 0 do 499 obiskovalcev na mesečni ravni, drugi razred od 500 do 1.999 obiskovalcev, tretji razred od 2.000 do 9.999 obiskovalcev in četrti razred več kot 10.000 obiskovalcev na mesečni ravni. Na sliki 16 sem prikazala strukturo obiskovalcev na spletnih straneh podjetij, vendar sem upoštevala zgolj strukturo tistih podjetij, ki so znala odgovoriti na vprašanje.

Slika 14: Povprečno mesečno število obiskovalcev na spletnih straneh podjetij



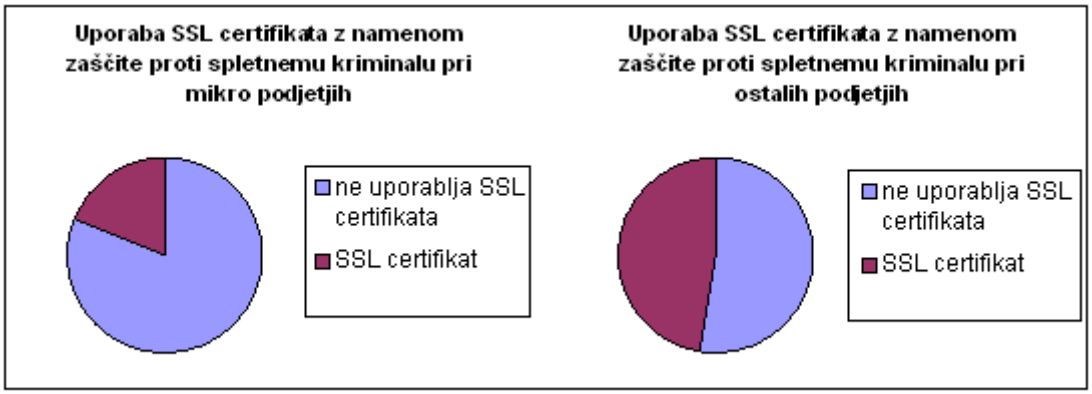
Vir: Podatki iz ankete, 2009.

8.2 Analiza izbranih vprašanj

Pri 11. vprašanju, ki se nanaša na uporabo zaščite, sem podrobneje preučila povezavo med velikostjo podjetja in zaščito, ki jo podjetja uporabljajo proti spletnemu kriminalu. Zaradi premajhnih frekvenc v posameznih celicah, sem le-te združila v dve kategoriji: mikro podjetja in ostala podjetja. V skupini mikro podjetja so zajeta zgolj mikro podjetja, v skupini ostala podjetja pa mala, srednje velika in velika podjetja.

Kot je razvidno iz slike 15, večina mikro podjetij ne uporablja SSL-certifikatov kot enega izmed mehanizmov za zaščito proti spletnemu kriminalu, saj kar 81,3 % mikro podjetij ne uporablja omenjene zaščite. V nasprotju pa ostala podjetja tovrstno zaščito uporabljajo bolj pogosto, in sicer kar 47,6 % vseh ostalih v vzorec zajetih podjetij.

Slika 15: Uporaba SSL-certifikata z namenom zaščite proti spletnemu kriminalu pri mikro in ostalih podjetjih



Vir: Podatki iz ankete, 2009.

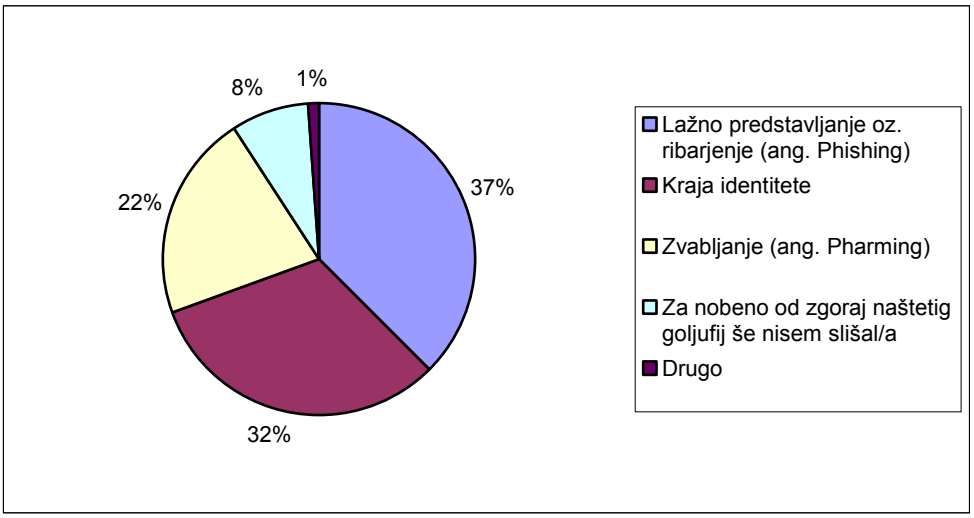
Do podobnih rezultatov sem prišla tudi pri primerjanju velikosti podjetij in uporabi nikakršne dodatne zaščite proti spletnemu kriminalu. Iz slike 16 je razvidno, da 6,8 % mikro podjetij ne uporablja nikakršne dodatne zaščite. Pri ostalih podjetjih je ta odstotek nižji, 2,2 % ostalih podjetij ne uporablja nikakršne dodatne zaščite. Pri tem vprašanju sem prišla do zaključka, da velika večina podjetij (89,6 %), zajetih v vzorec, uporablja dodatno zaščito proti spletnemu kriminalu.

Slika 16: Uporaba dodatnih zaščit proti spletnemu kriminalu v mikro in ostalih podjetjih

Vir: Podatki iz ankete, 2009.

Z anketo sem želela preveriti tudi, kako ozaveščena so podjetja o spletnih goljufijah. Pri 5. vprašanju, sem preverila, za katere vrste spletnih goljufij so podjetja že slišala oz. jih poznajo. Na voljo je bilo več možnih odgovorov, anketirana podjetja pa so lahko izbirala med sledečimi odgovori: (a) lažno predstavljanje oz. ribarjenje (angl. *phishing*), (b) zvabljanje (angl. *pharming*), (c) kraja identitete, (d) za nobeno od zgoraj naštetih goljufij še nisem slišal/-a in (e) drugo. Najbolj prepoznani spletni goljufiji sta bili lažno predstavljanje (37 %) in kraja identitete (32 %), nekoliko manj prepoznano pa je bilo zvabljanje (22 %), kar prikazuje slika 17.

Slika 17: Prepoznavanje spletnih goljufij

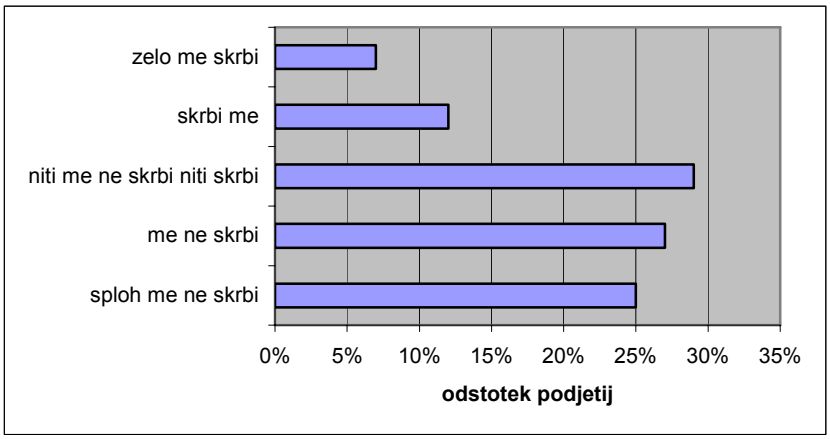


Vir: Podatki iz ankete, 2009.

Iz slike 18 je razvidno, da se podjetja v veliki meri počutijo varna, torej jih ne skrbi, da bodo

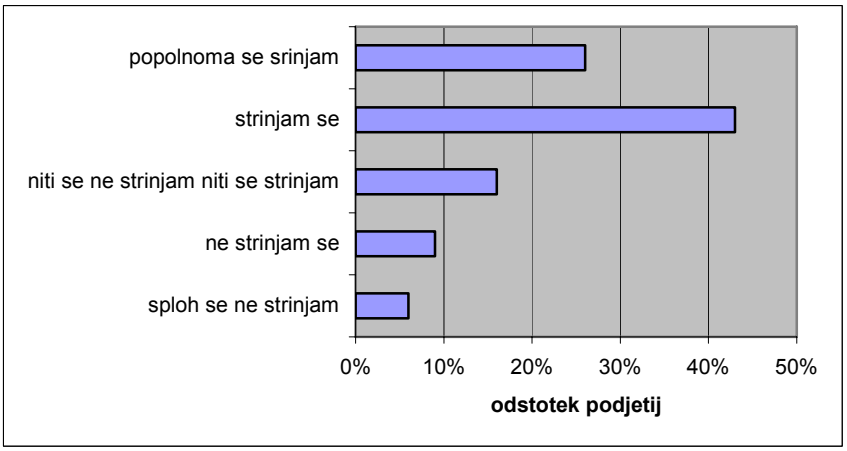
postali žrtev spletne goljufije, kar je razvidno tudi iz povprečne stopnje strinjanja, ki je bila 2,5 (1 = sploh nisem zaskrbljen/-a in 5 = zelo sem zaskrbljen/-a). Kljub temu pa se strinjajo, da spletni kriminal predstavlja resno nevarnost. Kot je prikazano na sliki 19 se večina podjetij (69 %) popolnoma strinja ali strinja s trditvijo, da spletni kriminal za podjetja predstavlja vedno večji problem. Povprečna stopnja strinjanja na 5-stopenjski lestvici je znašala 3,7.

Slika 18: Kako močno podjetja skrbi, da bi postali žrtve katere izmed spletnih goljufij



Vir: Podatki iz ankete, 2009.

Slika 19: Strinjanje s trditvijo, da spletni kriminal za podjetja predstavlja vedno večji problem



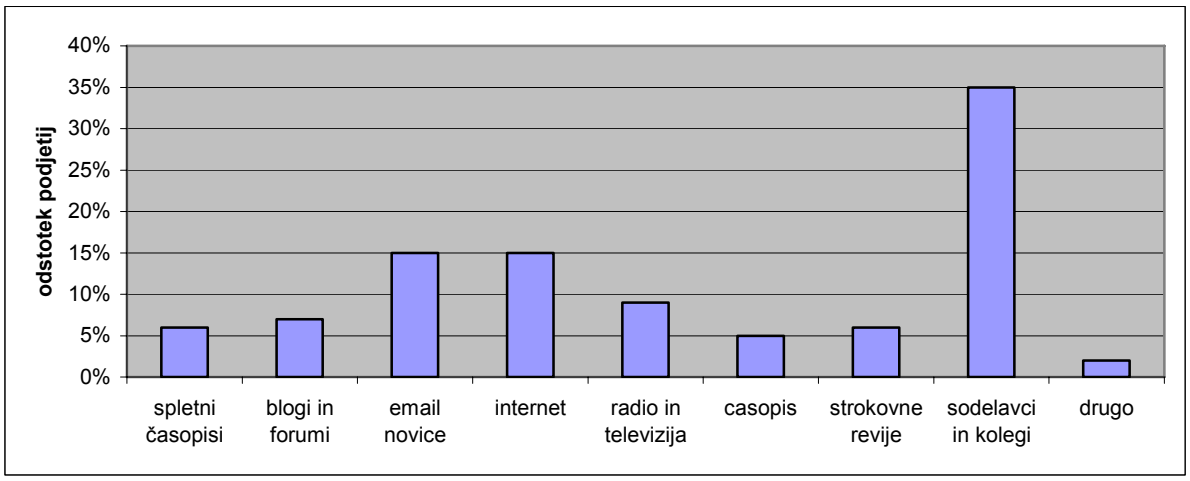
Vir: Podatki iz ankete, 2009.

Kot zanimivost bi k zgornjim rezultatom rada dodala še, da je 7 (8,2 %) podjetij v vzorcu že bilo žrtev spletnih goljufij, 69 (81,2 %) podjetij do zdaj še ni bilo žrtev nikakršne spletne goljufije, 9 (10,9 %) podjetij pa ni imelo podatka o tem, ali so že bili žrtev spletne goljufije ali ne (glej

prilogo 3.3).

Zaradi kasnejših možnih sklepov, sem podjetjem zastavila tudi vprašanje, kje dobijo največ informacij o varnosti na spletu in o zaščitah proti spletnim goljufijam. Največ podjetij (34,1 %) dobi največ tovrstnih informacij preko sodelavcev in kolegov. Preko spleta dobi informacije 15,3 % podjetij in prav toliko preko spletne pošte. Najmanj informacij o spletnih goljufijah podjetja pridobijo s pomočjo časopisov. Struktura podjetij po virih informacij o zaščiti na spletu in informacij o spletnih goljufijah je razvidna iz slike 20.

Slika 20: Kje podjetja dobijo največ informacij o varnosti na spletu in o zaščitah proti spletnim goljufijam



Vir: Podatki iz ankete, 2009.

Ali so podjetja pripravljena kupiti pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, sem želela ugotoviti s 7. in 12. vprašanjem. Pri 12. vprašanju, kjer sprašujem, ali bi v podjetju bili pripravljeni investirati v pečat, je 41,2 % podjetij odgovorilo pritrdilno, 18,8 % podjetij ni pripravljeno investirati, ostalih 40 % podjetij pa je na to vprašanje odgovorilo z ne vem (glej prilogo 3.4) Pri 7. vprašanju sem preverjala strinjanje s trditvijo: V vašem podjetju bi kupili storitev za zaščito naših strank (obiskovalcev) pred spletnimi goljufijami. Podjetja so pri strinjanju z omenjeno trditvijo bila manj naklonjena nakupu zaščite kot pri 12. vprašanju. 32,9 % podjetij se je s trditvijo strinjalo, 31,8 % se jih s trditvijo ni strinjalo, 35,3 % pa jih je bilo neodločenih (glej prilogo 3.5). Povprečna stopnja strinjanja pri tem vprašanju je znašala 3,0.

8.3 Preverjanje domnev

Za zavrnitev ali potrditev domnev sem si pomagala z različnimi statističnimi testi, s katerimi sem preverjala povezave med spremenljivkami. Pri pravilni izbiri statističnih testov sem si pomagala s knjigo Statistika 2 (Rogelj, 2002) in knjigo SPSS for Psychologists (Brace, Kemp & Snelgar, 2006).

8.3.1 Preverjanje domnev H1a – H1c

Z domnevo H1a sem predpostavljala, da bodo večja podjetja uporabljala več mehanizmov za zaščito proti spletnemu kriminalu. Pri preverjanju domneve sem uporabila t-test. Podjetja sem razdelila v dve skupini, v prvi so zajeta mikro podjetja, v drugi skupini pa mala, srednje velika in velika podjetja. Pri preverjanju hipoteze sem si pomagala z 11. in s 14. vprašanjem. 11. vprašanje v osnovi ne dopušča t-testa, saj gre v osnovi za nominalno lestvico, zato sem pri tem vprašanju upoštevala število obkroženih odgovorov.

Na podlagi vzorčnih podatkov sem ugotovila, da so razlike statistično značilne, saj je stopnja značilnosti enaka 0,004. Na podlagi rezultatov raziskave lahko zavrnem ničelno domnevo in sprejmem sklep, da večja podjetja uporabljajo več mehanizmov za zaščito proti spletnemu kriminalu (glej prilogo 4.1).

Z domnevo H1b sem predpostavljala, da bodo večja podjetja mnenja, da je cena 200 EUR na leto za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, bolj primerna, v nasprotju z manjšimi podjetji, ki bodo mnenja, da je cena manj primerna. Pri preverjanju domneve sem si pomagala z vprašanjema 10 in 14. Pri preverjanju domneve sem uporabila t-test (glej prilogo 4.2).

Na podlagi vzorčnih podatkov in pri stopnji značilnosti 0,048 lahko sprejmem sklep, da so večja podjetja v primerjavi z mnenjem manjših podjetij mnenja, da je cena 200 EUR na leto za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, bolj primerna.

V domnevo H1c sem vključila predpostavko, da velikost podjetja vpliva na ozaveščenost v podjetju glede različnih vrst spletnih goljufij. Predpostavljala sem namreč, da bodo večja podjetja bolj ozaveščena o spletnih goljufijah in da bodo le-ta prepoznala in poznala več naštetih vrst spletnih goljufij. Pri preverjanju domneve sem si pomagala s t-testom in z vprašanjema 5 in 14. Pri analizi sem upoštevala število spletnih goljufij kot spremenljivko.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da velikost podjetja vpliva na ozaveščenost v podjetju glede spletnih goljufij. Povprečno število poznanih spletnih goljufij v mikro podjetjih je celo višje od ostalih podjetij, vendar kot sem že omenila, med povprečji pri obeh skupinah ni statistično značilnih razlik (glej prilogo 4.3).

8.3.2 Preverjanje domnev H2a – H2c

Z domnevo H2a sem predpostavljala, da podjetja, ki nimajo spletne strani, menijo, da je cena 200 EUR na leto manj primerna za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, v primerjavi s podjetji, ki imajo spletno stran in menijo, da je cena 200 EUR na leto bolj primerna. Pri preverjanju domneve sem si pomagala s 1. in 10. vprašanjem in uporabila t-test. Pri prvem vprašanju sem združila dve skupini, in sicer podjetja ki imajo eno spletno stran in

tista, ki imajo več spletnih strani. Tako sem dobila zgolj dve skupini: podjetja, ki imajo spletno stran (eno ali več), in podjetja, ki je nimajo.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da podjetja, ki nimajo spletne strani, menijo, da je cena 200 EUR na leto manj primerna za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami.

V primeru večjega vzorca bi morda prišla do drugačne ugotovitve, saj so podjetja, ki nimajo spletne strani v povprečju ocenila primernost cene z oceno 2,69 in podjetja s spletno stranjo z oceno 3,10 (glej prilogo 4.4). Podatki v prilogi 4 nakazujejo, da se podjetjem, ki nimajo spletne strani, v povprečju navedena cena zdi manj primerna.

Z domnevo H2b sem predpostavljala, da podjetja, ki nimajo spletne strani, slabše poznajo spletne goljufije. Moja predpostavka temelji na mnenju, da podjetja, ki nimajo svojih spletnih strani, ne poznajo nevarnosti, ki prežijo na spletu, ker jih omenjena tematika v veliki meri ne zanima. Pri preverjanju domneve sem uporabila test kontingence in vprašanji 1 in 5. (5. vprašanje sem razdelila na posamezne skupine in preverila vsako skupino posebej s prvim vprašanjem.)

Na podlagi vzorčnih podatkov ne morem potrditi razlik pri prepoznavanju lažnega predstavljanja (angl. *phishing*) in kraje identitete med podjetji s spletnimi stranmi in podjetji brez spletnih strani. Na podlagi vzorčnih podatkov lahko potrdim zgolj razliko pri prepoznavanju zvabljanja (angl. *pharming*). Na rezultate testa se ne morem opreti, ker je bil kršen pogoj za uporabo χ^2 testa pri vseh testih razen pri prepoznavanju zvabljanja. Zaradi premajhnih frekvenc v posameznih razredih ne morem potrditi ali ovreči razlik pri podjetjih, ki ne prepoznajo nobene od naštetih spletnih goljufij (glej prilogo 5).

Zadnja domneva v drugem sklopu domnev, H2c, se je glasila, da v podjetjih, kjer nimajo spletne strani, zaposlene manj skrbi, da bi njihovo podjetje postalo žrtev spletne goljufije. Pri preverjanju domneve sem si pomagala s t-testom in vprašanjema 1 in 6.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da v podjetjih, kjer nimajo spletne strani, zaposlene manj skrbi, da bi njihovo podjetje postalo žrtev spletne goljufije (glej prilogo 4.5).

8.3.3 Preverjanje domnev H3a – H3c

Z domnevo H3a sem predpostavljala, da večje število obiskovalcev na spletni strani podjetja vpliva na to, da podjetja bolj skrbi, da bi postali žrtev katere izmed spletnih goljufij. Podjetja so razdeljena v štiri skupine, prva skupina od 0 do 499 obiskov, druga skupina predstavlja podjetja s številom obiskov od 500 do 1.990, tretja predstavlja podjetja s številom obiskov od 2.000 do

9.990 in četrta skupina predstavlja podjetja z več kot 10.000 obiski mesečno. Odgovorov, ki so se glasili »ne vem (ne razpolagam s temi podatki)«, pri preizkusu nisem upoštevala. Pri preverjanju domneve sem uporabila analizo variance. Pomagala sem si s 3. in 6. vprašanjem.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da večje število obiskovalcev na spletni strani podjetja vpliva na to, da podjetja bolj skrbi, da bi postali žrtev katere izmed spletnih goljufij. V primeru večjega vzorca bi se morda pokazale statistično značilne razlike, saj podjetja v prvi skupini v povprečju manj skrbi spletni kriminal kot podjetja v četrti skupini (glej prilogo 6.1).

Z domnevo H3b sem predpostavljala, da večje število obiskovalcev na spletni strani podjetja vpliva na večjo ozaveščenost zaposlenih o vrstah spletnih goljufij. Tudi v tem primeru sem uporabila analizo variance in upoštevala število goljufij kot spremenljivko. Pomagala sem si s 3. in 5. vprašanjem.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da večje število obiskovalcev na spletni strani podjetja vpliva na večjo ozaveščenost zaposlenih o vrstah spletnih goljufij (glej prilogo 6.2).

Z domnevo H3c sem predpostavljala, da večje število obiskovalcev na spletni strani podjetja vpliva na to, da so v podjetju mnenja, da je cena 200 EUR na leto bolj primerna za pečat, ki bi podjetje v veliki meri zaščitil pred spletnimi goljufijami. Pri preverjanju tretjega dela domneve sem si pomagala z analizo variance in z vprašanjema 3 in 10.

Na podlagi vzorčnih podatkov ne morem zavrniti ničelne domneve in sprejeti sklepa, da večje število obiskovalcev na spletni strani podjetja vpliva na to, da so v podjetju mnenja, da je cena 200 EUR na leto primerna za pečat, ki bi podjetje v veliki meri zaščitil pred spletnimi goljufijami. V primeru večjega vzorca bi morda prišla do drugačnega rezultata, saj so bila podjetja iz prve skupine v povprečju mnenja, da je omenjena cena manj primerna, kot podjetja iz četrte skupine (glej prilogo 6.3).

8.4 Ugotovitve in priporočila

Med potekom raziskave sem poizkušala narediti čim manj napak. V ta namen sem pred samim začetkom anketiranja preizkusila vprašalnik med znanci. Glavna ovira, na katero sem naletela, je strokovnost področja. Vprašalnike bi morali reševati zgolj v informacijskih oddelkih oz. zaposleni, ki imajo podatke in znanja o spletnih straneh svojega podjetja. Te ovire nisem imela možnost odpraviti, saj moja baza podatkov ni zajemala dovolj elektronskih naslovov informacijskih oddelkov. V kolikor bi se ponovno lotila raziskave, bi si prizadevala dobiti bolj natančno in popolno bazo podatkov. S tem bi se izognila odgovorom, kot so: ne vem, ne razpolagam s temi podatki itd. Pri samem vzorcu je bila slabost tudi velikost vzorca, saj mi zaradi majhnosti ni dovoljeval posploševanja. Pri vprašalniku bi spremenila vprašanje št. 13, ki

sem ga zastavila napačno. Z vprašanjem sem želela priti do odgovora, kdo v podjetju vpliva na odločitev o nakupu sistemov za varnost na spletu, vendar sem dobila predvsem odgovore, kdo v podjetju ima končno odločitev pri nakupu (v večini podjetij je to direktor in ne vodja oddelka za informatiko ali kakšnega drugega oddelka). Predvidevam, da sem do takšnih rezultatov prišla tudi zaradi vzorca, ki je vseboval preveč mikro podjetij. Ker ne vem, kako bi lahko drugače zastavila omenjeno vprašanje, ga v ponovitvi raziskave ne bi zastavila. Pri 5. vprašanju sem preverjala, za katere vrste spletnih goljufij so anketiranci že slišali oz. jih poznajo. Tega vprašanja nisem naknadno preverjala, zato vedno obstaja možnost, da anketiranci v resnici ne poznajo toliko goljufij, kot so jih obkrožili na vprašalniku.

V nadaljevanju na kratko povzamem najpomembnejša spoznanja, do katerih sem prišla na osnovi rezultatov trženjske raziskave. Glede na majhen vzorec rezultatov ne morem posploševati.

Vzorec je zajemal 85 % podjetij, ki imajo vsaj eno spletno stran, kar nakazuje na veliko razširjenost spleta v poslovnem okolju. S pomočjo ankete sem prišla do ugotovitve, da obstajajo razlike v zaščitenosti manjših in večjih podjetij. Večja podjetja, kamor sem uvrstila mala, srednje velika in velika podjetja, uporabljajo več zaščit proti spletnemu kriminalu kot mikro podjetja. Razlike v odstotkih so naslednje: 93,2 % manjših podjetij uporablja dodatne zaščite in 97,8 % večjih podjetij uporablja dodatne zaščite proti spletnim goljufijam. Največ podjetij (37 %) prepozna oz. so že slišali za obliko spletne goljufije, ki se imenuje lažno predstavljanje, kraja identitete je bila prepoznana v 32 %, nekaj manj podjetij (22 %) pa je že slišalo za zvabljanje. Na podlagi rezultatov bi podjetju CONNET, d. o. o., priporočila čim bolje informirati ciljno javnost o vrstah spletnih goljufij in o škodi, ki jo spletni goljufi lahko povzročijo podjetju.

Podjetja, ki so sodelovala v raziskavi, se na spletu počutijo varna, saj jih večino ne skrbi, da bi postala žrtev spletne goljufije. Vzorec je zajemal kar 8,2 % podjetij, ki so že bila žrtev spletne goljufije. Da bi podjetje CONNET, d. o. o., laže svetovala, po katerih komunikacijskih poteh naj trži svojo storitev oz. kako najlaže informirati ostala podjetja o nevarnosti na spletu, sem podjetjem zastavila vprašanje, kje dobijo največ informacij o varnosti na spletu in o zaščitah proti spletnim goljufijam. Po pričakovanju dobijo v podjetju največ informacij preko sodelavcev in kolegov, kar v 34,1 %. Veliko tovrstnih informacij dobijo v podjetju preko spleta (15,3 % podjetij), isti odstotek (15,3 %) podjetij dobi največ informacij preko spletne pošte. Na podlagi rezultatov bi na tem mestu podjetju CONNET, d. o. o., priporočila informiranje ciljne javnosti in trženje storitve CON preko elektronske pošte in spleta (blogi, spletni časopisi, spletni oglasi itd.).

Pri preverjanju domneve H1a sem prišla do zaključka, da večja podjetja uporabljajo več mehanizmov za zaščito proti spletnemu kriminalu. Pri domnevi H1b sem predpostavljala, da se večjim podjetjem cena 200 EUR na leto za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, zdi bolj primerna kot manjšim podjetjem. Domnevo sem potrdila in iz tega lahko sklepam, da večjim podjetjem 200 EUR letno ne predstavlja večjega stroška, v nasprotju z manjšimi podjetji, katerim se zdi cena manj primerna. Pri domnevi, da velikost podjetja vpliva na ozaveščenost glede različnih vrst spletnih goljufij (H1c), ni bilo statistično značilnih razlik. Iz

navedenih razlogov lahko zaključim, da velikost podjetja ne vpliva na ozaveščenost o spletnih goljufijah. Pri domnevi H2a sem predpostavljala, da podjetja, ki imajo spletno stran, ocenjujejo ceno 200 EUR na leto za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, za bolj primerno kot podjetja brez spletne strani. S preverjanjem te domneve nisem prišla do statistično značilnih razlik, ki bi se morda v primeru večjega vzorca le pokazale. Podjetju CONNET, d. o. o., bi na tem mestu priporočila oglaševanje svoje storitve tako podjetjem s spletnimi stranmi kot tudi podjetjem brez njih, saj prepoznavnost storitve vpliva tako na ena kot na druga podjetja. Posledica prepoznavnosti bi tako lahko bila, da bi stranke ob obisku spletne strani imele željo po dokazilu o pristnosti podjetja in njegove spletne strani. Pri preverjanju domneve H2c sem prišla do zaključka, da zaskrbljenost podjetja zaradi spletnih goljufij ni povezana s tem, ali podjetje ima spletno stran ali je nima. Zanimiv podatek, ki sem ga dobila s pomočjo ankete, je, da tako podjetja s spletnimi stranmi kot tudi tista brez njih niso v skrbeh, da bi postali žrtev spletne goljufije. Povprečna zaskrbljenost je bila pri obeh skupinah podjetij nižja od 3 (priloga 4.5). Kot so pokazale raziskave (Statistični urad Republike Slovenije, 2009) o množični uporabi spleta v slovenskih podjetjih, menim, da bi se vsa podjetja morala zavedati nevarnosti pri vsakodnevni uporabi spleta, saj podjetje prav tako hitro postane žrtev katere izmed spletnih goljufij ne glede na to, ali ima svojo spletno stran ali ne. Podjetju CONNET, d. o. o., bi priporočila čim več informiranja ciljne javnosti o nevarnosti na spletu, saj bi se z zavedanjem nevarnosti povečala tudi potreba po tovrstnih storitvah. Pri preverjanju domneve H3a, kjer sem predpostavljala, da podjetja, ki imajo več obiskovalcev na svoji spletni strani, bolj skrbi, da bi postali žrtev spletne goljufije, nisem ugotovila statistično značilnih razlik. Zopet lahko zgolj predpostavljam, da bi se v primeru večjega vzorca pokazale statistično značilne razlike. V kolikor bi se pojavile statistično značilne razlike, bi podjetju CONNET, d. o. o., priporočila osredotočenje oglaševanja zgolj na podjetja z več obiskovalci na svojih spletnih straneh. Velikost vzorca mi ne dopušča posploševanja, vendar sem pri preverjanju domneve H3a vseeno opazila razlike. Pri podjetjih z malo obiskovalci (od 0 do 499 obiskovalcev na povprečni mesečni ravni) na svoji spletni strani je povprečna ocena zaskrbljenosti, da bi podjetje postalo žrtev spletne goljufije, znašala 2,2 (1 = sploh nisem zaskrbljen/-a in 5 = zelo sem zaskrbljen/-a), povprečna ocena strinjanja zaskrbljenost pri podjetjih z več kot 10.000 obiskovalci na spletni strani pa je bila 3,1. Pri preverjanju domneve H3b nisem prišla do rezultatov, ki bi pokazali statistično značilne razlike in tako ne morem sklepati, da podjetja, ki imajo na svoji spletni strani več obiskovalcev, poznajo oz. so že slišali za več vrst spletnih goljufij. Tudi preverjanje H3c domneve, ni pokazalo statistično značilnih razlik, zato ne morem trditi, da se podjetja z večjim številom obiskovalcev v povprečju bolj strinjajo s trditvijo o primernosti cene 200 EUR.

Podjetju CONNET, d. o. o., bi priporočila, naj ponudijo CON kot storitev, ki jo spremljajo manj pomembni izdelki, ki samo storitev naredijo bolj privlačno. Glede na to, da imajo porabniki storitev različne želje, pričakovanja in vrednote, podjetju CONNET, d. o. o., priporočam izvedbo raziskave na temo omenjenih značilnosti, saj bi tako laže usmerili trženjske aktivnosti glede na to, kateri so dejanski in potencialni uporabniki CON, njihove demografske, psihografske, vedenjske značilnosti itd. Podjetju priporočam tržiti CON kot porabniško in podjetniško storitev glede na to, ali želijo storitev predstaviti končnemu porabniku ali drugemu podjetju. Vsekakor pa

v podjetju ne smejo pozabiti, da gre za novo storitev in temu je treba prilagoditi pristop trženja storitve. CONNET, d. o. o., bi priporočila, da se trženja storitve CON lotijo preudarno in načrtno. Pri takšnem načinu trženja je najprej treba opredeliti strateška izhodišča, ki ga podjetje opredeli s pomočjo poslanstva, vizije in jasnih ciljev. Nato je treba analizirati položaj, v katerem je trenutno storitev, in na tak način oceniti, kaj je treba izboljšati, kaj je prednost storitve in prav tako njene slabosti. V tej fazi podjetje določi tudi priložnosti, ki jih ponuja trg, in nevarnosti, katerim se je treba izogniti. V nadaljevanju podjetje določi strategijo trženja in nazadnje še trženjski program in nadzor njegovega izvajanja. Za konec pa bi podjetju CONNET, d. o. o., priporočila, naj oglašuje garancijo v obliki vračila denarja (v kolikor kupci ne bodo zadovoljni z njihovo storitvijo), saj bo na tak način ublažilo negativne učinke vrzeli, do katerih prihaja zaradi previsokih pričakovanj kupcev in zaznano kakovostjo.

S pomočjo raziskave sem prišla do zaključka, da so podjetja relativno dobro ozaveščena o spletnih goljufijah, ki so jim izpostavljena na spletu, vendar pa rezultata zaradi premajhnega vzorca ne smem posploševati. V raziskavi nisem preverjala, kako dobro podjetja poznajo spletne goljufije in če jih znajo prepoznati, predvidevam, da bi tovrstno preverjanje morda pripeljalo do drugačnega zaključka. V ta namen bi bilo treba najprej izvesti obsežno akcijo ozaveščanja podjetij o nevarnostih, ki prežijo na njih. Tovrstne akcije so finančno prevelik zalogaj za tako majhno podjetje, kot je CONNET, d. o. o., zato bi v tem primeru predlagala sodelovanje z Uradom za varovanje potrošnikov ali Ministrstvom za visoko šolstvo, znanost in tehnologijo, prav tako ne bi izključila Ministrstva za gospodarstvo. S takšnim sodelovanjem bi potrošniki prišli do pomembnih informacij o tem, kakšne spletne goljufije so najpogostejše in kako se pred njimi obvarovati.

Predvidevam, da so v podjetju CONNET, d. o. o., določili ceno storitve CON s cenovno politiko maksimalnega tržnega deleža. Takšna politika temelji na tem, da se postavi storitvi nizko ceno ob predpostavki, da je trg cenovno občutljiv. Takšna politika se imenuje tudi določanje cen za prodor na trg. Tovrstna politika je primerna za trg, občutljiv na ceno, saj se pri veliki prodaji znižajo stroški pri avtomatizaciji določenih procesov in pri izkušnjah, z nizko ceno pa podjetje lahko odvrne tudi bodočo konkurenco (Kotler, 1998, str. 492–493). Glede na rezultate ankete, ki so pokazali, da se večini podjetij v raziskavi zdi cena pečata primerna, vendar veliko teh podjetij ni pripravljenih kupiti storitve, ki bi jih v veliki meri varovala na spletu, bi CONNET, d. o. o., predlagala, da izbere cenovno politiko, ki ji Kotler (1998, str. 493) pravi: vodstvo v kakovosti izdelka. Takšna cenovna politika temelji na dražji storitvi, ki je visoko kakovostna. Takšno politiko bi podjetju svetovala v primeru, da so potencialni kupci predhodno že dobro seznanjeni z nevarnostmi, ki za njih obstajajo na spletu.

SKLEP

Storitve se razlikujejo od izdelkov in to dejstvo je treba upoštevati tudi pri njihovem trženju. Storitve so večinoma neopredmetene, neločljive, spremenljive in minljive. Prav zaradi omenjenih lastnosti se tudi življenjski ciklus in trženje razlikujeta od trženja izdelka.

Na spletu tako na podjetja kot tudi na posameznike preži veliko nevarnosti. Ena izmed teh so spletne goljufije. Spletni goljufi premorejo veliko domišljije in idej, kako od žrtev dobiti potrebne informacije. Spletne goljufije sem v diplomskem delu razdelila v tri skupine: kraja identitete, lažno predstavljanje in zvabljanje. Ker gre pri večini goljufij za uporabo psihologije in za dobro poznavanje delovanja računalniških sistemov, smo v boju proti spletnim goljufijam precej nemočni. Danes na trgu obstaja veliko število programov, ki so namenjeni zaščiti na spletu. Storitev, ki so namenjene boju proti spletnim goljufijam, je prav tako veliko, vendar je le peščica učinkovitih. Prav zaradi tega so pri podjetju CONNET, d. o. o., izoblikovali idejo o učinkoviti in unikatni storitvi. Storitev CON je sestavljena iz treh elementov: pečata na spletni strani podjetja, certifikata in verificirane spletne strani na verificirani domeni. Glavni namen storitve CON je zavarovati uporabnikovo podjetje in obiskovalce teh spletnih strani pred različnimi oblikami spletnih goljufij.

S trženjsko raziskavo sem ugotovila, da se podjetja v veliki meri ne zavedajo nevarnosti na spletu, saj se v povprečju počutijo varne. Tu tiči glavni problem trženja storitve CON, saj morajo podjetja najprej prepoznati potrebo po storitvi, šele nato jo lahko podjetje ponudi in proda. Glede na rezultate ankete, da 15,3 % podjetij dobi informacije o varnosti na spletu in o spletnih goljufijah prav na spletu in prav toliko odstotkov podjetij preko spletne pošte, bi podjetju CONNET, d. o. o., svetovala, naj se osredotoči na informiranje ciljne javnosti o svoji storitvi kar preko spletnega oglaševanja in spletne pošte.

Eden glavnih problemov podjetja CONNET, d. o. o., je, da se potencialni kupci ne zavedajo, kaj jim storitev CON lahko nudi oz. pred čim jih lahko obvaruje. Eno od rešitev vidim v obsežni raziskavi o ciljni skupini in nato v ozki usmeritvi osebne prodaje tej skupini. Kljub majhnemu zanimanju podjetij za nakup storitve lahko podjetje CONNET, d. o. o., s pravilnimi orodji tržno-komunikacijskega spleta spodbudi nakup storitve CON.

Glede na to, da sem raziskavo opravila na majhnem vzorcu, v katerem je bilo zajetih veliko zgolj mikro in majhnih podjetji, se zavedam dejstva, da podatkov zaradi naštetih omejitev ne morem posploševati. Zato predlagam podjetju CONNET, d. o. o., da poveča vzorec in raziskavo izvede ponovno.

LITERATURA IN VIRI

1. Anka Lipičnik, ustanoviteljica podjetja CoN. Osebni razgovor, 25.6.2009.
2. Anti-Phishing Working Group (2008). *Napadi z lažnim predstavljanjem (obdobje zadnje četrtine leta 2008)*. Najdeno 2. aprila 2009 na spletnem naslovu http://www.antiphishing.org/phishReportsArchive.html
3. Anti-Phishing Working Group (2008). *Phishing Activity Trends Report, 2nd Half 2008 (druga polovica 2008)*. Najdeno 2. aprila 2009 na spletnem naslovu http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf
4. Anti-Phishing Working Group (2009). *Global Phishing Survey: Trends and Domain Name Use in 1H2009 (za obdobje prve polovice 2009)*. Najdeno 30. januarja 2010 na spletnem naslovu http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf
5. ARNES, Akademska in raziskovalna mreža Slovenije. *»Phishing« – nova oblika spletne prevare (kraje)*. Najdeno 13. septembra 2010 na spletnem naslovu http://www.arnes.si/si-cert/obvestila/2004-06.html
6. ARNES, Akademska in raziskovalna mreža Slovenije. *Obvestila*. Najdeno 5. februarja 2009 na spletnem naslovu http://www.arnes.si/si-cert/obvestila/2004-06.html
7. Baza znanja Presentia. *Kako je sestavljen URL naslov*. Najdeno 17. marca na spletnem naslovu http://www.presentia.si/baza-znanja/entry/10/
8. Brace N., Kemp R., & Snelgar R. (2006). *SPSS for Psychologists*. London: Palgrave Macmillan.
9. Company on Net. Spletna stran podjetja. Najdeno 7. oktobra 2009 na spletnem naslovu http://si.company-on.net/
10. Cyber Score. *Forth annual UK online Fraud Report by Cyber Sorce.* Najdeno 12. maja 2009 na spletnem naslovu http://www.nasvet.com/pharming-napadi/
11. Cyber Source & dr. Khan, A. (b.l.). *Forth Annual UK Online Fraud Report*. Najdeno 24. maja 2009 na spletnem naslovu http://www.cybersource.co.uk/resources/downloads/uk_online_fraud_report_2008.pdf
12. Devetak, G. (2000). *Evropski marketing storitev*. Kranj: Moderna organizacija.
13. Dimec, M. (2004). *Strateški načrt trženja proizvodnega podjetja za trge nekdanje Jugoslavije.* Diplomsko delo. Ljubljana: Ekonomska fakulteta.
14. Domovanje.si. *Kaj je domena.* Najdeno 7. oktobra 2009 na spletnem naslovu http://www.domovanje.com/podpora-uporabnikom/?_m=knowledgebase&_a=viewarticle&kbarticleid=89&nav=0,3
15. Forstnerič, J. (2009, 11. maj). Kako pomembno je zagotavljanje lastne identitete na spletu. *Delo FT*, str. 28.
16. Fraj, K. (2007, 12. September). *Socialni inženiring*. Klemnov kot. Najdeno 8. oktobra 2009 na spletnem naslovu http://www.klemen.fraj.net/?p=1742
17. Gilbert A., & Churchill jr. (2001). *Basik marketing research* (4th edition). Harcourt inc. (college Publishers).

18. Grönroos, C. (2000). *Service Management and Marketing : A Customer Relationship Management Approach* (2nd ed.), Chichester: J. Wiley, cop.
19. Hajtnik T., & Stajič A. *Spletne prevare*. Najdeno 23. maja 2009 na spletnem naslovu http://www.gambit.si/izm/2006/msgovIZM151106/zanimivoIZM.htm
20. How Stuff Works. *How web server works*. Najdeno 17. marca 2010 na spletnem naslovu http://computer.howstuffworks.com/web-server.htm
21. Informacijski pooblaščenec. (b. l.). *Varstvo osebnih podatkov na internetu.* Najdeno 14. avgusta 2009 na spletnem naslovu http://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/
22. Jeran, M. (2006). *Testiranje koncepta nove storitve.* Diplomsko delo. Ljubljana: Ekonomska fakulteta.
23. Kač, D. (2004, september). Obvladovanje kakovosti storitev (2.). *Revija Obrtnik*. Najdeno 15. septembra 2009 na spletnem naslovu http://www.ozs.si/obrtnik/prispevek.asp?IDpm=944&ID=3186
24. Kotler, P., Armstrong, G., Starr, R. G. & Wong, V. (1996) *Principles of marketing*. (European ed.). London: Prentice Hall, Hemel Hempstead: Prentice Hall, Europe: Simon & Schuster International.
25. Kotler, P.,Armstrong, G. & Starr, R. G. (1991). *Principles of marketing. Annotated instructor's edition* (5th ed). Englewood Cliffs (New Jersey): Prentice Hall.
26. Lovelock, Christopher H. (2007). *Services marketing: people, technology, strategy* (6th ed.). Upper Saddle River (N.J.): Pearson/Prentice Hall.
27. MessageLabs Intelligence (2008). *2008 Annual Security Report.*
28. Microsoft Tech Net (2. november 2004). TCP/IP Fundamentals for Microsoft Windows. *Chapter 3 – IP Addressing*. Najdeno 15. marca 2010 na spletnem naslovu http://technet.microsoft.com/en-us/library/bb726995.aspx
29. Microsoft Tech Net (31. maj 2005). TCP/IP Fundamentals for Microsoft Windows. *Chapter 8 – Domain Name System oerview*. Najdeno 13. marca 2010 na spletnem naslovu http://technet.microsoft.com/en-us/library/bb727007.aspx
30. Nasvet, *Phishing napadi – internetna ribičija*. Najdeno 12. oktobra 2009 na spletnem naslovu http://www.nasvet.com/phishing/
31. Nejc Zupan, tehnični direktor podjetja CoN, osebni razgovor, 18.1.2010.
32. Neoserv, *SSL Certifikati*. Najdeno 12. oktobra 2009 na spletnem naslovu http://www.neo-serv.net/podpora/Gostovanje/SSLCertifikati
33. NiteoWeb. Spletna stran podjetja. Najdeno 12. oktobra 2009 na spletnem naslovu http://www.niteoweb.si/o-podjetju
34. Potočnik, V. (1998). *Uvod v trženje storitev* (1. izd.). Ljubljana: Ekonomska fakulteta.
35. Potočnik, V. (2004). *Trženje storitev s primeri iz prakse* (2. dop. Izd.). Ljubljana, GV založba.
36. Rogelj R. (1999) *Vaje iz statistike 2*. Ljubljana: Ekonomska fakulteta.
37. Rogelj, R. (2002) *Statistika 2.* Skripta. Ljubljana: Ekonomska fakulteta.

38. *Storm's Demise Gives Way to New Trends in Spam and Malware; Botnets Extend Their Reach.* Najdeno 24. maja 2009 na spletnem naslovu http://www.messagelabs.com/intelligence.aspx
39. Urych, T. (2004). *Analiza življenjskega ciklusa izdelka na primeru digitalnih fotoaparatov.* Diplomsko delo. Ljubljana: Ekonomska fakulteta.
40. Žabot, A. (2005) *Raziskava trga za potrebe upravljanja kabelskega interneta* (diplomsko delo). Maribor: Ekonomsko – poslovna fakulteta Maribor.

PRILOGE

KAZALO PRILOG

PRILOGA 1: SPREMNO PISMO K ANKETNEMU VPRAŠALNIKU

Spoštovani!

V okviru priprave diplomske naloge na Ekonomski fakulteti izvajam raziskavo o varnosti na internetu in spletnih goljufijah.

Vem, da je vaš čas dragocen, vendar vas prosim, da si vzamete **3 minute časa** in mi omogočite izvedbo raziskave. Za sodelovanje v raziskavi kliknite na spodnjo povezavo:

http://94.236.25.41/anketa/

Anonimnost vaših podatkov je popolnoma zagotovljena. Informacije, zbrane s pomočjo vprašalnika, bodo uporabljene samo za potrebe raziskave.

Za sodelovanje se vam že vnaprej najlepše zahvaljujem in vas lepo pozdravljam.

Saba Resnik

PRILOGA 2: ANKETNI VPRAŠALNIK

1. Ali ima vaše podjetje spletno stran?

- Ne (Če ste na vprašanje odgovorili z Ne, potem pojdite na 5. vprašanje)
- Da, eno spletno stran
- Da, več spletnih strani

2. Spletno stran vaše podjetje uporablja za :
Možnih je več odgovorov!

- Predstavitev podjetja
- Objavo novic
- Prodajo
- Sprejemanje naročil
- Plačila
- Rezervacije
- Zbiranje podatkov o kupcih
- Drugo

3. Koliko obiskovalcev v povprečju zabeležite na vaši spletni strani na mesečni ravni?

- Od 0 do 499
- Od 500 do 1.999
- Od 2.000 do 9.999
- Več kot 10.000
- Ne vem (ne razpolagam s temi podatki)

Na naslednje vprašanje odgovorite, če vaše podjetje prodaja izdelke/storitve preko spleta.

4. Kolikšen delež celotne prodaje (po vaši oceni) vaše podjetje ustvari s poslovanjem na spletu?

- o 0%
- o Od 0,1% do 9%
- o Od 10% do 29%
- o Od 30% do 49%
- o Več kot 50%
- o Ne vem (ne razpolagam s temi podatki)

5. Za katero vrsto spletnih goljufij ste že slišali oz. jih poznate?
Možnih je več odgovorov!

- o Lažno predstavljanje oz. ribarjenje (angl. Phishing)
- o Zvabljanje (angl. Pharming)
- o Kraja identitete
- o Za nobeno od zgoraj naštetih goljufij še nisem slišal/a
- o Drugo

6. Kako močno vas skrbi, da vaše podjetje postane žrtev katere izmed spletnih goljufij?
Obkrožite ustrezno številko glede na vašo zaskrbljenost (1= sploh nisem zaskrbljen/a, 5=zelo sem zaskrbljen/a)

1 2 3 4 5

7. Prosim označite v kolikšni meri se z navedenimi trditvami strinjate.
(1= sploh se ne strinjam, 5= popolnoma se strinjam)

Spletni kriminal za podjetja predstavlja vedno večji problem.	1 2 3 4 5
Skrbi me, da bo v prihodnosti naše podjetje postalo žrtev spletne goljufije.	1 2 3 4 5
Zaupam elektronskim sporočilom, ki jih dobim v spletni nabiralnik.	1 2 3 4 5
Obiskovalci spletne strani našega podjetja so varni pred spletnimi goljufijami.	1 2 3 4 5
V našem podjetju smo pripravljeni storiti več za varnost naših strank (pri obisku/uporabi naše spletne strani).	1 2 3 4 5
V našem podjetju bi kupili storitev za zaščito naših strank (obiskovalcev) pred spletnimi goljufijami.	1 2 3 4 5

8. Ali je vaše podjetje že bilo žrtev spletne goljufije?

- o Da, enkrat
- o Da, večkrat
- o Ne, še nikoli
- o Ne vem

9. Kje dobite NAJVEČ informacij o varnosti na spletu in o zaščitah proti spletnim goljufijam? Izberite zgolj en odgovor!

- o Preko spletnih časopisov
- o Preko blogov, na forumih
- o Preko email novic
- o Drugje na spletu
- o Preko radia, televizije
- o V časopisih
- o V strokovnih revijah
- o Preko sodelavcev in kolegov
- o Drugo

10. Ali se vam zdi cena 200 EUR na leto primerna za pečat, ki bi vas v veliki meri zaščitil pred spletnimi goljufijami?
Obkrožite številko glede na to, kako primerna se vam zdi zgoraj navedena cena. (1= popolnoma neprimerna cena, 5= popolnoma primerna cena)

1 2 3 4 5

11. Katere mehanizme vaše podjetje uporablja za zaščito proti spletnemu kriminalu?
Možnih je več odgovorov!

- o Posodobljeni spletni brskalniki
- o SSL certifikat
- o Pečat za ščitenje identitete podjetja
- o V podjetju ne uporabljamo nikakršne dodatne zaščite
- o Ne vem (ne razpolagam s temi podatki)
- o Drugo

12. Ali bi bili v vašem podjetju pripravljeni investirati v pečat, ki bi vas (in vaše stranke) v veliki meri zaščitil pred spletnimi goljufijami?

- o Da
- o Ne
- o Ne vem

13. Kdo v vašem podjetju vpliva na odločitev o nakupu sistemov za varnost na spletu?

- o Direktor
- o Informacijska služba (IT)
- o Finančna služba
- o Zunanji svetovalci oz. izvajalci
- o Drugi

14. Velikost vašega podjetja (število zaposlenih):

- Mikro podjetje (do 9 zaposlenih)
- Malo podjetje (od 10 do 49 zaposlenih)
- Srednje veliko podjetje (od 50 do 249 zaposlenih)
- Veliko podjetje (več kot 250 zposlenih)

15. V podjetju sem zaposlen/a:

- V informacijski službi
- V finančni službi
- V oddelku za računovodstvo
- V oddelku za trženje (marketing)
- Kot vodja
- Kot direktor
- Drugo

16. Dejavnost vašega podjetja:

- Gradbeništvo
- Trgovina, vzdrževanje in popravila motornih vozil
- Gostinstvo
- Informacijske in komunikacijske dejavnosti
- Finančne in zavarovalniške dejavnosti
- Poslovanje z nepremičninami
- Strokovne, znanstvene in tehnične dejavnosti
- Izobraževanje
- Kulturne, razvedrilne in rekreacijske dejavnosti
- Druge storitvene dejavnosti
- Proizvodnje dejavnosti

PRILOGA 3: REZULTATI ANKETE

3.1 Podjetje s spletno stranjo in podjetja brez spletne strani

Tabela 1: Ali ima vaše podjetje spletno stran?

	podjetja, ki nimajo spletne strani	podjetja, ki imajo eno spletno stran	podjetja, ki imajo več spletnih strani
število	13	46	26
odstotek	15,29	54,12	30,59

Vir: Podatki iz ankete, 2009

3.2 Zaposlitev anketirancev

Tabela 2: Anketiranec, ki je odgovarjal v imenu podjetja je zaposlen/a

	v informacijski službi	v finančni službi	v oddelku za računovodstvo	v oddelku za trženje	kot vodja	kot direktor	drugo
število	11	2	2	10	13	37	10
odstotek	12,94	2,35	2,35	11,76	15,29	43,53	11,76

Vir: Podatki iz ankete, 2009

3.3 Podjetje kot žrtev spletne goljufije

Tabela 3: Ali je vaše podjetje že bilo žrtev spletne goljufije?

	da	ne	ne vem
šetvilo	7	69	9
odstotek	8,23	81,18	10,59

Vir: Podatki iz ankete, 2009

3.4 Investiranje v pečat

Tabela 4: Ali bi v vašem podjetju bili pripravljeni investirati v pečat, ki bi vas (in vaše stranke) v veliki meri zaščitil pred spletnimi goljufijami?

	da	ne	ne vem
število	35	16	34
odstotek	41,18	18,82	40,00

Vir: Podatki iz ankete, 2009

3.5 Nakup storitve za zaščito na spletu

Tabela 5: V našem podjetju bi kupili storitev za zaščito naših strank (obiskovalcev) pred spletnimi goljufijami.

	S trditvijo se popolnoma strinjam	Strinjam se s trditvijo	Niti se strinjam, niti se ne strinjam s trditvijo	S trditvijo se ne strinjam	S trditvijo s popolnoma ne strinjam
število	12	16	30	13	14
odstotek	14,12	18,82	35,29	15,29	16,48

Vir: Podatki iz ankete, 2009

PRILOGA 4: PREIZKUS SKUPIN

4.1 Hipoteza H1a: Večja podjetja uporabljajo več mehanizmov za zaščito proti spletnemu kriminalu.

Group Statistics

	velikost	N	Mean	Std. Deviation	Std. Error Mean
uporabljene_zaščite	1,00	43	1,1163	,73060	,11142
	2,00	13	1,7692	,83205	,23077

Independent Samples Test

		Levene's Test for Equality of Variances	
		F	Sig.
uporabljene_zaščite	Equal variances assumed	,557	,459
	Equal variances not assumed		

Independent Samples Test

		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
uporabljene_zaščite	Equal variances assumed	-2,735	54	,008	-,65295
	Equal variances not assumed	-2,548	17,967	,020	-,65295

Vir: Podatki iz ankete, 2009

4.2 Hipoteza H1b: Večjim podjetjem se zdi cena 200€ na leto, za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami, bolj primerna kot manjšim podjetjem.

Group Statistics

	velikost	N	Mean	Std. Deviation	Std. Error Mean
primernost	1,00	64	2,9219	1,05867	,13233
	2,00	21	3,3810	1,16087	,25332

Independent Samples Test

		Levene's Test for Equality of Variances	
		F	Sig.
primernost	Equal variances assumed	,450	,504
	Equal variances not assumed		

Independent Samples Test

		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
primernost	Equal variances assumed	-1,684	83	,096	-,45908
	Equal variances not assumed	-1,606	31,657	,118	-,45908

Vir: Podatki iz ankete, 2009

4.3 Hipoteza H1c: Velikost podjetja vpliva na ozaveščenost v podjetju glede različnih vrst spletnih goljufij.

Group Statistics

	velikost	N	Mean	Std. Deviation	Std. Error Mean
splet_goljufije	1,00	64	1,9219	1,08824	,13603
	2,00	21	1,8571	1,10841	,24187

Independent Samples Test

		Levene's Test for Equality of Variances	
		F	Sig.
splet_goljufije	Equal variances assumed	,001	,975
	Equal variances not assumed		

Independent Samples Test

		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
splet_goljufije	Equal variances assumed	,235	83	,814	,06473
	Equal variances not assumed	,233	33,586	,817	,06473

Vir: Podatki iz ankete, 2009

4.4 Hipoteza H2a: Podjetja, ki nimajo spletne strani, menijo, da je cena 200€ na leto manj primerna za pečat, ki bi jih v veliki meri zaščitil pred spletnimi goljufijami.

Group Statistics

	splet_str	N	Mean	Std. Deviation	Std. Error Mean
primernost	1,00	13	2,6923	,94733	,26274
	2,00	72	3,0972	1,11532	,13144

Independent Samples Test

		Levene's Test for Equality of Variances	
		F	Sig.
primernost	Equal variances assumed	,303	,583
	Equal variances not assumed		

Independent Samples Test

		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
primernost	Equal variances assumed	-1,230	83	,222	-,40491
	Equal variances not assumed	-1,378	18,562	,185	-,40491

Vir: Podatki iz ankete, 2009

4.5 Hipoteza H2c: V podjetjih, kjer nimajo spletne strani, zaposlene manj skrbi, da bi njihovo podjetje postalo žrtev spletne goljufije.

Group Statistics

	splet_str	N	Mean	Std. Deviation	Std. Error Mean
zaskrbljenost	1,00	13	2,6154	1,26085	,34970
	2,00	72	2,4722	1,18645	,13982

Independent Samples Test

		Levene's Test for Equality of Variances	
		F	Sig.
zaskrbljenost	Equal variances assumed	,026	,871
	Equal variances not assumed		

Independent Samples Test

		t-test for Equality of Means			
		t	df	Sig. (2-tailed)	Mean Difference
zaskrbljenost	Equal variances assumed	,397	83	,693	,14316
	Equal variances not assumed	,380	16,074	,709	,14316

Vir: Podatki iz ankete, 2009

PRILOGA 5: KONTINGENČNA TABELA

Hipoteza H2b: Podjetja, ki nimajo spletne strani, slabše poznajo spletne goljufije.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
splet_str * phishing	85	100,0%	0	,0%	85	100,0%

splet_str * phishing Crosstabulation

			phishing		Total
			,00	1,00	,00
splet_str	1,00	Count	6	7	13
		Expected Count	3,5	9,5	13,0
		% within splet_str	46,2%	53,8%	100,0%
		% within phishing	26,1%	11,3%	15,3%
		% of Total	7,1%	8,2%	15,3%
	2,00	Count	17	55	72
		Expected Count	19,5	52,5	72,0
		% within splet_str	23,6%	76,4%	100,0%
		% within phishing	73,9%	88,7%	84,7%
		% of Total	20,0%	64,7%	84,7%
Total		Count	23	62	85
		Expected Count	23,0	62,0	85,0
		% within splet_str	27,1%	72,9%	100,0%
		% within phishing	100,0%	100,0%	100,0%
		% of Total	27,1%	72,9%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2,835(b)	1	,092		
Continuity Correction(a)	1,808	1	,179		
Likelihood Ratio	2,604	1	,107		
Fisher's Exact Test				,104	,093
Linear-by-Linear Association	2,802	1	,094		
N of Valid Cases	85				

a Computed only for a 2x2 table

b 1 cells (25,0%) have expected count less than 5. The minimum expected count is 3,52.

Splet_str * pharming

Crosstab

			pharming		Total
			,00	1,00	,00
splet_str	1,00	Count	6	7	13
		Expected Count	7,2	5,8	13,0
		% within splet_str	46,2%	53,8%	100,0%
		% within pharming	12,8%	18,4%	15,3%
		% of Total	7,1%	8,2%	15,3%
	2,00	Count	41	31	72
		Expected Count	39,8	32,2	72,0
		% within splet_str	56,9%	43,1%	100,0%
		% within pharming	87,2%	81,6%	84,7%
		% of Total	48,2%	36,5%	84,7%
Total		Count	47	38	85
		Expected Count	47,0	38,0	85,0
		% within splet_str	55,3%	44,7%	100,0%
		% within pharming	100,0%	100,0%	100,0%
		% of Total	55,3%	44,7%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,519(b)	1	,471		
Continuity Correction(a)	,174	1	,677		
Likelihood Ratio	,516	1	,473		
Fisher's Exact Test				,551	,337
Linear-by-Linear Association	,513	1	,474		
N of Valid Cases	85				

a Computed only for a 2x2 table

b 0 cells (,0%) have expected count less than 5. The minimum expected count is 5,81.

splet_str * k_iden

Crosstab

			k_iden		Total
			,00	1,00	,00
splet_str	1,00	Count	5	8	13
		Expected Count	4,4	8,6	13,0
		% within splet_str	38,5%	61,5%	100,0%
		% within k_iden	17,2%	14,3%	15,3%
		% of Total	5,9%	9,4%	15,3%
	2,00	Count	24	48	72
		Expected Count	24,6	47,4	72,0
		% within splet_str	33,3%	66,7%	100,0%
		% within k_iden	82,8%	85,7%	84,7%
		% of Total	28,2%	56,5%	84,7%
Total		Count	29	56	85
		Expected Count	29,0	56,0	85,0
		% within splet_str	34,1%	65,9%	100,0%
		% within k_iden	100,0%	100,0%	100,0%
		% of Total	34,1%	65,9%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,129(b)	1	,720		
Continuity Correction(a)	,002	1	,967		
Likelihood Ratio	,127	1	,722		
Fisher's Exact Test				,756	,474
Linear-by-Linear Association	,127	1	,721		
N of Valid Cases	85				

a Computed only for a 2x2 table

b 1 cells (25,0%) have expected count less than 5. The minimum expected count is 4,44.

splet_str * za_nobeno

Crosstab

			za_nobeno		Total
			,00	1,00	,00
splet_str	1,00	Count	11	2	13
		Expected Count	10,9	2,1	13,0
		% within splet_str	84,6%	15,4%	100,0%
		% within za_nobeno	15,5%	14,3%	15,3%
		% of Total	12,9%	2,4%	15,3%
	2,00	Count	60	12	72
		Expected Count	60,1	11,9	72,0
		% within splet_str	83,3%	16,7%	100,0%
		% within za_nobeno	84,5%	85,7%	84,7%
		% of Total	70,6%	14,1%	84,7%
Total		Count	71	14	85
		Expected Count	71,0	14,0	85,0
		% within splet_str	83,5%	16,5%	100,0%
		% within za_nobeno	100,0%	100,0%	100,0%
		% of Total	83,5%	16,5%	100,0%

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,013(b)	1	,909		
Continuity Correction(a)	,000	1	1,000		
Likelihood Ratio	,013	1	,908		
Fisher's Exact Test				1,000	,637
Linear-by-Linear Association	,013	1	,909		
N of Valid Cases	85				

a Computed only for a 2x2 table

b 1 cells (25,0%) have expected count less than 5. The minimum expected count is 2,14.

PRILOGA 6: ANALIZA VARIANCE

6.1 Hipoteza H3a: Večje število obiskovalcev na spletni strani podjetja vpliva na to, da podjetja bolj skrbi, da bi postali žrtev katere izmed spletnih goljufij.

Descriptives

zaskrbljenost

		N	Mean	Std. Deviation	Std. Error
1,00		20	2,2000	1,28145	,28654
2,00		19	2,6316	1,01163	,23208
3,00		9	1,8889	,92796	,30932
4,00		7	3,1429	1,46385	,55328
Total		55	2,4182	1,19708	,16141
Model	Fixed Effects			1,16625	,15726
	Random Effects				,23366

Descriptives

zaskrbljenost

		95% Confidence Interval for Mean		Minimum	Maximum	Between-Component Variance
		Lower Bound	Upper Bound			
1,00		1,6003	2,7997	1,00	5,00	
2,00		2,1440	3,1192	1,00	4,00	
3,00		1,1756	2,6022	1,00	3,00	
4,00		1,7890	4,4967	1,00	5,00	
Total		2,0946	2,7418	1,00	5,00	
Model	Fixed Effects	2,1025	2,7339			
	Random Effects	1,6746	3,1618			,10140

Test of Homogeneity of Variances

zaskrbljenost

Levene Statistic	df1	df2	Sig.
,550	3	51	,650

ANOVA

zaskrbljenost

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	8,015	3	2,672	1,964	,131
Within Groups	69,367	51	1,360		
Total	77,382	54			

Vir: Podatki iz ankete, 2009

6.2 Hipoteza H3b: Večje število obiskovalcev na spletni strani podjetja vpliva na večjo ozaveščenost zaposlenih o vrstah spletnih goljufij.

Descriptives

splet_goljufije

		N	Mean	Std. Deviation	Std. Error
1,00		20	1,9500	,94451	,21120
2,00		19	1,9474	1,02598	,23538
3,00		9	1,6667	1,32288	,44096
4,00		7	2,1429	1,34519	,50843
Total		55	1,9273	1,06900	,14414
Model	Fixed Effects			1,09145	,14717
	Random Effects				,14717[a]

Descriptives

splet_goljufije

		95% Confidence Interval for Mean		Minimum	Maximum	Between-Component Variance
		Lower Bound	Upper Bound			
1,00		1,5080	2,3920	,00	3,00	
2,00		1,4529	2,4419	,00	3,00	
3,00		,6498	2,6835	,00	3,00	
4,00		,8988	3,3869	,00	4,00	
Total		1,6383	2,2163	,00	4,00	
Model	Fixed Effects	1,6318	2,2227			
	Random Effects	1,4589[a]	2,3956[a]			-,06751

a. Warning: Between-component variance is negative. It was replaced by 0.0 in computing this random effects measure.

Test of Homogeneity of Variances

splet_goljufije

Levene Statistic	df1	df2	Sig.
1,631	3	51	,194

ANOVA

splet_goljufije

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	,955	3	,318	,267	,849
Within Groups	60,755	51	1,191		
Total	61,709	54			

Vir: Podatki iz ankete, 2009

6.3 Hipoteza H3c: Večje število obiskovalcev na spletni strani podjetja vpliva na to, da so v podjetju mnenja, da je cena 200€ na leto primerna za pečat, ki bi podjetje v veliki meri zaščitil pred spletnimi goljufijami.

Descriptives

primernost

		N	Mean	Std. Deviation	Std. Error
1,00		20	3,0500	1,09904	,24575
2,00		19	3,2105	,97633	,22399
3,00		9	2,7778	,97183	,32394
4,00		7	4,0000	1,29099	,48795
Total		55	3,1818	1,09021	,14700
Model	Fixed Effects			1,06332	,14338
	Random Effects				,21045

Descriptives

primernost

		95% Confidence Interval for Mean		Minimum	Maximum	Between-Component Variance
		Lower Bound	Upper Bound			
1,00		2,5356	3,5644	1,00	5,00	
2,00		2,7400	3,6811	2,00	5,00	
3,00		2,0308	3,5248	1,00	4,00	
4,00		2,8060	5,1940	2,00	5,00	
Total		2,8871	3,4765	1,00	5,00	
Model	Fixed Effects	2,8940	3,4697			
	Random Effects	2,5121	3,8516			,08058

Test of Homogeneity of Variances

primernost

Levene Statistic	df1	df2	Sig.
,731	3	51	,539

ANOVA

primernost

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6,518	3	2,173	1,922	,138
Within Groups	57,663	51	1,131		
Total	64,182	54			

Vir: Podatki iz ankete, 2009