Vloga in pomen informacijske varnosti na trgu konkurenčnosti sodobne družbe

Nataša Mrzdovnik, študentka, Fakulteta za varnostne vede, Univerza v Mariboru

Namen prispevka
Prispevek prikazuje pomen informacijske varnosti v sodobni družbi. Zakaj je le ta v porastu in kako vpliva urejena informacijska varnost organizacije na trg konkurenčnosti. Prikazati želim zakaj je organizacija, ki posveča pozornost informacijski varnosti v konkurenčni prednosti in zakaj se organizacije odločajo za urejenost omenjenega področja.

Metode
Prispevek temelji na avtorjevem poznavanju področja informacijske varnosti. V sladu z namenom prispevka sta uporabljeni deskriptivna metoda in analiza vsebin primarnih in sekundarnih pisnih virov.

Ugotovitve
Informacijska varnost in implementacija varnostne politike imata v tujini veliko večjo vrednost kot pri nas. Organizacija, ki v tujini objavi svojo varnostno politiko, si s tem pridobi velik ugled in postane zaupanja vreden partner. V Sloveniji se področje informacijske varnosti šele dodobra razvija, vendar zaradi tega njen pomen ni nič manjši.

Omejitve/uporabnost prispevka
Prispevek podaja splošna znanja iz področja informacijske varnosti saj je zaradi njegove strnjenosti izpuščenih še veliko pomembnih informacij.

Praktična uporabnost
Prispevek je uporaben pri širitvi znanja o pomembnosti informacijske varnosti. Ne mnogokrat je težko prepričati vodstvo organizacije v financiranje področja informacijske varnosti ali implementacijo varnostne politike. Prispevek prikazuje temeljne prioritete organizacije z urejenim področjem informacijske varnosti.

Izvirnost/pomembnost prispevka
Prispevek je namenjen vsem, uporabnikom informacijske tehnologije v organizaciji. Predvsem tistim, ki želijo v organizaciji izboljšati področje informacijske varnosti pa ne najdejo pristopa, s katerim bi to področje približali vodstvu podjetja.

Ključne besede: informacijska varnost, informacijski sistem, ekonomska prednost, konkurenčna prednost, ugled organizacije

1 UVOD

Informacijska varnost iz leta v leto pridobiva na svojem pomenu. Zavedanje organizacij o povezavah med ekonomsko uspešnostjo, konkurenčno prednostjo in področjem informacijske varnosti narašča. Vedno več svoje energije organizacije usmerjajo v urejenost informacijske varnosti, saj je to področje ključnega pomena pri dokazovanju na trgu konkurenčnosti sodobne družbe. Če želijo ostati zaupanja vreden partner, je njihova investicija v področje informacijske varnosti nujna.
Zadnja leta se število člankov na temo informacijske varnosti opazno povečuje v vseh revijah. Konferenca, ki je povezana z računalništvom in informatiko ne mine brez najmanj enega predavanja o informacijski varnosti. Vedno več pa je tudi konferenc, predavanj in izobraževanj, ki so namenjene izključno njej (Računalniške novice, 2009).
V sodobnem tenološkem svetu informacijska varnost vedno bolj pridobiva na svojem pomenu. Organizacije se iz dneva v dan bolj zavedajo da je investicija v področje informacijske varnosti potrebna, če želijo ostati zaupanja vreden partner. V Sloveniji se večina organizacij ne posveti

področju informacijske varnosti v tej meri, da bi implementirale krovno varnostno politiko in se certificirale. Vsaka pa se na svoj način hote ali ne hote dotika smernic, ki jih standardi ponujajo. Vsaj delno se posvečajo področju, ki ga zajema informacijska varnost. Področje informacijske varnosti je torej prisotno v vseh organizacijah, problematika, ki iz tega izhaja pa je urejenost omenjenega področja. Idealno za informacijsko varnost bi bilo, da bi naraščala vzporedno z razvojem tehnologije. Žal temu ni tako, zato je toliko bolj pomembno, da se področju informacijske varnosti posvetimo v navečji možni meri.

2 NAJŠIBKEJŠI ČLEN INFORMACIJSKEGA SISTEMA

Gane Spafford (Bowen, 2002:302) opisuje popolnoma varen sistem: »edini sistem, ki je zares varen, je takšen, ki je izključen in električnega omrežja, zaklenjen v sefu, narejenem iz titana, zakopan v betonskem bunkerju, ki ga obdaja plast živčnega plina in zelo dobro plačani oboroženi stražarji. Vendar niti takrat ne bi zastavil svojega življenja zanj«. Opis varnega sistema Gane Spafforda podaja osnovne smernice definiciji informacijske varnosti. Informacijska varnost je varnost podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, spremembo ali uničenjem (Peltier, 2002).

Informacijski sistem je varen, ko zagotovimo varnost podatkov pred nezakonitim dostopom, uporabo, razkritjem, spremembo ali uničenjem. Opis Gane Spafforda opozarja na to, da se zagotoviti varnega informacijskega sistema ne da.

Vedno bolj se dviga zavedanje, da je varovanje informacijskega sistema stoji na ekonomskih temeljih. Pomanjkljivo informacijsko varovanje lahko pomeni velike finančne izgube ali celo propad podjetja. Varovanje informacij v širšem smislu presega obseg tehničnih sredstev, ki zgolj omogočajo zagotavljanje zarovanja informacij in podatkov informacijskega sistema. Skrb za zagotavljanje informacijske varnosti se začne in preneha pri posamezniku, ki ima možnost dostopa do teh informacij (Kozar, 2010).

Zavedanje, da je človek najšibkejši člen varnostne verige narašča. Tehnologijo se sprogamira, naredi koristna komur koli to želimo in ve se kaj od nje pričakovati. Ljudje, niso narejeni po istem principu. Organizacijam je vedno največja nevarnost prav tisto, kar je za njih nepredvidljivo, ta nepredvidljivost pa v največji meri izvira iz lastnosti oseb, torej zaposlenih.

Ugotovitve raziskav Ernst and Younga o informacijski varnosti kažejo, da strokovni delavci na področju informacijske tehnologije največjo skrb izražajo glede škodljivih dejanj zaposlenih, ki so zapustili organizacijo in pomanjkanjem ustreznih proračunskih sredstev. Glede na to, da je gospodarstvo še vedno v krizi, največjo gospodarsko krizo pa eni celo šele napovedujejo, ne smemo zanemariti možnosti, da lahko odpuščeni delavci zamerijo nekdanjemu delodajalcu in poskušajo na različne načine onemogočiti delovanje organizacije (Savanovič, 2010).

Zanimivo je že samo dejstvo, da je iz raziskave razvidna največja skrb na področju zagotavljanju informacijske varnosti prav pri odpuščenih delavcih v organizaciji. Marsikatera organizacija v Sloveniji je namreč mnenja, da ji glede na njeno gospodarsko dejavnost zaposleni in bivši zaposleni ne morejo škodovati. Premalo je zavedanja, da se vsaka večja organizacija danes srečuje z informacijskim sistemom. Ranljiv informacijski sistem je lahko koristen pripomoček bivšim zaposlenim do povzročitve škode ali pa celo onemogočanja delovanja organizacije. Poleg tega, da moramo zagotoviti varen informacijski sitem je pomemben dejavnik pri človeškem faktorju, torej pri zaposlenih in bivših zaposlenih neke organizacije tudi nadzor dostopa. Dostop moramo urediti do te mere, da lahko do informacij dostopajo samo oziroma izključno uporabniki z dovoljenji. To sta sicer dva osnovna načina pri ojačevanju najšibkejšega člena verige. Kljub okrepitvi tega člena, je le ta še vedno najšibkejši in bo tako tudi ostal zaradi že prej omenjene lastnosti - nepredvidljivosti.

3 POMEN ZA ORGANIZACIJE

Dejstvo je, da gospodarske razmere, prinašajo vodjam informacijske varnosti trd oreh. Gospodarski pritiski vplivajo na informacijsko varnost. Zniževanje stroškov in povečevanje donosa, je moto vsake organizacije, v razmerah, katerih živimo, pa je ta moto iz dneva v dan močnejši. Ob že tako

zmanjšanih razpoložljivih finančnih sredstvih organizacije je težko prepričati vodstvo podjetja, da je investicija v informacijsko varnost potrebna, če ne celo nujna.
Obvladovanje tveganj, povezanih s človeškimi dejavniki, računalniškimi sistemi in tehnologijo, naravnimi vplivi okolja in obvladovanje tveganj izvedbe poslovnih procesov, so dovolj tehntni razlogi, da bi odločitev o urejeni informacijski varnosti moralo sprejeti vsaka organizacija, katere cilj je poslovati kakovostno, uspešno in učinkovito, predvsem pa dolgoročno. Pri tem je pomembno, da varnostne zahteve nastanejo kot posledica poslovnih zahtev in tako zagotavljajo učinkovitost organizacij, sledijo zakonskim in pogodbenim zahtevam, ter zagotavljajo zmanjševanje tveganj v organizaciji.
Želja po obvladovanju informacijskih tveganj je poslovne narave, saj zagotavljanje zaupnosti infomacij predstavlja konkurenčno prednost. Posledice zaradi morebitnega vdora v informacijski sistem, nedelovanje poslovnih funkcij, napake in nepravilnosti pri poslovanju lahko zelo hitro ogrozijo obstoj organizacije tako na domačem, kot tudi na tujem trgu. Informacije so vedno bolj pomemben dejavnik uspešnega delovanja organizacije, zato je potreba po vzpostavitvi ustreznega sistema varovanja informacij na temelju varnostnih standardov, zakonodaje in razpoložljive informacijske tehnologije nujna (Horjak, 2004).
Organizacije, ki bodo svoje delovanje uskladile s standardom bodo imele prednost pri sklepanju novih poslov tako na domačem, kot na tujem trgu. Prednosti takšnih organizacij so predvsem (Horjak, 2004):

- Konkurenčna prednost (tuje organizacije se lažje odločijo za sodelovanje s Slovenskimi podjetji, katere še ne poznajo)
- Ekonomska prednost (povečanje prodaje storitev in zmanjšanje stroškov)
- Ugled podjetja
- Zaupnost, celovitost in razpoložljivost informacij.
- Obvladovanje tveganj.

Vse omenjene prioritete so ključnega pomena pri konkuriranju na trgu. Zmanjševanje stroškov v podjetju, zagotavljanje zaupnosti ter obvladovanje tveganj dajejo zaupanje morebitnim partnerjem , ki se prav zaradi tega zaupanja odločajo o poslovanju. V kolikor dosežemo, da je to zaupanje na visokem nivoju, podkrepimo ga prav z omenjenimi prednostmi, lahko z zagotovostjo trdimo, da imamo ob sebi partnerja s katerim bomo lahko sodelovali dolgoročno.

3.1 Konkurenčna prednost

Organizacije, katere še ne poznajo novega poslovnega partnerja, se lažje odločijo za nekoga, katerega poslovanje temelji na usklajevanju standardov, če ne celo implementaciji varnostne politike. Razlog za to je enostaven – tovrsten partner deluje po določenih standardih, ki so organizaciji poznani. Posledica poznavanja delovanja pa je občutek vanosti.
Organizacije, katerih gospodarska dejavnost temelji na razvoju in vse tiste, za katere predstavljajo informacije pomemben vir poslovanja, se vsekakor vsaj dotikajo standardov in priporočil varnostne politike. Izdelana varnostna politika organizacije pomeni zagotovilo, da se le ta posveča področju varovanja informacij. Sodelovanje s takšno organizacijo poslovnim partnerjem daje večji občutek zaupanja, saj je za varnost dejansko tudi bolje poskrbljeno kot v drugih organizacijah. Ni novo, da naročniki pričakujejo od ponudnika izdelano politiko varovanja informacij. Torej je politika varovanja vsekakor konkurenčna prednost organizacije (Poznič, 2009).
Z zagotavljanjem konkurenčne prednosti v organizaciji, posledično zagotavljamo tudi ekonomsko prednost. Zmanjševanje stroškov, ter povečanje prodaje storitev nam prineseta boljše konkuriranje na trgu. Takšna organizacija se predstavlja kot ugoden ponudnik na trgu svojih storitev ali dobrin, ter tako pridobi več poslovnih priložnosti kot organizacije, katere temu področju ne posvečajo toliko pozornosti.

3.2 Ekonomska prednost

Implemetacija varnostne politike oziroma posvečanje področju informacijske varnosti pomeni izboljšanje ekonomike organizacije. Da se investicija v področje informacijske varnosti obrestuje, lahko vidimo s primerjavo stroškov, ki so potrebni za posodobitev infrastrukture dela informacijskega

sistema in oceno potrebnih virov za določitev, odobritev ter implementacijo varnostne politike. Vsekakor so stroški posodobitve infrastrukture dražji. Poleg tega, pa nam implementirana varnostna politika omogoča večji nadzor nad zaposlenimi, kar pomeni kakovostnejše in učinkovitejše delo.
Vedno več organizacij se zaveda pomena varovanja informacij. Tako izguba, kot tudi zloraba informacij lahko za organizacijo pomenita ogromno ekonomsko škodo. Organizacije, ki dajejo dovolj pozornosti področju varovanja informacij, se vsekakor kažejo kot zaupanja vreden partner (Poznič, 2009).
Zaupanje je eden izmed temeljev poslovnega sodelovanja. Tako nam ekonomska prednost prinese konkurenčnost, saj na sodobnem trgu lahko konkurira le organizacija, kateri je vredno zaupati. Svoje dobro ime si širi s to lastnostjo, ter si tako povečuje konkurenčno prednost a hkrati zmanjšuje stroške. Organizacija, ki deluje po tem načinu lahko brez kančka dvoma uspešno konkurira na trgu konkurenčnosti sodobne družbe. Takšno delovanje organizacije, bi moralo postati stalnica vseh organizacij v sodobni družbi.

3.3 Ugled podjetja

V tujini si poslovni subjekti z objavo lastne varnostne politike pridobijo velik ugled (Valenčič, 2000 in Parker 2001). V Sloveniji objava lastne varnostne politike določene organizacije še ne prinese velikega ugleda. Tiste organizacije, ki imajo urejeno varnostno politiko pa tudi pri nas uživajo med poslovni partnerji večje zaupanje. Kot v svojem članku pravi Hornjak (2004) se posamezniki odločamo za sklenitev življenjskega, nezgodnega, avtomobilskega zavarovanja, vendar vedno z mislijo, da tega najverjetneje ne bomo potrebovali. Podobno razmišljanje bi moralo veljati pri vodilnih v organizacijah glede zavarovanja pred izgubo ali razkritjem podatkov.

3.4 Zaupnost, celovitost in razpoložljivost

Zaupnost, celovitost in razpoložljivost so osnovne komponente informacijske varnosti iz katerih izhajajo vse dejavnosti povezane z vspostavljenjem in delovanjem informacijskega sistema. Komponenta celovitosti skrbi, da so podatki varovani pred nepooblaščenimi spremembami. Komponenta dostopnosti zagotavlja, da so podatki na voljo vedno, ko jih potrebujemo. Komponenta zaupnosti pa skrbi, da so podatki dostopni le pooblaščenemu osebju, ki ima za določene podatke tudi potrebo po vodenju (Kozar, 2010).
Komponente informacijske varnosti se pogosto povzemajo kot podajanje pravih informacij pravim osebam ob pravem času (Patru, 2003). Pomembnost omenjenega se vidi tako pri delovanju v organizaciji, kot pri poslovanju med organizacijami. Podajanje pravilnih informacij, ob pravem času, osebam, ki so za to pooblaščene, je ključnega pomena za uspešno poslovanje organizacije, ter njeno konkuriranje na trgu.

3.5 Obvladovanje tveganj

Ustrezno ravnanje ob informacijskih incidentih oranizaciji zagotavlja sprejemljivo oziroma čim nižjo škodo in čim manjši negativen vpliv na delovanje organizacije. V primerih katastrofalnih dogodkov je predvidena povezava upravljanja informacijskih tveganj ter incidentov na eni strani, s procesom upravljanja neprekinjenega poslovanja na drugi strani. Urejen proces neprekinjenega poslovanja zvišuje možnost, da bo organizacija preživela katastrofalen dogodek (Patru, 2003).
Tveganje ne moremo popolnoma izničiti, lahko pa ga znižamo na sprejemljivo raven. Za organizacijo je pomembno, da je pripravljena na različne incidente in se ob morebitnemu izbruhu hitro vrne na stare tire poslovanja. S tem pokaže, da se tudi ob morebitnih napakah hitro pobere in je prav zaradi tega škoda poslovanja minimalna. Poslovni parterji to lastnost organizacije prepoznajo kot minimalno tveganje ob morebitnih incidentih.

4 ZAKLJUČEK

Gospodarska kriza s sabo prinaša vodjam informacijske varnosti še več problemov. Že tako je bil na področju informacijske varnosti vedno pereč problem dokazati vodstvu organizacij zakaj se naložba v to področje izplača, v prihajajočih gospodarskih razmerah pa bo to vsekakor veliko težje. Ob že tako zmanjšanih razpoložljivih finančnih sredstvih organizacije je dejstvo, da bo težko prepričati vodstvo podjetja, da je investicija v informacijsko varnost potrebna, če ne celo nujna. Skozi prispevek smo poskušali prikazati zakaj je urejenost tega področja konkurenčna in ekonomska prednost in zakaj uživajo organizacije, ki imajo urejeno področje varnostne politike večji ugled. Prikazati smo torej želeli vzroke, kateri bi vodstvo organizacije prepričali, da je financiranje v področje informacijske varnosti nujno. Skozi njih smo dejansko prikazali dejstva, s pomočjo katerih lahko lažje vodilne prepričamo v investicijo področja informacijske varnosti. V Sloveniji se organizacije vse premalo zavedajo pomena urejenosti tega področja. Vsaka organizacija, bi morala imeti zavedanje, da je investicija v informacijsko varnost pomembna zgolj in samo zaradi uspešnosti nje same.
Organizacije, ki skrbijo za urejeno varnostno področje zagotavljajo večjo zaupnost in si s tem pridobivajo med poslovnimi partnerji upravičeno vredno zaupanje. Pri nas objava varnostne politike organizacije še ne pomeni posebnega ugleda med poslovnimi partnerji, vsaj ne tistimi poslovnimi partnerji, ki so iz Slovenije. Se pa organizacije poslužujejo priporočil in smernic informacijske varnosti, iz leta v leto bolj. Zavedanje o pomenu informacijske varnosti med organizacijami narašča in bo še naraščala. Kljub gospodarski krizi, ki napovedano šele prihaja je pomembno da se zavemo, da je investicija v področje informacijske varnosti ena izmed naložb, s katerimi v prihodnosti ne bomo na izgubi.

VIRI

Bowen, R. (2002). Apache Administrator's Handbook. Indianapolis. Sams publishing.

Horjak, M. (2004). Vpliv varne informacijske tehnologije na ekonomsko uspešnost podjetja.

Kozar, M. (2010). Varnost in zaščita: višješolski učbenik. Maribor. Doba Epis.

Parker, Robert G. (2001). Creating the Privacy Compliant Organization, Information Systems Control Jurnal.

Patru, P. (2003). Ukrepi v primeru informacijskih nesreč. Šempeter pri Gorici: Inštitut za informacijsko varnost.

Peltier, Thomas R. (2002). Information Security Policies and Standards: guidelines for effective information security management. Boca Raton, FL: Auerbach publications.

Poznič, T. (2009). Informacije so bogastvo podjetja. Računalniške novice.

Savanovič, D. (2010). Grožnje in priložnosti informacijske varnosti. MonitorPro

Valenčič, I. (2000). Postavitev in uvedba dobre varnostne politike. Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov – zbornik referatov.