Kompromisi pri zagotavljanju informacijske varnosti v organizacijah

Kaja Prislan, Igor Bernik

Namen prispevka:
Zagotavljanje informacijske varnosti je v organizacijskem okolju zahtevna naloga, saj pogoji ki jih postavlja zunanje okolje vodijo v sprejemanje varnostno-poslovnih kompromisov. Prispevek se nanaša na idejo, da morajo organizacije za pridobitev določene kvalitete informacijskega sistema žrtvovati ali zmanjšati drugo kvaliteto istega ali drugega poslovnega procesa. Namen je prikazati vpliv sprememb informacijske varnosti na povezane procese in predlagati priporočila, kako zagotoviti čim manjši vpliv ukrepov na obstoječe funkcionalnosti. Prav tako predstavljamo etične vidike informacijske varnosti, ki vodijo v sprejemanje slabih kompromisov.

Metode:V prispevku je uporabljena metoda deskriptivne analize znanstvenih in strokovnih virov, sinteza in interpretacija ugotovitev. Obstoječa spoznanja podpiramo s pregledom raziskav o trenutnem stanju informacijske varnosti.

Ugotovitve:
Ugotavljamo, da ukrepi s katerimi povečujemo informacijsko varnost vplivajo na dostopnost storitev, neprekinjeno poslovanje, zasebnost zaposlenih, njihove pravice in obveznosti ter uporabnost sistemov. Raziskave in strokovnjaki navajajo, da organizacije zaradi precenjevanja tveganj, psiholoških pritiskov in nepravilnega razporejanja varnostnih ter upravljavskih funkcij, pogosto sprejemajo napačne odločitve. Če želijo sprejemati dobre kompromise morajo prepoznati varnostne potrebe, neetično ravnanje varnostne stroke in zagotoviti konstruktivni konflikt med odgovornimi.

Praktična uporabnost:
Spoznanja prispevajo k boljšemu razumevanju sodobne varnostne dileme s katero se srečujejo organizacije. Uporabnost prispevka se kaže v pojasnjevanju razlogov nepravilnih odločitev, kar v kombinaciji s podanimi priporočili ponuja rešitve za sprejemanje dobrih kompromisov.
Izvirnost:
Izvirnost prispevka se kaže v njegovi aktualnosti. Prispevek je inovativen zato, ker obravnava problem, ki je v tujih virih parcialno obdelan, v Sloveniji pa se ga namensko še ni obravnavalo.

Ključne besede: informacijska varnost, varnostni kompromisi, organizacije, učinkovitost, etične dileme

1 Uvod

Sodobna organizacija se je z varnostnega vidika znašla v težko rešljivi in paradoksalni situaciji. Agresivna tekmovalnost med organizacijami povečuje pritisk na poslovne entitete in zaostruje zahteve po inovativnosti, razvoju in posledično po optimizaciji procesov. Tovrstne cilje v največji meri dosegajo s pomočjo sodobne informacijsko-komunikacijske tehnologije [IKT], ki lahko v primeru nepremišljenih odločitev privede do nasprotnih učinkov. S sodobno tehnologijo organizacije ustvarjajo posebno inter-organizacijsko okolje. V njem obstajajo od

fizičnega okolja in klasičnih varnostnih ukrepov neodvisne ranljivosti, ki jim je potrebno posvetiti ustrezno pozornost v celovitem varnostnem načrtu organizacije. Cilj vsake organizacije, ki želi zagotoviti lastni organizacijski obstoj mora biti zagotavljanje ustrezne stopnje varnosti informacij s katerimi upravlja, vendar zaradi številnih ovir in omejitev učinkovita informacijska varnost pogosto ostane neuresničen organizacijski cilj. Sočasne zahteve organizacij po večji varnosti in funkcionalnosti sistemov, ob kombinaciji s pomanjkanjem informacij, finančnih virov, prehitrim razvojem varnostnih rešitev in neetičnimi vplivi na sprejemanje odločitev, ustvarjajo velike dileme in pogosto vodijo v sprejemanje slabih in s tem napačnih odločitev in kompromisov.

2 Organizacijski in varnostni kompromisi

Da lahko organizacija zagotovi ustrezno stopnjo varnosti informacij s katerimi razpolaga, mora na različnih ravneh upravljanja zagotoviti varnostne ukrepe, ki vplivajo na uporabo in dostop do varovanega premoženja, ki je v organizacijsko okolje implementirano z namenom pospešiti in racionalizirati poslovne procese. Težave nastanejo, ker se zaradi optimizacije procesov ustvarja varnostne vrzeli, le-to pa vpliva na zaupnost in celovitost informacij. Zaradi kritičnega pomena podatkov, ki jih sodobna tehnologija shranjuje, prenaša oz. obdeluje, organizacije potrebujejo omejitve s strani varnostnih mehanizmov.

Vloga informacijske varnosti je v organizacijah podporne narave; kljub njenemu visokemu pomenu. Zagotoviti mora zaščito temeljnih poslovnih procesov in omogočiti njihovo nemoteno in kredibilno delovanje. Ta situacija pa vodi v nasprotovanje varnostnih in poslovnih procesov. Učinkovitost informacijske varnosti je odvisna od pravilne izbire ukrepov v poplavi standardiziranih postopkov; v nasprotnem primeru prihaja do negativnih vplivov na neprekinjeno poslovanje, skladnost postopkov, racionalnost razporejanja virov in na druge, z informacijsko varnostjo povezane poslovne procese. Koncept kompromisa pri zagotavljanju informacijske varnosti se nanaša na idejo, da je za pridobitev določene kvalitete sistema potrebno žrtvovati ali zmanjšati drugo kvaliteto istega oz. drugega sistema/procesa (Wolter in Reinecke, 2010), saj je, kot zapisano zgoraj, informacijsko varnostna funkcija v organizacijskem okolju kontradiktorna. Učinkovitost informacijske varnosti torej ni odvisna samo od uspeha posameznih varnostnih ukrepov (onesposobitev ali onemogočenje groženj), ki jih organizacija izbere, temveč od sprejemanja (dobrih) odločitev in kompromisov. Določeni ukrepi so lahko sicer uspešni in preprečujejo uresničitev neke grožnje, vendar so v določenem organizacijskem okolju nepotrebni. Ker je glede na nizko stopnjo ogroženosti organizacije njihova implementacija lahko moteča, se grožnja upravlja na manj invaziven način. V drugačnem, varnostnem okolju pa bi bila uporaba enakih ukrepov edini način zaščite oz. upravljanja tveganj (Schneier, 2008).

Zaradi tovrstnega razmerja med optimizacijo in varnostjo sistemov, se varnostni management oz. pristojni varnostni oddelki soočajo z neugodno situacijo, saj morajo vzporedno izpolnjevati nasprotujoče si zahteve in naloge. Zagotoviti morajo sisteme, ki delujejo nemoteno in hitro, hkrati pa so varni in preprečujejo zlorabe in napake. Pravilne in racionalne odločitve, ki vodijo v učinkovito informacijsko varnost morajo poleg ugotovitev analize ogroženosti in tveganj upoštevati tudi rezultate analize vpliva možnih ukrepov na povezane poslovne procese. V praksi organizacije takšne analize izvajajo redko, na račun informacijsko varnostnih ukrepov pa najpogosteje žrtvujejo uporabnost procesov, podatkov in sistemov ter zasebnost uporabnikov (npr. Anderson, 2006; Wolter in Reinecke, 2010; Conklin, White, Williams, Davis in Cothren, 2011). Tako zagotavljanje ravnovesja med varnostjo in omenjenima konceptoma predstavlja enega ključnih izzivov informacijske varnosti.

a. Varnost in funkcionalnost

Informacijska varnost ima kot poslovni proces vpliv na funkcionalnosti in uporabnost sistemov, ki jih varuje. Organizacije organizacijski uspeh primarno zagotavljajo z razvojem in optimizacijo poslovnih procesov in z izboljševanjem dostopnosti sistemov, programov, omrežja in informacij (Gupta in Zhdanov, 2004). Problem je v tem, da je programska oprema pogosto zasnovana varnostno pomanjkljivo, ob izkoriščenju ranljivosti pa lahko pride do hudih posledic za organizacijo. Te morajo stalno varnostno posodabljati nameščeno opremo, kar je velik finančni strošek, prav tako pa vpliva na kontinuiranost poslovnih in informacijskih sistemov (Ioannidis, Pym in Williams, 2012). Za upravljanje novo nastalih tveganj je varnostni management pogosto primoran omejiti ravno tiste kvalitete oz. prednosti sistema, zaradi katerih ga je organizacija implementirala: v zameno za večjo stopnjo varnosti in zaupnosti informacij mora (vsaj trenutno) žrtvovati njihovo dostopnost (Regan, 2003). S tega vidika prihaja do nasprotovanja znotraj varnostne funkcije same, saj se varnost nanaša na zahtevo po zaupnosti oz. na vprašanje, kaj sistem ne bo izvedel in katere aktivnosti bo preprečil; funkcionalnost pa se v veliki meri nanaša na dostopnost sistemov in vprašanje, kaj sistem lahko in bo izvedel (Ioannidis, Pym in Williams, 2012; Conklin, White, Williams, Davis in Cothren, 2011).

Na splošno velja prepričanje, da sta varnost in funkcionalnost obratno-sorazmerno povezana koncepta; večja kot je varnost manjša je uporabnost in obratno. Varnostni strokovnjaki zagovarjajo idejo, da lahko v triadi med varno, uporabno in poceni tehnologijo v tej kombinaciji zagotovimo zgolj varnost in uporabnost; varnost in cenovno ugodnost ali uporabnost in ugodnost, medtem ko vseh treh atributov sočasno ni mogoče zagotoviti. To pomeni, da mora biti organizacija pripravljena žrtvovati eno izmed omenjenih področij (Johansson, 2004). Ravno zaradi soodvisnosti omenjenih pojmov sta Carnor in Garfinkel (2004) mnenja, da varnost in uporabnost ni dobro razumeti kot medsebojno nasprotujoči si tendenci, temveč kot koncepta, ki ju je potrebno obravnavati skupaj. Sistem, ki je varen in neuporaben, je za organizacijo nekoristen; sistem, ki je uporaben vendar nezaščiten pa predstavlja (pre)veliko tveganje za organizacijo, da bi to zavestno dopustila. Iz tega razloga sta varnost in uporabnost kriterija, ki morata biti izpolnjena sočasno in zahtevata celovit pristop pri načrtovanju informacijske varnosti. In ravno to je temeljni problem oz. izziv, ki ga izpostavljajo varnostni managerji iz prakse (Conklin, White, Williams, Davis in Cothren, 2011); kako torej povečati ali izboljšati varnost tehnologije brez okrnjenja njene funkcionalnost oz. uporabnosti?

Rešitev omenjenega problema se kaže v tem, da je potrebno informacijsko varnost pri načrtovanju in izgradnji informacijske/tehnološke infrastrukture upoštevati kot njen temeljni in sestavni del. Varnost se ne sme načrtovati in uvajati naknadno, kot dodaten sloj infrastrukture, potem ko je sistem že implementiran, saj je cena na račun dostopnosti, funkcionalnosti in pristojnosti v tam primeru največje (Johnson in Goetz, 2007). Varnostni management mora informacijsko varnost obravnavati kot strateški oz. dolgoročni cilj in le takšno načrtovanje je podporne in ne omejevalne narave.

b. Varnost in zasebnost

Druga oblika kompromisov, s katerimi se sooča varnostni management, se pojavlja pri zagotavljanju ravnovesja med varnostjo in zasebnostjo. Tudi v tem primeru prihaja do nasprotovanja znotraj varnostne funkcije, saj je zasebnost eden izmed pod-pogojev informacijske varnosti. Le-ta se nanaša na zahtevo po zagotavljanju dveh temeljnih pravic; zasebnost zaupnih in zasebnih podatkov in zasebnost uporabnikov (Conklin, White, Williams, Davis in Cothren, 2011). Paradoksalna situacija nastane zaradi tega, ker je zahteva po varnosti izpolnjena le, kadar lahko natančno spremljamo aktivnosti uporabnikov, slednje pa je v primeru nepravilnih ukrepov, v nasprotju z interesom uporabnikov in pravico do zasebnosti

(Elahi in Yu, 2009). Na splošno se varnost zaupnih podatkov zagotavlja z metodami omejevanja in nadzorom dostopa, spremljanjem in beleženjem aktivnosti uporabnikov in zagotavljanjem sledljivosti ter kriptografskimi metodami. S tovrstnimi ukrepi vplivamo na pristojnosti uporabnikov, ki operirajo z informacijami oz. le-te uporabljajo pri opravljanju delovnih obveznosti: zmanjšujejo se njihove pravice, povečujejo obveznosti in kar je najpomembnejše, s povečanim nadzorom se posega v njihovo integriteto in zasebnost na delovnem mestu (Gupta in Zhdanov, 2004). Integriteta pa je tako kot varnost osebnih in zaupnih podatkov zakonsko opredeljena kot zahteva, ki jo mora izpolnjevati vsaka organizacija.

Kontradiktornost med zahtevo po varnosti osebnih podatkov in zasebnosti delojemalcev je odvisna od pravnega in kulturnega okolja v katerem organizacija posluje. V večini držav je zasebnost osebnih podatkov zaščitena z zakonodajo, ki organizacijam narekuje, kako lahko oz. morajo tovrstne podatke shranjevati, obravnavati in posredovati. Prav tako pa zakonodaja opredeljuje v kolikšni meri lahko na račun varnosti organizacije posegajo v pravice zaposlenih. Slovenska zakonodaja oz. Zakon o varstvu osebnih podatkov (ZVOP-1, 2007), ki je v tem primeru temeljni in izhodiščni zakon, narekuje, da mora organizacija osebne podatke obdelovati zakonito, sorazmerno in pošteno. Vse to pa so temeljni pogoji informacijske varnosti. Zakon organizacijam prepušča diskrecijsko pravico pri izbiri ustreznih ukrepov, ki jih morajo predpisati v internih aktih. Vzporedno z omenjenimi zahtevami po varnosti osebnih podatkov pa se ZVOP-1 nanaša tudi na pravice uporabnikov oz. zaposlenih na delovnem mestu. Uradno stališče Informacijskega pooblaščenca Republike Slovenije (2008) je, da je zasebnost zaposlenega na delovnem mestu njegova ustavna pravica, zato ga je o vsakem morebitnem nadzoru (npr. videonadzor, nadzor komunikacij, poštnih storitev, biometrija, sledenje ipd.) potrebno vnaprej obvestiti in opozoriti ter sestaviti pisni dogovor v katerem se delojemalec s takšnim nadzorom tudi strinja. Torej velja, da se mora zaposleni z nadzorom strinjati, privolitev pa mora biti prostovoljna in brez prisile, oziroma mora biti nadzor objektivno opravičljiv in sorazmeren.

Iz določil zakona je razvidno, da je dolžnost vsake organizacije poskrbeti za ustrezno varnost podatkov s katerimi upravlja. Z izbranimi ukrepi pa lahko, ob upoštevanju načela sorazmernosti posega tudi v zasebnost zaposlenih. Takšen poseg pa je lahko sorazmeren zgolj, kadar organizacija pozna grožnje in tveganja, ki ji pretijo ter kadar ob izvajanju nadzora upošteva pravice uporabnikov. V primeru pretiranega oz. prekoračenega posega v zasebnost zaposlenega pa se posega v pravico do zasebnosti, ki jo opredeljuje tudi 8. člen Evropske konvencije o človekovih pravicah (EKČP)[1]. Pri tem Informacijski pooblaščenec Republike Slovenije (2008) navaja, da se v praksi srečuje z mnogimi kršitvami in prekomernimi posegi v posameznikovo zasebnost na delovnem mestu, kar je pogosto posledica želje po zagotavljanju varnosti osebnih in zaupnih podatkov[2].

Iz navedenih zakonskih določil je razvidno, da mora varnostni management za zagotovitev legitimnosti in legalnosti informacijske varnosti, pri njenem načrtovanju upoštevati različne zakonske zahteve in izvajati zakonit, sorazmeren in upravičen nadzor nad zaposlenimi. Pretirane varnostne kontrole lahko posegajo v njihove pravice, kar ni samo v nasprotju s (slovensko in evropsko) zakonodajo, temveč tudi s temeljnimi pogoji učinkovite informacijske

[1] V Sloveniji ratificirana z Zakonom o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 /MKVCP/, Uradni list RS (7/1994).

[2] Najpogostejše kršitve ZVOP-1 v delovnih razmerjih so: neupravičeni vpogledi v elektronsko pošto zaposlenih in nadzor nad uporabo interneta; nepravilno izvajanje nadzora kot npr. neutemeljen videonadzor delovnih prostorov; neutemeljeno sledenje zaposlenim z GPS napravami, mobilnimi telefoni ipd.; neutemeljen nadzor nad telefonskimi klici zaposlenih; in prekomerno zbiranje osebnih podatkov zaposlenih.

varnosti. Pri izbiri varnostnih ukrepov velja upoštevati dejstvo, da nadzor in varnostna pravila vplivajo na legitimno uporabo zaupnih podatkov. (Pretirane) Kontrole lahko drastično zmanjšajo produktivnost zaposlenih in povečajo njihov odpor do varnostno pozitivnega vedenja. Post in Kagan (2007) ugotavljata, da v primeru prekomernih in nerazumljivih pravil ter omejitev, zaposleni raje zaobidejo kontrole in varnostne mehanizme, kot da na ta račun žrtvujejo lastno produktivnost in delovno uspešnost.

Učinkovita informacijska varnost je racionalna takrat, ko je prilagojena varnostnim potrebam posameznega poslovnega procesa in skladna z zakonskimi zahtevami. Ustrezno sprejemanje kompromisov med varnostjo, zasebnostjo in funkcionalnostjo ter pravilne odločitve za izvedbo varovanja informacij so lahko rezultat zgolj kadar se zasebnost zaposlenih načrtuje vzporedno z varnostjo zaupnih podatkov in kadar je zagotovljen minimalen vpliv na legitimne uporabnike, ki se zavedajo varnostnih pravil in razumejo razloge njihove uvedbe.

3 Trenutno stanje

Iz opisanih kompromisov, ki jih je potrebno sprejemati pri zagotavljanju (informacijske) varnosti je razvidno, da je proces njenega zagotavljanja v organizacijskem okolju izjemno kompleksen, v praksi pa nanj vplivajo tudi druge situacije, ki ta proces še otežijo. Odločitve pri načrtovanju informacijske varnosti so pogojene z različnimi organizacijskimi dejavniki, ki variirajo ter so odvisni od vsake organizacije in managementa posebej. Se pa vsa podjetja soočajo z večinoma neugodnim stanjem v zunanjem poslovnem okolju, zaradi konkurenčnosti in tekmovalnosti ter tudi vpliva gospodarske krize. V tem kontekstu z vidika informacijske varnosti največjo oviro predstavlja omejenost razpoložljivih virov ali njihovo neracionalno razporejanje. Posledice finančne in gospodarske krize v organizacijskem okolju kažejo v pomanjkanju finančnih virov, manjši stopnji splošne učinkovitosti organizacij in slabšem upravljanju varnostnih ter poslovnih procesov (TMT Global security study, 2011)[3]. Podjetja se srečujejo z visokimi finančnimi in poslovnimi omejitvami, ki se odražajo tudi na področju informacijske varnosti, kar potrjujejo tudi študije vpliva finančne krize na informacijsko varnost (PriceWaterhouseCoopers [PwC], 2009[4] ; Global information security survey, 2012[5] ; TMT Global security study, 2011; Global state of information security survey, 2013). Raziskave ugotavljajo, da je informacijska varnost, zaradi njenega vpliva na finančno stabilnost organizacij, postala ena izmed glavnih prioritet organizacij, saj tveganja na tem področju stalno naraščajo. Kljub povečanemu pomenu informacijske varnosti in večjim tveganjem pa iste raziskave ugotavljajo, da varnostne pomanjkljivosti oz. razhajanja med dejansko in želeno varnostno situacijo naraščajo, kar se pretežno pripisuje slabi varnostni zasnovi IKT, neustreznim postopkom in pomanjkljivim upravljanjem s človeškimi viri – uporabniki.

Raziskave ocenjujejo, da v praksi 52 odstotkov organizacij neučinkovito razporeja obstoječe vire (TMT Global security study, 2011), zgolj osem odstotkov podjetij oz. varnostnega managementa pa se vede varnostno odlično. Splošno neučinkovitost organizacij pri vzpostavljanju informacijske varnosti se zato najpogosteje povezuje z neučinkovitim managementom. Analiza 9,300 podjetij v 128 državah je pokazala, da ima zgolj 42 odstotkov organizacij proaktivno informacijsko varnostno strategijo, medtem ko imajo preostale pomanjkljive varnostne načrte (ali pa jih sploh nimajo) in se na grožnje odzivajo pretežno reaktivno (Global state of information security survey, 2013). Še bolj zaskrbljujoč pa je zaključek raziskave, ki ugotavlja, da bi se 97 odstotkov od 855 zaznanih incidentov v letu 2011,

[3] Mednarodna raziskava opravljena v 138 organizacijah.
[4] Raziskava opravljena med 7,200 pripadniki top managementa v 130 državah.
[5] Mednarodna raziskava o stanju informacijske varnosti v organizacijah z 9,600 izpraševanci.

lahko preprečilo z enostavnimi oz. osnovnimi varnostnimi rešitvami (Data breach investigation report, 2012), ki pa jih organizacije ne razvijajo. Opisani problemi in predstavljene varnostne dileme dokazujejo, da je učinkovitost informacijske najpogosteje ogrožena zato, ker organizacije v poizkusih sledenja hitremu razvoju tehnologije in tehničnim ukrepom pozabljajo na osnovne varnostne predpostavke in prispevek človeškega faktorja k varnostnem stanju v organizaciji (Ashraf, 2005). Najbolj problematična je ugotovitev, da informacijsko varnost v organizacijah zelo pogosto najbolj ogrožajo tisti, ki so odgovorni za njeno učinkovitost in predstavljajo zgled vsem zaposlenim. To potrjujejo tudi intervjuji s 300 strokovnjaki odgovornimi za management (informacijske) varnosti v različnih organizacijah, kjer je bilo ugotovljeno, da 42 odstotkov teh meni, da varnostna pravila in postopki zanje ne veljajo. Ti pri opravljanju svojih aktivnosti ne upoštevajo oz. ignorirajo procesne ukrepe zagotavljanja varnosti, hkrati pa imajo dostop do zaupnih informacij. V primeru neupoštevanja pravil in neodgovornega vedenja vodstva, takšnemu zgledu navadno sledijo tudi preostali zaposleni, zaradi česar varnostni ukrepi ne morejo doseči svojega namena. Ob predpostavki, da za zagotavljanje informacijske varnosti organizacije razpolagajo s povprečnimi tehničnimi rešitvami in da lahko na dejavnike iz zunanjega okolja vplivamo le v manjši meri, je posameznik in njegovo vedenje eden izmed ključnih dejavnikov učinkovitosti informacijske varnosti v organizacijah. Predvsem pa so lastniki, upravljavci, nadzorniki in varnostni management glavni nosilci korporativne varnosti (Vršec, 2013). Iz ugotovitev prikazanih raziskav v splošnem sklepamo, da organizacije niso učinkovite pri zoperstavljanju kibernetskim grožnjam in zoperstavljanju vsem oblikam kibernetske kriminalitete, prav tako pa sprejemajo neracionalne odločitve in slabe kompromise. V trenutni gospodarski situaciji, ko je propadanje organizacij vsesplošen trend, je njihov obstoj in preživetje odvisen od preudarnih in učinkovitih odločitev.

Sprejemanje kompromisov, finančne in kadrovske omejitve in neustrezna vodstvena mentaliteta pa niso edine dileme s katerimi se srečuje odgovorni varnostni management. Pogost razlog neustreznega varnostnega stanja so tudi kompleksni trendi na področju varnostnih in tehnoloških rešitev, ki jih je zaradi stalnega razvoja vse težje razumeti in jim slediti. Problem pri sprejemanju odločitev o zagotavljanju varnosti v organizacijskem okolju predstavljajo tri glavne psihološke ovire; to so strah, negotovost in dvom. Omenjeni psihološki dejavniki predstavljajo problem, kadar se pojavijo pri varnostnem managementu, ki zaradi tega sprejema neracionalne odločitve, tveganja precenjuje ali podcenjuje in implementira nepotrebne varnostne kontrole.

Strah, negotovost in dvom se najpogosteje pojavijo pri tistih posameznikih, ki nimajo na voljo ustreznega znanja in razumevanja o informacijski varnosti ter kadar pri njenem urejanju ne izhajajo iz dejanskega stanja. V kombinaciji z nasičenostjo trga s tehnološkimi in varnostnimi rešitvami pa se negotovost in dvom pri odločevalcih še povečujeta. Takšno situacijo zelo pogosto izkoristijo neetični varnostni strokovnjaki, ki lahko na ta način pospešijo svoj posel (Baddeley, 2011). Gre za poznano marketinško taktiko, ki se jo pogosto poslužujejo vodilna ali monopolna podjetja za ohranjanje konkurenčne prednosti. Kot ugotavlja že Pfaffenberger (2000) je na področju IKT taktika povečevanja strahu med uporabniki informacijskih sistemov zelo pogosta praksa. Podjetja, ki se ukvarjajo s proizvodnjo in prodajo tehnoloških rešitev uporabljajo poleg omenjenih metod še druge načine, s katerimi preprečujejo nakup in uporabo konkurenčnih proizvodov, kot npr. svarila in opozorila uporabnikov pred novimi, tveganimi sistemi; izgradnja takšnih sistemov, ki so nekompatibilni s konkurenčnimi proizvodi ali pa otežijo kasnejšo zamenjavo sistemov; višje cene popravil sistemov v primeru njihove kombinacije z drugimi proizvodi, ipd. Monopolna podjetja z omenjenimi metodami zlorabljajo svojo moč, zavirajo razvoj konkurence in produktov, potrošnike/organizacije pa silijo v nakup slabših proizvodov, ki so precenjeni. Vse to ima lahko še hujše posledice kot samo precenjevanje produktov in tveganj, saj lahko zaradi tega uporabniki postanejo ravnodušni ali neobčutljivi na realna in nevarna tveganja, hitri in učinkoviti odzivi pa niso izvedljivi, saj se

pozornost preusmeri na manj pomembna področja. Takšna situacija predstavlja etično dilemo, ko se varnostni management odloča o outsourcingu informacijske varnosti in postopkih certifikacije po varnostnih standardih s pomočjo varnostnih svetovalcev.

4 Sklep

Raziskave o (trenutnem) stanju učinkovitosti informacijske varnosti in analiza potreb po sprejemanju poslovno varnostnih kompromisov potrjujejo predpostavko, da zunanje poslovno okolje ustvarja velik pritisk na varnostni management in povzroča številne dileme pri vzpostavljanju informacijske varnosti. Ker je informacijska varnost, kljub svojemu pomenu, v organizaciji podporne narave, pa se ji z vidika sprejemanja odločitev za reševanje problemov ne namenja poglobljene pozornosti, kar je domnevno posledica neustrezne organizacijske varnostne mentalitete.

Ugotavljamo tudi, da lahko poizkusi (hitrega) prilagajanja sodobnim varnostnim trendom in tehničnim novostim vodijo v povečane ranljivosti. To se navadno zgodi takrat kadar organizacije tega ne počno premišljeno in analitično ter novosti uvajajo na podlagi priporočil prodajalcev, ki imajo lahko dvomljive namene. Pri zagotavljanju učinkovitosti informacijske varnosti je zato v primeru načrtovanja in vzpostavljanja varnostnih načrtov potrebno upoštevati prednosti in slabosti sodobnih informacijsko varnostnih trendov in razumeti tveganja, ki jih povzroča implementacija takšnih ukrepov (kot npr. prenos odgovornosti na zunanje subjekte).

Najboljše poslovno varnostne kompromise lahko organizacije dolgoročno sprejemajo z razvijanjem proaktivnega pristopa in socialne prevencije, v smislu ozaveščanja zaposlenih, razvijanja politike, dokumentiranja postopkov in procesov ter zagotavljanja njihove doslednosti in kontinuiranosti kot je ugotavljal že Anderson (2006). Pri tem mora biti takšen pristop zasnovan na podlagi točnih in aktualnih podatkov, saj je za sprejem racionalnih in pravilnih odločitev potrebno imeti na voljo zadostno količino informacij o dejanskem varnostnem stanju. Ob tem se na podlagi informacij o izhodiščni situaciji, priporoča personalizacija tveganj za varnostni management, s katerim se dviga ozaveščenost in upravlja psihološke dejavnike, kot so strah, negotovost in dvom. To pomeni, da se za vsako potencialno tveganje prikažejo možni scenariji posledic in njihov vpliv na zaposlene in management. Na ta način so tveganja in morebitne posledice uresničenih groženj bolj razumljiva, lažja pa je tudi odločitev o načinih njihovega upravljanja (Johnson in Goetz, 2007). Refleksivni in analitični pristopi so najboljši način minimaliziranja subjektivnosti in napak pri odločanju. In kot ugotavlja Jacobs (2011), se morajo odgovorni pri sprejemanju odločitev vprašati, kakšni so razlogi določene odločitve in kakšne so možnosti preverjanja njihove pravilnosti.

Informacijska varnost je učinkovita zgolj kadar je kompatibilna s potrebami poslovnega procesa in uporabnika. Hkrati mora informacijska varnost biti kot proces fleksibilna in ne toga – torej prilagojena posameznim tveganjem in ne enotna za celotno organizacijsko področje (Post in Kagan, 2007). Celovito obravnavo povezanih varnostnih in poslovnih procesov pa je s pomočjo omenjenih postopkov mogoče zagotoviti zgolj z razpršeno odgovornostjo za zagotavljanje funkcionalnosti tehnološke infrastrukture ter njene varnosti. Na ta način se odpravijo dileme in nasprotujoče si naloge, za katere bi bil zadolžen isti management/kader. Z medsebojnim sodelovanjem in povezovanjem različnih pristojnih oseb, se lahko sprejemajo dobri kompromisi in zagotovi konstruktiven konflikt, ki je eden izmed pogojev učinkovite informacijske varnosti.

Pri sprejemanju odločitev naj se upošteva tudi socialna komponenta informacijske varnosti. Ta naj podpira uporabnike, izpolnjuje oz. upošteva zahteve skupnosti, zaposlenih, partnerjev in strank; naj bo proaktivna in vidna, in ne rigidna, prikrita in zgolj zadovoljiva.

Literatura

Anderson, A. (2006). Effective management of information security and privacy. *Educause Quartely, 6*(1), 15-20.

Ashraf, S. (2005). *Organization need and everyone's responsibility: Information security awareness - Global Information Assurance Certification Paper.* Bethesda, MD: SANS Institute. Pridobljeno na http://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113

Baddeley, M. (2011). *Information security: Lessons from behavioural economics.* Cambridge: Gonville and Caius College.

Carnor, L. F. in Garfinkel, S. (2004). Secure or usable? *IEEE Security and Privacy, 2*(5), 16-18.

Conklin, W. A., White, G., Williams, D., Davis, R. in Cothren, C. (2011). *CompTIA security: Certification guide.* Columbus, GA: McGraw-Hill.

Data breach investigation report. (2012). New York, NY: Verizon. Pridobljeno na http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

Elahi, G. in Yu, E. (2009). Modeling and analysis of security trade-offs - A goal oriented approach. *Data & Knowledge Engineering, 68*(7), 579-598.

Global information security survey: Fighting to close the gap (2012). London: Ernst&Young. Pridobljeno na http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Global state of information security survey: Changing the game. (2013). London: PWC. Pridobljeno na http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf

Global state of information security survey: Eye of the storm. (2012). London: PWC. http://www.pwccn.com/webmedia/doc/634653330562192188_rcs_info_security_2012.pdf

Gupta, A. in Zhdanov, D. (2004). *Provisioning network security: Tradeoff between ionfrmation access and level of security.* Minneapolis, MN: Carlson School of Management.

Informacijski pooblaščenec Republike Slovenije. (2008). *Zasebnost na delovnem mestu.* Pridobljeno na https://www.iprs.si/fileadmin/user_upload/Pdf/brosure/Zasebnost_na_delovnem_mestu.pdf

Ioannidis, C., Pym, D. in Williams, J. (2012). Confidentiality vs. availabilty. *European Journal of Operational Research*, *216*(2), 434–444.

Jacobs, J. (2011). A call to arms: It's time to learn like experts. *ISSA Journal.* Priobljeno na http://beechplane.files.wordpress.com/2011/11/a-call-to-arms_issa1111.pdf

Johansson, J. M. (2004). *The fundamental tradeoffs.* Microsoft security techcentre. Pridobljeno na http://technet.microsoft.com/en-us/library/cc512573.aspx

Johnson, M. E. in Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy, 5*(3), 16-24.

Pfaffenberger, B. (2000). The rhetoric of dread: Fear, uncertainty and doubt in information technology marketing. *Knowledge, Technology & Policy, 13*(3), 78-92.

Post, G. V. in Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computer & Security, 26*(3), 229-237.

PWC. (2009). *Trial by fire: What global executives expect of information security in the middle of the world's worst economic downturn in thirty years.* London: PWC. Pridobljeno na http://www.ukmediacentre.pwc.com/imagelibrary/downloadMedia.ashx?MediaDetailsID=1557

Regan, K. (2003). Is Internet Security Killing E-Business? *E-Business: Security*. Pridobljeno na http://www.ecommercetimes.com/story/21462.html

Schneier, B. (2008). *The psychology of security*. Pridobljeno na http://www.schneier.com/essay-155.html

TMT Global security study: Raising the bar. (2011). New York, NY: Deloitte. Pridobljeno na http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/TMT/dttl_TMT%202011%20Global%20Security%20Survey_High%20res_191111.pdfTrček, D. (2006). Managing Infomation Systems Security and Privacy. Berlin: Springer.

Vršec, M. (2013). Varovanje poslovnega informacijskega sistema na osnovi politike varovanja informacij. *Korporativna varnost, 2*(3), 9-11.

Wolter, K. in Reinecke, P. (2010). Performance and security tradeoff. V A. Aldini, M. Bernardo, A. Di Pierro in H. Wiklicky (ur.), *Formal methods for quantitative aspects of programming languages*, 135-167. Berlin: Springer-Verlag.

Zakon o varstvu osebnih podatkov [ZVOP-1]. (2007). *Uradni list RS*, (94/07).