Nekateri varnostni vidiki informacijskih tehnologij na področju turizma v Sloveniji

[1]Matej Rebec, [2]Cene Bavec
[1]Ministrstvo za notranje zadeve, Policija; [2]Univerza na Primorskem, Fakulteta za management Koper
matej_rebec@yahoo.com; cene.bavec@guest.arnes.si

Izvleček

V članku so povzeti rezultati empirične raziskave o varovanju informacijskih tehnologij v organizacijah s področja nastanitvenega turizma. Pokazalo se je, da so razlogi, da se le malo anketiranih turističnih podjetij odloča za uporabo posebnih programskih rešitev za menedžment odnosov s strankami, tudi v dilemah, povezanih z varnostjo sistema, zato smo podrobneje analizirali stanje na tem področju. V anketiranih podjetjih je s tehnološke plati kakovost varovanja pod slovenskim in tudi evropskim povprečjem. Posebno preseneča dejstvo, da nekatera podjetja ne uporabljajo najosnovnejših varnostnih ukrepov, povezanih z virusi in vohunskimi programi. Rezultati med drugim potrjujejo tudi hipotezo, da imajo podjetja z lastnimi strokovnjaki za informatiko bolj kakovostno varovanje in manj varnostnih težav, kot jih imajo druga.

Ključne besede: varovanje opreme, varnost informacijske tehnologije, varovanje podatkov, varnostne težave, turistične nastanitvene organizacije.

Abstract

Some Aspects of Information Technology Security in Tourist Organizations in Slovenia

In the paper we present results of empirical research on IT security issues in touristic organizations in Slovenia. The results indicate that one of the reasons that the majority of organizations do not use specialized Customer Relations Management systems lies among others in their concern over data protection and security of information systems. For that reason we analyzed present security issues. We confirmed that the level of security in tourist organizations was under Slovenian and the EU average. Some organizations do not use even basic technological security measures concerning virus and anti-spy programs. The results also confirm the hypothesis that organizations with their own IT staff have better system security and less security threats than others.

Key words: IT security, data security, security threats. tourist organizations.

1 UVOD

Svetovni trendi kažejo, da je turizem panoga, ki nenehno raste. To dejstvo potrjujejo podatki Svetovne turistične organizacije (UNWTO, 2011), ki za leto 2010 poroča o 935 milijonih mednarodnih turistov, do leta 2020 pa naj bi se to število skoraj podvojilo in preseglo milijardo in pol turistov. Podoben trend se bo zanesljivo nadaljeval tudi pri nas kljub 5,8-odstotnem upadu tujih gostov v letih 2008 in 2009 kot posledici svetovne gospodarske krize (STO, 2010). Čeprav je turizem naglo se razvijajoča gospodarska panoga, pa turistična podjetja delujejo v specifičnem in izjemno konkurenčnem okolju. Posebnost turističnega gospodarstva je njegova neposredna usmerjenost k strankam, pa naj gre za organizirane ali posamezne turiste (Kalakota in Whinston, 1997). Turistične organizacije seveda ugotavljajo, da lahko dvignejo svojo konkurenčnost in si zagotovijo dolgoročen obstoj na trgu turističnih storitev predvsem s tem, da povečajo svojo vidnost na internetu in posvetijo izrazito individualno pozornost svojim strankam. Zato je postal menedžment odnosov s strankami (CRM – Customer Relationship Management) pomemben del poslovne strategije celotnega turističnega gospodarstva (Fox in Stead, 2001; Bull, 2003). Dolgoročno gledano pa uvedba sistema CRM zmanjšuje tudi stroške prodaje kapacitet in storitev posameznega namestitvenega podjetja z natančnejšim usmerjanjem v določeno stranko, hkrati pa omogoča hitro prilagajanje tržnim pogojem (Gray in Byun, 2001; Buhalis 2003).

Učinkovito sodelovanje s strankami seveda zahteva ustrezno informacijsko podporo. V preprostejših primerih zadostujejo preprostejše računalniške rešitve,

vendar se večje turistične organizacije v tujini praviloma odločajo za integralno informacijsko podporo, ki jo omogočajo specializirani informacijski sistemi za menedžment odnosov s strankami (CRM). Njegov temelj je enotna osrednja zbirka podatkov, ki je dostopna vsem, ki jo potrebujejo ali lahko vanjo prispevajo potrebne podatke (Rigby, Reichheld in Berez, 2002). Podjetje zapisuje vse demografske, pa tudi psihografske podatke o strankah ter odnose in stike zaposlenih z vsako stranko. S tem podjetje gradi informacijske temelje za bolj oseben pristop k stranki. Problemi menedžmenta odnosov s strankami v turizmu so podobni problemom v drugih panogah, ki obdelujejo veliko število strank, pa naj gre za organizacije ali posameznike. Pomembna razlika pa je v izboru osebnih podatkov, ki v turizmu bistveno presega običajne identifikacijske podatke. Turistične organizacije praviloma obdelujejo širok spekter osebnih podatkov, ki so povezani s konkretnimi potovanji ter z osebnimi željami in s preferencami posameznikov, kar omogoča oblikovanje individualnih ponudb, ki so v celoti prilagojene stranki.

Jedro informacijskih sistemov v turističnih in še posebno v nastanitvenih organizacijah, pa naj gre za enostavne evidence ali pa integrirane sisteme za menedžment odnosov s strankami, so osebni podatki, povezani s preferencami posameznega turista. Na videz ti podatki niso posebno občutljiva kategorija podatkov, vendar ta videz precej vara. Razkritje ali nedovoljena izmenjava teh podatkov je lahko za posameznike izrazito neprijetna. Tega se zavedajo tudi turistične organizacije, ki se med drugim izogibajo morebitnim odškodninskim zahtevkom (Rosen, 2000; Istraturist, 2011). Veliko občutljivih osebnih podatkov postavlja te organizacije in njihove informacijske sisteme pred zahtevne varnostne izzive. Na načelni ravni se postavlja že vprašanje, koliko podatkov sploh zbirati in katere, da se po nepotrebnem in pretirano ne poseže v zasebnost strank (Zorman, 2001). Večja kot je količina osebnih podatkov, večjo zakonsko in etično odgovornost si nalagajo turistične organizacije, kar se odraža predvsem v vedno večjih zahtevah po ustreznih varnostnih ukrepih. Pri tem ne kaže pozabiti, da je zbiranje osebnih podatkov zakonsko urejeno, zato njihova nenamenska uporaba in slabo varovanje lahko vodita v materialne in poslovne posledice za organizacijo, ki ji dokažejo kakršno koli zlorabo ali malomarnost.

Vendar vsa turistična podjetja tega področja ne obvladujejo tako, kot bi pričakovali in želeli. To velja tako za organizacijske kot za tehnološke varnostne ukrepe (Bin, 2010). Varovanje informacijskih sistemov je kompleksno področje, ki pa je zanesljivo le toliko, kot je zanesljiv najšibkejši člen v verigi varovanja (Bottitta, 2005). Pogosto se namreč pokaže, da se lahko kompleksni in na videz zelo zanesljivi sistemi zrušijo zaradi enega samega slabega člena v omenjeni verigi. Zato ne kaže podcenjevati tudi nekaterih na prvi pogled trivialnih problemov ali izzivov. Posebno je treba poudariti, da veliko organizacij – ne samo turističnih – ni sposobnih vpeljati niti temeljnih varnostnih ukrepov, za katere bi povprečen računalniški strokovnjak mislil, da so razumljivi sami po sebi. V to kategorijo spada elementarna zaščita pred virusi, trojanskimi konji in podobnimi zlonamernimi kodami, šifriranje podatkov in tudi elektronski podpisi. Če se omejimo predvsem na tehnološke vidike, potem lahko naštejemo celo vrsto razlogov, ki zmanjšujejo varnostno raven. Perše (2000) navaja preslabo varnostno in tehnološko opremljenost in nezmožnost uvajanja novih varnostnih standardov. Lawrence, Loeb, Lucyshyn in Richardson (2004) omenjajo zaščito podatkov in fizičnih komponent sistema pred nenamerno ali namerno zlorabo. Acar in Michener (2002) izpostavljata problem, da še vedno mnoga podjetja o varnosti razmišljajo kot o kategoriji, ki bo dodana, ko bodo imeli čas ter ustrezna sredstva ipd.

Samo kot primer omenimo raziskavo o osnovni zaščiti informacijske in komunikacijske tehnologije in težavah podjetij z varnostjo, ki jo je objavil Eurostat (2005), v kateri je ocenjena tudi Slovenija. Po tej raziskavi je bila Slovenija skoraj po vseh merilih nekje v povprečju EU, kljub temu pa so nekateri podatki zaskrbljujoči. Le 78 odstotkov podjetij, ki imajo več kot 10 zaposlenih in ne spadajo v finančni sektor, je v zadnjih treh mesecih obnovilo sistemsko zaščito. Posledica je, da je v Sloveniji 31 odstotkov podjetij imelo varnostne težave, precej jih je izgubilo vsaj nekaj podatkov zaradi virusov, med 1 in 2 odstotkoma pa jih je zabeležilo zlorabo osebnih podatkov, zlorabe pri plačilu, nepooblaščene dostope in izsiljevanje in grožnje. Čeprav je od raziskave preteklo že precej let, so rezultati indikativni in kažejo presenetljivo visok odstotek elementarnih varnostnih težav. Predvidevanja strokovnjakov za leto 2007 kažejo celo na povečanje števila kršitev na področju varovanja podatkov. Problem varovanja podatkov naj bi se celo povečal

leta 2008. Ocenjujejo, da je leta 2007 utrpelo težave z varovanjem podatkov 79 do 162 milijonov uporabnikov (Coenen, 2008).

Omenjene ugotovitve so nas spodbudile, da smo opravili raziskavo o nekaterih vidikih varovanja opreme in podatkov v izbranih turističnih organizacijah v Sloveniji. Zanimalo nas je, kaj mislijo o specializiranem sistemu za vodenje odnosov s strankami in kje vidijo zadržke, probleme in morebitne omejitve. Na podlagi predhodnih neformalnih pogovorov v turističnih organizacijah smo namreč dobili vtis, da je eden od temeljnih razlogov za omahovanje pri uvajanju kompleksnejših informacijskih rešitev očitno nezaupanje v varnostne mehanizme in občutek tveganja. Zato smo želeli preveriti, kako v sedanjih razmerah varujejo svojo opremo in posledično osebne podatke ter kakšni so trenutno njihovi varnostni izzivi in problemi.

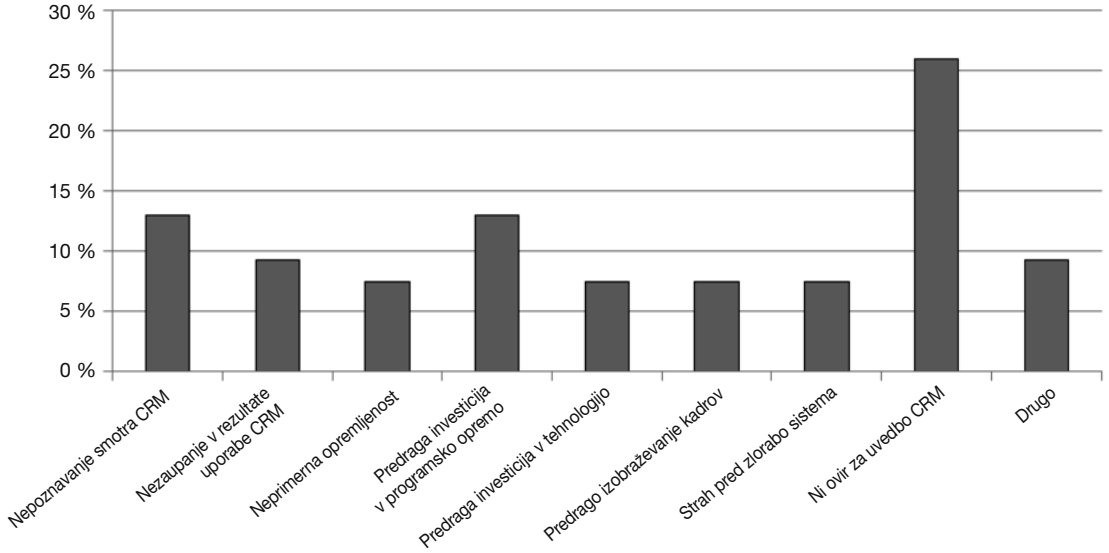
2 PREDSTAVITEV REZULTATOV

V raziskavi smo se omejili le na tisti del organizacij, ki so ponudnice turističnih namestitev (hoteli, moteli in penzioni). Anketni vprašalnik je bil sestavljen iz osemnajstih vprašanj zaprtega tipa in petih sklopov: splošni podatki o podjetju, stanje informacijske opreme v podjetju, varovanje elektronskega poslovanja v podjetju, podatki o sistemu CRM ter glavne ovire in prednosti za vzpostavitev sistema CRM. Od 184 ponudnikov turističnih namestitev je anketni vprašalnik v celoti izpolnilo le 43 podjetij. Izbrani vzorec je vključeval ponudnike turističnih namestitev v Sloveniji, objavljene v hotelskem ceniku za leto 2007. V raziskavo smo vključili samo ponudnike, ki imajo med podatki navedeno elektronsko pošto, prek katere smo anketirali.

Pri tem smo se srečali s podobnim problemom kot druge raziskave, ki so se spuščale v razmeroma občutljive podrobnosti in probleme, ki jih podjetja nerada razkrivajo. Poleg tega so bila vprašanja precej tehnično obarvana, kar je brez dvoma povzročalo probleme tistim organizacijam, ki nimajo svojih strokovnjakov s področja informatike. Kljub vsemu je bil vzorec dovolj velik, da smo lahko opravili signifikantne statistične obdelave. Del podatkov pa smo pridobili iz sekundarnih informacijskih virov, predvsem EU.

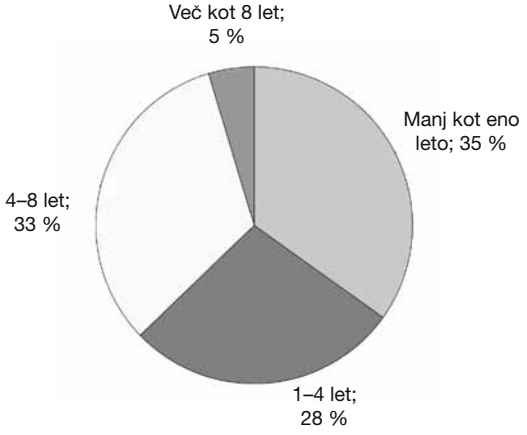
Anketirancem smo morali pojasniti, kaj si predstavljamo pod izrazom menedžment odnosov s strankami. Zavedali smo se, da imajo določene podatke o strankah vse anketirane organizacije in da je za marsikoga že enostavna evidenca zadostna informacijska podpora menedžmentu odnosov s strankami. Druga skrajnost pa so specializirani informacijski sistemi za menedžment odnosov s strankami. Zanje smo uporabili kratico CRM, kot je to običajno v jeziku ponudnikov takih rešitev.

Glede na to, da smo že pred raziskavo vedeli, da le malo turističnih namestitvenih organizacij uporablja specializirane sisteme, so nas najprej zanimali vzroki za tako stanje. Ugotovili smo, da le 7 odstotkov anketiranih podjetij uporablja omenjene sisteme. Poskušali smo analizirati, kje so razlogi za tako zadržanost (slika 1). Le 26 odstotkov organizacij



Slika 1: **Razlogi za neuporabo posebnih programskih rešitev za vodenje CRM (Vir: raziskava)**

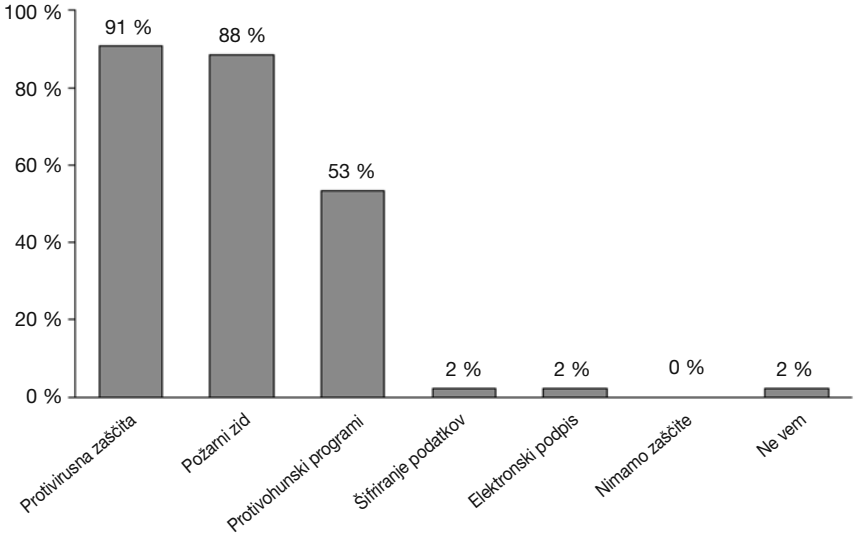
ni omenjalo ovir za uvedbo CRM, ostale tri četrtine so omenjale različne razloge, ki so podjetja odvračali od uvedbe CRM. Če odštejemo 13 odstotkov podjetij, ki so kot razlog za neuporabo navedla nepoznavanje, so vsa druga tako ali drugače omenjala probleme z opremo in s kadri ter nezaupanje in strah pred zlorabo. Vsi omenjeni zadržki so neposredno ali pa vsaj posredno povezani z varnostnimi vidiki. To ne velja le za računalniško opremo, temveč tudi za kadre, brez katerih seveda ne moremo izvajati potrebnih varnostnih ukrepov. Odgovori so razmeroma enakomerno porazdelili probleme z neprimernostjo obstoječe računalniške opreme, predrago investicijo v programsko in strojno opremo ter kadre, strah pred zlorabo in nezaupanje v rezultate uporabe CRM.



Slika 2: **Povprečna starost računalniške opreme v anketiranih podjetjih (Vir: raziskava)**

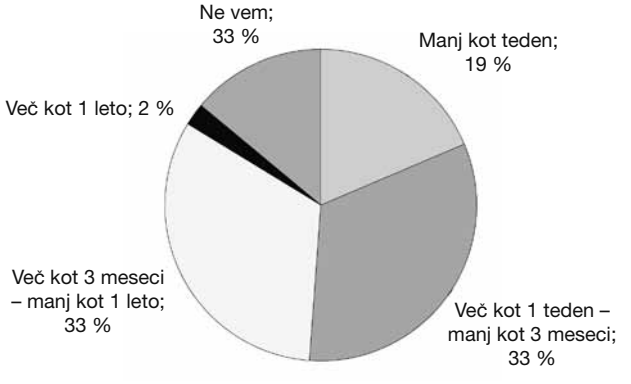
Tehnološko plat raziskave smo začeli z analizo starosti opreme, saj smo predpostavljali, da je starost opreme eden od dejavnikov, ki vpliva na varnost (slika 2). Več kot tretjina obstoječe opreme je starejša od štirih let, tretjina pa je stara manj kot leto. Ker v raziskavi nismo šli v podrobnosti, katera oprema se za kaj uporablja, lahko le sklepamo, da je starejša oprema predvsem v funkciji osebne uporabe in ne strežnikov, ki so nosilci skupnih podatkov. Vendar tega nismo posebej preverjali. Čeprav gre za subjektivno oceno, lahko vseeno ugotovimo, da je oprema v anketiranih podjetjih razmeroma stara in lahko pomeni težavo pri vzpostavljanju ustreznih varnostnih mehanizmov.

Seveda pa je varnost odvisna tudi od varnostne programske opreme. Držali smo se metodologije EU, da smo lahko rezultate anketiranih turističnih nastanitvenih podjetij postavili v širši kontekst. Slika 3 kaže, da je uporaba protivirusne zaščite in požarnih zidov na videz zelo široka, kljub temu pa presenetljivo veliko podjetij ne uporablja niti najbolj osnovnih tehnik varovanja. To je težko sprejeti ali razumeti, saj gre v njihovem primeru za obdelavo osebnih podatkov. Če k temu dodamo, da le malo več kot polovica podjetij uporablja zaščito proti vohunskim programom, lahko ugotovimo, da je varnost precej problematična. Zanimivo je tudi, da skoraj nihče ne šifrira podatkov, s čimer bi lahko bistveno povečali varnost osebnih podatkov (Min, 2010). Zato lahko podvomimo v učinkovito varovanje podatkov v večini anketiranih podjetij. Ti rezultati lahko pojasnijo tudi strah anketirancev pred zlorabo sistema CRM (slika 1), saj se očitno zavedajo, da njihova trenutna oprema ni dovolj varovana.



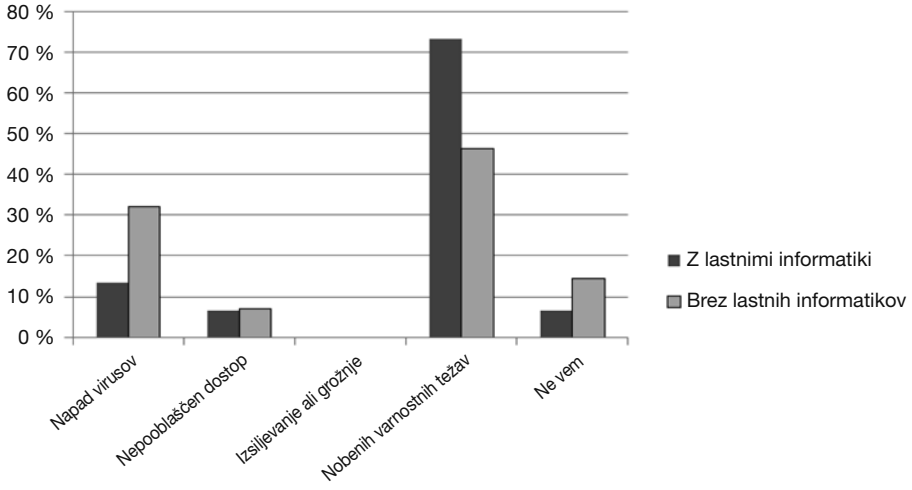
Slika 3: **Varovanje računalniške opreme v anketiranih podjetjih (Vir: raziskava)**

Statistika EU iz leta 2005 je pokazala, da v Sloveniji skoraj četrtina podjetij v zadnjih treh mesecih ni obnovila zaščite. V primeru anketiranih podjetij pa je stanje celo slabše, saj jih v zadnjih treh mesecih kar tretjina ni obnovila zaščite, kar ponovno kaže, da je stanje na področju varovanja pod slovenskim in seveda tudi evropskim povprečjem.



Slika 4: **Nazadnje obnovljena zaščita v anketiranih podjetjih (Vir: raziskava)**

V končni fazi pa so nas zanimale posledice omenjenih varnostnih problemov in konkretne varnostne težave. Pokazalo se je, da je imelo v celoti 33 odstotkov anketiranih podjetij varnostne težave, kar je zopet občutno slabše od slovenskega povprečja. Omeniti pa je treba, da so imela podjetja z lastnimi zaposlenimi informatiki bistveno manj varnostnih težav kot podjetja brez svojih informatikov (slika 5). Ta rezultat je presenetljiv, saj zunanje izvajanje teh dejavnosti običajno ne postavlja v ospredje večjega varnostnega tveganja. Lahko le predpostavljamo, da anketirana podjetja nimajo ustrezno urejenih dogovorov in odnosov z zunanjimi strokovnjaki s področja informatike.



Slika 5: **Odstotek anketiranih podjetij z zaposlenimi informatiki in podjetji brez lastnih informatikov, ki so zaznale varnostne težave (Vir: raziskava)**

V slikah 1 do 5 smo predstavili neposredne rezultate raziskave. Vendar smo poskušali analizirati tudi določene vzročne in funkcijske povezave. Zbrane podatke smo uporabili zato, da smo analizirali povezave med varnostnimi težavami, starostjo opreme ter ravnjo in kakovostjo zaščite. Vpeljali smo štiri nove agregatne spremenljivke, ki smo jih izračunali iz osnovnih podatkov, pridobljenih z anketo:

- *varnostne težave* – podjetja smo razvrstili v dve skupini. V prvi so podjetja, ki niso ugotovila nobenih varnostnih težav, v drugi pa tista, ki so ugotovila katero od težav (slika 5);
- *varnostna zaščita* – tudi v tem primeru smo podjetja razdelili v dve skupini. V prvi so podjetja z dobro varovano opremo, ki uporabljajo vsaj tri varnostne metode (slika 3), kot slabo varovano opremo pa smo šteli primere, ko ima podjetje le dva zaščitna ukrepa ali manj;
- *pogostnost obnavljanja zaščite* – v skladu z metodologijo EU je ena skupina podjetij redno obnavljala

zaščito, če so to storila manj kot v treh mesecih, in neredno, če tega niso storila v zadnjih treh mesecih (slika 4);
- *starost opreme* – podjetja, ki imajo opremo, mlajšo od štirih let, so bila v eni skupini, v drugi pa podjetja z opremo, ki je starejša od štirih let (slika 2).

Soodvisnost izbranih spremenljivk smo ocenjevali s hi-kvadrat (χ^2) testom. Ugotovili smo:
- soodvisnost med *varnostnimi težavami* in *varnostno zaščito* je statistično značilna ($p<0,01$), saj je kontingenčna tabela stabilna, ker znaša frekvenca 5,97 in zadošča pogoju o minimalni frekvenci večji od 5. S tem smo pokazali, da tudi v primeru anketiranih turističnih podjetij velja, da boljša varnostna zaščita zmanjša varnostne težave in seveda obratno.
- statistično je značilna tudi soodvisnost med *varnostnimi težavami* in *pogostnostjo obnove zaščite* ($p<0,01$), saj je tudi v tem primeru kontingenčna tabela stabilna (frekvenca znaša 6,12). Tako smo pokazali, da se podjetja, ki neredno obnavljajo opremo, pogosteje srečujejo z varnostnimi težavami in obratno.
- Kot zadnji test smo analizirali soodvisnost med *starostjo opreme* in *pogostnostjo obnavljanja zaščite*. Test je potrdil soodvisnost (frekvenca znaša 7,78 in $p<0,05$), kar pomeni, da uporabniki z novejšo računalniško opremo pogosteje obnavljajo zaščito informacijskega sistema. Predpostavljamo, da se novejša oprema uporablja za zahtevnejše in posledično bolje varovane obdelave.

Omenjene soodvisnosti so sicer pričakovane in jih zasledimo tudi v drugi panogah, vendar se nam je zdelo pomembno, da jih kljub temu potrdimo tudi za anketirana turistična podjetja, saj pomenijo pomemben argument za celovitejši pristop k uvajanju in izvajanju ustreznih varnostnih ukrepov.

3 POVZETEK UGOTOVITEV

Slovenska nastanitvena turistična podjetja skoraj ne uporabljajo specializiranih sistemov CRM in kažejo vrsto zadržkov proti njihovi uporabi, saj je ta v precejšni meri povezana tudi z varnostnimi vidiki. Vendar je glavni vzrok še vedno dejstvo, da so to globalno gledano razmeroma majhna in nepovezana podjetja, ki imajo temu primerne tudi finančne in tehnološke omejitve. To se odraža v razmeroma velikem odstotku podjetij brez lastnih kadrov s področja informatike in zanje drage programske ter strojne opreme. Kljub temu da ne uporabljajo integriranih sistemov CRM, pa vodijo veliko evidenc o svojih strankah, vendar to počno na preprostejši način, ob uporabi neintegriranih programskih rešitev. Tako razdrobljene aplikacije praviloma pomenijo tudi težje vzdrževanje in predvsem težji nadzor nad njihovo uporabo. Med te probleme lahko uvrstimo tudi varnostne ukrepe. Ne glede na to, kakšno programsko opremo uporabljajo, raziskava kaže, da v povprečju varnostnim vidikom ne posvečajo dovolj pozornosti. Varnostna zavest je na splošno pod slovenskim povprečjem. Poudariti pa je treba, da je med anketiranimi podjetji tudi nekaj takih, za katere lahko trdimo, da so odlična na področju varovanja.

Ker je večina anketiranih turističnih namestitvenih podjetij manjših in si ne morejo privoščiti lastnih računalniških strokovnjakov, mora menedžment ustrezno urediti sodelovanje z zunanjimi izvajalci in njihovimi strokovnjaki. Rezultati naše raziskave, ki kažejo izrazito manj varnostnih težav v podjetjih z lastnimi računalniškimi strokovnjaki, kot v podjetjih, ki jih nimajo, pa odpirajo vrsto problemov in vprašanj, povezanih z menedžmentom zunanjega izvajanja. Seveda ne kaže podcenjevati prednosti kakovostnih lastnih strokovnjakov, vendar si tega očitno ne morejo privoščiti vsi. Delo z zunanjimi izvajalci ne bi smelo vplivati na kakovost storitev ali na raven varovanja. Po naši oceni je temeljni problem v večini analiziranih podjetij v organizaciji zunanjega izvajanja, kar se v končni fazi odraža na povsem tehnoloških področjih.

Z računalniškimi strokovnjaki je povezan problem uporabljene varnostne programske opreme, njeno posodabljanje in vzdrževanje. Rezultati raziskave kažejo, da v veliko podjetjih računalniški strokovnjaki svoje funkcije ne opravljajo prav vzorno. Samo sklepamo lahko, da je problem tudi v njihovi usposobljenosti. Razlago lahko najdemo tudi v izrazito nizkih investicijah v opremo, 21 odstotkov podjetij omenja predrago tehnologijo, saj s staro in neustrezno opremo ni mogoče zagotoviti potrebne varnosti. Zanimiva je povezava med starostjo opreme in pogostnostjo posodabljanja programske opreme, saj potrjuje domnevo, da anketirana podjetja generalno podcenjujejo pomen informacijske tehnologije za svoje poslovanje ali pa so tako na robu rentabilnosti, da si ne morejo privoščiti sodobne opreme in ustreznih kadrov. To, da je tretjina opreme starejše od štirih let, samo potrjuje navedeno domnevo. Posebno so presenetljivi tisti rezultati, ki kažejo, da mnoga

podjetja ne uporabljajo tudi najbolj osnovne varnostne zaščite (protivirusni programi, požarni zidovi in protivohunski programi), ki v splošnem predstavlja izjemno majhen strošek. To pa je, brez dvoma, napaka računalniških strokovnjakov.

Če poskušamo umestiti rezultate naše raziskave v širši slovenski in evropski kontekst, lahko omenimo raziskavo, ki jo je opravilo dansko podjetje Secunia (RIS, 2008), ki ugotavlja, da je večina računalnikov ogroženih prav zaradi pomanjkljivega posodabljanja programske opreme z izboljšanimi različicami, saj so virusi zadnje generacije sposobni obiti mnoge protivirusne zaščite, jih celo izključiti oz. onesposobiti (Androutsellis, Spinellis in Vlachos, 2010). Sicer jih protivirusna zaščita odkrije, vendar ne vsebuje orodij za preprečitev škodljivih posledic. Po mnenju Secunie bi morali posodobitve nameščati vsaj enkrat mesečno. Tega merila pa ne izpolnjuje več kot polovica anketiranih podjetij. To pomeni, da je bil naše trimesečno merilo za sprejemljivo pogostnost obnavljanja zaščite opazno preblago. Če bi se odločili, da je meja te sprejemljivosti le en mesec, bi bili rezultati raziskave precej bolj neugodni. Vendar je to razmeroma lahko rešljiv problem, saj ne zahteva posebnih vlaganj, zahteva samo urejenost na tehnološki in organizacijski ravni.

4 SKLEP

Ko smo začeli z raziskavo, smo predpostavljali, da vidijo slovenska turistična podjetja v sistemih CRM rešitev svojih tehnoloških in organizacijskih problemov, povezanih s poslovanjem s strankami. Pokazalo se je, da je za večino podjetij to le oddaljena možnost, na katero v bližnji prihodnosti ne računajo. Njihova organizacijska razdrobljenost in razmeroma draga tehnologija sta glavni oviri. Če bodo želela dolgoročno izrabiti tržne prednosti, ki jih potencialno dajejo sistemi CRM, bodo najbrž morala iskati rešitve tudi v medsebojnem sodelovanju na tehnološki ravni. Vendar bodo morala pri tem veliko večjo pozornost posvetiti konceptualnim vprašanjem, povezanim z informacijskimi sistemi in ustrezno tehnologijo. Med ta vprašanja spada tudi varnost opreme in predvsem osebnih podatkov, saj trenutno stanje v večini analiziranih turističnih organizacij ni zadovoljivo.

Čeprav smo v raziskavi analizirali predvsem tehnološke vidike sistemov ter varovanja opreme in podatkov, pa je varovanje v bistvu zadeva vodstva podjetja. Po eni strani mora vodilni menedžment zagotoviti organizacijske in seveda finančne pogoje, da sistem varovanja sploh lahko zaživi, ne glede na tehnološke rešitve. Po drugi strani pa mora problem v okviru svojih kompetenc tudi razumeti in nadzorovati. Menedžment mora sprejeti dejstvo, da sta razvoj in delovanje informacijskih sistemov, ki vsebujejo individualne osebne podatke, kočljiva zadeva, ki je med drugim tudi zakonsko regulirana in sankcionirana. Te odgovornosti pa ne more prenesti na računalniške strokovnjake. Nepoznavanje in nezaupanje v informacijski sistem ter strah pred varnostnimi problemi in potencialno zlorabo je seveda nekaj, s čimer se mora poleg informatikov spopasti predvsem menedžment. Informatiki morajo zagotoviti samo ustrezno tehnično zaščito in jo vgraditi v delovne procese.

Za turistična podjetja je značilno, da so komunikacije med njimi in strankami pogosto dvosmerne, saj v optimalnih razmerah omogočajo stranki, da si sama kreira svoj profil in določa svoje individualne želje. To pa je seveda mogoče le prek interneta in razmeroma odprtih in uporabniško prijaznih programskih rešitev. Taki sistemi pa so notorično varnostno ranljivi, še posebno v primeru manjših turističnih podjetij, ki si ne morejo privoščiti vrhunskih programskih in strojnih zaščit. Zato je očitno, da je treba najti kompromis med varnostjo in stroški obratovanja, ki bo zagotovil potrebne varnostne standarde. Marsikaterih ukrepov, ki ne zahtevajo velikih vlaganj, bi pa bistveno povečali varnost sistemov, velika večina podjetij ne uporablja. Omenimo samo šifriranje podatkov in ne nazadnje tudi varne elektronske podpise.

Kakovostno varovanje opreme in podatkov pa ima tudi drugo dimenzijo. Posamezniki so vedno bolj osveščeni o varnostnih vidikih interneta in na njem zasnovanih storitev, zato se glas o neustreznem varovanju lahko kaj hitro razširi. Izkušnje kažejo, da se v takih primerih zanimanje za določeno podjetje dramatično zmanjša, posledično pa se bistveno zmanjša poslovna uspešnost. Zato je dobro varovanje tudi dobra marketinška poteza, ki jo podjetja, ki delujejo v tako konkurenčnem okolju, ne bi smela zanemariti.

V raziskavi se s tem problemom sicer nismo posebej ukvarjali, vendar je z varovanjem podatkov posredno povezan tudi izbor in obseg individualnih podatkov, ki jih zbira in obdeluje posamezno podjetje. Po eni strani se s povečanim obsegom individualnih podatkov povečuje možnost zlorab v primeru vdora v sistem, povečuje pa se tudi možnost zlorab

v podjetju. S tem pa se že dotikamo poslovne filozofije in etike podjetij, ki je povezana z namenom in načinom uporabe podatkov ter seveda tudi z implementacijo sistemov CRM. Če k temu dodamo različne marketinške in tehnološke trike, povezane z iskanjem podatkov na internetu, s katerimi se samodejno zbirajo informacije o potencialnih in tudi konkretnih strankah, potem postaja vedno bolj jasno, da je problem zbiranja in varovanja osebnih podatkov v turističnih organizacijah širok in resen. Tehnološki vidiki varovanja so le vrh ledene gore in predstavljajo le manjši del problemov, s katerimi se srečujejo turistične organizacije. Ustrezna tehnologija, ki jo simbolizirajo sistemi CRM, pa lahko pomaga pri učinkovitem reševanju teh problemov.

Omeniti je treba tudi dve pomembni omejitvi naše raziskave. Najprej je bila omejena na razmeroma majhno število organizacij, ki so sodelovale v njej, saj je bila iz že omenjenih razlogov stopnja odgovarjanja razmeroma nizka. Rezultati so sicer statistično signifikantni, vendar bi večji vzorec omogočal podrobnejši vpogled v strukturo posameznih odgovorov. Druga značilnost izbranega vzorca pa je velikost organizacij, saj so individualni ponudniki turističnih nastanitvenih storitev praviloma manjše organizacije, ki imajo omejene možnosti za uvajanje zahtevnejših tehnoloških rešitev, kot so integrirani sistemi CRM. Zato se sama po sebi ponuja mogoča rešitev v združevanju sil na tem področju, zunanjem izvajanju v skupnih centrih, v uporabi enotnih programskih rešitev, skupnem izobraževanju, svetovanju ipd. Vendar bi bilo treba tudi v tem primeru vložiti precej naporov v iskanje enotnih organizacijskih in tehničnih rešitev, ki bi ustrezale vsem udeležencem, predvsem pa rešitev, ki bi zagotovile potrebno varovanje podatkov.

5 VIRI IN LITERATURA

[1] Acar, Tolga in John R. Michener. 2002. *Risks in Features vs. Assurance*. CACM Inside Risks. Http://www.csl.sri.com/users/neumann/insiderisks.html.

[2] Androutsellis, Stefanos, Diomidis Spinellis in Vasileios Vlachos. 2010. Biological Aspects of Computer Virology. *Social Informatics and Telecommunications Engineering* 26: 209–219.

[3] Bin Ibrahim, Al-Fattah. 2010. *Customer profile management system using CRM.* Faculty of Computer Science and Information Systems, Technological University of Malaysia.

[4] Bottitta, Silvestro. 2005. *Una Revisione, Caratterizzazione ed Implementazione per la Comprensione del Concetto di Trust*. Http://homepages.inf.ed.ac.uk/mfelici/ TrustGames/tesi_sb.pdf.

[5] Buhalis, Dimitrios. 2003. *eTourism: information Technology for strategic Tourism Marketing*. Upper Saddle River (New Jersey): Prentice-Hall.

[6] Bull, Christopher. 2003. Strategic issues in customer relationship management (CRM) implementation. *Business process management journal* 9(5): 592–602.

[7] Coenen, Tracy. 2008. *More Data Security Problems Expected in 2008*. Http://www.allbusiness.com/crime-law-enforcement-corrections/criminal-offenses-fraud/5843128-1.html.

[8] Eurostat. 2005. *Raziskava o IKT*. Http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/ home/.

[9] Fox, Tricia in Steve Stead. 2001. *Customer Relationship Management: Delivering the Benefits*. Http://www.crmuk.co.uk/downloads/CRM01.pdf.

[10] Gray, Paul in Jongbok Byun. 2001. *Customer Relationship Management*. Centre for Research on Information Technology and Organisations. California: University of California.

[11] Istraturist. 2011. *Privacy Policy on the Website*. http://www.istraturist.com/en/info/privacy_policy.

[12] Kalakota, Ravi in Andrew Whinston. 1997. *Electronic commerce. A Managers guide*. London: Adison Wesley Longman Inc.

[13] Lawrence, A. Gordon in drugi. 2004. *Computer Crime and Security Survey*. San Francisco: Computer Security Institute Publications.

[14] McAllister, Thomas. 2004. *Customer Relationship Management – A Case for e-business Strategy*. Maryland: University of Maryland.

[15] Min, Wei. 2010. Construction of Marketing Management Information System of Travel Agency Based on Customer Relationship Management. *Journal of Convergence Information Technology* 5 (8).

[16] Perše, Zoran. 2000. Varstvo in zaščita osebnih podatkov pri elektronskem poslovanju*. Gospodarski vestnik* 11.

[17] Raba interneta v Sloveniji (RIS). 2008. *Uporabniki računalnikov ne skrbijo dovolj za posodabljanje programske opreme*. Http://www.ris.org/ index.php?fl=2&lact=1&bid =8442&menu=0.

[18] Rebec, Matej. 2009. *Management ravnanja s kupci na področju turizma v Sloveniji z vidika elektronskega varovanja podatkov.* Magistrsko delo. Koper: Fakulteta za management.

[19] Rigby, Darrell, Fred Reichheld in Steve Berez. 2002. Custom fit*. Optimize*, December 2002, 26–36.

[20] Rosen, Charles. 2000. *Customer Intelligence Gets Smarter*. New York: InformationWeek. Http://www.informationweek.com/bizint/biz804/customer.htm.

[21] Slovenska turistična organizacija (STO). 2010. *Slovenski turizem v številkah 2009*. Http://www.slovenia.info/pictures%5CTB_board%5Catachments_1%5C2010 %5C_stoVStevilkah_09_web_9710.pdf.pdf.

[22] UNWTO. 2011. *2010 International Tourism Results and Prospects for 2011.* Http://www.unwto.org/facts/eng/pdf/barometer/UNWTO_HQ_Fitur11_JK_1pp.pdf.

[23] Zorman, Marijana. 2001. Vas skrbi zloraba osebnih podatkov? *Gospodarski vestnik* 39: 64–65.

▪

Matej Rebec je diplomiral na Ekonomski fakulteti v Mariboru, leta 2009 pa je na Fakulteti za management Koper magistriral s področja elektronskega varovanja podatkov. Zaposlen je v policiji kot kriminalistični inšpektor specialist in pokriva delovno področje računalniške kriminalitete. Aktivno se udeležuje znanstvenih konferenc, predvsem s področja informatike ter turizma.

▪

Cene Bavec je redni profesor na Fakulteti za management Univerze na Primorskem in pokriva področje splošnega menedžmenta in menedžmenta informacijskih tehnologij. Redno predava tudi na Fakulteti za matematiko, naravoslovje in informacijske tehnologije Univerze na Primorskem.