UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

ZAUPANJE KOT DEJAVNIK USPEŠNOSTI E-POSLOVANJA

Ljubljana, oktober 2007 GREGOR BOŽIČ

IZJAVA

Študent GREGOR BOŽIČ izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisala pod mentorstvom mag. ALEŠA POPOVIČA in dovolim objavo diplomskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne 10. oktobra 2007 Podpis: _____

Kazalo

KAZALO TABEL

KAZALO SLIK

1. Uvod

Vedno večja dostopnost strojne ter programske opreme in razvoj vedno zmogljivejših informacijskih orodij nam na vseh področjih odpira neskončne možnosti, omejene le z domišljijo posameznika. Ekonomija in poslovanje nista izjemi. Razvoj je poslovanje spremenil do te mere, da lahko praktično vse vrste izdelkov in storitev nakupimo od doma, »iz naslonjača«. Nakupi, ki so bili v preteklosti povezani z velikimi napori, nam lahko dandanes vzamejo le nekaj minut. Elektronsko poslovanje prinaša vsem izjemne možnosti ustvarjanja dobička, če jih le znamo izkoristiti. V nasprotnem primeru se lahko zgodi, da slabosti pretehtajo prednosti in se tako e-poslovanje izkaže za neekonomično.

Namen diplomskega dela je kritično predstaviti vlogo, ki jo ima zaupanje poslovnih partnerjev pri zagotavljanju uspešnosti elektronskega poslovanja. Zavedam se, da je v sodobnih gospodarstvih število click-and-mortar[1] podjetij vedno večje, vendar se ta diplomska naloga osredotoča le na elektronsko poslovanje teh podjetij. Predstavil bom različne poglede na zaupanje ter različne načine in orodja, ki jih podjetja uporabljajo z namenom povečevanja le-tega. Med vsemi »orodji«, ki se uporabljajo pri ustvarjanju in večanju zaupanja v spletne portale, bom podrobneje predstavil izjavo o politiki zasebnosti podjetja, njeno vlogo in smisel. Predstavil bom tudi vse sestavine, ki jih mora podjetje upoštevati pri pisanju in spletnem objavljanju izjave o politiki zasebnosti. Poleg tega pa želim v diplomski nalogi predstaviti stanje na področju izjave o politiki zasebnosti v Sloveniji, predvsem z vidika spletnih deskarjev. V tem delu si bom pomagal s kratkim anketnim vprašalnikom, ki ga bom pripravil po zgledu vprašalnika iz neke druge ameriške raziskave.

Cilj diplomskega dela je zgraditi in podrobneje predstaviti celovit model, ki združuje različne vidike na proces vzpostavljanja in večanja zaupanja v spletna podjetja. Poleg tega pa je cilj tudi preveriti, ali se spletni deskarji zavedajo nevarnosti, ki nanje preži med deskanjem, ali so, in pod katerimi pogoji, pripravljeni svoje osebne podatke prostovoljno zaupati spletnim portalom oz. njihovim lastnikom, ali poznajo orodja, ki se uporabljajo za večanje zaupanja v spletni portal, ter kakšen je odnos do enega izmed teh orodij – izjave o politiki zasebnosti.

Diplomsko delo bo razdeljena na tri poglavja. Začela se bo s poglavjem o elektronskem poslovanju. Poglavje bo namenjeno splošnemu pregledu zgodovine in razvoja e-poslovanja, pregledu prednosti in slabosti, ki jih to prinaša, ter opisu modelov e-poslovanja, ki so se razvijali skozi čas. Poglavje se bo nadaljevalo s podrobnejšim opisom spletnega trgovanja, kot širši javnosti najbolj poznanega modela e-poslovanja, zaključilo pa se bo s podpoglavjem o novih oblikah upravljanja z denarjem.

Vsebino drugega poglavja lahko združimo v en pojem: zaupanje. Poglavje bo namenjeno opredelitvi pojma zaupanja iz različnih vidikov in različnih virov. Sledila bo analiza vpliva zaupanja na e-poslovanje, zadnji del poglavja pa bo namenjen obravnavi načinov in orodij za ustvarjanje in povečevanje zaupanja. Izmed vseh opisanih orodij bo najpodrobneje opisana izjava o politiki zasebnosti. Poleg njene definicije bodo podrobneje opisane tudi sestavine, ki jih ima dobra izjava, ter zakonodaja v Republiki Sloveniji na

[1] Besedna zveza opisuje podjetja, ki se ukvarjajo tako s fizičnim kot elektronskim poslovanjem.

področju varovanja osebnih podatkov. Konec poglavja bo namenjen opisu razvoja izjave o politiki zasebnosti.

Tretje poglavje bo v celoti namenjeno raziskavi, ki jo bom opravil po zgledu raziskave iz ZDA. Ta preučuje, kakšno je mnenje uporabnikov svetovnega spleta v zvezi z izjavo o politiki zasebnosti. Raziskava bo opravljena med slovenskimi »deskarji« in se bo zato nanašala na slovensko populacijo. Podana bo interpretacija rezultatov in ugotovitve analize.

2. E-poslovanje

Kovačič et al. (2004) opredeli elektronsko poslovanje kot »poslovanje v elektronski obliki, z uporabo informacijske in komunikacijske tehnologije«. Gradišar et al. (2005) pa e-poslovanje označi kot »katerokoli obliko poslovanja, pri katerem stranke delujejo elektronsko, namesto da bi delovale fizično, oziroma ne da bi bile v neposrednem medsebojnem fizičnem stiku«. Glede na stopnjo izrabe možnosti elektronskega poslovanja lahko poslovanje podjetij razdelimo v tri kategorije: popolnoma klasično oz. fizično poslovanje, povsem elektronsko poslovanje ali pa poslovanje, ki se poslužuje tako klasičnih kot elektronskih metod. Največ podjetij uporablja slednji način; še vedno poslujejo na klasičen način (s papirnatimi dokumenti), vendar se vse bolj poslužujejo možnosti, ki jih prinaša elektronsko poslovanje.

Pojem elektronskega poslovanja je star že več kot 25 let. Prvotna ideja je bila omogočiti izmenjavo poslovnih podatkov elektronsko, brez uporabe klasičnih papirnatih dokumentov. Šlo je za povezovanje računalniških sistemov ter za prenos podatkov med njimi. Koncept so poimenovali računalniška izmenjava podatkov - RIP (angl. Electronic Data Interchange - EDI). Prednosti uporabe RIP so kmalu postale očitne. Čeprav so ga uporabljala nekatera izmed najuspešnejših podjetij, standard na globalnem nivoju ni bil tako uspešen. Zaradi visokih začetnih stroškov vpeljave so predvsem manjša in srednje velika podjetja ostala pri klasičnem načinu izmenjave papirnatih dokumentov.

2.1. Zgodovina

Razvoj e-poslovanja se je začel z razvojem računalniških omrežij v 60-ih letih. Prvi projekti na tem področju so bili usmerjeni v povezavo več računalnikov v skupno omrežje, z namenom izmenjave pomembnih podatkov na več dislociranih lokacijah, vendar so bili ti projekti zelo dragi in večinoma neuspešni. Rezultat teh neuspehov je bilo spoznanje, da je za prenos podatkov med podjetji potrebna neka enotna oblika podatkov. Tako sta nastala prva standarda, ki sta regulirala elektronsko poslovanje. V ZDA je to bil t.i. X12, ki ga je razvil ANSI (Ameriški inštitut za standarde), v Evropi pa UN/EDIFACT (Semeja, 2001, str. 5). Z zniževanjem cen, tako strojne kot programske opreme, se je tudi število takih projektov povečevalo. Tako se je začelo e-poslovanje uveljavljati na različnih področjih, predvsem na področjih bančništva, zavarovalništva in nato na področju povezovanja podjetij v oskrbovalne verige in verige vrednosti.

Z razvojem interneta je tudi e-poslovanje pridobilo nove razsežnosti. Čeprav je internet nastal v ZDA za potrebe ameriškega obrambnega ministrstva, je 30. aprila 1993 postal javno omrežje omrežij. Ta prelomnica pomeni močno znižanje stroškov izmenjave poslovnih podatkov, saj več ni potrebno imeti lastnih ali najetih telekomunikacijskih vodov. Poleg tega stalno povečevanje zmogljivosti prenosa

omogoča tudi prenos slik ter avdio in video datotek v le nekaj sekundah. Vsebina je tako hitreje dosegljiva velikemu številu končnih uporabnikov.

Uporabo interneta v poslovne namene lahko delimo v tri faze (Semeja, 2001, str. 5). V prvi fazi se internet uporablja kot enosmerni komunikacijski vir, preko katerega lahko podjetja dosežejo potencialne kupce oz. stranke. Internet je obravnavan kot medij za objavo katalogov, cenikov in ostalih ponudb.

V drugi fazi se internet ne uporablja več kot enosmerno komunikacijsko sredstvo, temveč se uporabniku doda možnost, da se na ponudbo odzove. Tako je statičnim spletnim stranem dodana možnost naročanja izdelkov.

V tretji fazi poteka poslovanje med dvema ali več znanimi subjekti. Govorimo o B2B fazi. K njej prištevamo pojav elektronskih dražb, borz in tržnic (Semeja, 2001, str. 5).

2.2. Vrste in oblike e-poslovanja

Udeležence e-poslovanja lahko razdelimo v tri skupine: podjetja, vlado in posamezne fizične osebe (kot končni uporabniki). Glede na sodelovanje zgoraj omenjenih kategorij, pa lahko e-poslovanje razdelimo na več vrst (Gradišar et al., 2005, str. 267-268):

- med podjetji (B2B, angl. Business to Business),
- med podjetji in potrošniki (B2C, angl. Business to Consumer),
- med potrošniki (C2C, angl. Conumer to Consumer),
- med javno upravo in podjetji (G2B, angl. Government to Business),
- med javno upravo in državljani (G2C, angl. Government to Consumer) ter
- znotraj javne uprave (G2G, angl. Government to Government).

Tabela 1: Vrste elektronskega poslovanja s primeri

	Podjetja	***Država***	***Potrošniki***
Podjetja	B2B (izmenjava dokumentov, povezovanje v verigo vrednosti…)		
Država	G2B (Plačevanje davkov, storitve e-uprave, javni razpisi…)	G2G (izmenjava podatkov med resorji…)	
Potrošniki	B2C (spletne trgovine, elektronski katalogi…)	G2C (naročanje različnih dokumentov, oddajanje napovedi za odmero dohodnine…)	C2C (spletne dražbe, e-klepetalnice…)

Vir: Gradišar et al., 2005, str. 140-146; Lastna prilagoditev.

Potrošnikom je najbližja oblika B2C, ki je velikokrat zmotno obravnavana kot najpomembnejša. Analitiki ocenjujejo, da je, merjeno v vrednosti transakcij, B2B najpomembnejši del e-poslovanja (Gradišar et al., 2005, str. 140). Ta del zajema vse transakcije, ki se opravijo med dvema pravnima osebama. To vključuje vse, od bančništva za pravne osebe do transakcij znotraj oskrbovalne verige. Poseben segment, ki pridobiva na veljavi, je poslovanje subjektov z javno upravo. Pri tem ločimo njeno

poslovanje s podjetji (npr. javni razpisi), poslovanje znotraj javne uprave (npr. izmenjava podatkov med resorji) ter poslovanje z državljani (npr. oddajanje napovedi za odmero dohodnine). Potrebno je poudariti, da se področje internetnega sodelovanja države in državljanov v Sloveniji zelo hitro širi. Tako lahko državljani preko spletnega portala javne uprave že naročajo dokumente, spreminjajo svoje podatke, dostopajo do različnih javno dostopnih registrov ipd.

2.3. Prednosti e-poslovanja

Če je do tako velikega uspeha e-poslovanja sploh prišlo, pomeni, da imajo uporabniki od tega določene koristi. Te so (Kovačič et al., 2004, str. 269-272):

- **Zniževanje stroškov nakupa**

To dosežemo s poenostavljenjem nakupnega cikla[2]. Nakupovanje (še posebno, če gre za nakupovanje med podjetji) je povezano z velikim številom aktivnosti (izmenjave dokumentov in podatkov ipd.). Avtomatizacija opravil omogoča, da zaposleni lahko posvetijo več časa pogajanju za boljše nakupne pogoje. Poleg tega lahko tesnejše sodelovanje pripomore k dodatnemu skrajšanju nakupnega cikla.

- **Zniževanje obsega zalog**

Podjetja, ki so s svojimi dobavitelji slabše povezana, morajo imeti na zalogi večjo količino materialov, surovin, izdelkov in polizdelkov. Razlog za večjo zalogo je, da lahko podjetje zagotovi nemoteno izvajanje poslovnega procesa, tudi v primeru ko dobavitelj ne dostavi naročenega materiala v dogovorjenem roku. Večji obseg zaloge za podjetje pomeni višje stroške skladiščenja in vzdrževanja le-te. Elektronsko poslovanje lahko na tem področju zelo pomaga: podjetja, ki dobro načrtujejo svoj poslovni proces, lahko s tesnejšo povezavo z dobaviteljem zagotovijo, da jim bo dobavitelj naročeno blago dostavil ravno ob pravem času (JIT, angl. Just in time). Tako se bo podjetje izognilo večjim zalogam in stroškom, povezanih z njimi.

- **Skrajševanje poslovnega cikla**

Tesno povezovanje podjetja v verigo vrednosti (povezovanje s svojimi dobavitelji in kupci) lahko skrajša čas pošiljanja in prejemanja raznih dokumentov (računov, dobavnic, naročilnic ipd.). Tako se cikel, zaradi hitrejšega prenosa dokumentov in posledično tudi materiala, krajša. Sodelujoča podjetja pa imajo tudi možnost povezovanja in skupinskega dela. Internet namreč omogoča povezovanje ljudi na različnih lokacijah. Videokonferenca omogoča sprejemanje nujnih in pomembnih odločitev, čeprav so odločevalci med seboj geografsko zelo oddaljeni.

- **Povezovanje v verigo vrednosti**

Organizacije, ki svoje storitve ali izdelke ponujajo preko interneta, lahko zelo razbremenijo svoje prodajalne. Na ta način si lahko zagotovijo tudi veliko večji promet, kot bi ga imele poslovalnice. Odjemalci, ki imajo neposreden vpogled v bazo izdelkov, ki jih ima podjetje na zalogi, lahko v krajšem času in z manj stroški naročijo želeno blago. Poleg tega pa imajo odjemalci tudi vpogled v stanje njihovih naročil. Vse to povečuje zadovoljstvo odjemalcev in njihovo zaupanje.

- **Zniževanje stroškov prodaje in trženja ter ustvarjanje novih poslovnih priložnosti**

Obseg prodaje je v prodajalnah omejen zaradi določene količine prodajalcev in omejenega prodajnega prostora, ki jim je na voljo. Če želijo obseg prodaje povečati, morajo zaposliti dodatne prodajalce in zgraditi novo trgovino, kar vodi v povečanje stroškov poslovanja. V spletni trgovini pa se lahko obseg prodaje poveča brez občutnega povečanja stroškov poslovanja. Internet nudi tudi nove priložnosti.

[2] Nakupni cikel je niz aktivnosti, ki jih mora kupec opraviti v procesu nakupa. (The buying cycle, 2007)

Majhna trgovina lahko preko spleta predstavi svojo ponudbo na veliko širšem geografskem področju, česar brez uporabe elektronske in komunikacijske tehnologije ne bi mogla narediti (v razumnih stroškovnih mejah).

Opozoriti velja, da se lahko, ob neprimernem načrtovanju in implementaciji e-poslovanja v praksi, njene prednosti sprevržejo v slabosti oz. šibke točke našega podjetja. Veriga vrednosti mora biti tako dobro načrtovana, njeno delovanje pa mora biti brezhibno. Zatajitev le enega člena v verigi lahko prinese do velikih zastojev in izgub pri vseh naslednjih členih. Prav tako velja podvomiti v smiselnost računalniške izmenjave dokumentov med podjetji, če se znotraj njih te dokumente tiska, prenaša in shranjuje v klasični papirnati obliki.

2.4. Težave in problemi e-poslovanja

Poleg vseh prednosti, ki jih ta različica poslovanja prinaša, je potrebno omeniti tudi nekatere slabosti oz. pomanjkljivosti, ki njen hitrejši razvoj onemogočajo. Te težave lahko razdelimo v dve kategoriji. Prva kategorija nastopi **pri prehodu iz klasičnega v elektronsko poslovanje**. V tem kontekstu se najpogosteje pojavljajo naslednji problemi (Lesjak, Sulčič, 2004, str. 6-7):

- pomanjkanje časa za vrednotenje projekta,
- prekoračenje načrtovanih stroškov,
- problemi z znanjem, potrebnim pri vrednotenju projekta,
- pomanjkanje znanja za e-poslovanje,
- problemi z izobraževanjem uporabnikov,
- problemi s podizvajalci ter
- podaljšanje trajanja projekta.

Čeprav je projekt vzpostavljanja e-poslovanja zelo težaven in dolgotrajen proces, med katerim naletimo na veliko (zgoraj omenjenih) težav, se s temeljitim načrtovanjem in izvedbo lahko večini težav izognemo in tako ostanemo v okviru stroškovnih in časovnih meja.

Na naslednji stopnji, ko je e-poslovanje v podjetju že vzpostavljeno, se pojavita dva popolnoma drugačna problema (UEAPME position paper on the consultation on e-business, 2006). Prvi je problem identitete. Pri klasičnem načinu poslovanja namreč točno vemo, s kom se pogovarjamo, saj imamo osebo pred seboj. Pri elektronskem poslovanju pa ne moremo zagotovo vedeti, kdo sedi za drugim računalnikom. Težava je torej pri določanju identitete našega poslovnega partnerja. Drugi vidik istega problema pa je določanje starosti osebe, ki posluje z nami. Ta vidik pride predvsem do izraza v primeru spletnega nakupa izdelkov ali storitev, ki so mladoletnim osebam prepovedani (npr. alkoholne pijače in podobni izdelki, pa tudi pri spletnih storitvah, kot so spletne stavnice ali spletne igralnice). Razvoj strojne in programske opreme ponuja več tehničnih možnosti za reševanje problema identifikacije ali »avtentikacije« (Hadziahmetovic, 2007, str. 34-38):

- **Piškotki** so šibek način identifikacije, saj so lahko postavljeni na računalnik, ki ga uporablja več oseb. Grobo rečeno so piškotki sredstvo za identifikacijo računalnika, ne pa osebe, ki ga uporablja.

- **ID in geslo** sestavljata dvofaktorski sistem identifikacije. Pri tem je ID (ali uporabniško ime) nekaj, kar imam, geslo pa je nekaj, kar le jaz vem. Ker je uporabniško ime pogosto javno ali dostopno drugim osebam, je glavni faktor identifikacije geslo. Moč identifikacije je zato odvisna le od moči gesla.

- **Sistem s povratnim zahtevkom gesla** je prav tako dvofaktorski sistem identifikacije. Deluje tako, da strežnik generira naključen niz znakov. Uporabnik ga mora nato na določen način (navadno z matematičnim algoritmom) prevesti v drugi niz, ki ga pošlje nazaj strežniku, le-ta pa potrdi ali zavrže identifikacijo.

- **Digitalni certifikati** temeljijo na kriptografiji in so še varnejši način identifikacije, vendar še vedno niso zelo razširjeni. Glavni razlog je težavnost pridobitve in uporabe, poleg tega pa so certifikati navadno shranjeni na lokalnih računalnikih in so zato podvrženi krajam. Obnovitve certifikatov se navadno izkažejo kot drage, še posebej za velike organizacije. Dodatno težavo predstavlja tudi ugotavljanje veljavnosti certifikata.

- **Biometrična identifikacija** se uporablja, ko je potreba po minimiziranju možnosti nepooblaščenega dostopa velika. Identifikacija poteka s pomočjo elektronske naprave, ki prepozna določeno značilnost osebe (prstni odtis, obliko roke ali prsta, glas osebe, vzorec očesne mrežnice ipd.). Zaradi visoke cene takih naprav se taka vrsta identifikacije uporablja le v primerih, ko so stvari, ki jih želimo zaščititi, zelo pomembne.

- **Pametne kartice** so večnamenske naprave, opremljene z mikroprocesorjem in spominom za shranjevanje podatkov. So majhne in prenosne. Mikroprocesor zagotavlja aktivno delovanje in komuniciranje kartice z računalniki ali drugimi napravami ter omogoča obdelavo podatkov, izračun kompleksnih kalkulacij. Kartice se lahko uporablja kot sredstvo identifikacije. Nekatere delujejo le ob kontaktu med kartico in drugo napravo, druge delujejo brez kontakta, s pomočjo radio signalov.

Druga kategorija težav so **nasprotja v zakonu, ki jih mora podjetje upoštevati**. Na eni strani naj bi se osebni podatki o uporabnikih takoj brisali, zaradi zagotavljanja zasebnosti, po drugi strani pa morajo oblastem zagotoviti vse podatke, ki so potrebni za odkrivanje morebitnih vdorov ali kraj podatkov. Tako se mora podjetje odločiti, katere vrste podatkov bo hranilo ter koliko časa jih bo hranilo, v okvirih, ki jih postavljata omenjeni zakonski zahtevi, kar pa ni vedno lahko.

Kljub problemom elektronskega poslovanja so mu njegove prednosti omogočile hiter razvoj. Tak trend lahko pričakujemo tudi v prihodnosti, saj vedno cenejša računalniška in programska oprema omogoča vedno širši krog uporabnikov take ali drugačne vrste e-poslovanja.

2.5. Modeli elektronskega poslovanja

Ob vpeljavi elektronskega poslovanja ne zadostuje nakup informacijske in komunikacijske tehnologije. Potrebno je spremeniti tudi način poslovanja in ga prilagoditi novim razmeram. Te spremembe v načinu poslovanja so privedle do nastanka novih poslovnih modelov.

Modele elektronskega poslovanja delimo na (Kovačič et al., 2004, str. 276-278):

- spletno oglaševanje,
- virtualne skupnosti,
- spletno trgovino,
- posredniški model,
- informacijske portale ter
- predplačniške modele.

Model spletnega oglaševanja uporablja internet kot podaljšano roko, s katero lahko podjetja svoje izdelke in storitve predstavijo širšemu občinstvu. Spletne strani vsebujejo predvsem reklamna sporočila in specifikacije izdelkov in storitev.

Virtualne skupnosti predstavljajo bazo brezplačnega znanja, ki jo najdemo na internetu. So neprofitne in zbirajo brezplačne informacije, ki jih lahko uporabnik uporablja zastonj.

Spletna trgovina je zelo podobna klasični trgovini, le da se dogaja v virtualnem prostoru. Tako lahko kupec izbira med vrsto izdelkov, jih vstavi v »košarico« ali »nakupovalni voziček« in jih na koncu kupi ali pa prekliče naročilo. Pogosto se ta oblika uporablja kot dopolnilo klasični trgovini.

Posredniški model povezuje kupce in prodajalce. Omogoča izmenjavo in prodajo različnih dobrin in storitev neposredno med fizičnimi in pravnimi osebami (Kovačič et al., 2004, str. 277). Predstavnici takega modela sta blagovna borza in avkcija. Na blagovnih borzah se trguje z različnimi vrstami blaga. Ponudnik ponudi svoje blago, nato pa se na objavo odzovejo kupci. Pri avkcijah pa najpogosteje srečamo ponudnika, ki ponuja blago v omejeni količini (navadno en proizvod). Na ponudbo se nato odzivajo kupci (navadno v določenem časovnem intervalu), izmed katerih je izbran tisti, ki je za ponujeni izdelek pripravljen plačati najvišjo ceno.

Informacijski portali ponujajo spletnemu obiskovalcu veliko informacij, ki so navadno brezplačne. Financirajo se s pomočjo oglasov, ki jih je mogoče objaviti na portalu. Obenem pa nekateri portali, predvsem tisti s specializirano vsebino, že zaračunavajo dostop do strani.

Predplačniški model je podoben informacijskemu portalu. Del vsebine, ki jo portal ponuja, je brezplačen, preostali del pa je na voljo le predplačnikom.

Ocenjujem, da je med uporabniki svetovnega spleta najbolj poznan model spletne trgovine. Le-ta ponuja tako kupcem kot prodajalcem veliko prednosti, slabosti, ki jih prinaša, pa so relativno majhne. Razmah je spletna trgovina dosegla tudi zaradi izjemno velikega kroga potencialnih uporabnikov, saj lahko kot takega opredelimo vsako osebo, ki nakupuje kakršnekoli izdelke ali storitve (v fizičnem nakupu) in ima na voljo internet. Vsaka oseba, ki ustreza tem pogojem, lahko opravi spletni nakup. Velika razširjenost spletnega nakupovanja botruje dejstvu, da se v ta namen preko interneta izmenjuje in posreduje veliko informacij o kupcih. Zato je še toliko bolj pomembno, da pri izmenjavah podatkov

poskrbimo za varnost le-teh in njihovih lastnikov. Le tako lahko pridobimo zaupanje kupcev v spletni portal, kar je ključnega pomena za njegovo uspešnost, saj lahko že majhna napaka v sistemu prinese nezaupanje kupcev in posledično ogromne izgube prihodkov. Na podlagi do sedaj povedanega bom v naslednjem poglavju podrobneje predstavil spletno trgovanje ter njegove prednosti in slabosti tako za kupce, kot za trgovce.

2.6. Spletna trgovina

Spletno trgovanje je področje elektronskega poslovanja, ki je fizičnim uporabnikom najbolj znano in jim je najbližje. Predstavlja največji delež B2C poslovanja. Spletna trgovina vključuje potrošnikovo zbiranje informacij, izbiro (fizične ali digitalne) dobrine ali storitve, naročilo le-te in njeno elektronsko dobavo. (Groznik, Lindič, 2004, str. 37). V spletnih trgovinah lahko kupujemo raznoliko paleto izdelkov in storitev. Glede na obliko izdelka ločimo izdelke v fizični (npr. računalniška ali strojna oprema, obutev, ipd.) ali pa digitalni obliki (npr. programska oprema, digitalne knjige, ipd.). Trgovine pa lahko glede na raznolikost ponujenih izdelkov ločimo na specializirane, kjer je ponudba omejena na točno določen segment izdelkov (npr. spletni ponudniki obutve, glasbenih zgoščenk ipd.), in na veleblagovnice, kjer je na voljo široka paleta izdelkov (npr. veleblagovnica.com).

2.6.1. Prednosti spletnega trgovanja

Proces trgovanja vključuje aktivnosti dveh razredov udeležencev: ponudnikov in kupcev. Uvedba spletnega trgovanja prinaša prednosti in slabosti za oba razreda udeležencev.

Prednosti za ponudnike

Prva prednost je ta, da spletna trgovina omogoča virtualno razširitev potencialnega trga ponudnikov na cel svet. Nakup preko spleta je omogočen tudi kupcem, ki so od ponudnika fizično zelo oddaljeni. Pred spletnim trgovanjem je bilo to mogoče le z visokimi dodatnimi stroški na strani kupca ali prodajalca. Spletno trgovanje pa te stroške omeji na stroške poštnine.

S pomočjo spletnega trgovanja se ponudniki hitreje odzivajo na spremembe želja kupcev. Prilagodijo se tako, da dodajo v svojo ponudbo nove izdelke, odobrijo dodatne popuste (npr. na izdelke, po katerih je veliko povpraševanje), spremenijo cene ipd. Podjetje lahko to doseže z občutno nižjimi stroški in v krajšem odzivnem času.

Splet omogoča tudi veliko natančnejše sledenje potrebam oz. željam kupcev (npr. z evidenco že nakupljenih izdelkov, s pomočjo piškotkov ipd.). Tako lahko s pomočjo preteklih nakupov ugotovimo, katera področja jih zanimajo, in na podlagi teh podatkov pripravimo kupcu prilagojeno ponudbo, za katero je bolj verjetno, da jo bo sprejel.

Prednost spletnega trgovanja je tudi sledenje »pomikanju« kupcev skozi spletne strani. Tako lahko ugotovimo, na katerih straneh se kupci najpogosteje ustavijo ter na katerih straneh prekinejo sejo oz. zapustijo portal. Ugotovitve uporabimo za posodobitev oz. izboljšanje portala in ponudbe.

Do znižanja stroškov pridemo zaradi nižjih fiksnih stroškov (npr. nižji stroški najema poslovnih prostorov) in tudi zaradi nižjih stroškov oglaševanja (npr. ni stroškov tiskanja in pošiljanja oglasov, saj jih lahko enostavno objavimo na spletnem portalu).

Prednosti za kupce

Prednosti, ki jih prinaša spletna trgovina je veliko. Raziskava, objavljena na spletni strani Hitrost postavlja v ospredje 10 prednosti spletne trgovine, ki kupcem tako ali drugače olajšajo, skrajšajo ali pocenijo proces nakupovanja(Deset razlogov za spletno trgovino, 2007):

- **Nikoli zaprto**

Malo je trgovin, ki so odprte 24 ur na dan, 7 dni na teden in 365 dni na leto. S spletno trgovino je ponujeno prav to. Vse spletne trgovine so lahko vedno odprte, kar omogoča, da se čas nakupovanja prilagodi potrošniku.

- **Udobje**

Ena glavnih prednosti spletne trgovine je nakup iz udobnega naslonjača od kjerkoli. Ni se potrebno pripraviti in odpraviti v trgovino, ni težav z vremenom, z zastoji na cestah ali s parkiranjem. Poanta udobnosti spletne trgovine je tako vsem takoj jasna.

- **Čas je denar**

Poslovanje na internetu je običajno hitrejše od tistega, ki smo ga vajeni v resničnem življenju. Hitrost pomeni prihranek časa, ta pa je, kot pravi znan pregovor, denar.

- **Oddaljenost ni pomembna**

Naročila se vršijo od kjerkoli na zemeljski obli.

- **Varnost**

Zaradi modernih postopkov kodiranja in enkripcije podatkov pri spletnih trgovinah je prav mogoče, da sploh ne obstaja varnejši način poslovanja.

- **Ceneje**

Spletne trgovine potrebujejo manj prostora in manj zaposlenih, zato imajo tudi nižje stroške delovanja. Vse to pa se lahko odraža tudi pri cenah, ki so lahko nižje kot v običajni trgovini.

- **Avtomatizacija in personifikacija ponudbe**

S pomočjo piškotkov in posebnih programov lahko spletni portal analizira nakupe vsakega kupca posebej. Tako lahko strežnik samodejno, vsakemu kupcu posebej, ob naslednjem obisku spletne trgovine ponudi določene izdelke glede na prejšnje nakupe.

- **Hiter pregled celotne ponudbe**

Še ena prednost, ki jo potrošnik zelo ceni, je možnost primerjave cen v različnih spletnih trgovinah. Tako je potrošniku omogočena izbira najugodnejše ponudbe, saj vsi vemo, kako drago in naporno je letati od ene običajne trgovine do druge, da se nam ne bi slučajno zgodilo, da bi nas »pohlepni« trgovci »ogoljufali« s previsoko ceno.

- **Zgodovina nakupov**

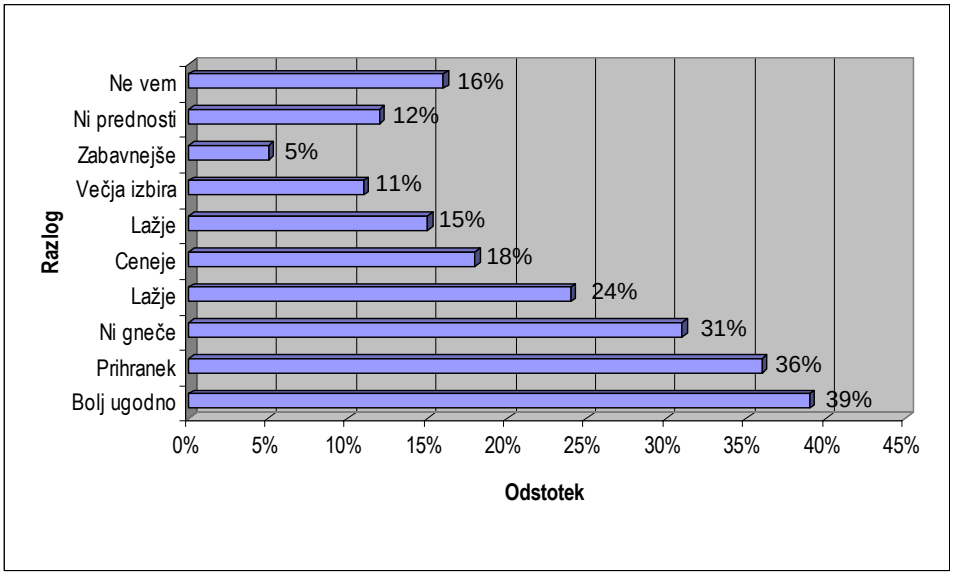
Vsaka spletna trgovina ponuja pregled preteklih nakupov kupcev.

- **Velikost ponudbe ni omejena**

Običajna trgovina je omejena z velikostjo prostora, v katerem domuje. Prav tako njeno skladišče. Zato lahko ponudi le omejeno količino artiklov omejeni količini strank v določenem času. Spletna trgovina to pomanjkljivost skoraj v celoti odpravi.

Raziskava DTI (Department of trade and industry) je pokazala, da spletno nakupovanje prinaša kupcu predvsem naslednje prednosti (Informing Customers About e-commerce, 2006, str. 19):

Slika 1: Razlogi za spletno nakupovanje



Vir: Informing Customers About e-commerce, 2006, str. 19.

2.6.2. Pomanjkljivosti in nevarnosti spletnega trgovanja

Poleg številnih že naštetih prednosti, ki jih prinaša e-trgovanje, obstaja tudi nekaj slabosti, ki zavirajo še hitrejšo rast te vrste poslovanja. Ti razlogi se nanašajo predvsem na nezaupanje potencialnega kupca. Razlogi za nezaupanje pa so morebitne izgube zasebnosti oz. zlorabe osebnih podatkov in možnost spletne prevare (Gradišar et al., 2005, str. 148). Dodatna pomanjkljivost je tudi ta, da dejansko ne pridemo v fizični stik z izdelkom, ne moremo si ga natančneje ogledati, ga otipati, povohati ali pomeriti. To zmanjšuje zaupanje kupca, ki ima občutek, da kupuje »mačka v žaklju«.

Možnosti spletne prevare

Z novim kanalom poslovanja je prišlo tudi do neomejenih možnosti prevar. Možnost pridobitve nezakonitega zaslužka se zdi prevarantom še bolj privlačna, če za to niso potrebni osebni stiki.

Definicija spletne prevare pravi, da je to vsaka vrsta prevare, ki uporablja spletno pošto, spletne portale ali klepetalnice za pridobitev potencialnih žrtev, za izvedbo prevarantskih transakcij ali za prenos iztržka prevar na druge finančne ali nefinančne institucije, povezane s prevaranti (Wikipedia, 2007).

Zvezni urad za preiskave (FBI) in Ministrstvo za pravosodje Združenih držav Amerike (United States Department of Justice) poročata, da so najpogostejše vrste prevar sledeče (Internet fraud, 2007; What is internet fraud, 2007) :

- **Prevare na spletnih dražbah**

Spletne dražbe ponujajo veliko možnosti prevarantom. Prevaranti ponavadi na dražbi ponudijo drage in visokokakovostne izdelke (npr. ure dragih blagovnih znamk), ki privabijo veliko število potencialnih kupcev. Ob sklenitvi kupčije (z naključnim kupcem) mora kupec poslati ponudniku denar. V zameno naj bi ponudnik kupcu poslal obljubljeno blago, vendar se to ne zgodi ali pa ponudnik dostavi blago nižje kakovosti.

- **Priložnosti dela/Delo na daljavo**

Prevarant uporablja internet kot oglaševalsko sredstvo in obljublja visok mesečni dobiček. Prevarani mora podjetju poslati določen denarni znesek v zameno za material, ki naj bi bil potreben za zagon poslovanja, vendar pa ta ni nikoli dostavljen.

- **Kraja identitete**

Prevarant na nelegalen način pridobi podatke o določenih fizičnih osebah in nato sklepa kupčije preko interneta z nevednostjo lastnika identitete. Znan je primer, ko je prevarant z državne spletne strani pridobil osebne podatke določenih oseb, ki jih je nato uporabil za pridobitev kreditov pri različnih bankah (What is internet fraud, 2007).

- **Investicijske prevare**

Prevaranti na borzi nakupijo delnice nizko kotiranih podjetji. S sistematičnim izdajanjem lažnih novic in podatkov, povzročijo dvig cene delnic teh podjetij. Nato svoje delnice prodajo po višji ceni, kot so jih nakupili. Možen je seveda tudi obraten scenarij, torej da visoko kotiranim podjetjem povzročijo padec vrednosti delnic, ki jih nato kupijo. Ob ponovnem dvigu cene pa lahko te delnice z velikimi dobički prodajo.

- **Prevare s pomočjo kreditnih kartic**

Ta vrsta prevare je najbolj strah vzbujajoča. Za plačilo preko interneta nakupljenih artiklov mora kupec poslati podatke o svoji kreditni kartici. Podatki se pošljejo podjetju, ki je zadolženo za izvajanje plačil (npr. paycom.net, ibill.com). Do težav pride, ko do podatkov o kreditni kartici pride nepooblaščena oseba. Ta lahko podatke uporablja za lastne nakupe in tako oškoduje lastnika kartice.

- **Druge prevare**

Različne možnosti za nelegalno pridobivanje denarnih sredstev preko spletnih prevar so neskončne. Omejene so le z domišljijo različnih kriminalcev in kriminalnih združb. Žrtve takih prevar so lahko prav vsi, ne glede na dohodek, izobrazbo ali sloj v družbi.

Kot primer navajam sledečo resnično zgodbo. Nekatere spletne strani so si kot cilj izbrale pare, ki so se želeli ločiti. Preko interneta so oglaševali možnost, da se za le skromno vsoto lahko par hitro loči v tuji državi, ne da bi bilo potrebno zapustiti ZDA. Te strani pogosto ponujajo napačne, zavajajoče ali nenatančne pravne informacije. Žrtve takih prevar navadno dobijo na dom določeno potrdilo (npr. potrdilo, da so uradno ločeni), vendar to nima pravne veljavnosti (What is internet fraud, 2007).

Fizična neotipljivost izdelkov

Pri spletnem nakupovanju pridemo do prvega fizičnega stika s kupljenim izdelkom šele takrat, ko nam ga dostavijo (Nakupovanje po internetu, 2006, str. 10). Čeprav je na spletnih straneh spletne trgovine možno pridobiti vedno več raznovrstnih podatkov o želenih izdelkih (tehničnih podatkov, slik, priročnikov

za uporabo, tridimenzionalnih modelov ipd.), pa še vedno obstaja možnost, da z njimi ne bomo zadovoljni.

Rešitev tega problema velja iskati v Zakonu o varstvu potrošnikov (Zakon o varstvu potrošnikov, 2004). Glavne določbe zakona (in s tem rešitev problema fizične neotipljivosti izdelka) so v skrajšani obliki navedene v nadaljevanju.

Potrošnik lahko pri nakupu v spletnih trgovinah brez navedbe razloga v petnajstih dneh po prejemu izdelka od nakupa odstopi: sporoči trgovcu, da kupljenega izdelka ne želi več. V naslednjih petnajstih dneh mora nepoškodovan izdelek trgovcu vrniti. Trgovec mora potrošniku vrniti vse stroške: kupnino za izdelek, stroške pošiljanja in morebitne druge stroške. Edini strošek, ki bremeni potrošnika, je strošek vračanja blaga. Vračilo plačil mora trgovec opraviti takoj, najpozneje pa v petnajstih dneh po prejemu sporočila o odstopu od pogodbe. Če spletni trgovec zamudi z vračilom, mora potrošniku, poleg zakonitih zamudnih obresti, plačati še desetino prejetega plačila za vsakih dopolnjenih trideset dni zamude pri vračilu (Nakupovanje po internetu, 2006, str. 10).

Poudariti velja, da je dolžina zgoraj navedenih rokov odvisna od državne zakonodaje v posameznih državah. Tako je npr. v Veliki Britaniji minimalen rok za odpoved brez razloga sedem delovnih dni, v Nemčiji pa je ta rok daljši in znaša 14 delovnih dni.

V primeru, da trgovec potrošnika ne obvesti o pravici do odstopa od pogodbe brez navedbe razloga, se rok, v katerem je možen odstop brez razloga, podaljša na tri mesece. Enak rok je določen tudi v drugih članicah EU. Po tem časovnem obdobju pa pravica do odstopa od pogodbe brez navedbe razloga mine.

Pravico do odstopa od pogodbe velja razlikovati od pravice do reklamiranja izdelka zaradi napake. Le-ta je pri spletnem nakupu enaka kot pri klasičnem fizičnem nakupu. Če izdelek ni tehnično brezhiben lahko kupec od prodajalca zahteva, da odpravi napako, zamenja izdelek z novim in brezhibnim, vrne celotno kupnino (pri tem kupec vrne izdelek) ali pa vrne le del kupnine, pri čemer je vrnjeni del v sorazmerju z napako.

Pod določenimi pogoji pa kljub vsemu ne moremo odstopiti od pogodbe (Zakon o varstvu potrošnikov, 2004):

- če je vrednost izdelka ali storitve odvisna od dogajanj na finančnih trgih, na katere trgovec ne more vplivati (če npr. po internetu kupujemo delnice),
- če je izdelek narejen po navodilih potrošnika in prilagojen njegovim potrebam ali če gre za pokvarljiv izdelek ali izdelek, ki mu je že potekel rok uporabe (npr. hrana, pijača, oblačila narejena po meri),
- če je potrošnik že odprl varnostni pečat pri avdio- in videoposnetkih in računalniških programih,
- če gre za dobavo časopisov, revij in periodičnih publikacij ter
- če gre za igre na srečo ali loterijo.

Izguba zasebnosti

Omeniti velja dve težavi, s katerimi se lahko srečamo v primeru, da pridejo naši osebni podatki v napačne roke (Gradišar et al., 2005, str. 159). Prva težava se kaže v obliki nezaželene pošte (spam, junk mail). Za pošiljatelja (navadno spletne trgovine, ki svoje proizvode oglašujejo preko spletne pošte) predstavlja pošiljanje reklamnih sporočil preko spletne pošte izredno nizek strošek, zaradi česar jo veliko podjetij izkorišča. Druga težava pa je trgovanje z zbranimi podatki brez vednosti ali privolitve njihovih lastnikov. Glavni razlog trgovanja z osebnimi podatki je pridobitev spiska kontaktnih podatkov (med njimi tudi naslov spletne pošte), s pomočjo katerih lahko podjetja svoje izdelke ali storitve oglašujejo na cenen način. Pa smo spet pri polnem poštnem predalu. Tako kot s kontaktnimi se lahko trguje tudi z drugimi podatki, vključno s finančnimi, kar lahko predstavlja še večjo nevarnost.

Pri deskanju po svetovnem spletu smo lahko priča pošiljanju podatkov tretjim osebam. Vsakič, ko prispemo na spletno stran je namreč mogoče, da smo avtorju ali lastniku le-te posredovali vsaj en podatek, to je naš IP naslov. Vendar IP naslov ni edini podatek, ki ga lahko izdamo. Podatke, ki jih podjetje pri obisku spletnih portalov hranijo, lahko razdelimo v tri kategorije (Meinert et al., 2006, str. 132):

- **Kontaktni podatki** so podatki, preko katerih lahko, kdor jih pozna, stopi v stik z nami, npr. naslov spletne pošte, ime, poštni naslov, telefonske številke ipd.
- **Biografski podatki** so podatki o naših preferencah, konjičkih, željah ali pa letnem dohodku ipd.
- **Finančni podatki** so podatki, ki nam omogočajo finančno poslovanje preko spleta, npr. številka kreditne kartice, datum veljavnosti kartice, številka bančnega računa ipd.

Število in vrsta podatkov, ki jih »izdamo« pri deskanju, se razlikujejo med posameznimi spletnimi portali. Odvisni so tudi od pravic, ki jih želimo na posameznem spletnem portalu imeti. V primeru, da na portal zaidemo slučajno in si želimo le ogledati vsebino portala, nam v večini primerov ni potrebno izdajati podatkov. Če želimo opraviti nakup preko spletnega portala, pa moramo izdati najmanj kontaktne podatke, v določenih primerih tudi finančne podatke. Dejanska težava ni v izdajanju svojih podatkov, tako osebnih kot drugih, temveč v možnosti njihove zlorabe.

3. Zaupanje kot dejavnik uspešnosti e-poslovanja

Zaupanje od vedno velja za enega najpomembnejših dejavnikov uspešnosti klasičnega poslovanja. Enako velja za nekoliko spremenjen način poslovanja, to je elektronsko poslovanje. Razlike med obema se kažejo v naporih, ki jih je potrebno vložiti v zagotavljanje oz. povečevanje zaupanja v podjetje pri poslovnih partnerjih in kupcih. Včasih je bil stisk roke že znak, da si poslovna partnerja zaupata, toda v sedanjem času, času minimalnega fizičnega kontakta med njima, to ni več dovolj. Zaupanje moramo graditi na drugačen način.

Količina podatkov, ki se prenašajo preko interneta ali drugih omrežij, je vedno večja (vsakič ko »dviamo« denar na bankomatu, ko plačujemo s kartico preko POS terminala, ko plačujemo z Moneto ipd.). Prav tako so tudi podatki, ki se prenašajo, vedno bolj specifični, osebni. Kjerkoli v procesu prenosa podatkov se lahko zgodi, da si jih kdo nezakonito prilasti, ne da bi kdorkoli drug to občutil ali opazil. Zato je potrebno za svoje podatke dobro skrbeti in jih ne posredovati kar vsakomur. V primeru

zlorabe je najmanj, kar se nam lahko zgodi, da nam poštni predal zasujejo z nezaželenimi reklamnimi sporočili, lahko pa ostanemo tudi s praznim bančnim računom.

3.1. Opredelitev zaupanja

Opredelitev zaupanja je mnogo. Najprej velja omeniti, da se študije o zaupanju pojavljajo na veliko področjih (v psihologiji, sociologiji, ekonomiji in podobno). Vsako področje obravnava zaupanje iz določenega vidika, zatorej definicije niso splošno uporabne na vseh ostalih področjih. Seveda se bom v diplomskem delu osredotočil na ekonomsko definicijo zaupanja.

Zaupanje je tako emocionalno, kot logično. Emocionalno, ko razkrijemo svojo ranljivost, v prepričanju, da tega ne bo nihče izkoristil, logično, ko pretehtamo verjetnosti izgube in dobička, preračunamo pričakovano vrednost in iz sklepov ugotovimo, ali bo druga oseba delovala na predvidljiv način (What is trust, 2007). Čustva, ki so povezana z zaupanjem so tovarištvo, prijateljstvo, ljubezen, sloga, sprostitev, lagodnost ipd. Zaupanje lahko definiramo na več načinov, z vidika več dimenzij (prilagojeno po What is trust, 2007):

3.1.1. Predvidljivost

Je običajni del človeškega nenehnega napovedovanja prihodnosti. Ljudje si neprestano postavljamo lastne, notranje modele sveta, ki temeljijo na naših preteklih izkušnjah in na posredovanih izkušnjah drugih, s pomočjo katerih nenehno ugibamo, kaj se bo v prihodnosti zgodilo. Tako se lahko pripravimo na nevarnosti, pa tudi načrtujemo in dosegamo dolgoročne cilje.

Definicija: Zaupanje pomeni zmožnost predvidevanja, do kakšnih situacij bo prišlo in kako bodo drugi v teh situacijah delovali. Če se uspemo obdati z osebami, ki jim zaupamo, si lahko zagotovimo varno sedanjost in tudi boljšo prihodnost.

3.1.2. Izmenjava vrednosti

Večino interakcij z drugimi osebami lahko opišemo kot izmenjavo, ki je temelj vseh poslovnih kot tudi drugih, enostavnejših odnosov. V najenostavnejši obliki lahko opišemo izmenjavo dobrin. Izračun vrednosti blaga, ki ga izmenjujemo, je enostaven, če zamenjamo eno materialno dobrino za drugo (npr. 1 zlatnik za 2 srebrnika). Stvari se zapletejo, ko se izmenjuje nematerialne stvari. Podjetja tako ne izmenjujejo le plače za delo, temveč tudi dobre delovne pogoje za intelektualne in fizične napore zaposlenih. Izmenjava vrednosti deluje na principu, da vsak posameznik dobrine in storitve vrednoti drugače. Zaupanje pri izmenjavi vrednosti se pojavi, ko udeleženci v izmenjavi nimajo popolnih informacij o objektu izmenjave (izdelku ali storitvi). Takrat namreč nismo prepričani ali bomo res dobili tisto, kar pričakujemo. Ko kupujemo avtomobil ne želimo kupiti »kripe«, za katero prodajalec ve, da ne deluje pravilno.

Definicija: Zaupanje nastopi pri izmenjavi z nekom, ko nimamo popolnih informacij o njem, njegovih namenih ali o stvareh, ki nam jih ponuja.

3.1.3. Odložena vzajemnost

Izmenjava lahko poteka tudi na drugačen način, brez potrebe po takojšnji izmenjavi. Kar omogoča delovanje vsake skupnosti, je možnost, da nekaj dobimo sedaj, plačamo pa (ne)kdaj v prihodnosti. Prednost te možnosti je bolj fleksibilno okolje, kjer lahko oseba stvari dobi takoj, ko jih potrebuje, ne da bi morala za to dolg čas prej varčevati.

Zaupanje postane v transakcijah te vrste zelo pomembno, saj brez njega ne bi nihče nič dal oz. zamenjal brez takojšnjega plačila. Odlog plačila v transakcijo vnese veliko mero negotovosti, katero moramo omiliti z zaupanjem.

Zlato pravilo za ustvarjanje zaupanja je znan pregovor: »Ne stori drugemu, kar ne želiš da on stori tebi.« Pravilo postavlja dinamiko za transakcijo, ko jaz nekaj dam in hkrati upam, da bom nekoč v prihodnosti za to dobil določeno stvar v zameno.

Definicija: Zaupanje pomeni izročiti določeno dobrino sedaj, v pričakovanju, da bo poplačana v nedoločeni obliki in v nekem nedoločenem trenutku v prihodnosti.

3.1.4. Izpostavljena ranljivost

Zaupanje drugim ne pomeni le izročanje nečesa v upanju, da bomo to dobili poplačano v prihodnosti, temveč tudi možnost izpostavljanja nas samih na način, da lahko drugi izkoristijo našo ranljivost. Če kupujemo avtomobil in ne poznamo njegove »dobre« cene, nas lahko prodajalec prepriča, da je cena avtomobila veliko višja od njegove realne vrednosti, seveda v svojo korist in našo škodo. Če sodelavcu zaupamo težave, ki jih imamo na delovnem mestu, lahko le-ta te informacije uporabi proti nam.

Definicija: Zaupanje pomeni drugim ljudem omogočiti, da izkoristijo naše ranljivosti, ob pričakovanju, da se to ne bo zgodilo.

Še nekatere definicije zaupanja so podane v nadaljevanju:

Dve dodatni definiciji zaupanja sta:

- Zaupanje je pripravljenost biti izpostavljen (ranljiv) dejavnostim poslovnega partnerja (Mayer, Davis, Schoorfman, 1995).
- Zaupanje je prepričanje, da bo poslovni partner deloval v skladu z našim pričakovanjem. (Luhmann, 1982).

Slovar slovenskega knjižnega jezika pa zaupanje razlaga kot prepričanje, da je kdo sposoben, voljen narediti, kar se pričakuje (Slovar slovenskega knjižnega jezika, 2006).

Kljub nekaterim različnim predpostavkam, pa imajo vse definicije zaupanja tudi nekaj skupnega. Vse definicije namreč temeljijo na dejstvu, da je za obravnavanje zaupanje najprej potrebno imeti določeno percepcijo tveganja. Če je namreč izid naše akcije popolnoma predvidljiv ali neodvisen od delovanja tretjih oseb ali institucij, potem tudi zaupanja ne potrebujemo.

3.2. Spekter zaupanja

Zaupanje ni diskretna spremenljivka, temveč zvezna. Zaupanje si lahko predstavljamo kot trak, ki ima dve skrajnosti in določen del med njima. Posamezni deli »traku« oziroma deli spektra zaupanja so opisani v nadaljevanju.

Na eni strani spektra se nahaja slepa vera, kjer naivna oseba naredi vse, kar jo prosimo. Oseba namreč verjame, da so vsi zaupanja vredni, tudi če osebi dokažemo, da temu ni tako. Le malo ljudi je tako naivnih, da slepo verjamejo vsem, pa čeprav vsakdo med nami verjame v določene stvari. To se zgodi, ko naša emocionalnost pretehta nad racionalnostjo, npr. slepo verjamemo, da lahko nogometna ekipa, za katero navijamo, premaga vsako drugo ekipo, čeprav se ob racionalnem razmisleku zavemo, da temu ni tako. Druga skrajnost je paranoja. Paranoična oseba ne zaupa nikomur. Verjame, da so jo vsi pripravljeni oslepariti, če jim le ponudi to možnost. Nekje med paranojo in slepo vero se nahaja razumno zaupanje. V tej točki lahko oseba zaupa ali ne, glede na dokaze in izkušnje, ki jih ima. V tem delu spektra se nahaja velika večina oseb.

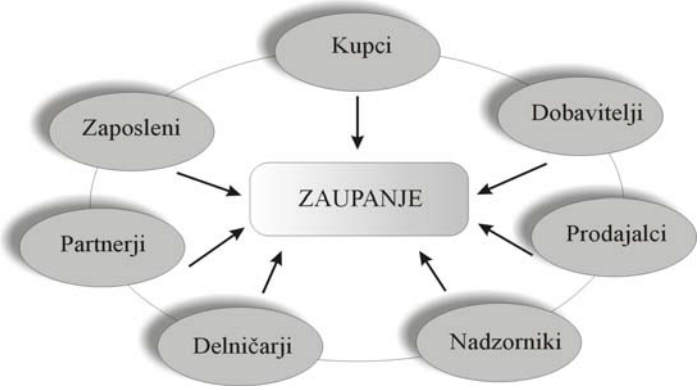
3.3. Vpliv zaupanja na e-poslovanje

Zaupanje je torej ključnega pomena, če je izpolnjena vsaj ena od naslednjih predpostavk (Clarke, 2002, str. 58):

- velika izpostavljenost tveganju enega ali več udeležencev,
- daljši čas, ko obstaja izpostavljenost tveganju,
- malo znanja enega ali več udeležencev o drugem udeležencu, predmetu trgovanja, procesu trgovanja ali možnih izidih trgovanja ali
- osnove za pomanjkanje zaupanja enega ali več udeležencev o drugih udeležencih, o predmetu trgovanja, procesu trgovanja ali možnih izidih trgovanja.

Elektronsko poslovanje izpolnjuje vsaj eno izmed zgoraj naštetih predpostavk, zaradi česar je prisotnost zaupanja zelo pomembna. Kupec namreč večinoma nima informacij o spletnem trgovcu in o izdelkih, ki jih kupuje. Po drugi strani pa lahko pomanjkanje zaupanja predstavlja velik problem. Čeprav je zaupanje kupcev v podjetje zelo pomemben del, pa velja poudariti, da gre zaupanje graditi tudi med vsemi drugimi subjekti, ki s podjetjem sodelujejo. V ta krog zaupanja spadajo še:

Slika 2: Krog zaupanja podjetja



Vir: Clarke, 2002; Lastna prilagoditev.

Na področju ugotavljanja vpliva zaupanja na elektronsko poslovanje, so bile izvedene različne raziskave. Rezultati vseh raziskav pa so enotni; zaupanje je nujno potrebno, če želi podjetje vzpostaviti dolgoročne poslovne odnose (Clarke, 2002, str. 56) s svojimi poslovnimi partnerji. Zaupanje je pomembno tudi kot napovednik zadovoljstva poslovnih partnerjev (Driscoll, 1978). Le poslovni partnerji, ki so z nami zadovoljni, nam lahko zaupajo. Tako lahko iz stopnje zaupanja, ki jo naše podjetje uživa, predvidimo stopnjo zadovoljstva naših poslovnih partnerjev. Ganesan (1994, str. 3) meni, da je posledica zaupanja dolgoročni odnos izmenjave (dobrin in storitev), Morgan in Hunt (1994) pa k temu dodajata še omogočen proces kooperacije.

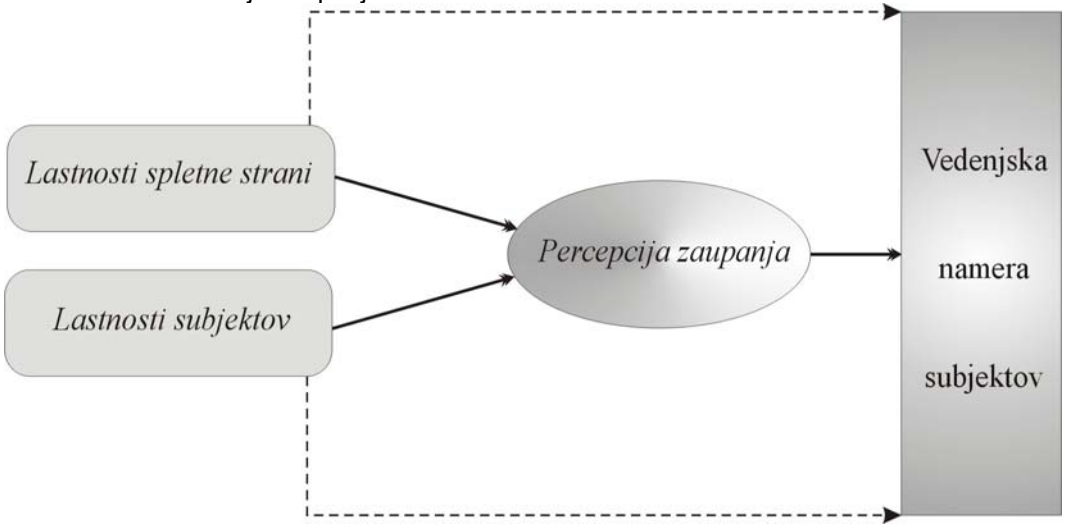
Shankar, Sultan in Urban (2002, str. 335) pravijo, da lahko posledice zaupanja razdelimo v tri kategorije:

- namera izvedbe dejanja (angl. intent to act),
- zadovoljstvo in zvestoba poslovnih partnerjev ter
- učinek podjetja.

Med namero izvedbe dejanja študija prištevamo odnos do spletnega podjetja, percepcijo tveganja, pripravljenost nakupa/poslovanja s podjetjem ter dolgoročno usmerjenost k podjetju. Med zadovoljstvo in zvestobo poslovnih partnerjev lahko štejemo še zavezo k podjetju ter ponovni nakup/interakcijo s podjetjem. Glede na učinek podjetja pa zaupanje vpliva na promet na spletni strani, dohodek podjetja, profitabilnost/ROI ter na vrednost delnic (Shankar, Sultan, Urban, 2002).

Druga raziskava (Sultan et al., 2006, str. 8-9) pa je pokazala, da je zaupanje dejavnik, ki deluje kot vezni člen med lastnostmi spletne strani in lastnostmi subjektov ter med vedenjsko namero subjektov. Lastnosti spletne strani in lastnosti posameznih subjektov namreč vplivajo na percepcijo zaupanja v spletno stran. Nadaljnje vedenje subjekta pa je odvisno prav od zaznanega zaupanja. Če je to veliko, se bo subjekt morebiti odločil za nakup ali poslovno sodelovanje z nami. V nasprotnem primeru pa se bo subjekt verjetno odločil zapustiti spletni portal.

Slika 3: Vezna funkcija zaupanja



Vir: Sultan et al., 2006, str. 35.

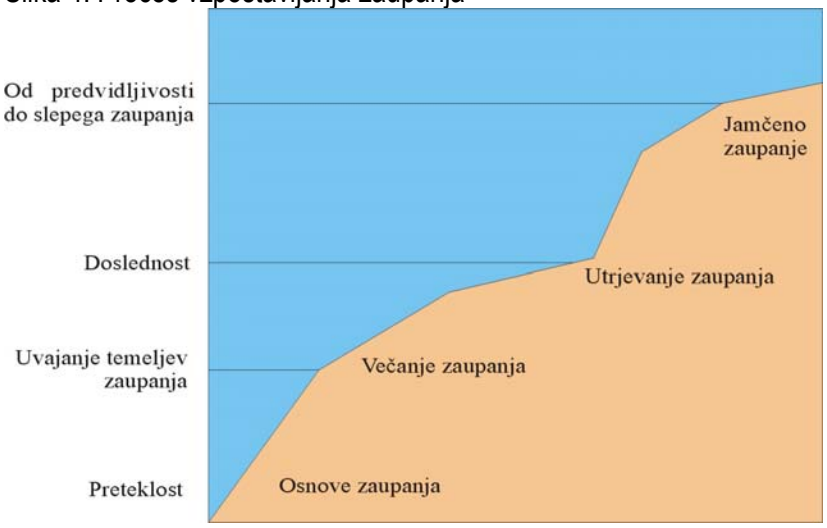
Iz povedanega lahko zaključimo, da je zaupanje res pomembno pri poslovanju s pomočjo tako brezosebnega medija, kot je svetovni splet. Zaradi pomanjkanja ključnih informacij za poslovanje, prevzema zaupanje vodilno mesto v modernem elektronskem poslovanju. Brez zaupanja, ki deluje kot vezni člen med nami in našimi poslovnimi partnerji, bi namreč vsak posel, pa naj bo ta velik ali majhen, padel v vodo. Zato morajo spletna podjetja veliko časa in tudi denarja nameniti vzpostavljanju zaupanja, to pa je dolgotrajen proces.

3.4. Ustvarjanje zaupanja

Podjetja, ki so pravočasno zaznala pomembnost zaupanja in so začela graditi zaupanje že v zgodnjih letih razvoja interneta, imajo sedaj ključno konkurenčno prednost. Kot primer lahko navedem spletna portala Amazon.com in eToys.com (poudariti je potrebno, da so to podjetja, ki so se povsem osredotočila na spletno trgovanje). Oba portala sta začela z gradnjo zaupanja takoj, ko se je pojavila možnost poslovanja preko interneta. Tako sedaj uživata največjo mero zaupanja na svojem področju. Konkurenti, ki se niso osredotočili na možnost elektronskega poslovanja, takoj ko je le-ta postala aktualna, sedaj lahko le sledijo vodilnima podjetjema (Bilstad, Enright, 2007).

Vzpostavljanje zaupanja je zelo težavno in dolgotrajno. Potrebno je upoštevati veliko dejavnikov, tudi takih, ki morda niso v celoti pod našo kontrolo. Proces lahko ponazorimo z grafom:

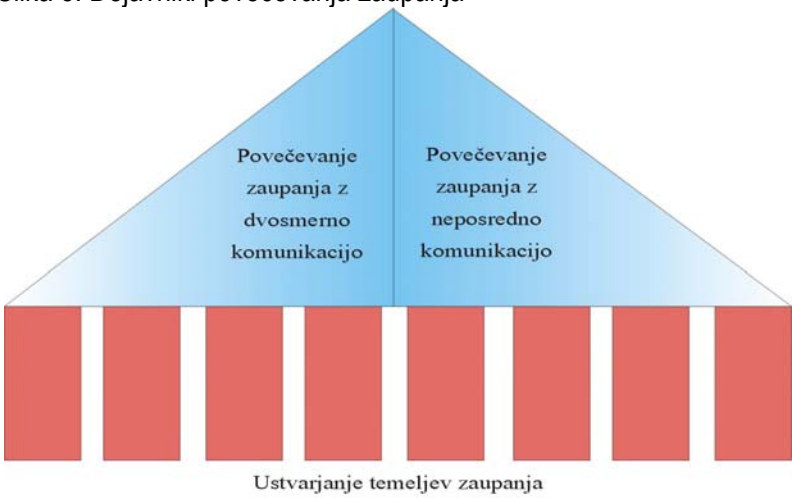
Slika 4: Proces vzpostavljanja zaupanja



Vir: PriceWaterhouseCoopers, 2006, str. 9.

Število študij s področja obravnavanja vloge zaupanja v elektronskem poslovanju se hitro povečuje. Večina njihovih ugotovitev je skladnih (npr. da je zaupanje ključni dejavnik uspeha), vendar se med študijami pojavljajo razlike predvsem v načinu, kako izgraditi, obdržati in povečevati zaupanje. Pričakujem, da se bo število študij še povečevalo, saj je to področje še relativno slabo raziskano. To tezo podpira dejstvo, da v člankih in študijah nisem našel nobenega modela, ki bi v celoti prikazal dejavnike, ki omogočajo in povečujejo zaupanje. Tak model sem poskusil prikazati v naslednji sliki:

Slika 5: Dejavniki povečevanja zaupanja



Vir: Lasten.

3.4.1. Ustvarjanje temeljev zaupanja

V sklopu izgradnje temeljev, ki podpirajo zaupanje, se mora podjetje osredotočiti na (PriceWaterhouseCoopers, 2006, str. 15-23):

- tehnologijo,
- zanesljivost procesov,
- tokove podatkov ter
- zaščito pred kriminalom.

Tehnologija

V času, ko tehnologija napreduje s »svetlobno hitrostjo«, je zelo pomembno, da podjetje skrbi za to, da bo tehnološka infrastruktura podjetja nudila vso podporo poslovnim procesom ne le v sedanjosti, temveč tudi za določen čas v prihodnosti. Če tehnologija tega ne more zagotoviti, se ji ne da zaupati. Podjetje lahko, zaradi težav s strojno opremo, izgubi velik del dohodka, kar pa ni veliko, če poleg enkratnega dohodka izgubi tudi kakšnega večjega stalnega odjemalca oz. poslovnega partnerja. Poleg tega pa lahko izgubo prinese tudi slabo načrtovana prihodnja uporaba tehnologije, saj se lahko število obiskov na portalu poveča v nepredvideni meri, povzroči prenasičenost in posledično prekinitev delovanja strežnika.

PRIMER: Primer zatajitve strežnika zaradi nepredvidenega števila obiskov in ogledov določene vsebine prihaja iz podjetja, od katerega bi to najmanj pričakovali. Maja 1997 se je za vse ljubitelje šaha in računalništva odvil junaški boj med človekom in računalnikom. Ruski šahovski velemojster Gary Kasparov se je namreč »bojeval« z IBM-ovim superračunalnikom Deep Blue. IBM je na svojem spletnem portalu ponudil možnost ogleda dvoboja v živo, preko računalnika. V podjetju pa niso predvideli in pričakovali tako velikega odziva, kot se je dejansko zgodil. Preveč šahovskih zanesenjakov si je namreč poskušalo ogledati dvoboj na spletni strani »www.chess.ibm.com«, tako velikega števila dostopov pa strežnik ni mogel zagotoviti. Zato so uporabniki, namesto dvoboja, od strežnika dobili sporočili "Waiting for reply" in "Failed to connect to server" (Chess fans overload IBM's Web site, 2007). Veliko uporabnikov je tako ostalo brez želene vsebine, kar je nedvomno omajalo zaupanje v tako veliko

konglomeracijo, kot je IBM, ki bi morala bolje predvideti število dostopov in količino prenesenih podatkov ter zagotoviti strežnik, ki bi tak prenos lahko zagotovil.

Zanesljivost procesov

Vsi procesi morajo biti tako sestavljeni, da podjetju zagotavljajo čim hitrejše delovanje (izpolnjevanje naročil, sprejemanje reklamacij ipd.) ob sprejemljivi ravni stroškov. Potrebno je tudi zagotoviti, da pride do čim manj zapletov pri izpolnjevanju zadanih nalog.

PRIMER: Nezanesljivi procesi lahko privedejo do nepričakovanih zastojev v izvrševanju naročil ali reševanju reklamacij. Tako se je zgodilo več osebam, ki so želele kupiti osebni računalnik preko spletnega podjetja CyberMax (Make sure your fast new Web-ordered computer gets to you quickly, 2006). Rok dobave naročenih računalnikov je bil 2 do 3 tedne. Po 8 tednih pa je David Nappi še vedno čakal na dostavo svojega. Po poizvedbi o stanju naročila je izvedel, da na zalogi ni bilo želene grafične kartice. Zanjo je bil predviden rok dobave še dodatni mesec. Poleg grafične kartice je bila pomanjkljiva tudi zaloga procesorjev, katerih rok dobave je bil nedoločen. V tem primeru ni bila zagotovljena zanesljivost procesov. Procesi v verigi vrednosti niso bili zadovoljivo postavljeni in definirani, tako znotraj podjetja kot med podjetjem in dobavitelji, zato je prišlo do zastojev pri dobavi naročenega blaga. Seveda je David izjavil, da bi se odločil za drugačen nakup, če bi vedel za težave, ki jih bo imel pri CyberMax-u. Zagotovo pa lahko trdimo, da se bo temu prodajalcu izogibal tudi v prihodnje.

Tokovi podatkov

Z informatizacijo poslovanja se je povečala tudi količina podatkov, ki jih imajo podjetja shranjene v elektronski obliki. Vsak proces, ki se odvija v podjetju sproži določene tokove podatkov, ki se razbežijo na različne oddelke podjetja; v skladišče, v računovodstvo, v prodajo, ipd. Skrb podjetja za podatke je v tem, da mora zagotoviti vsakemu udeležencu v procesu samo tiste podatke, ki jih ta potrebuje. Premalo podatkov lahko pomeni nezmožnost izpolnitve ciljev procesa, preveč podatkov pa poleg tega, da upočasnjuje pretok le-teh, nudi možnost zlorabe. Potrebno je poskrbeti, da so morebitni tokovi podatkov, ki se gibljejo znotraj in izven meja podjetja, primerno zaščiteni.

PRIMER: Primer velikega kriminalnega dejanja je kraja podatkov v ZDA, ki je do sedaj prizadela 676.000 imetnikov računov pri različnih bankah (Data theft involving four banks could affect 500,000 customers, 2007). Osumljenci so, ko so bili zaposleni na bankah, kopirali podatke o bančnih računih, karticah in transakcijah, ki so jih nato posredovali kriminalnim združbam. Raziskave kriminalistov so pokazale, da je povprečni bančni uslužbenec vsak dan potreboval podatke o 50 bančnih računih, medtem ko so »tatovi« dostopali do podatkov o več kot 500 bančnih računih dnevno. Torej so imeli dostop do podatkov, ki jih dejansko niso potrebovali. Banke bi morale to preprečiti tako, da bi imeli uslužbenci dostop le do podatkov oseb, ki so dejansko pri okencu. To bi lahko zagotovili tako, da bi pred dostopom do podatkov o kartici, morali vtipkati PIN številko kartice, ki jo pozna le lastnik kartice.

Zaščita pred kriminalom

Podjetje mora zagotoviti, da so podatki in procesi nedostopni osebam, ki zanje niso pooblaščene. S primernim požarnim zidom mora preprečiti, da bi se posamezniki mirno »sprehajali« po strežniku in

kradli kakršnekoli podatke. Poleg internetnega dostopa mora podjetje poskrbeti tudi za onemogočanje dostopa do podatkov zaposlenim, ki bi jih lahko izkoristili.

PRIMER: Junija 2005 je kriminalna združba vlomila v podatkovno bazo plačilnega procesorja CardSystems, ki je vsebovala podatke o več kot 40 milijonih kreditnih kartic (Credit card breach: Tracing who dunnit, 2007). V tem primeru bi morala biti zagotovljena celovitost in nedotakljivost podatkovne baze.

3.4.2. Povečevanje zaupanja z neposredno komunikacijo

Ta del piramide sem poimenoval tako zaradi načina komunikacije, ki jo lastnik spletne strani uporablja, da bi povečal ali pa vsaj zadržal obstoječe zaupanje obiskovalcev le-te. Spletna stran v tem primeru služi kot direktna oglasna deska, ki prenaša zaupanje. Očem vsakega obiskovalca so izpostavljene določene sestavine spletne strani, ki mu tako na zavednem ali nezavednem nivoju sporočajo, da je podjetje, ki je lastnik spletnega portala, vredno zaupanja. Sestavin spletne strani, ki povečujejo zaupanje je veliko (Sultan et al., 2006, str. 8-14):

Oblika spletne strani

Že sama oblika spletne strani veliko pove o podjetju. Čeprav se lahko grafični izgled spletnih strani zelo razlikuje, imajo vse boljše spletne strani veliko skupnega. Najpogostejša skupna lastnost strani je velika uporaba belega prostega prostora. Stran mora dajati vtis urejenost in enostavnosti. Uporabnik mora v vsakem trenutku vedeti, kje v shemi spletne strani se nahaja. V nasprotnem primeru se lahko zgodi, da bo uporabnik zmeden in se bo raje odločil za sklepanje poslov z drugim podjetjem; s takim, katerega spletna stran bo enostavnejša in popolnejša.

Navigacija

Navigacija omogoča uporabnikom, da dosežejo željen cilj, ki je lahko nakup ali rezervacija vozovnice, pa tudi povečanje limita na bančnem spletnem portalu. Seveda pa mora biti to opravilo čim hitrejše in čim enostavnejše, zato mora biti navigacija po spletnem portalu intuitivna. Možno je tudi, da ima spletni portal različno navigacijo za različne uporabnike. Npr. Amazon.com ponuja možnost nakupa knjig in ostalih proizvodov z enim klikom. Seveda je pogoj za tak nakup ta, da je uporabnik na portalu že registriran in da je v preteklosti že opravil vsaj en nakup preko tega portala. Tudi drugi portali uporabljajo skrajšano navigacijo za uporabnike, ki pogosto posegajo po njihovih izdelkih in storitvah. Taka vrsta navigacije povečuje zaupanje v spletni portal.

Zasebnost in varnost

Zasebnost in varnost sta ključna pri zagotavljanju visoke ravni zaupanja. Palmer, Bailey in Faraj (2000) ugotavljajo, da izjava o varstvu osebnih podatkov in sodelovanje z drugimi podjetji (npr. pri izvedbi plačila preko spleta) zmanjšuje negotovost in povečuje zaupanje v spletno stran.

Pečati zaupanja (odobritve)

Zaupanje se povečuje, če so na spletni strani prisotni pečati, ki potrjujejo, da spletna stran ustreza določenim standardom. Področij, na katere se nanašajo standardi, je veliko. Spletna stran je lahko odlična npr. na področju oblike, varnosti podatkov, enostavnosti uporabe, primernost spletnega portala

za dostop oseb s posebnimi potrebami ipd. (Department of Justice: Web seals of approval, 2006). Priznan podeljevalec takih pečatov je Trust Guard, primeri njegovih pečatov pa sledijo.

Slika 6: Primeri pečatov zaupanja

Vir: Trust Guard, 2007.

Organizacije, ki podeljujejo take pečate, podjetjem, ki jih želijo pridobiti, postavljajo različne standarde (Department of Justice: Web seals of approval, 2006). Podjetja morajo za pridobitev pečata izpolnjevati določene pogoje in upoštevati standarde. Nato lahko za določeno ceno pridejo do znaka, ki zagotavlja ustreznost spletnega portala.

Kljub temu, da različne organizacije pečatov zaupanja delujejo na enakih področjih, za pridobitev pečata postavljajo različne pogoje in standarde, kar predstavlja težavo. To namreč pomeni, da pečati različnih organizacij niso enakovredni. Težava je tudi v tem, da obiskovalec spletnega portala ne more biti absolutno prepričan, da, kljub izpostavljenem pečatu, portal dejansko izpolnjuje določene pogoje. Znan je namreč primer, ko je spletna trgovina ToySmart.com, kljub izpostavljenemu pečatu TRUSTe, skušala prodati zaupne in osebne podatke o svojih kupcih (Bankruptcy Sale of Children's Personal Information, 2007).

Zaščitni znak

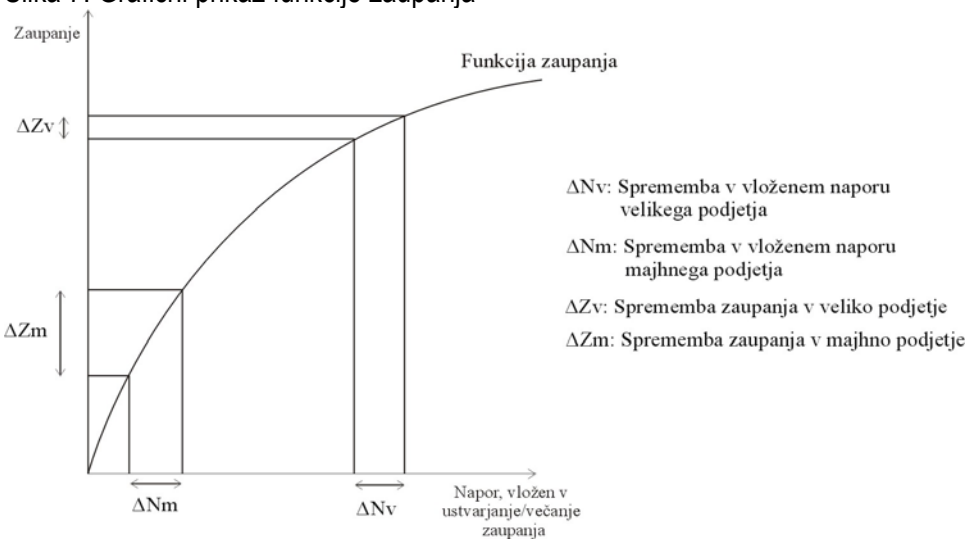
Zaščitni znak (angl. brand) je zelo pomembna sestavina, s katero podjetje nastopa v javnosti. Njen namen je lažja prepoznavnost izdelka, skupine izdelkov ali celotnega podjetja. Čeprav so se prvotni znaki uporabljali pri klasičnem »brick-and-mortar«[3] poslovanju podjetja, se je z razvojem internetnega poslovanja njihova uporabnost še povečala. Zaupanje v zaščitni znak začnejo podjetja graditi takoj po njegovem prvem pojavu v javnosti. Zelo je pomembno, da podjetje vloži zadosti napora v to, da bi zaupanje v znak raslo, in ne dovoli, da bi nepredvideni dogodki omajali to zaupanje.

Ob uporabi zaščitnega znaka na spletnem portalu je zaupanje v portal premo sorazmerno zaupanju v zaščitni znak. To pomeni, bolj kot je bilo podjetje uspešno pri zagotavljanju zaupanja v svoj zaščitni znak, večje bo zaupanje v spletni portal, ki bo s tem znakom opremljen. Posledično lahko podjetje pričakuje tudi večji poslovni uspeh portala.

[3] Podjetja, ki delujejo v fizičnem okolju in ne poslujejo elektronsko.

Raziskave kažejo, da se učinek izpostavljenega zaščitnega znaka razlikuje med portali (Sultan et al., 2006, str. 22). Učinkovitost pečata je večja pri portalih, ki niso znani, medtem ko se pri že zelo znanih in poznanih portalih ta učinkovitost zmanjša. Znani portali namreč že uživajo določeno stopnjo zaupanja s strani kupcev, zato imajo dodatni napori, vloženi v grajenje zaupanja, manjši doprinos, kot pri portalih, ki zaupanja še ne uživajo. To dejstvo lahko posplošimo na vse dejavnike povečevanja zaupanja in prikažemo tudi grafično:

Slika 7: Grafični prikaz funkcije zaupanja



Vir: Lasten.

S pomočjo analiziranih raziskav sem poskusil grafično prikazati funkcijo zaupanja. Prikazuje jo slika 7. Če majhno podjetje vloži določen napor v ustvarjanje ali povečevanje zaupanja (ΔNm), bo doseglo določeno spremembo v stopnji zaupanja znotraj kroga zaupanja (ΔZm). Če pa bo večje podjetje, ki že uživa določeno mero zaupanja (večjo od majhnega podjetja), vložilo enako velike napore (ΔNv), bo njihov učinek precej manjši (ΔZv). Sklepamo lahko, da so vsi inštrumenti povečevanja zaupanja veliko bolj uspešni, ko podjetje zaupanja še ne uživa ali pa je le-to zelo majhno. Večje kot je zaupanje v podjetje, več napora bomo morali vložiti, če ga bomo hoteli še dodatno povečati.

Pri ustvarjanju zaupanja v spletni portal v podzavesti subjektov, ki načrtovano ali naključno obiščejo spletno stran, pa so sestavine spletne strani tudi v primerjavi druga z drugo različno učinkovite. Raziskava (Sultan et al., 2006) kaže, da je izmed sestavin spletne strani najučinkovitejša navigacija. Sledi izpostavljenost zaščitnega znaka podjetja. Na tretjem mestu se nahajata zasebnost in varnost, sledi jima pa oblika spletne strani in, na zadnjem mestu, pečati zaupanja.

3.4.3. Povečevanje zaupanja z dvosmerno komunikacijo

Zaupanje v spletni portal se lahko spreminja glede na izkustvo in doživljanje, ki ju je oseba občutila pri preteklem poslovanju preko portala. Vsakič, ko ima oseba določene stike s portalom, le-ta pusti v podzavesti osebe nekaj povečanega ali zmanjšanega zaupanja. Temu se ne moremo izogniti. Lahko pa skušamo doseči, da bodo izkustva s portalom vedno pozitivna in tako bo zaupanje v portal vedno večje. Izkustva, ki lahko povečajo zaupanje, so obravnavana v vrstnem redu, od tistih, ki so najbolj direktna in verjetna, do tistih manj direktnih in verjetnih (Clarke, 2002).

Neposredno razmerje

Količina in pogostost opravljanja poslov preko spletnega portala lahko v poslovnem partnerju vzbudi vedno močnejši občutek zaupanja. Bolj ko so poslovna razmerja pogosta in več ko jih je, večje bo zaupanje med partnerjema. Seveda je potrebno omeniti, da se morata oba udeleženca ravnati po pričakovanjih partnerja. V nasprotnem primeru do medsebojnega zaupanja seveda ne bo prišlo, pa tudi vso prihodnje poslovno sodelovanje je postavljeno pod vprašaj. Zato je neposredno razmerje med poslovnima partnerjema najmočnejši in najkredibilnejši dejavnik, ki povečuje zaupanje v poslovni portal.

Neposredna izkušnja

Pot do neposrednega razmerja pelje preko neposredne izkušnje. Pri tem gre za to, da vsaj enkrat opravimo transakcijo preko spletnega portala ali vsaj vidimo, kako jo drugi opravijo. Veliko spletnih portalov ima možnost, da se registrirani uporabniki »sprehodijo« skozi vse korake transakcije, vendar se do zadnjega koraka, ko se transakcija dejansko potrdi in izvede, ne zgodi nič. Namen tega je, da prva neposredna izkušnja vzbudi dobre občutke o portalu in posledično zaupanje le-temu.

Predano zaupanje

Predano zaupanje je najmanj kredibilno. Pri tem gre za potovanje zaupanja »od ust do ust«. Kdor je že imel bodisi neposredno izkušnjo bodisi neposredno razmerje preko poslovnega portala, lahko o njej poroča svojim poslovnim partnerjem, prijateljem, sorodnikom. Preko socialnih mrež lahko to poročanje doseže zelo široko publiko, vendar lahko pri prenosu teh sporočil pride do distorzije[4], zato so manj kredibilna.

3.4.4. Pet enostavnih in preizkušenih napotkov za povečanje zaupanja

Ob pomanjkanju zaupanja naših poslovnih partnerjev lahko naš portal deluje proti nam. Kot največje razloge za pomanjkanje zaupanja lahko opredelimo(Top 5 Easy & Proven Ways to Increase Consumer Trust Online, 2007):

- strah poslovnih partnerjev, da nismo tisti, za katere se izdajamo,
- strah pred izgubo podatkov ter
- skrb, da se ne bodo imeli kam obrniti v primeru izjalovitve posla.

Z namenom zagotavljanja in povečanja zaupanja v naše podjetje je v nadaljevanju opisanih pet enostavnih in poceni napotkov (povzeto po Top 5 Easy & Proven Ways to Increase Consumer Trust Online, 2007):

- **Spletni portal mora biti zaščiten pred hekerji**

Ob neštetih poročilih o ukradenih podatkih kreditnih kartic ni čudno, da so naši poslovni partnerji zaskrbljeni. Kako so lahko prepričani v varnost njihovih podatkov, če še velike banke ne morejo zagotoviti varnosti? Obrniti se moramo na specializirane internetne organizacije, ki bodo potrdile, da je naš portal zaščiten pred hekerji. Nato njihov znak prikažemo na vsaki spletni strani. Ta način je enostaven in hiter. Najbolj znani organizaciji, ki se ukvarjata z zaščito pred hekerji, sta Xentinel Security in Scan Alert.

[4] Sprememba smisla sporočila ali sporočila samega.

Slika 8: Hackerfree pečat

Vir: Xentinel, 2007.

- **Uporabite Square Trade**

Square trade pečat se je hitro razširil in postal sredstvo za večanje zaupanja v vseh vrstah transakcij. Square Trade certifikat nam pomaga, saj vliva našim poslovnim partnerjem zaupanje in jamči varnost spletne transakcije.

Slika 9: Square trade pečat

Vir: Squaretrade, 2007.

- **Slika pove več kot tisoč besed**

Na spletni portal postavite svojo sliko. To pomaga ustvariti iluzijo fizičnega kontakta, kar poveča zaupanje. Poslovni partnerji vas bodo tako videli kot dejansko osebo in ne več kot le enega izmed mnogih spletnih prodajalcev.

- **Naj poslovni partnerji govorijo**

Vprašati moramo za mnenja in komentarje naših poslovnih partnerjev vselej, ko je to mogoče. Ta mnenja postavimo na spletni portal. Če je možno, lahko k tekstu postavimo še sliko avtorja mnenja.

- **Postavimo tveganje na nasprotno stran**

Zajamčiti moramo, da se tveganje prenese s strani partnerja k nam. Če bo ta videl, da smo odgovorni, delovni in da smo nase prevzeli tveganje, bo pripravljen seči v žep. Naše zagotovilo o prevzetem tveganju moramo ponosno razkazovati na vsaki strani spletnega portala, tako grafično kot tekstovno.

Najbolj razširjeni način vzpostavljanja in večanja zaupanja je izjava o politiki zasebnosti (Meinert et al., 2006), ki je uradna izjava podjetja, ki pojasnjuje kako podjetje zbira, obdeluje in posreduje podatke, komu jih posreduje ter kako lahko lastnik podatkov do njih dostopa in jih briše. Izjava o politiki zasebnosti je ena izmed enostavnejših in cenejših metod povečevanja zaupanja (Pennington, Wildcox, Grover, 2004).

3.5. Politika zasebnosti

V srednjem veku so bili ljudje prepričani, da se v imenu skriva velika moč, zato svojih pravih imen niso nikoli prostovoljno izdajali. V modernih časih pa vemo, da se v imenu ne skriva moč, ampak veliko denarja. Internet je prepoln oseb in organizacij, ki na vsak način želijo izvedeti naše pravo ime, »internetno« ime oz. vzdevek, naslov elektronske pošte ipd. Brezplačne informacije, brezplačne slike, brezplačno snemanje različnih datotek… vse ima svojo ceno – izgubo mrežne zasebnosti. Veliko ljudi samo skomigne z rameni in prostovoljno izda podatke, saj »je to samo ime in elektronski naslov, v čem je težava?«. Kaj pa z reklamnimi sporočili napolnjen poštni predal? Lahko ji rečemo »spam«,

nezaželena ali vsiljena pošta, vendar dejstvo je, da takoj, ko izdamo elektronski naslov in se vpišemo v katerikoli poštni seznam, s tem lahko dovolimo, da podjetje pošilja take vrste pošte na naš naslov. Poštni seznami, ki privabljajo s pretvezo zastonj informacij, ustvarjajo milijone in milijone dobička s prodajo imen, naslovov elektronske pošte in drugih podatkov vseh, ki so zadosti naivni, da se na tak seznam vpišejo. Verjetnost, da bomo s tem postali žrtev vsiljene pošte, je zelo velika. Na internetu je namreč anonimnost zelo dragocena dobrina, ki jo le stežka obdržimo. V letih začetnega razvoja interneta je bila anonimnost še lahko dosegljiva. Nihče ni vedel, kdo se skriva za vzdevkom. Sedaj pa to skoraj ni več mogoče. Sedaj vsi vedo, kdo je kdo in kaj kdo dela. Nelagodno se počutimo, ko zazvoni telefon. Bojimo se dvigniti telefonsko slušalko, da nas oseba na drugi strani slušalke ne bi nadlegovala s telefonsko anketo ali prodajo, prav tako pa se bojimo odpreti e-poštni predal, da ne bi v njem našli reklame za najnovejšo zeliščno Viagro.

Število izgub podatkov v podjetjih je vedno večje. Razlogi za tako izgubo so različni; vdor v računalniški sistem, izguba podatkov med prenosom, kraja podatkov s strani zaposlenih v podjetju in ukradeni diski, prenosni računalniki ipd. (Pricewaterhousecoopers, 2006, str. 5-8). Vendar za potrošnike to ne bi predstavljalo večje težave, če se v informacijskih sistemih ne bi nahajali določeni podatki o njih samih. Zato je še toliko bolj pomembno, katere podatke zaupamo spletnim portalom oz. podjetjem.

Katere podatke zbirajo podjetja

Podjetja zbirajo podatke, tako o dostopih do spletnih strani kot podatke o osebah, ki do njih dostopajo. Podatke o dostopih zbirajo zaradi izdelave statistike o spletnih straneh. Tega se lahko lotijo sama, lahko pa uporabijo storitve drugih podjetij. Najbolj znana je storitev Google Analytics, ki je na voljo brezplačno in zbira veliko podatkov o uporabnikih spletnih strani (Google, 2006): od števila dostopov do vsake spletne strani, do prehodov med določenimi spletnimi stranmi. Poleg tega pa nazorno prikaže tudi, iz katerega geografskega območja so osebe, ki se na spletno stran povežejo.

Osebne podatke (o obiskovalcih strani), ki jih podjetje zbira, lahko razdelimo na tri kategorije (Meinert et al., 2006, str. 132). V prvo kategorijo spadajo kontaktni podatki. Mednje štejemo ime uporabnika, naslov, elektronski naslov, telefonsko številko, ipd. Ob morebitni izgubi teh podatkov nas lahko doleti le nadlegovanje preko spletne pošte, pošte ali telefona. Drugi so biografski podatki. Primer le-teh so podatki o letnem prihodku, o osebnih zanimanjih, preferencah, hobijih ipd. Tretja vrsta pa so finančni podatki. Ti so številka kreditne kartice, datum poteka kartice, številke bančnih računov ipd.

Zakaj podjetja zbirajo podatke

Kot je bilo že napisano, so podatki vedno bolj vredne dobrine, za katere so podjetja pripravljena veliko plačati. Če pa lahko podjetje pride do podatkov tako, da jih dobi skoraj brez stroškov, so še toliko bolj dragoceni. To lahko dosežejo z zbiranjem podatkov o obiskovalcih spletne strani.

Podatke o statistiki spletnih strani, torej o številu dostopov do posamezne strani, sosledje strani ipd. je lahko za podjetje zanimivo, ker lahko tako določi, katere strani so za kupce najbolj privlačne, katere strani niso zanimive, na kateri spletni strani je verjetnost dokončane transakcije največja, na kateri je največja verjetnost prekinitve seje ipd. Te podatke lahko podjetje uporabi za izboljšanje svoje ponudbe

(tako, da izloči nezanimive izdelke ali storitve). Prav tako so uporabni tudi za izboljšanje izgleda in funkcionalnosti spletnega portala, saj lahko z njihovo pomočjo tudi ugotovimo, zakaj kupci prekinejo transakcijo in je ne dokončajo.

Kontaktni podatki so za podjetje zanimivi predvsem iz marketinškega vidika. S pomočjo poštnega seznama, na katerega se vpišejo obiskovalci portala, lahko podjetje svoja reklamna sporočila pošilja preko spletne pošte. Poleg tega, da je taka vrsta oglaševanja tako rekoč brezplačna, ima tudi vrsto drugih prednosti. Reklama tako doseže večji krog naslovnikov, ki so bolj geografsko razpršeni, kot jih lahko katerakoli druga vrsta reklame. Poleg tega pa velja, da lahko tako reklamo posredujemo občinstvu, ki se za naše izdelke ali storitve res zanima, saj se sicer naslovniki ne bi nahajali na poštnem seznamu.

Biografski podatki podjetju predstavljajo enostavno možnost, kako reklamna sporočila personaliziramo glede na naslovnika. Glede na izražena zanimanja in preference podjetje ve, ali naj določeni osebi pošlje ponudbo za najnovejši fotoaparat ali za nov šivalni stroj. Poleg tega pa lahko na podlagi dohodka osebe personaliziramo ponudbo na ta način, da ponudimo izdelke nižjega ali višjega kakovostnega in cenovnega razreda.

Izguba **finančnih podatkov** lahko lastniku le-teh prinese veliko denarno izgubo. Posamezniki izdajo te podatke, ko se odločijo dokončati nakup preko spletne strani. Podjetje jih seveda potrebuje, da lahko izvrši transakcijo. Čeprav bi lahko, podjetja navadno nimajo lastne aplikacije, ki bi omogočala izvedbo plačila na portalu, zato to prepustijo drugim, specializiranim podjetjem. Dve taki podjetji sta Ccbill.com in PayPal.com. Na ta način je razpolaganje s finančnimi podatki, ki jih ima podjetje, omejeno, zato je verjetnost zlonamernega ravnanja z njimi zmanjšana. Potrebno je povedati, da število podjetji, ki za plačilo strank uporabljajo aplikacije drugih podjetij, narašča. Razlog je seveda v večjem zaupanju specializiranim aplikacijam.

Podjetja torej zbirajo podatke iz več razlogov. Vsaka vrsta podatkov ima tako določene lastnosti, zaradi katerih jih je vredno shraniti in uporabiti. Vsem podatkom, ne glede na vrsto je skupno, da jih lahko podjetje v vsakem trenutku posreduje ali celo proda tretjim osebam ali podjetjem, kar je lahko zelo dobičkonosna dejavnost. Koristi od tega imata tako podjetje, ki zbira in proda podatke, kot podjetje, ki jih odkupi. Največjo škodo utrpi seveda nič hudega sluteči obiskovalec strani, ki je svoje podatke izdal nekemu portalu. Ta škoda se kaj kmalu pokaže v obliki z reklamnimi sporočili nabasanega poštnega predala. Bolj ko se nato trudimo brisati ta nadležna sporočila, več jih prihaja. Poštni naslov se tako razširi in shrani v ogromnem številu poštnih seznamov. Četudi poskušamo vse naslove dodati v spisek blokiranih pošiljateljev, se število poštnih seznamov, na katerem se naš elektronski naslov nahaja, vztrajno in hitro veča. Onemogočiti vse pošiljatelje je zato nemogoče.

Kako podjetja pridobijo podatke

Pridobivanje podatkov poteka na različne načine. Trije najpogostejši načini so avtomatično zbiranje podatkov s pomočjo strežniškega programa, zbiranje podatkov s strani podjetij, ki na naši strani

oglašujejo z reklamnimi pasicami, in podatki posredovani samovoljno, s strani kupcev (Bilstad, Enright, 2007).

Večina strežniških programov avtomatično zbira veliko količino podatkov o navadah pri spletnem brskanju: katere strani obišče uporabnik, čas in trajanje obiska strani, oglase, ki si jih uporabnik na strani ogleda in sledi njihovi povezavi, o opravljenih nakupih, katere ključne besede je uporabnik uporabil pri poizvedovanju po bazi oz. portalu ipd. Še več, večina spletnih programov avtomatično zbira podatke o uporabniškem IP naslovu, imenu računalnika, s katerega uporabnik dostopa, vrsti spletnega brskalnika, lastniku omrežja, v katerem se računalnik nahaja in domeno (Bilstad, Enright, 2007).

Kot primer zbiranja podatkov preko drugih spletnih strani in portalov, lahko obravnavamo namišljeno oglaševalno mrežo DoubleDealer.com. Ta mreža postavlja svoje reklamne pasice na vsebinsko različne portale, ki ponujajo različne izdelke in storitve. Doubledealer z uporabo piškotkov gradi profile uporabnikov in njihovih zanimanj in želja, ki jih dolgoročno posodablja. Tako ima vsakdo, ki je kdajkoli pogledal njihov oglas, ustvarjen svoj profil. Vsakič, ko si uporabnik ogleda oglasno pasico te mreže na katerемkoli spletnem portalu, njegov računalnik pošlje Doubledealer-ju sporočilo o vrsti takrat obiskane spletne strani. S pomočjo teh profilov lahko podjetja svojo ponudbo personalizirajo in jo posredujejo osebam, pri katerih je verjetnost nakupa največja.

Tretji način zbiranja podatkov se nanaša na prostovoljno posredovanje podatkov s strani uporabnikov oz. obiskovalcev strani. Na voljo sta dva načina, s katerimi lahko vsakdo posreduje podatke lastniku spletnega portala. Prvi je pošiljanje spletne pošte. Čeprav se e-mail sporočila ponavadi uporabljajo za pridobivanje informacij (potreba uporabnika po dodatnih informacijah, pojasnilih, ipd.), pa lahko uporabnik z njim, hote ali nehote, posreduje svoje podatke. Najpogosteje so to naslov spletne pošte, ime in priimek, lahko pa se pošiljajo tudi drugi podatki, od naslova do številke kreditne kartice. Potrebno je poudariti, da so tako pridobljeni podatki zelo nestrukturirani. Zaradi tega se veliko podjetij odloča za uporabo drugega načina komunikacije. To je uporaba spletnih obrazcev. Uporabniki se največkrat srečajo s spletnimi obrazci, ko je potrebno spletnemu portalu posredovati podatke o naših zanimanjih ali preferencah. Poleg tega se obrazci uporabljajo tudi pri vnašanju podatkov ob morebitnem nakupu oz. plačilu preko spleta. Navadno obrazec od nas zahteva vnos imena in priimka, naslova, ipd. Kot že omenjeno, pa veliko podjetij uporablja spletne obrazce kot način komunikacije s partnerji. V tem primeru moramo v spletni obrazec, poleg imena in priimka, vnesti tudi svoje vprašanje ali potrebo po informaciji. Navadno je na voljo dodatno polje, kamor lahko vpišemo svoj e-mail naslov, v primeru, da želimo odgovor prejeti po elektronski pošti. Čeprav niti ta način ni popolnoma strukturiran, pa je njegova strukturiranost večja, kot v primeru neposrednega elektronskega sporočila. Zato je tudi njegova uporabnost večja.

Tehnologija zbiranja podatkov

Podatki uporabnikov spletnih strani se zbirajo in shranjujejo na več načinov. Najbolj uporabljena dva načina sta zbiranje podatkov s pomočjo piškotkov in s pomočjo spletnih svetilnikov (Bilstad, Enright, 2007).

Piškotki
Spletni portali pošiljajo piškotke na uporabnikov računalnik, kjer se le ti v obliki datoteke shranijo na trdem disku in služijo kot identifikacija uporabnika. V primeru, da uporabnik ponovno obišče isti portal, le-ta zazna obstoj piškotka na disku in tako ve, da je uporabnik na tem portalu že bil. Čeprav lahko uporabniki na spletnem brskalniku onemogočijo uporabo piškotkov, nekateri portali zahtevajo njihovo uporabo. V primeru, da uporabnik skuša obiskati tak portal in ima onemogočeno uporabo piškotkov, se strani ne bodo odprle.

Piškotki imajo dva namena. Prvi je ta, da si spletna stran zapomni uporabnika. Na ta način se lahko spletni portal prilagodi potrebam in željam uporabnika. Primer je uporaba piškotkov za avtomatično pridobivanje uporabniškega imena in gesla na spletnem portalu.

Drugi namen je uporaba piškotkov, ki je bila že omenjena, za izgradnjo profila uporabnika. Tako se pri uporabniku kopičijo podatki o obiskanih straneh in opravljenih nakupih. Oglaševalna agencija le zbere te podatke in jih shrani v centralno podatkovno bazo.

Spletni hrošči
Poznamo še veliko imen, pod katerimi se skriva ista nadloga; sledilni hrošč (angl. tracking bug), pikselski označevalec (angl. pixel tag) in prozorni gif (angl. clear gif). Spletni svetilniki so slikice, ki so dodane spletnim stranem ali HTML-oblikovani spletni pošti. Navadno so očem nevidne, saj je njihova velikost omejena na eno piko (en piksel višine in en piksel širine). Vsakič, ko uporabnik naloži stran s spletnim svetilnikom, ta pošlje ping[5] na strežnik spletnega oglaševalca (kot je DoubleClick.com), kjer se zabeležijo podatki o IP naslovu uporabnika, času dostopa do spletne strani, vrsti spletnega brskalnika, obstoju piškotkov domačega strežnika ipd.

Mnenje mnogih strokovnjakov je, da so spletni svetilniki bolj nevarni od piškotkov. Razlog ni le v tem, da svetilnikov ne vidimo in se jih ne da onemogočiti na spletnem brskalniku (kot to velja za piškotke), temveč tudi v tem, da lahko spletni svetilniki vsebujejo izvršljive računalniške programe, ki pregledujejo vsebino datotek na uporabnikovem disku in jo celo razpošiljajo tretjim osebam in organizacijam. Ker lahko spletni svetilniki obstajajo tudi v oglaševalnih pasicah, se njihovega obstoja morebiti ne zaveda niti lastnik spletnega portala.

Varstvo podatkov
Podjetja morajo zagotoviti popolno varnost podatkov, od trenutka, ko so ti vnešeni, do trenutka, ko so popolnoma uničeni oz. izbrisani. Glede na življenjski cikel podatkov lahko razdelimo potrebo po varovanju podatkov v tri faze.

V prvi fazi mora podjetje zagotoviti varnost in integriteto podatkov med prenosom podatkov od njihovega lastnika k podjetju, torej v tistem intervalu, ko spletni deskar na spletnem portalu klikne na gumb »pošlji« ali »submit« (če gre za spletni obrazec) in ko se podatki dejansko zapišejo na disk strežnika. Med tem prenosom so podatki izpostavljeni različnim nevarnostim, od napak pri prenosu,

[5] Podatkovni paket.

prestrezanja podatkov, pa do napak komunikacijskega omrežja (Kajić, 1996). Prav tako so podatki izpostavljeni nevarnostim med drugimi prenosi podatkov znotraj in izven podjetja.

Načini preverjanja pravilnosti prenosa podatkov so se v zgodovini zelo spreminjali. Prvi način je bil parnostni bit (angl. parity check), vendar so se zaradi pomanjkljivosti tega načina razvili novi, vse bolj zapleteni načini.

Do napak v omrežju lahko, kljub napredni tehnologiji, vseeno pride. »ISO[6] s svojimi modeli za zagotavljanje varnosti v zvezi z napakami v komunikacijskih omrežjih predvideva njihovo odkrivanje, zapisovanje, obveščanje uporabnikov in (v mejah zmožnosti) njihovo avtomatično odpravljanje, s čimer omogoča neprekinjeno delovanje teh omrežij.« (Kajić, 1996)

Tretja možna nevarnost je prestrezanje podatkov. Pri tem gre za prilastitev podatkov, ki se prenašajo preko omrežij, s strani tretjih oseb.

Za razliko od preverjanja pravilnosti podatkov in napak v omrežju, na katere podjetje (lastnik portala) nima vpliva, pa lahko pri prestrezanju podatkov igra ključno vlogo. Z uporabo kriptografije[7] zagotovi, da so podatki, ki jih kdorkoli prestreže, zanj neberljivi in torej neuporabni.

Da bi zagotovil integriteto in nedotakljivost med prenosom podatkov tudi v primeru prestrežene komunikacije, mora lastnik portala uporabiti vse možne načine zaščite. Enkripcijo se kot tak način zaščite uporablja na različne načine (Secure data transmission methods, 2007). Spletno pošto (s pripadajočimi priponkami) lahko zaščitimo s pomočjo spletnih storitev ali pa s pomočjo PKI[8]. Enkripcija spletnih portalov poteka s pomočjo standarda SSL[9], ki šifrira podatke, ki se preko teh spletnih portalov prenašajo. Šifriranje je potrebno vsakič, ko obstaja možnost, da bodo podatki prišli v roke ne le naslovniku, temveč tudi nepooblaščenim osebam. Zato je šifriranje potrebno še v naslednjih primerih:

- Nekatere organizacije uporabljajo izmenjavo podatkov med različnimi aplikacijami, tako preko zasebnega omrežja kot preko interneta, zato je šifriranje nujno potrebno.
- Tudi komunikacija oddaljenega uporabnika predstavlja potencialno tveganje prestrezanja podatkov.
- Podatki, shranjeni na prenosnih računalnikih, dlančnikih in podobnih napravah so zelo podvrženi krajam, že zaradi vrednosti naprave, ki jih nosi. Zato je za organizacije priporočljivo take podatke šifrirati.
- Organizacije (navadno večje) uporabljajo brezžično omrežje, do katerega imajo dostop tudi nepooblaščene osebe. Zato je potrebno šifriranje vseh podatkov, ki se preko takega omrežja prenašajo.

Druga faza zaščite podatkov obsega zaščito podatkov v času, ko so shranjeni na disku strežnika ali katerega drugega računalnika v podjetju. Gre za zaščito podatkov pred zaposlenimi v podjetju. V tej fazi

[6] ISO – International Organization for Standardization – Mednarodna organizacija za standardizacijo
[7] Metoda šifriranja podatkov.
[8] Pulic Key Infrastructure, infrastruktura javnih ključev.
[9] Secure Socket Layer, sloj varnih vtičnic.

so grožnje precej raznolike. Lahko namreč pride do napak ali spregledov pri vnašanju ali popravljanju podatkov, ponaredb ali kraj podatkov, sabotaž s strani nezadovoljnih zaposlenih, fizičnih poškodb, izgube integritete ter zaupnosti podatkov ter nepopolnega brisanja podatkov. Wugmeister in Lyon (2007) ugotavljata, da je faktor zaposlenih zelo zapostavljen. Ugotavljata, da se v smislu varnosti podatkov vse preveč izpostavlja možnosti vdorov (hekerjev) in se obenem ne omenja tveganja, ki ga predstavlja sodelavec v sosednji pisarni. Večina zaposlenih je sicer vrednih zaupanja in zanesljivih, vendar se v trenutku naglice, jeze ali pohlepnosti lahko spremenijo v resno grožnjo podjetju in njegovim podatkom. V medijih tako pogosto zasledimo veliko primerov iz resničnega življenja o takih ali drugačnih izgubah podatkov:

- Zaposleni neke finančne institucije je nenamerno pustil svoj prenosni računalnik, v katerem so se nahajali podatki o vseh strankah, v odklenjenem avtomobilu, iz katerega je bil ukraden.
- Nekdanji zaposleni podjetja je med dostopanjem do baze podatkov podjetja izbrisal vse podatke o plačah, nagradah in transferih zaposlenih.
- Nek zaposleni je na skrivaj kopiral osebne podatke pol milijona strank in je podjetju grozil, da jih bo objavil na internetu, če mu podjetje ne bo plačalo milijonske odkupnine.

Sullivan (2007) tako ugotavlja, da se 70% kraj identitete v ZDA začne s krajo podatkov s strani zaposlenih. Zato je omejevanje dostopa do podatkov prvi ukrep za zagotavljanje varnosti le-teh. Vsakemu zaposlenemu moramo omogočiti dostop le do tistih podatkov, ki jih potrebuje za poslovanje, in hkrati onemogočiti dostop do drugih podatkov.

Zavedati se je potrebno, da podatki v podjetju niso vsi enaki. Različne vrste podatkov potrebujejo različno stopnjo zaščite. Zato je potrebno v podjetju narediti popolno klasifikacijo podatkov, tako da se vsakemu izmed njih določi stopnjo zaupnosti oz. potrebno stopnjo zaščite. Poleg klasifikacije podatkov je potrebno ugotavljanje vseh načinov prenosov podatkov znotraj in izven podjetja. Podatki se namreč prenašajo na različne načine; preko spletne pošte, s pomočjo prenosnih računalnikov, dlančnikov, spominskih ključkov in nenazadnje na tiskanih medijih. Potrebno je identificirati vsak način prenosa podatkov in tudi temu določiti stopnjo zaupnosti. Nato mora vodstvo podjetja določiti, katere načine lahko zaposleni uporabljajo, kateri so prenevarni oz. preveč izpostavljeni kraji podatkov in pod katerimi pogoji se lahko določeni načini prenosa uporabljajo (npr. prenosniki morajo biti primerno zaščiteni z geslom, spletna pošta mora biti kodirana).

Naslednja stopnja je identifikacija nosilcev procesov v podjetju. Na ta način lahko določenemu procesu dodelimo »lastnika«, ki je nato odgovoren za zagotavljanje varnosti podatkov znotraj svojega procesa. Nosilec procesa pa je odgovoren tudi za dolgoročni razvoj politike varnosti podatkov, seveda v okvirih svojega procesa.

Vsako podjetje mora izdelati svojo politiko varnosti, ki mora opisovati klasifikacijo podatkov podjetja, možne načine prenosov podatkov, zaščito le-teh pri prenosu, dostop do podatkov ipd. Varnostna politika mora prikazati tudi nosilce vseh procesov in tako spodbujati zaposlene, da se z vprašanji ali skrbmi o določenem procesu obrnejo neposredno na nosilca.

Najpomembnejša stopnja je učenje zaposlenih. Pri tem ni zadosti, da zaposlenim pošljemo kopijo varnostne politike preko spletne pošte in nato predvidevamo, da so jo vsi prebrali in razumeli. Potrebna je diskusija z zaposlenimi, med katero se obravnavajo ne le osnovni, temveč tudi specifični pogledi politike varnosti. Potrebno je jasno razložiti, kakšen odziv zaposlenih se v določenih situacijah pričakuje in kaj morajo le-ti storiti v primeru izgube podatkov ali suma vdora v sistem ali podatkovno bazo.

Zadnja in najbolj radikalna stopnja zaščite podatkov pred zaposlenimi je (video) nadzor (Data protection and monitoring at work, 2007). Čeprav je lahko videonadzor zelo vsiljiv in nadležen, predstavlja najzanesljivejši način, kako preprečimo zlorabo podatkov, če pa se že zgodi, lahko s pomočjo posnetkov ugotovimo, kdo je zanjo kriv. Zavedati se moramo, da ima lahko videonadzor negativne posledice, saj nedvomno vpliva na prisotnost stalnega pritiska na zaposlene, vendar je pomemben dejavnik zagotavljanja varnosti tako podatkov kot zaposlenih v podjetju.

Tretja faza zahteva zaščito podatkov pred nepooblaščenim dostopom tretjih oseb. Nevarnosti, ki jih v tej fazi zaznamo, so zlonamerni vsiljivci in zlonamerni programi.

Vsiljivci, znani tudi pod imenom »hackerji« ali »crackerji«, so osebe, ki vdirajo v računalniške sisteme iz različnih razlogov. Navadno je razlog za različne vdore le samodokazovanje, lahko pa se zgodi, da je namen bolj pridobitniški. Vladimir Levin, ruski matematik, je tako svoj vdor v sistem banke Citibank izkoristil za prenos 10,7 milijonov ameriških dolarjev na različne račune v različnih državah (Wikipedia, 2007). Med zlonamerne programe štejemo viruse, črve (angl. worms), trojanske konje (angl. trojan horses), logične bombe ter druge programe.

Podjetje mora zagotoviti primerno zaščito pred vdori vsiljivcev, kar lahko doseže s primernim požarnim zidom, ki ga je potrebno posodabljati. Požarni zid je sistem za preprečevanje nedovoljenih dostopov do zasebne mreže (Webopedia, 2007). Lahko je implementiran tako v strojno kot v programsko opremo. Požarni zid se najpogosteje uporablja za onemogočanje dostopa nepooblaščenih oseb, ki skušajo preko interneta vdreti v zasebna omrežja ali intranet podjetja. Požarni zid lahko pregleda tudi vsa odhodna in dohodna sporočila in izključi tista, ki se ne skladajo z določenimi varnostnimi kriteriji.

Virus je program, ki je sposoben kopirati sam sebe in se tako prenaša z računalnika na računalnik brez vednosti uporabnika. Namen nekaterih virusov je povzročitev škode, tako da poškodujejo programe, izbrišejo datoteke ali formatirajo diske, namen drugih pa ni povzročiti škodo, temveč le njihova reprodukcija in prikaz njihove prisotnosti uporabniku, preko tekstovnih, grafičnih ali avdio sporočil. Trojanske konje lahko označimo kot programe znotraj programov. So programi, ki so na prvi pogled uporabni in zanimivi, ko pa jih namestimo se poleg osnovnega programa prenese tudi drug, nezaželen program, ki povzroča škodo. Čeprav črvi ne kradejo podatkov, ne brišejo datotek in ne podtikajo drugih nezaželenih programov, pa so lahko še kako nadležni. Le-ti se namreč razmnožujejo v spominu, zasedajo prost delovni spomin in tako onemogočajo normalno delovanje sistema in drugih programov.

Prisotnost zlonamernih programov je potrebno konstantno preverjati s pomočjo protivirusnih programov. To so programi, namenjeni ugotavljanju prisotnosti znanih virusov na računalniških diskih (PcMag,

2007). Večina takih programov ima možnost samodejnega posodabljanja baze znanih virusov preko interneta.

3.5.1. Zakonodaja na področju varstva osebnih podatkov

Področje varstva osebnih podatkov v Sloveniji urejajo naslednji zakoni in pravilniki:

- zakon o varstvu osebnih podatkov (ZVOP-1): Uradni list RS, št. 86/2004,
- zakon o elektronskih komunikacijah (ZEKom): Uradni list RS, št. 43/2004,
- zakon o informacijskem pooblaščencu (ZInfP): Uradni list RS, št. 113/2005,
- zakon o inšpekcijskem nadzoru (ZIN): Uradni list RS, št. 56/2002,
- kazenski zakonik (154. člen): Uradni list RS, št. 95/2004,
- pravilnik o metodologiji vodenja registra zbirk osebnih podatkov: Uradni list RS, št. 28/2005 ter
- pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države: Uradni list RS, št. 79/2005.

ZVOP-1 (Zakon o varstvu osebnih podatkov, 2004, 1. člen) določa »pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov«.

Tretje poglavje zakona se osredotoča na zavarovanje osebnih podatkov in določa, da zavarovanje osebnih podatkov poteka na te načine (Zakon o varstvu osebnih podatkov, 2004, 24. člen):

- varovanje prostorov, opreme in sistemsko programske opreme, vključno z vhodno-izhodnimi enotami,
- varovanje aplikativne programske opreme, s katero se obdelujejo osebni podatki,
- preprečevanje nepooblaščenega dostopa do osebnih podatkov pri prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih,
- zagotavljanje učinkovitega načina blokiranja, uničenja, izbrisa ali anonimizacije osebnih podatkov ter
- omogočanje poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

Zakon posveča poglavje tudi obveščanju o zbirkah osebnih podatkov. Določa, da mora upravljavec osebnih podatkov za vsako zbirko osebnih podatkov vzpostaviti katalog zbirke osebnih podatkov, ki vsebuje različne podatke o zbirki (Zakon o varstvu osebnih podatkov, 2004, 26. člen). Naslednji člen v prvem odstavku določa, da mora upravljavec Državnemu nadzornemu organu za varstvo osebnih podatkov, najmanj 15 dni pred vzpostavitvijo zbirke, posredovati podatke iz kataloga zbirke (Zakon o varstvu osebnih podatkov, 2004, 27. člen). 28. člen zakona pa se nanaša na register zbirk podatkov, ki ga vodi Državni nadzorni organ za varstvo osebnih podatkov (Zakon o varstvu osebnih podatkov, 2004, 28. člen).

ZEKom (Zakon o elektronskih komunikacijah, 2004, 1. člen): »ureja pogoje za zagotavljanje elektronskih komunikacijskih omrežij in za izvajanje elektronskih komunikacijskih storitev, ureja zagotavljanje univerzalne storitve, upravljanje radiofrekvenčnega spektra, izrabo številskega prostora, določa pogoje za omejitev lastninske pravice, določa pravice uporabnikov, ureja delovanje omrežij in storitev v izrednih stanjih, ureja zaščito tajnosti in zaupnosti elektronskih komunikacij, ureja reševanje sporov med subjekti na trgu elektronskih komunikacij, ureja pristojnosti, organizacijo in delovanje Agencije za pošto in elektronske komunikacije RS kot neodvisnega regulativnega organa ter pristojnosti drugih organov, ki opravljajo naloge po tem zakonu, in ureja druga vprašanja, povezana z elektronskimi komunikacijami.«

V prvem odstavku 103. člena je zagotovljena zaupnost komunikacij, ki se nanaša na vsebino komunikacij, podatke o prometu in dejstev in okoliščin neuspešnih poskusov vzpostavitve zvez (Zakon o elektronskih komunikacijah, 2004, 103. člen).

109. člen zakona obravnava nezaželene komunikacije. Prvi odstavek določa, da je, poleg drugih načinov neposrednega trženja, pošiljanje elektronske pošte za namene neposrednega trženja dovoljeno le, če se naslovnik predhodno strinja z njim. Drugi odstavek zakona pravi, da lahko fizična ali pravna oseba, ki od svojih kupcev pridobi naslov elektronske pošte, ta naslov uporablja za neposredno trženje svojih izdelkov, vendar mora kupcu dati možnost, da na brezplačen in enostaven način kadarkoli zavrne takšno uporabo njegovega elektronskega naslova (Zakon o elektronskih komunikacijah, 2004, 109. člen).

Z že omenjenim **ZinfP (Zakon o informacijskem pooblaščencu, 2005)** je Republika Slovenija, dne 31.12.2005, pridobila samostojen in neodvisen državni organ; informacijskega pooblaščenca. »Ta združuje dostop do informacij javnega značaja in varstvo osebnih podatkov. Informacijski pooblaščenec je prekrškovni organ, pristojen za nadzor nad zakonom, ki ureja varstvo osebnih podatkov ter ima naslednje pristojnosti:

- organizira in usklajuje delo vseh zaposlenih, vključno državnih nadzornikov za varstvo osebnih podatkov,
- izvaja druga pooblastila predstojnika državnega organa ter
- opravlja inšpekcijski nadzor po zakonu, ki ureja varstvo osebnih podatkov.« (Zakon o informacijskem pooblaščencu, 2005, 2. člen)

Zakon o inšpekcijskem nadzoru (2002, 19. člen) pripisuje inšpektorjem pooblastilo, da pri opravljanju inšpekcijskega nadzora lahko pregledajo vse knjige, pogodbe, listine in druge dokumente, shranjene na elektronskem mediju, ki se nanašajo na poslovanje fizične ali pravne osebe. Poleg tega lahko inšpektor tudi pridobi osebne in druge podatke o zavezancu iz uradnih evidenc in drugih zbirk podatkov, če so le ti pomembni za izvajanje inšpekcijskega nadzora.

Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (2005, 1. člen) določa »pravila za vodenje in vzdrževanje registra zbirk osebnih podatkov ter določa vsebino registra, obliko in način

posredovanja podatkov, vsebovanih v katalogih zbirk osebnih podatkov, način vodenja registra ter način objave registra.«

Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (2005, 1. člen) določa »informacije o ustrezni ravni varstva osebnih podatkov, ki so potrebne za odločanje Državnega nadzornega organa za varstvo osebnih podatkov o dopustnosti iznosa osebnih podatkov v tretje države ter načini in oblike njihovega pridobivanja.«

Kazenski zakonik (2004, 154. člen) določa kazni, ki doletijo osebo, ki v nasprotju z zakonom uporabi osebne podatke, ki se smejo voditi samo na podlagi zakona ali na podlagi osebne privolitve posameznika, na katerega se osebni podatki nanašajo ter osebo, ki vdre v računalniško vodeno zbirko z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.

Zakonska podlaga je usmerjena predvsem v zaščito tako komunikacijskih kanalov kot uporabnikov teh kanalov (zaščita pred prisluškovanjem, prestrezanjem ipd.), vendar se ga vsi ne držijo. Zaradi takih posameznikov, ki zakon kar obidejo, obstaja med uporabniki spletnih storitev toliko večji strah pred morebitnimi zlorabami podatkov. Zato morajo ponudniki spletnih storitev prevzeti vajeti v svoje roke in poskusiti prepričati potencialne kupce, da je tveganje pri uporabi njihove storitve manjše, kot se zdi na prvi pogled.

Poleg slovenskih zakonov in predpisov velja omeniti še nekatere druge mednarodnopravne predpise, ki jih morajo podjetja prav tako upoštevati pri operiranju z osebnimi podatki: (Informacijski pooblaščenec, 2007):

- **Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, Strasbourg, 28.1.1981.**
- **Direktiva 95/46/ES z dne Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov OJ L 281, 23/11/1995.**
- **Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002** o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah).
- **Uredba (ES) št. 45/2001** evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov.
- **Schengenski sporazum** med vladami gospodarske unije Benelux, Zvezno državo Nemčijo in Republiko Francijo o postopnem odpravljanju mejne kontrole na medsebojnih mejah.[10]
- **Konvencija o izvršitvi Schengenskega sporazuma**, dne 14.junija 1985, med vladami gospodarske unije Benelux, Zvezno državo Nemčijo in Republiko Francijo o postopnem odpravljanju mejne kontrole na medsebojnih mejah.[11]

[10] Schengen Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

- **Odredba sveta Evrope EC No 871/2004**, dne 29. aprila 2004, ki zadeva uvedbo nekaterih novih funkcij v SIS (Schengenskem informacijskem sistemu), vključujoč boj proti terorizmu.[12]
- **Sklep sveta Evrope 2005/211/JHA**, dne 24. februarja 2005, ki zadeva uvedbo nekaterih novih funkcij v SIS, vključujoč boj proti terorizmu.[13]

3.5.2. Kaj je politika zasebnosti

Kot smo videli, smo lahko priča velikemu prometu s podatki preko interneta. Podjetja na različne načine podatke zbirajo in jih tudi na različne načine uporabljajo. Zaradi možnosti izgube spletne identitete smo spletni deskarji vedno bolj pozorni na podatke, ki jih posredujemo, pa tudi lastniki spletnih portalov so postali bolj pozorni na to skrb njihovih obiskovalcev. Zato je prišlo do razvoja izjave o politiki zasebnosti podjetja.

Vsaka, še tako majhna skupnost, potrebuje določena pravila, v skladu s katerimi se vsi pripadniki obnašajo. Pravila so potrebna za usklajen soobstoj in možnost napredovanja družbe. Taka pravila so potrebna tudi v podjetjih oz. gospodarskih družbah.

V podjetjih se to kaže kot skupek kodeksov, pravil in politik. Ena izmed politik je tudi politika zasebnosti ali politika varovanja zasebnosti. Čeprav med pojmoma politika zasebnosti in izjava o politiki zasebnosti obstaja razlika, večina študij obravnava pojma kot sinonima. Razliko je potrebno poudariti in razumeti. Politika varovanja zasebnosti, kot ostale politike podjetja, postavlja okvire, v katerih se lahko podjetje giblje na področju zbiranja in operiranja s podatki, ki jih preko spletnega portala pridobi od poslovnih partnerjev. Cilj izjave o politiki zasebnosti podjetja pa je obveščanje poslovnih partnerjev o za njih pomembnejših določilih politike zasebnosti.

Najpomembnejši del izjave o politiki zasebnosti navadno obravnava načine, kako podjetje zbira podatke ter komu jih posreduje (Wikipedia, 2007). Čeprav se na prvi pogled zdi, da je razvoj politike zasebnosti enostaven, pa temu ni tako. Veliko je sestavin in načel, ki jih moramo upoštevati. Namen izjave o politiki zasebnosti je povečati zaupanje sedanjih in potencialnih poslovnih partnerjev. Prepričati jih je namreč potrebno, da v poslovanju z nami ne bo prišlo do zlorabe podatkov, ki nam jih bodo posredovali.
Raziskave kažejo, da je lahko izjava o politiki zasebnosti zelo pomembna pri zagotavljanju zaupanja poslovnih partnerjev v podjetje, čeprav jo podjetje sàmo izdela in zapiše[14].

---

[11] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders

[12] Council regulation EC No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the SIS, including the fight against terrorism.

[13] Council decision of 24 February 2005, concerning the introduction of some new functions for the SIS, including the fight against terrorism.

[14] Podjetje sàmo napiše izjavo o politiki zasebnosti in je zanjo odgovorno. Nihče (razen podjetja samega) ne zagotavlja, da se je bo dejansko držalo.

3.5.3. Razvoj izjave o politiki zasebnosti

Najpomembnejše pri razvoju izjave o politiki zasebnosti je, da imamo vedno pred očmi osebo, ki bo to izjavo prebirala. V tem kontekstu moramo paziti predvsem na razumljivost teksta in na ne preveliko zapletenost izražanja. Povprečni uporabnik namreč ne pozna pomena zapletenih informacijskih ali pravnih izrazov. Potrebno je uporabiti enostavnejše besede, ki jih razume tudi manj izobražena oseba. Kljub izčrpnim informacijam, ki jih mora vsebovati izjava pa moramo paziti tudi na to, da ne bo predolga. Dolga izjava namreč odvrača osebe od branja. Za olajševanje branja izjave je ta navadno razdeljena na več poglavij, od katerih vsako obravnava določen del vprašanja zasebnosti. Tak način zapisa izjave olajša branje in poveča njeno privlačnost.

Poglavja izjave se, kot že rečeno, nanašajo na določen del oz. vidik varnosti pri spletnem poslovanju, gledano v celoti pa mora izjava obravnavati vse mogoče vidike. Izjava mora izražati zagotovilo, da je poslovanje s podjetjem popolnoma varno in brez nevarnosti.

Dejavniki dobre izjave o politiki zasebnosti se med seboj lahko izključujejo. Tako mora dobra izjava vsebovati vse vidike, ki se nanašajo na manipuliranje podjetja s podatki, hkrati pa mora biti kratka. Napisana mora biti strokovno, vendar razumljivo. Zato je potrebno najti pravilno ravnotežje med vsemi zahtevami. Le tako lahko zagotovimo uspešnost pri razvoju izjave.

Izjavo o politiki zasebnosti sestavimo iz odgovorov na več vprašanj. Potrebno je poudariti, da lahko, glede na področje dejavnosti podjetja in na lastnosti spletnega portala, določena vprašanja (vidike) tudi izpustimo iz izjave. Če npr. spletni portal ne zbira nobenih podatkov, lahko to navedemo in drugih sestavin avtomatično ne potrebujemo navajati.

Vprašanja, opisana v nadaljevanju, so povzeta in zbrana iz izjav o politiki zasebnosti, najdenih na različnih spletnih portalih in po priporočilih različnih organizacij, ki obravnavajo razvoj izjave o politiki zasebnosti.

Katere podatke zbiramo

V prvem poglavju moramo bralce obvestiti o tem, katere podatke zbiramo na svojem spletnem portalu. Potrebno je poudariti in našteti vse podatke, ki jih naša spletna stran zbira avtomatično ali na katerikoli drug način.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Istrabenz d.d. (Izjava o politiki zasebnosti podjetja Istrabenz, 2007)

»Za vsakega obiskovalca naših spletnih strani spletni strežnik avtomatično prepozna ime obiskovalčevega področja, ne pa tudi njegovega elektronskega naslova. Od avtomatično zbranih podatkov zbiramo samo skupne informacije o tem, katere strani obiskovalci odpirajo in obiskujejo in koliko časa se na posamezni strani zadržijo.«

Zakaj podatke potrebujemo

Bralcu moramo obrazložiti, zakaj podatke sploh zbiramo in kako jih uporabljamo. Potrebno je zagotoviti, da je uporaba njihovih podatkov v skladu z zakonom in da podatki ne bodo uporabljeni na nezakonit način in ne posredovani tretjim osebam.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Mobisux d.o.o. (Izjava o politiki zasebnosti podjetja Mobisux, 2007)

»Vse informacije, ki jih pridobimo v prej opisanih postopkih, uporabimo za izboljšanje kakovosti naših spletnih strani in za spremljanje statistike, ki je na ogled našim obiskovalcem in oglaševalcem:

Za pošiljanje dnevnega arhiva sporočil na forumu uporabnikom, ki so se za to možnost prostovoljno odločili, Mobisux uporabi prave elektronske naslove uporabnikov. Teh podatkov (mailing lista) Mobisux ne deli s tretjimi osebami, kot so npr. oglaševalci in partnerji.

Za informacije o tem, katere strani so uporabnikom všeč in katere ne, Mobisux uporablja prej opisane tehnologije (piškotki). Mobisux ne spremlja, kaj posamezni uporabnik bere - spremlja le število ogledov posamezne strani.

Mobisux dnevno izdeluje statistiko obiska naših storitev, ki so na voljo obiskovalcem in oglaševalcem.«

Zakaj podatkov ne bomo uporabili

Opcijsko lahko v izjavo zapišemo tudi, zakaj podatkov ne bomo uporabili. Navadno se v tem poglavju obiskovalcu zagotovi, da podatkov ne bomo uporabili v nelegalne ali škodljive namene.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Bolnišnica Golnik (Izjava o politiki zasebnosti podjetja Bolnišnica Golnik, 2007)

»Po e-pošti vam ne pošiljamo nobenih sporočil, reklam ali obvestil, razen v primerih, ko gre za pomembna obvestila v zvezi z vašo storitvijo in smo vas o tem dolžni obvestiti.«

Kako podatke zbiramo

Razložiti moramo tudi, kako spletni portal zbira podatke. Najbolje je, če nakažemo vse načine, ki jih naš portal uporablja za zbiranje podatkov, in zraven naštejemo, katere podatke zbiramo na posamezen način. Tako lahko uporabniku oz. obiskovalcu nakažemo, katere podatke zbiramo avtomatično, tako rekoč brez njegove vednosti, in katere mora vnesti sam.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Istrabenz d.d. (Izjava o politiki zasebnosti podjetja Istrabenz, 2007)

»Na spletnem strežniku… se zbirajo nekateri podatki, ki jih prostovoljno vpisujete v formularje, in drugi, ki se zbirajo avtomatično, in nimajo narave osebnih podatkov. Nekatere Istrabenzove spletne strani včasih odložijo v obiskovalčev računalnik posamezne informacije, ki jih imenujemo "Piškotki". Piškotki nam lahko povedo, kako in katere strani na spletnih straneh obiskujejo ljudje in v kakšnem številu…«

Kateri zunanji osebki imajo dostop do podatkov

Zapisati moramo tudi, katere tretje osebe ali institucije imajo dostop do naših podatkov. Navadno je dostop tretjim osebam onemogočen, vendar je v nekaterih primerih nujno, da se določeni podatki iz katerihkoli razlogov posredujejo drugim.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Volvo Car Austria GmbH (Izjava o politiki zasebnosti podjetja Volvo Car, 2007)
»Zbrane podatke ne bomo razkrili nikomur izven podjetja Volvo Car Corporation, našim trgovcem ali drugim partnerjem, ki opravljajo storitve v našem imenu.«

Čeprav je v zgornjem izseku zagotovljeno, da podatkov »ne bodo razkrili…«, pa si vseeno zagotovijo možnost, da jih posredujejo »svojim« trgovcem in drugim partnerjem, kar predstavlja dokaj veliko mrežo podjetij. Zatorej ne moremo biti prepričani, da naši podatki ne bodo končali na kakšnem poštnem seznamu.

Kako ščitimo osebne podatke

Podatke je potrebno varovati tako v času prenosa med našim računalnikom in strežnikom, kot tudi na samem strežniku. To poglavje izjave je zelo pomembno pri vzbujanju zaupanja v spletni portal.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Moje Delo.com (Izjava o politiki zasebnosti podjetja Moje delo, 2007)
»Vsi podatki na spletni strani, zlasti v članskem delu, so zaščiteni s posebnimi programskimi orodji. Uporabljamo t.i. SSL (Secure Sockets Layer) tehnologijo, ki je defacto standard v svetu in preprečuje možnost dostopa tujih oseb do podatkov, ki ste jih vnesli na svojem računalniku.«

Dostop in brisanje osebnih podatkov

Kako lahko uporabniki pridejo do svojih lastnih podatkov, je naslednje vprašanje, na katerega mora izjava odgovoriti. Potrebno je nakazati, na kakšen način lahko obiskovalec pride do svojih podatkov in jih spremeni, ko ne odražajo več dejanskega stanja (npr. zamenjava naslova, telefonske številke, ipd.). Poleg tega je potrebno zagotoviti način, kako lahko uporabnik posredovane podatke izbriše iz baze podjetja. Med te podatke spadajo tudi podatki o registraciji uporabnika.

Primer: Izsek iz izjave o politiki zasebnosti podjetja e-shop.si (Izjava o politiki zasebnosti podjetja E-shop, 2007)
»Registrirani uporabniki lahko kadar koli prekličejo svojo registracijo. Če in ko odpovejo registracijo, ne bodo več prejemali e-sporočil. Zaupnost vaših podatkov (zasebnost) bomo zaščitili v okviru te izjave o varovanju zaupnosti tudi v primeru, če se boste odločili za preklic registracije.«

Druge sestavine

Poleg zgornjih osnovnih zahtev, na katera mora izjava odgovoriti, obstaja še veliko drugih podrobnosti, ki jih lahko obrazloži. Možno je, da lahko uporabnik dostopa do strani popolnoma brez posredovanja oz. izdajanja podatkov. Tudi to moramo v izjavi poudariti, saj lahko na ta način (brez posredovanja podatkov) povečamo obisk strani. Občutek zaupanja v portal se namreč tako poveča.

Prav tako lahko podjetja v izjavo vključijo varovanje zasebnosti podatkov otrok, ki obiščejo njihovo stran.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Volvo Car Austria GmbH (Izjava o politiki zasebnosti podjetja Volvo Car, 2007)
»…prav zato nikoli ne hranimo ali zbiramo podatkov z naših spletnih strani od oseb, za katere vemo, da so mlajše od 13 let, brez pridobitve ustreznega dovoljenja staršev in ne pogojujemo

sodelovanja otroka pri pridobivanju dodatnih osebnih podatkov o istovetnosti, kot ga narekuje trenutna aktivnost…«

Možno je tudi podrobneje opisati mesto in čas shranjevanja podatkov, če se podatki po določenem času izbrišejo.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Volvo Car Austria GmbH (Izjava o politiki zasebnosti podjetja Volvo Car, 2007)
»Za stalno nudenje visoke ravni uslug vam, našim strankam, naše spletne strani upravljamo z različnih lokacij, ne glede na to, kje se nahajate…. Podjetje Volvo hrani podatke v varnem in zaščitenem okolju tako dolgo, kolikor smatramo, da nam pomagajo pri boljšem razumevanju, kako vam lahko ustrežemo in spoštujemo vaše želje.«

Na koncu izjave o varovanju zasebnosti pa se lahko nahaja tudi klavzula, v kateri si podjetje zagotovi možnost spreminjanja vsebine izjave.

Primer: Izsek iz izjave o politiki zasebnosti podjetja Moje Delo.com (Izjava o politiki zasebnosti podjetja Moje delo, 2007)
»Našo politiko varovanja vaših osebnih podatkov bomo v bodoče spreminjali glede na možne dopolnitve Zakona o varstvu osebnih podatkov. O tem bomo vse registrirane uporabnike teh spletnih strani tudi obvestili s pomočjo e-pošte.«

4. Analiza stanja na področju politike zasebnosti med slovenskimi uporabniki interneta

4.1. Raziskave na področju politike zasebnosti

Področje raziskovanja politike zasebnosti in njenega vpliva na poslovanje je še relativno mlado. Večina raziskav, ki se nanašajo na učinkovitost izjave o politiki zasebnosti, je narejenih v smislu ugotavljanja vpliva posameznih sestavin spletnih portalov in spletnih strani na uspešnost poslovanja spletnih podjetij. V literaturi se najbolj omenjajo raziskave sledečih avtorjev: Sultan et al. (2006), Yoon (2002), Fogg et al. (2007), Fogg et al. (2001) in Shankar, Sultan, Urban (2002). V teh raziskavah je izjava o politiki zasebnosti zgolj omenjena kot eden izmed dejavnikov, ki povečujejo zaupanje v spletne portale. Namen omenjenih raziskav je namreč ugotoviti, kateri dejavniki spletnih portalov in spletnih strani imajo največji vpliv na uspešno grajenje zaupanja v portal. Raziskave so med seboj bolj ali manj enotne in se strinjajo, da izjava o politiki zasebnosti ni najpomembnejši dejavnik, vendar je eden izmed pomembnejših (Fogg et al., 2001; Sultan et al., 2006). Omenjene raziskave se med seboj razlikujejo predvsem v načinu zbiranja podatkov in v razvoju konceptualnega modela raziskave. Ne glede na to, kako raziskovalci postopajo, so ugotovitve vedno bolj ali manj podobne.

V tej raziskavi sem se zgledovali po Meinertu (Meinert et al., 2006), raziskavi iz ZDA, opravljeni na vzorcu 374 že diplomiranih študentov. Za razliko od ostalih raziskav se ta ne osredotoča na razvrščanje sestavin spletnih strani in portalov po učinkovitosti, temveč na vprašanje, ali bi regulacija na področju politike zasebnosti ugodno vplivala na zaupanje v spletna podjetja in posledično na njihovo uspešnost. Raziskava tako ugotavlja mero zaupanja, ki ga imajo anketiranci v spletne portale, ki jih obiskujejo, in

odnos anketirancev do izdajanja različnih vrst podatkov (kontaktnih, biografskih in finančnih) tem portalom. Na kratko so predstavljeni načini večanja zaupanja, vendar pa je fokus postavljen na izjavo o politiki zasebnosti. Poleg tega skuša raziskava ugotoviti vpliv »moči« izjave o politiki zasebnosti na pripravljenost izdajanja podatkov.

V aprilu in maju 2007 sem na spletni strežnik postavil anketo. Povezava do ankete je bila postavljena na vse večje slovenske iskalnike. Namen ankete je ugotoviti stanje na področju politike zasebnosti v slovenskem prostoru. Ta dva meseca sem izbral zato, ker je v obdobju med zimskimi in poletnimi počitnicami več oseb v službah in šolah. Na ta način sem lahko pričakoval večje število odgovorov na spletno anketo. Ciljna populacija raziskave so bili vsi uporabniki svetovnega spleta. Vzorčenje je bilo naključno. Na anketo je odgovorila 101 oseba. Anketa je podana v prilogi 1, rezultati ankete pa v Prilogi 2.

4.2. Namen ankete

Namen ankete je bil ugotoviti, ali se slovenski uporabniki interneta dobro zavedajo nevarnosti kraje podatkov, ki jih preko interneta posredujejo, in ali so jih kljub temu pripravljeni v okoliščinah, ko je njihova varnost zagotovljena, brez večjih problemov izdati. Prav tako me je zanimalo, ali poznajo različne načine, s katerimi podjetje veča zaupanje v portal in v podjetje, predvsem izjavo o politiki zasebnosti. Zanimalo me je, ali jo redno berejo z namenom zmanjšanja možnosti izgube podatkov.

4.3. Interpretacija rezultatov

Ker sem se pri izdelavi anketnega vprašalnika zgledoval po raziskavi Meinerta (2006), se bom tudi pri interpretaciji rezultatov navezoval nanj. Nekatere rezultate velja zaradi vsebine raziskave primerjati tudi z raziskavo Sultan et al.(2006). V nadaljevanju je podana analiza ankete.

4.3.1. Demografske lastnosti vzorca

Med demografskimi lastnostmi anketirancev sta me zanimali le spol in starost. Razlika v številu moških in ženskih anketirancev je bila minimalna, saj je na anketo odgovorilo 50 moških in 51 žensk.

Meje razredov pri vprašanju o starosti so bile postavljene ob upoštevanju raziskave Statističnega urada RS, ki je ugotovil, da je največ uporabnikov interneta starih med 10 in 34 let (Uporaba interneta v gospodinjstvih, Slovenija, 1. četrtletje 2006, 2007). Starostna porazdelitev anketirancev je pričakovana, saj je na anketo odgovorilo največ oseb med dvajsetim in petindvajsetim letom starosti. Sledil je razred nad 35 let, vendar pa verjetno le zaradi širine razreda.

Meinert (2006) ugotavlja, da je povprečna starost anketirancev 32,9 let. To si velja razlagati z dejstvom, da so anketiranci že diplomirane osebe. Na njegovo anketo je odgovorilo nekoliko več moških, kot žensk.

4.3.2. Odnos do interneta

Več kot polovica anketiranih uporablja svetovni splet vsak dan, skoraj tretjina pa ga uporablja celo večkrat na dan. Zanimivo je bilo ugotoviti, da izmed več kot 100 oseb ni bilo nikogar, ki bi internet uporabljal le enkrat na teden ali manj.

Pri vprašanju pogostosti obiskovanja interneta so bile meje pri Meinert et al. (2006) nekoliko drugače postavljene. Zato so rezultati neprimerljivi. Primerljivo pa je dejstvo, da je Meinert ugotovil, da se več kot 86% anketirancev poveže z internetom vsak dan, kar je skladno z rezultati moje ankete.

Največji delež anketirancev je kot namen obiskovanja spleta označilo osebne namene (85,1%). Sledila je uporaba v šolske namene in uporabna v službene namene. Proti pričakovanjem pa so razlike med različnimi nameni uporabe zelo majhne.

Med storitvami, ki jih splet nudi, se največ uporablja spletno pošto (86 oseb). Tesno ji sledi iskanje podatkov (83 oseb). Na dnu lestvice pa sta spletno bančništvo (30 oseb) in spletno nakupovanje (11 oseb).

4.3.3. Odnos anketirancev do izdajanja osebnih podatkov

Prvo vprašanje, ki se je nanašalo na odnos anketirancev do izdajanja osebnih podatkov, je bilo: »Ali ste že kdaj obiskali spletni portal, ki je o Vas zbiral podatke?«. Pravi namen tega vprašanja je bil nekoliko prikrit. Spletni portal lahko o osebi zbira podatke, ne da jo o tem kakorkoli obvesti in ne da obiskovalci to sploh opazijo. Nekdo, ki se tega zaveda, na to vprašanje ne more odgovoriti z »ne«. Zavedam se, da določeni portali dejansko ne zbirajo nobenih podatkov o obiskovalcih, vendar je to zapisano v politiki zasebnosti portala. Torej v primeru, da obiskovalec ne prebere izjave o politiki zasebnosti, ne more zagotovo trditi, da njegovih podatkov ni nihče shranil. Ker večina tistih, ki so na to vprašanje odgovorili z ne, ne bere izjav o politiki zasebnosti ali jih bere redkokdaj, lahko zaključimo, da se veliko ljudi sploh ne zaveda, da lahko vsak spletni portal shranjuje določene podatke o nas in naših obiskih.

Tabela 2: Povezava med branjem izjave o politiki zasebnosti in obiskovanjem portala, ki o obiskovalcih zbira podatke

Branje izjave PP/ Obisk portala, ki zbira podatke	***Nikoli***	***Nekajkrat***	***Pogosto***	***Vedno***	***Skupna vsota***
Da	23	26		3	52
Ne	25	19	3		47
Skupna vsota	48	45	3	3	99

Vir: Lasten.

Presenetilo me je tudi število oseb, ki je preko interneta že posredovalo svoje (kontaktne) podatke. Delež takih oseb je bil skoraj 80%. Nameni, za katere so anketiranci posredovali svoje podatke, so različni. Najpogosteje je razlog za posredovanje podatkov registracija pri portalu, na dnu lestvice pa najdemo spletni nakup. Vmes pa se nahajata vpis v poštni seznam (angl. mailing list) in izpolnjevanje anket.

Meinert je vprašanje izdajanja podatkov omejil le na izdajanje naslova spletne pošte, rezultati pa so pokazali, da je devet desetin anketirancev ta podatek že posredovalo tretjim osebam ali organizacijam.

Naslednje vprašanje je obravnavalo razloge, zaradi katerih osebe ne želijo posredovati svojih podatkov. Čeprav je bil odziv na to vprašanje pod pričakovanji (odgovorila je slaba polovica anketirancev), so rezultati pričakovani. Največ oseb se namreč boji zlorabe podatkov.

Glede varnosti izmenjave podatkov preko svetovnega spleta so mnenja anketiranih dokaj skladna. Splošno mnenje je, da so podatki slabo zaščiteni, tako s tehnološkega vidika (79,2%), kot z vidika preprečevanja dostopa nepooblaščenih oseb (84,1%).

V kontekstu posredovanja podatkov me je zanimalo tudi, pod katerim pogojem so anketirane osebe pripravljene preko interneta posredovati podatke o svoji kreditni kartici. Kreditno kartico sem izbral zato, ker je škoda ob zlorabi te vrste podatkov (finančni podatki) največja. Rezultati so pokazali, da so slovenski uporabniki spleta še vedno zelo skeptični in nezaupljivi, kar se tiče izdajanja finančnih podatkov. Po drugi strani pa preseneča, da je več ljudi pripravljenih izdati finančne podatke v primeru, da njihovo varnost zagotovi podjetje, kot pa država. Le dve anketirani osebi sta pripravljeni posredovati finančne podatke brez dodatnega zagotovila o njihovi varnosti.

Iz kombinacije vprašanj o izdajanju podatkov o kreditni kartici (finančni podatki) in o posredovanju drugih podatkov (predvsem kontaktnih) je razvidno, da so anketiranci pripravljeni izdajati slednje, ne pa finančnih. Ugotovitve so skladne z raziskavo iz ZDA, kjer je pripravljenost izdajanja podatkov največja pri kontaktnih podatkih, nekoliko nižja pri biografskih podatkih, najnižja pa pri finančnih podatkih.

4.3.4. Odnos anketirancev do izjave o politiki zasebnosti

Med anketiranimi osebami je bila večina takih, ki so za izraz »privacy policy« oz. »politika zasebnosti« že slišali, vendar je njihov delež pod pričakovanji (le 59,4%). V ZDA je ta delež občutno večji, saj je oseb, ki poznajo ta izraz, skoraj 80 %.

Prav tako ni bila pričakovana struktura pogostosti branja izjav o politiki zasebnosti podjetij. Med vsemi je 48 oseb takih, ki izjave še niso nikoli prebrali. Nekaj manj (45 oseb) je takih, ki so jo prebrali nekajkrat, le 6 oseb pa izjavo bere pogosto ali vedno. Na tem mestu je potrebno poudariti, da je bila izjava o politiki zasebnosti postavljena tudi na stran, kjer je bila objavljena anketa. Namen le-te je bil raziskati, koliko oseb jo bo dejansko prebralo. Takih osebe so bile le štiri. Zanimiva je tudi povezava med vprašanjem o pogostosti branja izjav o politiki zasebnosti in med tem ali so anketiranci izjavo prebrali. Med štirimi osebami, ki so sledile povezavi do izjave o politiki zasebnosti na spletni strani ankete, sta dve osebi namreč odgovorili, da izjave ne bereta nikoli, ostali dve osebi pa, da sta izjavo prebrali nekajkrat. Po drugi strani pa tisti, ki so odgovorili, da izjave berejo vedno, je pri izpolnjevanju ankete niso prebrali.

Glede na raziskavo iz ZDA je stanje na področju branja izjav o politiki zasebnosti podobno. Tudi v tej raziskavi je ugotovljeno, da je izmed anketirancev približno polovica takih, ki so izjavo vsaj enkrat prebrali.

Kot razlog, zakaj izjav o politiki zasebnosti anketiranci ne berejo bolj pogosto, je dobra polovica anketirancev dejala, da je predolga. Drugi razlog je ta, da izjava anketirancev ne zanima, takoj za tem pa sledi zapletenost. Izjava naj bi bila pogosto prezapleteno napisana.
Nato so bili anketiranci naprošeni, da s svojimi besedami opišejo kaj je izjava o politiki zasebnosti oz. kakšen je njen namen. Med 31 odgovori jih je nekaj, ki so zadeli bistvo izjave o politiki zasebnosti. Najboljši odgovor je: »Namen je tistega, ki podatke daje, obvestiti o tem kaj se bo s podatki dogajalo, za kakšne namene bodo uporabljeni/ne bodo uporabljeni.«. Iz nekaterih odgovorov pa je razvidno, da nekateri ne razumejo bistva izjave. Poleg tega pa je iz določenih odgovorov razvidno tudi, da nekateri še vedno dvomijo v smiselnost izjave.

V naslednjem vprašanju sem želel izvedeti, kakšne lastnosti anketiranci pripisujejo dobri izjavi o politiki zasebnosti. Dobra polovica je označila, da mora biti izjava enostavno berljiva. Druga lastnost je, da mora biti kratka. Tudi pri tem vprašanju obstaja prikrit cilj. Kot odgovore sem namenoma ponudil dva para bolj ali manj izključujočih si lastnosti. Če želimo imeti kratko izjavo, ne moremo vsake njene točke podrobno razčleniti. Če pa želimo enostavno berljivo izjavo moramo pogosto izpustiti strokovne izraze. Med anketiranci tako najdemo 4 osebe, ki si želijo kratko vendar podrobno izjavo ter 3 osebe, ki želijo enostavno berljivo vendar strokovno. Če obravnavamo najpogostejšo kombinacijo različnih dejavnikov, mora biti izjava kratka in enostavno berljiva (21 oseb).

V zadnjem delu ankete me je zanimalo, kako bi na zaupanje uporabnikov vplivala regulativa države na področju izjave o politiki zasebnosti. Skoraj vsi anketirani (96%) se strinjajo, da bi se zaupanje posameznikov do storitev in proizvodov, ki jih podjetja ponujajo preko spleta, povečalo, če bi država z zakonodajo uredila področje izjav o politiki zasebnosti. Iste osebe pa menijo, da bi od državne regulative bolje deloval varnostni pečat države (angl. seal of approval) na straneh, ki bi ustrezale določenim standardom, ki bi jih država postavila.

Ameriška raziskava je izjave o politiki zasebnosti podjetij razdelila na tri kategorije, glede na »moč«[15] izjave. Ugotovitev je predvidljiva; pripravljenost izdajanja podatkov se veča z močjo izjave.

Ugotovitev raziskave v ZDA, ki me je najbolj presenetila je, da anketiranci menijo, da bi se zaupanje v spletni portal bolj povečalo v primeru, da bi za varnost podatkov odgovarjala podjetja, kot če bi zanje odgovarjala država. Torej je zaupanje v etiko podjetij večje, kot zaupanje v učinkovitost zagotavljanja upoštevanja zakonske podlage v ZDA.

4.4. Ugotovitve in implikacije raziskave

S pomočjo anketnega vprašalnika sem ugotovili, da se slovenski spletni deskarji zavedajo nevarnosti izdajanja podatkov preko svetovnega spleta. Seveda je potrebno ločiti med vrstami podatkov. Večina jih je že brez večjih težav izdala osebne podatke (kontaktne podatke). Na področju izdajanja finančnih podatkov pa so še vedno nekoliko skeptični, nezaupljivi, in jih zato neradi izdajajo, kljub zagotovilom podjetja, da je njihovo izdajanje varno. Izjav politike zasebnosti Slovenci ne spremljajo in ne berejo pogosto. Večina jih ima o njej neko nejasno mnenje. Vedo, da obstaja, vendar ne poznajo njenega

[15] Tri kategorije moči izjave so opisane v Prilogi 3.

namena. Kombinacija nepoznavanja njenega namena in tega, da je izjava navadno daljša in zapleteno (strokovno) napisana, botrujeta dejstvu, da je večina oseb ne bere.

Čeprav vpliv izjave o politiki zasebnosti na zaupanje ni zanemarljiv, pa zelo malo spletnih deskarjev bere izjavo o politiki zasebnosti, kar potrjujejo ugotovitve te raziskave. Kljub vsemu bi morala država zagotoviti zakonodajo, ki bi enolično določala, katere sestavine mora vsaka izjava imeti. Vendar pa kljub trudu države obstaja dvom, da bodo deskarji v prihodnje pogosteje brali izjave. Zato je spet na potezi država, ki bi morala s svojim pečatom zaupanja nagraditi spletne portale, ki ustrezajo določenim standardom na področju varovanja podatkov in torej zagotavljajo varnost podatkov z vseh njegovih vidikov. Na ta način bi zagotovila standard na tem področju, velik vpliv pa bi to imelo tudi na zaupanje obiskovalcev portalov. Le-ti bi namreč ob dostopu do strani videli pečat države, ki bi jim, kljub neprebrani izjavi, povečal zaupanje v portal.

4.5. Omejitve

Prvo omejitev raziskave predstavlja pomanjkanje pilotske raziskave, s katero bi lahko, na podlagi prejetih rezultatov, anketni vprašalnik nekoliko bolj prilagodil na podlagi prejetih rezultatov. S pomočjo pilotske raziskave bi lahko tudi določil potrebno velikost vzorca za raziskavo, na podlagi katerega bi bilo možno posploševanje rezultatov raziskave na celotno slovensko populacijo. Drugo omejitev torej predstavlja velikost vzorca, ki postavi pod vprašaj možnost posplošitve ugotovitev. Odločitev, da se osebne podatke razporedi v tri kategorije (kontaktni, biografski ter finančni), predstavlja tretjo omejitev. Rezultati bi se morebiti razlikovali, če bi namesto združevanja v kategorije podatkov, anketa analizirala posamezne podatke (npr. številka kreditne kartice, leto rojstva, število otrok ipd.). Četrta omejitev je zanemarjanje drugih dejavnikov, ki imajo lahko velik vpliv na zaupanje v spletni portal (npr. tekst izjave, pozicija izjave ipd.). V anketi je namreč poudarjena le vsebina izjave o politiki zasebnosti, medtem ko se drugi faktorji ne upoštevajo. Peto omejitev pa lahko ponazorimo s statičnostjo zajemanja podatkov. Poudariti velja, da je zaupanje dinamična kategorija, ki se sčasoma spreminja. Za raziskavo pa je bil mogoč le statičen zajem podatkov in ugotavljanje stanja zaupanja v določenem trenutku, ne da bi upoštevali, da je lahko stanje na tem področju že v naslednjem trenutku drugačno, kot kažejo analize.

4.6. Prihodnje raziskave

Raziskavo bi veljalo v prihodnje ponoviti in še razširiti. Razširitev v smislu večanja vzorca bi pripomogla k njegovi večji reprezentativnosti in možnosti posplošitve rezultatov na celotno slovensko populacijo. Poleg tega bi bilo zanimivo raziskavo razširiti in zamenjati kategorije podatkov s točno določenimi vrstami podatkov (npr. kategorijo finančnih podatkov bi veljalo zamenjati s številko kreditne kartice, PIN kodo ipd.). Na ta način bi lahko poleg razlik v pripravljenosti izdajanja podatkov med kategorijami, ugotovili tudi razlike med posameznimi vrstami podatkov. Zanimivo bi bilo raziskavo ponoviti v enakem obdobju prihodnjega leta in tako ugotoviti časovno dinamiko zaupanja ter odnosa deskarjev do izjave o politiki zasebnosti. Tako bi lahko opazovali povečanje ali zmanjšanje zaupanja v spletne portale in večanje ali manjšanje števila oseb, ki berejo izjavo o politiki zasebnosti. Na ta način bi v raziskavo vključili njen dinamični vidik. Možno pa bi bilo tudi narediti analizo odvisnosti in tako ugotavljati odvisnost med zaupanjem v spletna podjetja in posameznimi lastnostmi anketirancev (npr. izobrazbe, starosti, spola).

5. Sklep

Podatke, ki igrajo ključno vlogo pri zagotavljanju konkurenčne prednosti podjetij in so zato zelo dragoceni, je potrebno tudi primerno zaščiti in z njimi ravnati v skladu z zakoni in s pričakovanji njihovih lastnikov. Le na ta način lahko v očeh vseh soudeleženih v poslovanju zgradimo in utrdimo zaupanje, ki je prav tako pomemben dejavnik uspešnosti poslovanja.

Podjetja se pomembnosti zaupanja zavedajo in zato ga skušajo s pomočjo raznih orodij povečati. Eno izmed takih orodij je tudi izjava o politiki zasebnosti podjetja, ki je poceni in učinkovito orodje. Po drugi strani pa raziskave iz tujine kažejo, da jo prebira le malo spletnih deskarjev kljub temu, da igra pomembno vlogo.

Veljavnost ugotovitev iz tujine sem s pomočjo anketnega vprašalnika preverili v slovenskem prostoru. Analiza rezultatov je pokazala, da se rezultati bistveno ne razlikujejo. Tudi slovenski deskarji namreč izjave o politiki zasebnosti ne berejo pogosto.

Slovenski deskarji so še vedno nezaupljivi do spletnih podjetij, ki od njih zahtevajo podatke, zato jih neradi izdajajo Pripravljenost izdajanja podatkov pa je seveda odvisna od vrste podatkov, ki se od njih zahtevajo. Zato morajo spletna podjetja vložiti dodatne napore v proces vzpostavljanja zaupanja. Le tako si lahko zagotovijo uspešno prihodnost in obstoj na dolgi rok.

Zaupanje bo tudi v prihodnje ostala ključna vrednota modernega poslovnega sveta, vendar ga bo potrebno graditi na nove načine. Tudi izjava o politiki zasebnosti bo sčasoma postala zastarela in jo bo potrebno zamenjati z drugimi orodji. Že danes lahko opazimo ta trend. In če velja rek, da slika pove več kot tisoč besed, potem velja tudi da varnostni pečat pove več kot izjava o politiki zasebnosti. Pričakujem namreč, da bodo pečati zaupanja prevzeli vlogo graditelja zaupanja, saj se jih lahko prikaže na vsaki spletni strani in ni potrebno vedno znova prebirati, čemu služijo in kaj zagotavljajo. V ta namen je seveda potrebna kredibilna inštitucija, ki bo pečate podeljevala. Glede na rezultate anket, opravljenih v slovenskem in ameriškem prostoru, pa ta inštitucija ne sme biti državna, temveč poslovna tvorba. Sama mora določiti kriterije za pridobitev pečatov, ter jih podeljevati le tistim podjetjem, ki izpolnjujejo kriterije, neodvisno od državnih oblasti. Na ta način bo inštitucija kredibilna in del te kredibilnosti bo podedoval njen pečat. Taka poenostavitev prinaša prednosti tako spletnim portalom (saj bo zaupanje vanje večje) kot spletnim deskarjem (imeli bodo institucijo, na katero se bodo lahko obrnili, v primeru zlorab podatkov, zato bo njihovo zaupanje v pečat in portale, ki ga izpostavljajo, večje).

Zaupanje bo, kot je veljalo v preteklosti, potrebno graditi in povečevati tudi v prihodnosti, saj lahko le zaupanje omogoči podjetju, spletnemu podjetju ali spletnemu portalu dolgoročni obstoj in razvoj.

Literatura

1. Bilstad Blake T., Enright Keith P.: Consumer Privacy. Harvard. [URL: http://cyber.law.harvard.edu/ecommerce/privacytext.html], 10.3.2007.
2. Clarke Roger: Trust in the context of e-business. Internet law bulletin, Canberra, 5(2002), 4, str. 56-59.
3. Department of Justice: Web seals of approval. Victoria, 20 str. [URL: http://www.consumer.vic.gov.au/CA256902000FE154/Lookup/CAV_Publications_Reports_and_Guidelines/$file/webseals_of_approval.pdf], 18.11.2006.
4. Driscoll James W.: Trust and participation in organizational decision making as predictors of satisfaction. The Academy of Management Journal, New York, 21(1978), 1, str. 44-56.
5. Fogg BJ et al.: How do People evaluate a Web Site's Credibility? Results from a Large Study, 105 str. [URL: http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf], 15.2.2007.
6. Fogg BJ et al.:What Makes Web Sites Credible? A report on a large Quantitative Study. Conference on Human Factors in Computing Systems, Minneapolis, 3(2001), 1, str. 61-68.
7. Ganesan Shankar: Determinants of long-term orientation in buyer-seller relationships. Journal of marketing, Chicago, 58(1994), 2, str. 1-19.
8. Gradišar Miro et al.: Osnove poslovne informatike. Ljubljana : Ekonomska fakulteta, 2005. 327 str.
9. Groznik Aleš, Lindič Jaka: Elektronsko poslovanje. Ljubljana : Ekonomska fakulteta, 2004. 85 str.
10. Hadziahmetovic Amir: Digital identity management – Challenges and benefits. Copenhagen: IT university of Copenhagen. 113 str. [URL: http://digitalidentitymanagement.files.wordpress.com/2006/07/digitalidentitymanagementthesisbyamirhadziahmetoviccomplete.pdf], 15.3.2007.
11. Kajić Milan:Varovanje podatkov. Magistrsko delo. Ljubljana : Ekonomska fakulteta, 1996. 132 str.
12. Kovačič Andrej et al.: Prenova in informatizacija poslovanja. Ljubljana : Ekonomska fakulteta, 2004. 345 str.
13. Lesjak Dušan, Sulčič Viktorija: Ekonomika elektronskega poslovanja. Koper : Fakulteta za management, 2004. 12 str.
14. Luhmann Niklas: Trust and power. New Jersey : John Wiley and Sons, 1982. 228 str.
15. Mayer Roger C., Davis James H., Schoorfman David F.: An integrative model of organizational trust. The Academy of Management Review, New York, 20(1995), 3, str. 709-734.
16. Meinert David B. et al.: Would regulation of web site privacy policy statements increase consumer trust?. Informing science journal, Santa Rosa, 2006, 9, str. 123-143.
17. Morgan Robert M., Hunt Shelby D.: The commitment-trust theory of relationship marketing. Journal of marketing, Chicago, 58(1994), 3, str. 20-38.
18. Palmer Jonathan W., Bailey Joseph P., Faraj Samer: The role of intermediaries in the development of trust in the WWW. Journal of computer-mediated communication, Maryland, 5(2000), 3. [URL: http://jcmc.indiana.edu/vol5/issue3/palmer.html], 18.9.2007.
19. Pennington Robin, Wildcox Dixon H., Grover Varun: The role of system trust in business-to-consumer transactions. Journal of management information systems, New Jersey, 20(2004), 3, str. 197-226.

20. PriceWaterhouseCoopers: E-business: A matter of trust. PriceWaterhouseCoopers. 52 str. [URL: http://www.pwc.fr/assets/files/pdf/2006/redesign/2/pwc_trust.pdf], 15.10.2006.
21. Semeja Aleš: Elektronsko poslovanje v novi ekonomiji. Diplomsko delo. Ljubljana : Ekonomska fakulteta, 2001. 45 str.
22. Shankar Venkatesh, Sultan Fareena, Urban Glenn L.: Online trust: A stakeholder perspective, concepts, implications and future directions. Journal of strategic information systems, Amsterdam, 11(2002), 3, str. 325-344.
23. Sultan et al.: Determinants and role of trust in e-business:A large scale empirical study. Pennsylvania State University. 44 str. [URL: http://dspace.mit.edu/bitstream/1721.1/1826/2/4282-02.pdf], 17.9.2006.
24. Wugmeister Miriam, Lyon Christine E.: The most overlooked component of Data Security: Your employees. Morrison & Foerster LLP. [URL: http://library.findlaw.com/2004/Jul/20/133512.html], 10.6.2007.
25. Yoon Sung-Joon: The Antecedents and Consequences of Trust in Online Purchase Decisions. Journal of Interactive Marketing, New Jersey, 16(2002), 2, str. 47-63.

Viri

1. Bankruptcy Sale of Children's Personal information. TrustE. [URL: http://www.truste.org/consumers/watchdog_advisories/0600_toysmart.php], 13.3.2007.
2. Chess fans overload IBM's Web site. CNN. [URL: http://www.cnn.com/WORLD/9705/03/chess.rematch/index.html], 14.3.2007.
3. Credit card breach: Tracing who dunnit. CNN. [URL: http://money.cnn.com/2005/06/28/pf/security_hackers/], 14.3.2007.
4. Data protection and monitoring at work. Out Law. [URL: http://www.out-law.com/page-445], 14.6.2007.
5. Data theft involving four banks could affect 500,000 customers. ComputerWorld. [URL: http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101831,00.html], 17.4.2007.
6. Deset razlogov za spletno trgovino. Hitrost. [URL: http://hitrost.com/elektronsko_poslovanje/razlogi_za_spletno_trgovino.html], 23.4.2007.
7. Google. [URL: http://www.google.com/analytics/features.html], 15.10.2006.
8. Informacijski pooblaščenec. [URL: http://www.ip-rs.si/index.php?id=415], 24.4.2007.
9. Informing Customers About e-commerce. Department of Trade and Industry. [URL: http://www.mori.com/polls/2001/pdf/dti-e-commerce.pdf], 17.10.2006.
10. Internet Fraud. FBI. [URL: http://www.fbi.gov/majcases/fraud/internetschemes.htm], 24.4.2007.
11. Izjava o politiki zasebnosti podjetja Bolnišnica Golnik. [URL: http://www.klinika-golnik.si/varovanje_zasebnosti.php], 13.2.2007.
12. Izjava o politiki zasebnosti podjetja E-shop. [URL: http://www.e-shop.si/VarovanjeZasebnosti.aspx], 13.2.2007.
13. Izjava o politiki zasebnosti podjetja Istrabenz. [URL: http://www.istrabenz.si/slo/pravnaobvestila/458], 13.2.2007.

14. Izjava o politiki zasebnosti podjetja Mobisux. [URL: http://www.mobisux.com/mobisux/izjava.php/], 13.2.2007.
15. Izjava o politiki zasebnosti podjetja Moje delo. [URL: http://www.mojedelo.com/delo/mojedelo_pravno_obvestilo.aspx], 13.2.2007.
16. Izjava o politiki zasebnosti podjetja Volvo Car. [URL: http://www.si.volvocars.com/footer/privacypolicy/], 13.2.2007.
17. Kazenski zakonik (Uradni list RS, št. 95/2004).
18. Make sure your fast new Web-ordered computer gets to you quickly. CNN. [URL: http://archives.cnn.com/2000/TECH/computing/04/26/pc.delivery.idg/index.html], 26.11.2006.
19. Nakupovanje po internetu. Zveza potrošnikov Slovenije. [URL: http://www.zps-zveza.si/ZPSstrani/zpsV1.0.nsf/VSE/1E7A9EECD88FE1EDC1256E130050FA52/$file/internet%20nakupi.pdf], 8.12.2006.
20. PcMag. [URL: http://www.pcmag.com/encyclopedia_term/0,2542,t=antivirus+program&i=37832,00.asp], 8.6.2007.
21. Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (Uradni list RS, št. 28/2005).
22. Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (Uradni list RS, št. 79/2005).
23. Secure data transmission methods. Search Security. [URL: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1159630,00.html], 8.6.2007.
24. Slovar Slovenskega knjižnega jezika. [URL: http://bos.zrc-sazu.si/cgi/a03.exe?name=sskj_testa&expression=zaupanje&hs=1], 18.8.2006.
25. Squaretrade. [URL: http://www.sqaretrade.com], 26.2.2007.
26. Sullivan Bob: ID theft usually an inside job. MSNBC [URL: http://www.msnbc.msn.com/id/5015565], 15.6.2007.
27. The buying cycle. QuizWiz. [URL: http://www.quizwiz.biz/samtutorial/samtut12.html], 27.6.2007.
28. Top 5 Easy & Proven Ways to Increase Consumer Trust Online. Duct Tape Marketing. [URL: http://www.ducttapemarketing.com/article/articles/136/1/Top-5-Easy--Proven-Ways-to-Increase-Consumer-Trust-Online/Page1.html], 22.2.2007.
29. Trust Guard. [URL: http:// www.trust-guard.com], 26.2.2007.
30. UEAPME position paper on the consultation on e-business. UEAPME. [URL: http://www.ueapme.com/docs/pos_papers/2004/pp_ebusiness.doc], 22.11.2006.
31. Uporaba interneta v gospodinjstvih, Slovenija, 1. četrtletje 2006. Statistični urad RS. [URL: http://www.stat.si/novica_prikazi.aspx?id=473], 14.3.2007.
32. Webopedia. [URL: http://www.webopedia.com/], 8.6.2007.
33. What is Internet Fraud. United States Department of Justice. [URL: http://www.usdoj.gov/criminal/fraud/internet/], 24.4.2007.
34. What is trust?. Changing Minds. [URL: http://changingminds.org/explanations/trust/what_is_trust.htm], 15.1.2007.
35. Wikipedia. [URL: http://en.wikipedia.org/wiki/], 26.2.2007.
36. Xentinel. [URL:http:// www.xentinelsecurity.com], 26.2.2007.

37. Zakon o elektronskih komunikacijah (Uradni list RS, št. 43/2004).
38. Zakon o informacijskem pooblaščencu (Uradni list RS, št. 113/2005).
39. Zakon o inšpekcijskem nadzoru (Uradni list RS, št. 56/2002).
40. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/2004).
41. Zakon o varstvu potrošnikov (Uradni list RS, št. 98/2004).

Slovarček slovenskih prevodov tujih izrazov

Izraz v angleščini	*Slovenski prevod izraza*
Brand	Zaščitni znak
Challenge response system	Sistem s povratnim zahtevkom gesla
Clear gif	Prozorni gif
Cookie	Piškotek
Intent to act	Namera izvedbe dejanja
Just in time	Ravno ob pravem času
Mailing list	Poštni seznam
Ping	Podatkovni paket
Pixel tag	Pikselski označevalec
Seal of approval	Pečat zaupanja (odobritve)
Spam mail	Nezaželena pošta
Web bug	Spletni hrošč
Tracking bug	Sledilni hrošč

Priloge

Priloga 1: Anketni vprašalnik

Pozdravljeni! Sem Gregor Božič, študent ekonomske fakultete v Ljubljani. Za dokončanje študija pripravljam diplomsko nalogo na temo: Zaupanje kot dejavnik uspešnosti e-poslovanja. Na to temo sem pripravil kratek anonimni vprašalnik in Vas prosim, da mi nanj odgovorite.

Hvala za sodelovanje!

Vprašanje	*Možni odgovori*
Spol?	☐ Moški ☐ Ženski
Starost?	☐ do vključno 15 let ☐ 15 do vključno20 let ☐ 20 do vključno 25 let ☐ 25 do vključno 30 let ☐ nad 30 let
Kako pogosto obiskuješ spletne strani?	☐ večkrat na dan ☐ vsak dan ☐ 2 do 4 krat tedensko ☐ največ enkrat tedensko
V kakšne namene uporabljaš internet?	☐ v študijske namene ☐ v zasebne namene ☐ v službene namene
Kako najpogosteje uporabljaš internet?	☐ pregledovanje spletne pošte ☐ za iskanje podatkov v različne namene ☐ za spletno nakupovanje ☐ za storitve spletnega bančništva
Ali si že kdaj obiskal spletni portal, ki je o tebi zbiral podatke?	☐ da ☐ ne
Si že kdaj samovoljno posredoval svoje kontaktne podatke preko spletnih portalov?	☐ da ☐ ne
V kakšne namene si podatke posredoval?	☐ vpis na poštni seznam ☐ spletni nakup ☐ reševanje anket ☐ registracija na spletnih portalih

Zakaj podatkov nisi nikoli posredoval?	☐ ne obiskujem portalov, ki zbirajo podatke ☐ ne želim razkrivati svojih podatkov ☐ ne zaupam lastnikom, katerih spletne portale obiskujem ☐ strah me je zlorabe oz. morebitne kraje podatkov
Ali meniš, da so tokovi podatkov, ki se izmenjujejo preko interneta, tehnološko zadosti zaščiteni?	☐ da ☐ ne
Ali meniš, da so tokovi podatkov, ki se izmenjujejo preko interneta, dobro zaščiteni pred dostopom nepooblaščenih oseb?	☐ da ☐ ne
Pod katerim pogojem bi spletnemu podjetju preko interneta zaupal številko svoje kreditne kartice?	☐ pod nobenim pogojem ☐ pod pogojem zagotovila podjetja, da je prenos podatkov zadostno varovan ☐ pod pogojem zagotovila države, da je prenos podatkov zadostno varovan ☐ številko bi posredoval brez dodatnih zagotovil
Ali poznaš izraz 'Privacy policy' oz. 'politika zasebnosti'?	☐ da ☐ ne
Kako bi s svojimi besedami opisal namen politike zasebnosti?	
Katera izjava po tvojem mnenju najbolje opisuje politiko zasebnosti?	☐ Smernice podjetja pri zbiranju in obdelovanju podatkov, ki jih pridobi od obiskovalcev spletne strani. ☐ Uradna izjava podjetja, ki pojasnjuje katere podatke zbira. ☐ Uradna izjava podjetja, ki pojasnjuje katere podatke podjetje zbira, ter kako jih uporablja. ☐ Uradna izjava podjetja, ki pojasnjuje kako podjetje zbira, obdeluje in posreduje podatke, komu jih posreduje ter kako lahko lastnik podatkov do njih dostopa.

Kako pogosto bereš izjave o politiki zasebnosti?	☐ nikoli je še nisem prebral ☐ prebral sem jo že nekajkrat ☐ berem jo pogosto ☐ berem jo na vsakič, ko pregledujem novo spletno stran
Zakaj izjav o politiki zasebnosti ne bereš pogosteje?	☐ je predolga ☐ je preveč zapleteno napisana ☐ povezave do nje pogosto ne najdem ☐ preveč je nerazumljivih pravnih izrazov ☐ me ne zanima Drugo:
Katere so lastnosti dobre izjave o politiki zasebnosti?	☐ Je kratka ☐ Je podrobno napisana ☐ Je enostavno berljiva ☐ Je strokovno napisana
Ali meniš, da bi državna regulativa (zakon) na področju politike zasebnosti pripomogla k večjemu zaupanju posameznikov do storitev in proizvodov, ki jih podjetja ponujajo preko spleta?	☐ da ☐ ne
Ali meniš, da bi bilo od državne regulative boljši njen varnostni pečat (garancija države, da je posredovanje podatkov popolnoma varno) na 'varnih' straneh?	☐ da ☐ ne

Priloga 2: Rezultati ankete

Tabela 1: Spol

Spol?	*Frekvenca*	*Odstotek*
Moški	50	49,5%
Ženski	51	50,5%

Vir: Lasten.

Tabela 2: Starostni razred

Starost?	*Frekvenca*	*Odstotek*
15 do 20 let	2	2%
20 do 25 let	67	66,3%
25 do 30 let	14	13,9%
Nad 30 let	18	17,8%

Vir: Lasten.

Tabela 3: Pogostost obiskovanja spleta

Kako pogosto obiskuješ spletne strani?	*Frekvenca*	*Odstotek*
Največ enkrat tedensko	0	0%
2 do 4 krat tedensko	19	18,8%
Vsak dan	52	51,5%
Večkrat na dan	30	29,7%

Vir: Lasten.

Tabela 4: Namen obiskovanja spleta

V kakšne namene uporabljaš internet?	*Frekvenca*	*Odstotek*
V službene namene	56	55,4%
V šolske namene	71	70,3%
V osebne nemene	86	85,1%

Vir: Lasten.

Tabela 5: Uporabljene spletne storitve

Kako najpogosteje uporabljaš internet?	*Frekvenca*	*Odstotek*
Spletna pošta	86	85,1%
Iskanje podatkov	83	82,2%
Spletno nakupovanje	11	10,9%
Spletno bančništvo	30	29,7%

Vir: Lasten.

Tabela 6: Obiskovanje portalov, ki zbirajo podatke

Ali si že kdaj obiskali spletni portal, ki je o tebi zbiral podatke?	*Frekvenca*	*Odstotek*
Da	52	51,5%
Ne	47	46,5%
Neodgovorjene	2	2%

Vir: Lasten.

Tabela 7: Prostovoljno posredovanje podatkov

Ali si že kdaj prostovoljno posredovali svoje kontaktne podatke preko spletnih portalov?	*Frekvenca*	*Odstotek*
Da	79	78,2%
Ne	22	21,8%

Vir: Lasten.

Tabela 8: Namen posredovanja podatkov

V kakšne namene si podatke posredoval?	*Frekvenca*	*Odstotek*
Poštni seznam	40	39,6%
Spletni nakup	39	38,6%
Izpolnjevanje anket	50	49,5%
Registracija na portalu	67	66,3%

Vir: Lasten.

Tabela 9: Zakaj podatkov ne posredujete

Zakaj podatkov nisi nikoli posredoval?	*Frekvenca*	*Odstotek*
Ne obiskujem spletnih portalov	9	8,9%
Podatkov ne želim razkrivati	14	13,9%
Ne zaupam lastnikov spletnega portala	12	11,9%
Strah me je zlorabe podatkov	15	14,9%

Vir: Lasten.

Tabela 10:Tehnološka zaščita tokov podatkov preko spleta

Ali meniš, da so tokovi podatkov, ki se izmenjujejo preko interneta, tehnološko zadosti zaščiteni?	*Frekvenca*	*Odstotek*
Da	21	20,8%
Ne	80	79,2%

Vir: Lasten.

Tabela 11: Zaščita podatkov pred nepooblaščenimi dostopi

Ali meniš, da so tokovi podatkov, ki se izmenjujejo preko interneta, dobro zaščiteni pred dostopom nepooblaščenih oseb?	*Frekvenca*	*Odstotek*
Da	12	11,9%
Ne	85	84,1%
Brez odgovora	4	4%

Vir: Lasten.

Tabela 12: Pogoji posredovanja finančnih podatkov

Pod katerim pogojem bi spletnemu podjetju posredoval številko svoje kreditne kartice?	*Frekvenca*	*Odstotek*
Pod nobenim pogojem	52	51,5%
Pod pogojem zagotovila podjetja, da je prenos podatkov zadosti varovan	35	34,7%
Pod pogojem zagotovila države, da je prenos podatkov zadosti varovan	12	11,9%
Brez dodatnih zagotovil	2	2%

Vir: Lasten.

Tabela 13. Poznavanje izraza politike zasebnosti

Ali poznaš izraz »privacy policy« oz. »politika zasebnosti«?	*Frekvenca*	*Odstotek*
Da	60	59,4%
Ne	41	40,6%

Vir: Lasten.

Tabela 14: Opisi namena izjave o politiki zasebnosti

Kako bi s svojimi besedami opisal namen izjave o politiki zasebnosti?
Tvoji podatki so samo TVOJI!
upam da drži vse in jo kdo nadzira
spoštovanje zasebnosti posameznika
seznanit bralca o varovanju podatkov
ne obstaja!
prodaja utopije, da to obstaja
varovanje osebnih podatkov
gre za neko varstvo osebnih podatkov
varovanje podatkov, ki so preneseni preko spleta
Informiranje o načinu, vsebini in količini hranjenja osebnih podatkov.
namen je tistega, ki podatke daje, obvestiti o tem kaj se bo s podatki dogajalo, za kaksne namene bodo uporabljeni/ne bodo uporabljeni.
zaščititi zasebnost uporabnikov?
podjetje zbira podatke uporabnikov za obdelavo, ki pa so hkrati zaščiteni in jih ni mogoče zlorabiti
Vsak ima pravico za varovanje in skrivanje svojih podatkov.
varovanje človekove zasebnosti, podatkov o njem...
Podatki so vidni le tistim, za katere želimo/ozirmo smo obveščeni, da jim bodo vidni
varovanje osebnih podatkov; če jih neki instituciji zaupaš, jih le ta ne sme posredovati dalje oz. izkoriščati
upravljanje z podatki osebe
da ne zlorabljajo tvojih podatkov v kakšne npr. oglaševalske namene
Vsak človek ima pravico do svoje zasebnosti in se sam odloča, katere podatke o sebi bo posredoval naprej in katere ne.
Deklaracija podjetja o zagotavljanju varnosti osebnih podatkov
bo kr neki
Politika podjetja, da bi zagotavljalo varovanje osebnih podatkov pred tem, da nepooblaščene osebe ne morejo priti do določenih podatkov.
podjetje hrani podatke le za svojo uporabo in za namen za katerega si jih njim posredoval ter jih ne posreduje naprej.

varnost prenosa podatkov in zagotovilo da podatke ne posredujejo naprej
Neposredovanje zasebnih podatkov nepooblaščenim osebam oz. javnosti.
zagotovilo v kakšne namene uporabljajo naše podatke in kako jih varujejo
Zasebni podatki se lahko uporabljajo le za namene za katere so bili posredovani in se ne smejo prenašati naprej.
Podatke, ki jih posreduješ, uporablja le stran oz. družba, ki je lastnica strani, ostalim pa podatki niso dostopni.

Vir: Lasten.

Tabela 15: Izbira najprimernejše izjave

Katera izjava po tvojem mnenju najbolje opisuje namen politike zasebnosti?	***Frekvenca***	***Odstotek***
Smernice podjetja pri zbiranju in obdelovanju podatkov, ki jih pridobi od obiskovalcev spletne strani.	11	10,9%
Uradna izjava podjetja, ki pojasnjuje katere podatke zbira.	7	6,9%
Uradna izjava podjetja, ki pojasnjuje katere podatke podjetje zbira, ter kako jih uporablja.	14	13,9%
Uradna izjava podjetja, ki pojasnjuje kako podjetje zbira, obdeluje in posreduje podatke, komu jih posreduje ter kako lahko lastnik podatkov do njih dostopa.	61	60,4%

Vir: Lasten.

Tabela 16: Pogostost branja izjave o politiki zasebnosti

Kako pogosto bereš izjave o politiki zasebnosti?	***Frekvenca***	***Odstotek***
Nikoli je še nisem prebral	48	47,5%
Prebral sem jo nekajkrat	45	44,7%
Berem jo pogosto	3	3%
Vedno jo preberem	3	3%
Neodgovorjeno	2	2%

Vir: Lasten.

Tabela 17: Zakaj izjav ne berete pogosteje

Zakaj izjav o politiki zasebnosti ne bereš pogosteje?	***Frekvenca***	***Odstotek***
je predolga	52	51,5%
je preveč zapleteno napisana	25	24,8%
povezave do njih pogosto ne najdem	4	4%
preveč je nerazumljivih pravnih izrazov	10	9,9%
me ne zanima	28	27,7%

Vir: Lasten.

Tabela 18: Lastnosti dobre izjave

Katere so lastnosti dobre izjave o politiki zasebnosti?	*Frekvenca*	*Odstotek*
Je kratka	32	31,7%
Detaljno napisana	24	23,8%
Enostavno berljiva	51	50,5%
Strokovno napisana	17	16,8%

Vir: Lasten.

Tabela 19: Učinki državne regulative na zaupanje

Ali meniš, da bi državna regulativa na področju politike zasebnosti pripomogla k večjemu zaupanju posameznikov do storitev in proizvodov, ki jih podjetja ponujajo preko spleta?	*Frekvenca*	*Odstotek*
Da	97	96%
Ne	4	4%

Vir: Lasten.

Tabela 20: Učinki državnega varnostnega pečata na zaupanje

Ali meniš, da bi bilo od državne regulative boljši njen varnostni pečat (garancija države, da je posredovanje podatkov popolnoma varno) na 'varnih' straneh?	*Frekvenca*	*Odstotek*
Da	97	96%
Ne	4	4%

Vir: Lasten.

Tabela 21: Dejansko prebrana izjava

Ali je anketiranec prebral mojo izjavo o politiki zasebnosti?	*Frekvenca*	*Odstotek*
Da	4	4%
Ne	97	96%

Vir: Lasten.

Priloga 3: Opis »moči« izjave o politiki zasebnosti

Tabela 22: Moč izjave o politiki zasebnosti

Moč izjave	*Opis izjave*
Močna	Močna izjava razlaga, kako podjetje operira s podatki, pridobljenimi od svojih poslovnih partnerjev. Poleg tega pa le-tem jasno in nedvoumno jamči, da podatkov ne bodo pod nobenim pogojem delili z nobeno organizacijo, podjetjem ali posameznikom.
Zmerna	Zmerna izjava razlaga, kako podjetje operira s podatki, pridobljenimi od svojih poslovnih partnerjev. Poleg tega lastnikom osebnih podatkov zagotovi, da bodo njihovi podatki ostali zaupni. Zagotavlja tudi omejeno posredovanje podatkov, v primeru, ko lastnik spletnega portala meni, da je posredovanje podatkov v lastnem interesu, v interesu lastnika osebnih podatkov ali pa v interesu obeh.
Šibka	Šibka izjava razlaga, kako podjetje operira s podatki, pridobljenimi od svojih poslovnih partnerjev, vendar pa ne ponuja nobenega zagotovila, da podatkov ne bo delila s tretjimi osebami.

Vir: Meinert et al., 2006, str. 131.