Informacijska varnost v procesu odločanja

Darko Prašiček, podiplomski doktorski študent na Univerzi v Mariboru, Fakulteta za varnostne vede
Iztok Podbregar, dr., redni profesor, Univerza v Mariboru, Fakulteta za varnostne vede
Teodora Ivanuša, dr., docentka, Univerza v Mariboru, Fakulteta za varnostne vede

Namen in cilj prispevka:
Prispevek poudarja pomembnost pridobivanja podatkov in informacij iz javnih virov, ki so pomoč managementu v procesu odločanja. Produkt obveščevalne dejavnosti/analitike je informacija, ki lahko nastopa tudi kot podatek v primeru, ko jo pridobi konkurenčna organizacija ali posameznik oziroma kriminalna organizacija s kriminalnimi ravnanji, zaradi pomanjkljivega varovanja informacij organizacije. Sodobna osredotočenost na pridobivanje podatkov iz javnih virov iz medmrežja in informacijskega oblaka terja predstavitev izbranih primerov in raziskav, s katerimi je prikazana pomembnost ustrezne strategije informacijske varnosti in informacijskih tehnologij v vsaki organizaciji. Predstavljeni so tudi izbrani načini zoperstavljanja tovrstnim grožnjam ter standardi varovanja in nadzora nad izvajanjem politike informacijske varnosti v organizaciji. Osrednji cilj prispevka je ozaveščanje tako strateškega kot operativnega managementa in zaposlenih v organizaciji, o pomenu in odgovornem odnosu do informacijske varnosti v organizaciji.

Metodologija:
Prispevek temelji na pregledu in analizi izbrane strokovno-znanstvene literature na področju pridobivanja podatkov iz javnih virov in informacijske varnosti ter ravnanj zaposlenih na področju informacijske varnosti. Literatura je bila izbrana na podlagi sekundarnih analiz raziskav, opravljenih v letih 2010 in 2011, o vodenju in upravljanju s procesi tveganja na področju informacijske varnosti.

Ugotovitve in omejitve:
Iz strokovno-znanstvene literature na področju informacijske varnosti izhaja, da je vsaka organizacija, ki nima strategije upravljanja s tveganji na področju informacijske in tehnološke varnosti, zelo ranljiva. Varnostni incidenti na področju informacijske varnosti in v informacijskih tehnologijah niso nujno škodljivi samo za prizadeto organizacijo, ampak tudi za druge, ki sodelujejo z organizacijo preko informacijskih sistemov. Ogrožanje organizacije je možno prek vseh obstoječih informacijskih poti in v vseh smereh. S sekundarnimi analizami podatkov iz opravljenih raziskav ugotavljamo, da se tako strateški kot operativni management ne zaveda dovolj celovito pomembnosti procesa upravljanja s tveganji na področju informacijske varnosti. Prav tako lahko govorimo o pomanjkljivem in nezadostnem izobraževanju vseh zaposlenih v organizacijah. Zato obstajajo za organizacije omejitve predvsem na ugledu organizacije navzven in zaupanju vanjo.

Izvirnost:
Prispevek sistematično prikazuje pomembnost zbiranja podatkov in informacij iz javnih virov ter njihovo vlogo v procesu odločanja. Nazorno so prikazane pomanjkljivosti v procesih upravljanja s tveganji na področju informacijske varnosti. Prav tako je povzet tudi razvoj nekaterih novih sistemov informacijske tehnologije, ki bodo na trgu verjetno povzročili obsežne spremembe. Predstavljena je tudi ena od možnosti preverjanja ranljivosti informacijskega sistema z uporabo t. i. etičnih hekerjev. Prispevek je uporaben tudi kot možno subjektivno izhodišče za razmišljanje o ranljivosti organizacij in posameznikov na področju informacijske varnosti ter nujnosti sistematičnega in sistemskega izobraževanja na tem področju.

Ključne besede: javni viri, tveganja, informacijska varnost, proces odločanja

1 UVOD

Hitre družbene in ekonomske spremembe so težko predvidljive in segajo v temelje družbe. Zato spremembe v ekonomiji zahtevajo sprotno in takojšnje odzivanje na nova tveganja, kar se kaže v nujnih spremembah managerskih sistemov vodenja. Ob tem pa globalizacija ponuja možnosti za

širitev podjetništva na globalni ravni. Pri tem ne gre spregledati morebitnih podjetnikov z »apetiti« po velikem in hitrem zaslužku ter morebitnih zakonsko prepovedanih, kriminalnih dejanj.
Za uspešno sprejemanje odločitev so nujno potrebni podatki, ki jih organizacija lahko pridobi iz javnih virov. Da imajo razpoložljive podatki vrednost, morajo skozi proces analitične obdelave podatkov, ki obsega zbiranje, analiziranje, združevanje in interpretacijo podatkov (Lowenthal, 2009), da podatki postanejo pomembna informacija za odločanje (Podbregar in Ivanuša, 2010).
Pomembnosti in prednosti razpolaganja z informacijami so se zavedali že veliko pred nami. Od iznajdbe pisave obstajajo zapisi o pomembnosti obveščevalnih podatkov. V obdobju od 400 do 320 pr. n. št. je Sun Tzu (2007) izdal priročnik *Umetnost vojne* (izvirnik: *The Art of War*), v katerem navaja pomen pridobivanja podatkov za odločanje o nadaljnjih strategijah.
Javni viri informacij so lahko tisk, knjige, zemljevidi, strokovna literatura, kasete, elektronski mediji, medmrežje, radio in televizija (Podbregar, 2008), sejmi, ljudje in drugo. Javni vir informacij je tudi neposredno zaznavanje s čutili na javnem kraju, ki ga Zakon o varstvu javnega reda in miru [ZJRM-1] (2006) določa kot tak vsak prostor, ki je brezpogojno ali pod določenimi pogoji dostopen vsakomur.
Zbiranje, analiziranje, združevanje zbranih podatkov in interpretacija informacij so v različni tuji in domači strokovni literaturi interpretirani kot obveščevalna dejavnost. Izraza obveščevalna dejavnost in obveščevalne informacije bosta uporabljana v smislu zbiranja, analiziranja, združevanja in interpretacije podatkov iz javnih virov. Zbiranje podatkov iz javnih virov ne poteka na način, kot informacije pridobivajo obveščevalno-varnostne službe, ki običajno intenzivno posegajo v posameznikove pravice in svoboščine, katerih informacije so po zakonu stopnjevane in namenjene le ozki skupini ljudi ali posameznikom (Podbregar, Mulej, Pečan, Podbregar in Ivanuša, 2010: 20).
Zbiranje podatkov na način, kot to izvajajo obveščevalno-varnostne službe za organizacije ni mogoče, ker je takšen način zakonsko prepovedan in tudi kazniv. Zato je področje zbiranja informacij iz javnih virov, kjer ne gre za poseganje v človekove pravice in svoboščine za organizacije, najprimernejši način. Informacije so posebej pomembne v času kriz, saj ima vsakdo, ki razpolaga s kakovostnimi informacijami, potrebno znanje in je v prednosti pred konkurenti, ki informacij nima. Težava se pojavi, ko je treba iz vseh razpoložljivih podatkov, potrebnih za odločanje, izluščiti nujno potrebne in zadostne informacije za odločanje v konkretnem času. Pri tem je v veliko pomoč vključevanje sodobne informacijske tehnologije ter primerno število usposobljenih in motiviranih sodelavcev. Pomembni javni viri v obveščevalni dejavnosti organizacij so poleg časopisov, medijev, ipd. informacije, pridobljene s pomočjo informacijskih tehnologij iz medmrežja in informacij v oblaku, ker pri teh dejavnostih nikoli ne posegamo v človekovo zasebnost in ne kršimo veljavne zakonodaje. Zato so informacije, pridobljene iz javnih virov, pomemben segment podpore odločanju (Podbregar in Ivanuša, 2010: 191).

2 INFORMACIJSKA VARNOST

Razpolaganje organizacije z informacijami, ki so ključnega pomena v procesu odločanja strateškega managementa in so shranjene v informacijskem sistemu organizacije, od organizacije zahteva, da vodi ustrezno informacijsko varnostno politiko. Opredeliti je treba ustrezne okvirje, politike in postopke, ki so razumljivi vsem v organizaciji. Tako bodo zaposleni razumeli pomen in način upravljanja informacijske varnosti. Z vključevanjem zaposlenih pri zagotavljanju informacijske varnosti na področjih politike, minimalnih pravil ravnanja, dostopov, obdelovanja, shranjevanja, prenašanja in uničenja informacijskih podatkov bodo zaposleni bolje vključeni in tako seznanjeni s celotnim sistemom zagotavljanja informacijske varnosti (Selan, 2011). "Čeprav se varnost informacij najpogosteje obravnava kot tehnično vprašanje, zadeva tudi upravljanje." Upravljanje obsega "obvladovanje tveganj, spremljanje rezultatov, upravljanje incidentov, poročanje in tudi odgovornost" (Selan, 2011: 9).
Zagotavljanje informacijske varnosti poteka na strateški in operativni ravni. Odgovornost na strateški ravni se nanaša na zagotavljanje sredstev, financ in zastopanje, ki je potrebno v programu informacijske varnosti. Tako ima pregled nad operativno ravnijo in ga tudi nadzira. Operativna raven odgovarja za obvladovanje tveganj, informacijsko varnostno politiko, postopke, standarde, smernice, izhodišča, klasifikacije, izobraževanja in organizacijo ter je tako v celoti zadolžen za izvajanje informacijske varnosti. Z varnostno politiko informacijske varnosti so določeni predpisi in pravila, ki urejajo splošne principe ravnanj, dostopov, obdelav, shranjevanj, prenosov in uničenj informacijskih

podatkov v organizaciji (Selan, 2011: 18). Seveda samo zagotavljanje informacijske varnosti ni dovolj za dosego uspeha na področju informacijskega varovanja organizacije. Kot z vsakim sredstvom je tudi z informacijsko varnostjo potrebno odgovorno upravljanje. Upravljanje informacijske varnosti je določanje pravil za vpeljavo, vzdrževanje, pravočasno, nenehno izboljševanje informacijske varnosti (Von Solms in Von Solms, 2009) in upravljanje z dejavnostmi, ki zagotavljajo varovanje informacij ter sredstev informacijske strukture pred izgubo, zlorabo, razkritjem in poškodovanjem. Pomembna dejavnost upravljanja informacijske varnosti je izvajanje nadzora organizacije za čim učinkovitejše upravljanje z morebitnimi tveganji (Selan, 2011: 15).

Bistvena sestavina informacijske varnosti je informacijska varnostna politika, ki združuje določena pravila in prakse. Obvezujoča pravila in predpisi, ki se nanašajo na splošne principe ravnanja, dostopa, obdelave, hranjenja, prenašanja in uničevanja informacijskih podatkov v organizaciji, veljajo tako za organizacijo kakor tudi za vse zaposlene in druge zunanje sodelavce, ki imajo dostop do informacijskih virov organizacije (Von Solms in Von Solms, 2009: 97). Na podlagi združenih določenih pravil in praks usmerja organizacijo, kako naj prenaša in ščiti informacije. Cilji informacijsko varnostne politike so v zagotavljanju varovanja informacij skladno z zakonodajo, pogodbenimi obveznostmi in cilji poslovanja organizacije, ščitenje in varovanje informacijskih virov, ki bi v primeru njihovega razkritja lahko privedlo do ogrožanja ali zlorabe informacij in zagotavljanje nemotenega poslovanja organizacije ter s preprečevanjem posledic škodljivih informacijskih varnostnih dogodkov zmanjšuje posledice in nastalo škodo v organizaciji, povzeto po (Von Solms in Von Solms, 2009: 62–70).

Zagotavljanje varnosti je odvisno od različnih dejavnikov, ki se medsebojno povezujejo in dopolnjujejo. Tudi informacijsko varnost sestavljajo dejavniki, ki se med seboj prepletajo, dopolnjujejo in obsegajo vse informacijske procese, tehnično in elektronsko opremo, pomanjkanje ali vključevanje ljudi in tehnologij ali odnosov s poslovnimi partnerji, strankami in tretjimi osebami. Glavni elementi informacijske varnosti, ki so med seboj povezani, temeljijo na: a) zaupnosti (angl. *confidentiality*), ki se nanaša na razkrivanje informacij nepooblaščenim osebam ali sistemom; b) celovitosti (angl. *integrity*), ki označuje skrb, da se ne spreminjajo ali uničujejo podatki na nedovoljen način, in c) razpoložljivosti (angl. *availability*) za obdelavo informacij z varnostno kontrolo varovanja, ki zagotavlja, da so informacije na razpolago in pravilne, ko se pokaže potreba po informacijah (IT Governance, 2006: 15).

Uspeh zagotavljanja informacijske varnosti je večji, če se v organizaciji izoblikuje varnostna kultura, ki jo omogočajo pogoji za upravljanje z informacijskimi podatki, kompetence za vzdrževanje varnostne kulture, odnos do varovanja informacijskih podatkov, postopki za zagotavljanje varnosti informacijskih podatkov, evidentiranje in odpravljanje kršitev v postopku varovanja informacijskih podatkov in organizacijski postopki za upravljanje področja varovanja informacijskih podatkov (Čaleta, Rančigaj in Lobnikar, 2011: 224).

3 INFORMACIJSKA TEHNOLOGIJA

Upravljanje informacijske varnosti je v organizaciji prepleteno z upravljanjem informacijskih tehnologij. Upravljanje informacijskih tehnologij se kaže v sodelovanju vseh strokovnjakov v organizaciji, ki se ukvarjajo z upravljanjem informacijske varnosti, in ne le ekspertov na področju informatike (Von Solms in Von Solms, 2009) in elektronskih komunikacij, čeprav so informatiki v glavnem zadolženi za operativne naloge informacijske varnosti. Povezovanje upravljanja informacijskih tehnologij in upravljanja informacijske varnosti pomembno vpliva na strategije in načine varovanja, zato informacijske tehnologije predstavljajo pomemben tehnološki vidik (Von Solms in Von Solms, 2009).

Globalizacija se odraža tudi na področju znanosti informacijskih tehnologij. Posledično je spodbudilo tudi šolstvo, ki je pričelo z uvajanjem študijskih programov ter idej na področju informacijskih tehnologij (Spencer, Aromaa, Junninen, Markina, Saar in Viljanen, 2006).

Razvoj znanosti in večje število izobraženih posameznikov s področja informacijskih tehnologij je, po raziskavah, povzročilo raznolike in pogosto neomejene kriminalne dejavnosti posameznikov kot organiziranega kriminala in njihovega medsebojnega kriminalnega sodelovanja (Felson, 2006: 7–8). Veliko povečanje kibernetske kriminalitete je razvidno iz poročanj organizacij, ki se ukvarjajo s preprečevanjem in varnostjo medmrežja. Težava organizacij v preprečevanju medmrežnega kriminala

se kaže v nejasni opredelitvi, kaj medmrežni kriminal je in majhnem številu znanih obtožb na sodiščih (Bernik in Meško, 2011: 85).
Hiter razvoj informatike zahteva nenehno seznanjanje z razvijanjem, novostmi na tem področju in nenehnim izobraževanjem. Če management in zaposleni v organizaciji ne spremljajo razvoja informatike, lahko to privede do premajhnega zavedanja pomena zagotavljanja in upravljanja informacijske varnosti. Seveda je nenehno spremljanje razvoja in novosti ter osveščanje s tem učinkovitejše z manj sredstvi, če organizacija zaposli ustrezen strokovni kader, ki ima primarno nalogo skrb za informacijsko varnost.

4 ZOPERSTAVLJANJE GROŽNJAM IN STANDARDI

Gotovo morajo vsi elementi varnosti izhajati iz strategije organizacije za zagotavljanje varnosti. Organizacije običajno uporabljajo običajne standarde varovanja in nadzora nad izvajanjem usmeritev za dostopanje zaposlenih v organizaciji v medmrežje, t. i. oblak in druga ravnanja v informacijskem sistemu organizacije. V ta namen organizacije uvajajo strojno opremo za samodejno zaznavanje potencialnih nevarnosti na ravni medmrežja ali oblaka, preprečuje poskuse vdorov in vdore v sistem, protivirusne programe, različno programsko varnostno opremo za pregledovanje tako centralnih domenskih kot mobilnih naprav. Iz raziskavi Selanove (Selan, 2011) je razvidno, da organizacije tehnično dobro skrbijo za informacijsko varnost s šifrirnimi sistemi, protivirusnimi programi, požarnimi zidovi, ipd.
Strategija zagotavljanja informacijske varnosti mora vključevati različne razvite varnostne standarde za zagotavljanje smernic in čim celovitejšega informacijskega varovanja (IT Governance, 2006: 16). Nekatere organizacije v večini uporabljajo uveljavljene standarde informacijske varnosti. Po mnenju strokovnjakov (Novak, 2011) je bilo leta 2011 v Republiki Sloveniji 22 podjetij s certifikatom ISO/IEC 27007 (ang. *Information technology – Security techniques – Guidelines for Information security management systems auditing*. Standard ISO 27000 je serija standardov ISO za področje informacijske varnosti in so se pridružili številnim drugim standardom, vključno z ISO 9000 (kakovost vodenja) in ISO 14000 (ravnanje z okoljem) (An Introduction to ISO 27001, ISO 27002....ISO 27008*)*. Organizacije se odločajo za pridobitev certifikata ISO 27001 (An Introduction To ISO 27001 (ISO27001) z namenom, da bi vpeljale večjo stopnjo varnosti ter povečale strokovnost, kredibilnost in zaupanje v organizacijo, lahko pa jih k temu napeljujejo želje poslovnih partnerjev (Bernik in Prislan, 2011) in zakonodaja (Novak, 2011). Nekatere organizacije pa smernice upoštevajo, saj je standard ISO 27001 ni pogoj, da lahko podjetja izvajajo upravljanje varnostnih incidentov, vendar se za pridobitev certifikata ne odločijo, ker certifikat ISO 27001 podaja priporočila na podlagi dobrih praks, ki jih podjetja ne glede na vrsto opravljanja dejavnosti lahko upoštevajo, in zaradi zakonodaje (Novak, 2011). V raziskavi je sodelovalo 17 podjetij, od katerih jih ima sedem certifikat ISO 27001. Na globalni ravni ni nepomembno, če se organizacija v procesu odločanja za določeni standard na področju informacijske varnosti glede na obstoječe razpoložljive in v uporabljane certifikate odloči za certifikat, ki je skladen z uporabljanimi certifikati v globalnem svetu, in certifikat vključuje standard nadzorstva, nepristranskosti za informacije in sorodno tehnologijo (ang. COBIT – *Control Objectives for Information and related Technology*), ISO 17799 in ostale, kot so FIPS Publication 200 (*Federal Information Processing Standards Publication* (FIPS, 2006)**)** in NIST 800-53 (Nist, 2009) v Združenih državah Amerike (IT Governance, 2006: 16; Markelj in Bernik, 2011: 41; Symplified and Solstice to Collaborate on Mobile Security for Cloud Applications, 2011).
V decembru 2010 je Selanova (Selan, 2011: 36–59) opravila raziskavo v 60-ih slovenskih podjetjih. Raziskava se je nanašala na management informacijske varnosti v slovenskih organizacijah z raziskovalnima vprašanjema, ali imajo organizacije po Sloveniji opredeljeno informacijsko varnost in koliko zaposlenih se ukvarja z informacijsko varnostjo ter njihova organizacijska razporeditev. Iz ugotovitev raziskave izhaja, da se z informacijsko varnostjo v največji meri ukvarja vodstveni in tehnični kader ter da velikost organizacije vpliva na skrb za informacijsko varnost. Z vprašanjem varovanja informacij se ukvarja kar 51,52 odstotkov zaposlenih z dodiplomsko univerzitetno izobrazbo. Kar je lahko zaskrbljujoče na področju strategije managementa, je ugotovitev, da podjetja namenjajo premalo pozornosti seznanjanju z informacijsko varnostjo zaposlenih, ki se z informacijsko varnostjo neposredno ne ukvarjajo. Za strateško upravljanje informacijske varnosti v organizaciji so običajno zaposlene tri osebe in sedem oseb na področju operativnega managementa informacijske

varnosti. Povprečna vrednost organizacij, ki imajo opredeljeno varnostno strategijo, znaša 1,19, pri organizacijah, ki varnostne strategije nimajo, pa je povprečna vrednost 1,83.
Z vidika informacijske varnosti je vsekakor pomembno prijavljanje varnostnih incidentov organizacij, saj le tako mogoče ugotavljati in preprečevati neželene vdore v informacijski sistem organizacije in tudi preprečevanje podobnih vdorov v informacijske sisteme konkurence, ker je organizacija zaradi poslovnih ali drugih stikov s konkurenco ali partnerji potencialna žrtev za nezaželeni vdor v informacijski sistem. Morebitne finančne in druge posledice, ki jih lahko organizacija utrpi zaradi ranljivosti informacijskega sistema, so razvidne iz podatkov Združenja bank Slovenije o izvedenih transakcijah v elektronskem bančništvu, ki jih je v intervjuju predstavil Bernik (Bernik, 2011). V letu 2000 je bilo s fizičnimi in pravnimi osebami na področju elektronskega bančništva opravljenih skupaj 1.167.000 transakcij v vrednosti približno 133 milijard tolarjev (472.803.347 €) v poslovanju doma in 68 milijard 24 milijonov (284.619.247 €) v tujino. Leta 2010 se je število transakcij fizičnih in pravnih oseb povečalo na skupaj 72.611.000 transakcij v vrednosti več kot 126 milijard 755 milijonov evrov pri poslovanju v Sloveniji in pri poslovanju s tujino v vrednosti skupaj 22 milijard 400 milijonov evrov. Na področju uporabe telebanke in mobilnega bančništva, je bilo leta 2005 opravljenih za več kot dva milijona transakcij v vrednosti več kot 62 milijard tolarjev (259.414.225 €) pri plačilnem prometu doma in za 880 milijonov tolarjev (3.682.008 €) v tujini. Leta 2010 pa je bilo transakcij za okrog 440 tisoč z vrednostjo 103 milijone evrov plačilnega prometa doma in 1,1 milijona evrov v tujini (Bernik, 2011).
Nepoznavanje obsežnosti posledic ali lahkomiselnosti pri zagotavljanju informacijske varnosti in informacijskih tehnologij v organizacijah je razvidno iz raziskave Novakove (2010), po kateri devet od sedemnajstih v raziskavi sodelujočih podjetij ne prijavlja varnostnih incidentov, šest podjetij prijavlja varnostne incidente različnim organom, npr. SI-CERTu – Slovenski center za posredovanje pri omrežnih incidentih – http://www.cert.si/ (ang. *Slovenian Computer Emergency Response Team*) (SI-CERT), eno podjetje ni imelo podatkov o varnostnih incidentih, prav tako je le eno podjetje le občasno prijavljalo incidente (Novak, 2011: 43).
Ker je računalništvo v t. i. oblaku (ang. *Cloud*) vse modernejše in čedalje pogosteje uporabljeno, je tudi verjetnost zlorabe shranjenih informacij in podatkov v oblaku večja. Zlorabe ne bodo povzročale vedno samo konkurenčne organizacije, ampak tudi kriminalni posamezniki ali kriminalne skupine, ki bodo izkoristili ranljivost oblaka in z nezakonitimi vdori pridobivali nezakonito koristi. Zato je varovanje informacij in podatkov v oblaku še toliko pomembnejše, ker bo škoda storjena ne samo organizaciji, ampak tudi posamezniku, ki z določeno organizacijo poslovno ali kako drugače sodeluje. Ponudniki informacijskih tehnologij in naslednikov informacijskih tehnologij, za katere skrbi vsak posameznik (ang. *Bring Your Own Device* – BYOD), so s temi napravami otežili prizadevanja v boju za politiko informacijske varnosti pri dostopanju v oblak iz pametnih telefonov, tabličnih računalnikov (androidov), ki jih uporabljajo zaposleni (Symplified and Solstice to Collaborate on Mobile Security for Cloud Applications, 2011). Informatiki organizacije lahko sami izdelajo oblak organizacije in tudi skrbijo za varnost oblaka, vendar pa se oblak organizacije običajno nahaja znotraj korporativnega omrežja. Lokacija javnega oblaka ni natančno definirana ampak se nahaja tam nekje v medmrežju (Markelj in Bernik, 2011). Pregled in revizija kot utrjena načina dela odkrivata mrtvo točko za spremljanje informacijske varnosti v organizaciji (Symplified and Solstice to Collaborate on Mobile Security for Cloud Applications, 2011).
Iz raziskave Weilla in Rosas (Weill in Ross, 2004) v 250-ih podjetij po svetu izhaja, da je iz politike informacijskih tehnologij jasno vidno, kako je načrtovanje in izvrševanje informacijskih tehnologij koristno v procesu upravljanja tveganj in odločanja v nejasno opredeljenih okoliščinah in kako bo strošek investicije prešel v donosno investicijo. V nasprotnem bo v kratkem času lahko nastala velika škoda (Sayer in Wailgum, 2008). Organizacije s kakovostno politiko informacijske tehnologije dosegajo več kot 25 odstotkov večje dobičke kot podjetja s skromno ravnjo politike informacijske tehnologije. Izvrševanje politike informacijske tehnologije je običajno na najvišji ravni organizacije za podporo strategiji organizacije. Po ugotovljenih tveganjih in spremembah informacijske tehnologije in začetnem ugotavljanju, se bo stopnja tveganja organizacije kazala s pravilno pripravo analize povezav, z izčrpno ocenitvijo tveganj in možnostmi za ocenitev in izbiro ustreznih ekonomsko razumnih obsegov (Stefan, Heise in Ulrich, 2010). Posledično mora oceno informacijskega tveganja najvišje vodstvo organizacije sprejemati s posebno pozornostjo (Rogers, Lukens in Lin, 2008).

Na koncu si morajo zaposleni, kot eden od najšibkejših členov informacijske varnosti v organizaciji, zapomniti, da je pri vsakokratni uporabi oblaka obvezno tudi vsakokratno ponovno prijavljanje v oblak, s prijavo (ang. *login*). Podjetje skupaj z zaposlenimi informatiki skrbi za varnostne metode, kot so gesla, enkripcija in redundanca informacij in podatkov, uporabniška imena, ipd. Zato je za varnost uporabe informacij in podatkov v oblaku ali medmrežju na mobilnih napravah predvideno vsakokratno posamezno nameščanje in ustvarjanje pregleda skladnosti, da lahko podjetje lahko naredi skupne informacije in podatke varnejše (Markelj in Bernik, 2011; Symplified and Solstice to Collaborate on Mobile Security for Cloud Applications, 2011).
Ugotavljanje, preprečevanje in odpravljanje morebitnih pomanjkljivosti je najboljši in ne nazadnje tudi najcenejši način za preprečevanje morebitnih nastalih posledic, ki bi jih utrpela organizacija zaradi pomanjkljivega informacijskega sistema oziroma vdora v informacijski sistem. Tako obstaja primerna rešitev s pregledom morebitnih pomanjkljivosti tudi z t. i. etičnimi hekerji. Etični heker počne vse, kar počne tudi zlonamerni heker, vendar z drugim namenom – da bi odkril ranljivost informacijskega sistema organizacije. Pri tem poskuša vdreti v določene informacijske sisteme, jih onesposobiti ter ukrasti pomembne informacije in podatke za ugotavljanje slabosti sistemov in njihove nadgradnje ter zaščite (Gabor, 2011).

5 RAZPRAVA

Globalizacija, hitrost razvoja znanosti informacijskih tehnologij in hitre spremembe v družbi v veliki meri pogojujejo uspešnost pri odločanju in razvoju organizacije. Na uspešnost odločanja in razvoj organizacije lahko ključno vplivajo informacije, s katerimi management razpolaga. Ker smo v času nenehnega razvoja informacijskih tehnologij, je najhitrejše pridobivanje podatkov/informacij iz javnih virov, do katerih dostopajo v medmrežju in informacijskem oblaku. Z vstopom v svetovni informacijski splet se postavi vprašanje informacijske varnosti. Zavedanje o pomenu informacijske varnosti je težko predstavljivo in razumljivo, ker ni neposredno in fizično oprijemljivo. Tako je veliko lažje razumljivo, da je potrebno dokumente ključnega pomena odločanja in razvoja organizaciji ustrezno hraniti in varovati. V glavnem se varujejo zaklenjenih v omarah ali celo v trezorjih. Odtujitev tako varovanih dokumentov lastnik zazna neposredno in fizično ter se zaveda prisotnosti tretje neželene osebe. Vstop v informacijskih sistem organizacije in odtujitev ključnih podatkov in informacij organizacije preko informacijskih tehnologij, pa velikokrat zaradi dejanske metafizike sploh ni zaznan. Odtujitev informacij organizacije nujno ne pomeni škode samo za organizacijo ampak tudi za posameznike, ki z organizacijo poslujejo. Zato je nujno potrebno zagotavljanje politike informacijske varnosti od managementa do vseh zaposlenih na vseh ravneh. Gledano širše, lahko izguba informacij organizacije in s tem v povezavi neuspešnost organizacije, vpliva na varnost ne samo organizacije, ampak na varnost v skupnosti. V primeru propada organizacije in s tem povezane izgube delovnih mest ljudi to pomeni slabši socialno-ekonomski položaj ljudi v skupnosti, kar prav gotovo vpliva na splošno varnost. Nezavedanje pomena informacijske varnosti in prenašanju ogromnih količin sredstev preko informacijskih sistemov s pomočjo informacijskih tehnologij v globalnem svetu, prav gotovo predstavlja grožnjo globalni varnosti na vseh področjih varnosti in ne samo informacijski.
Ugotovitve, da se strošek pravilnega načrtovanja in izvrševanja informacijske tehnologije pri odločanju pravzaprav na koncu predstavlja ¼ ali še višje dobičke organizacije kažejo v smeri pomena aktivnejšega sodelovanja med organizacijami samimi in izobraževalnimi institucijami. Sodelovanje med organizacijami bi bilo koristno pri izmenjavi informacij o uporabljeni informacijski tehnologiji za zagotavljanje informacijske varnosti. Z izmenjavo informacij o uporabljeni informacijski tehnologiji za zagotavljanje informacijske varnosti bi organizacije skupaj lahko dosegale učinkovitejšo informacijsko varnost in tako nedvomno zmanjševale stroške zagotavljanja informacijske varnosti. Z uporabo uveljavljenih standardov zagotavljanja informacijske varnosti, kot so ISO standardi, bi verjetno vse organizacije na območju Republike Slovenije skupaj nastopale pred konkurenco z večjim ugledom in zaupanjem v sodelovanju z organizacijami oziroma organizacijo, ki ima sedež na območju Republike Slovenije. Sodelovanje med organizacijami in izobraževalnimi ustanovami bi pomenilo večjo možnost za sprotno spremljanje in seznanjanje z novostmi informacijskih tehnologij in tako tudi hitrejšo uporabo najnovejših informacijskih tehnologij. Izobraževalne institucije bi s tesnejšim sodelovanjem z organizacijami lahko skozi izobraževalne programe razvijale in ustvarjale nove

informacijske tehnologije informacijske varnosti, ki bi bile bližje organizacijam oziroma bi bile za organizacije dostopnejše, cenejše ter hitreje in lažje uporabne. Za izobraževalne ustanove, bi to pomenilo dodaten vir sredstev za načrtovanje, razvijanje in izvajanje določenih študijskih programov.
Ob dejstvu, da se na področju informacijskih tehnologij za zagotavljanje informacijske varnosti uvajajo različni študijski programi na najvišjih stopnjah izobraževanja, obstaja tudi večja verjetnost, da se bodo pridobljena znanja s področja informacijskih tehnologij uporabila tudi za izvajanje škodljivih oziroma prepovedanih dejanj za pridobivanje pomembnih informacij s katerimi razpolagajo organizacije za potrebe odločanja, kakor tudi za nedovoljeno pridobivanje finančnih sredstev. To pa posledično, glede na hitrost razvoja informacijskih tehnologij pomeni nove in nove neomejene možnosti za izvajanja kriminalnih dejanj posameznikov kot organiziranega kriminala. Tudi iz tega razloga bo zagotavljanje informacijskih tehnologij za informacijsko varnost pri načrtovanju in odločanju o izvrševanju informacijske varnostne politike še toliko pomembnejše. Prav tako bo področje preprečevanja kibernetskega kriminala in zagotavljanja informacijske varnosti pomemben izziv za pristojne državne organe na tem področju.
Ker v Republiki Sloveniji obstaja organ Slovenski center za posredovanje pri omrežnih incidentih – SI-CERT – bi bilo smiselno razmišljati, da bi nastopal kot center, ki bi skrbel za spremljanje novosti, varnostnih incidentov, razvijanju informacijskih tehnologij in sodelovanje z izobraževalnimi institucijami. Za opravljanje takšne vloge, bi bilo potrebno polno sodelovanje vseh. Sodelovanje bi moralo temeljiti na izoblikovanju varnostne kulture za upravljanje z informacijskimi podatki, kompetencah za vzdrževanje informacijske kulture, varovanje informacijskih podatkov ter zagotavljanje varnosti, evidentiranja in odpravljanja kršitev v postopku varovanja informacijskih podatkov in organizacijski postopki za upravljanje področja varovanja informacijskih postopkov. V pomoč zagotavljanja informacijske varnosti so tudi ljudje oziroma organizacije, ki se ukvarjajo s preverjanjem in odkrivanjem ranljivosti informacijskih sistemov.
Glede pomena informacijske varnosti je osnova zavedanja pomena osveščanje in izobraževanje vseh, na vseh ravneh, z začetkom že v predšolski vzgoji. V osveščanje in izobraževanje bi bilo potrebno vključiti izobraževalne institucije, ki izvajajo izobraževanje na področju informacijske varnosti in informacijskih tehnologij, kakor tudi izobraževalne institucije, ki se ukvarjajo s poučevanjem otrok in odraslih.

6 ZAKLJUČEK

Tempo družbenih, ekonomskih in tehnoloških sprememb zahteva od organizacije takojšnje odzivanje na novodobna tveganja in hitro prilagajanje v procesih odločanja. Uspešno upravljanje s tveganji pri strateškem odločanju zahteva razpolaganje s kakovostnimi in relevantnimi podatki/informacijami pridobljenimi (in kasneje analiziranimi) iz medmrežje in informacijskega oblaka. Z vstopanjem na informacijsko avtocesto pa organizacija neizogibno postaja tudi ranljiva za vdore v informacijski sistem organizacije in odtujitev informacij. Za ustrezno varovanje in odzivanje v primeru varnostnih incidentov, mora zato organizacija imeti jasno izdelane strategije za upravljanje s tveganji informacijske varnosti in ustrezne informacijske tehnologije. Organizacija mora jasno opredeliti ustrezne okvirje, politike in postopke, razumljive vsem v organizaciji. Tako bodo zaposleni razumeli pomen in način upravljanja informacijske varnosti. Ob pravilnem in doslednem izvajanju informacijske varnostne politike se strošek informacijske varnosti in informacijskih tehnologij na koncu izkazuje v dobičku organizacije. Globalizacija na vseh področjih življenja je kriminalno usmerjenim posameznikom in organiziranemu kriminalu prineslo nova znanja in priložnosti za izrabljanje informacijskih tehnologij v namene nezakonitega pridobivanja premoženja. Osveščanje in izobraževanje vseh zaposlenih v organizaciji, ki uporabljajo informacijske tehnologije je med najučinkovitejšimi načini zoperstavljanja informacijskim incidentom. Le osveščeni in izobraženi zaposleni se bodo na področju informacijske varnosti zavedali nevarnosti informacijskih incidentov in pomembnosti izvajanja vseh zaščitnih pravil in ukrepov, da informacijskih varnostnih incidentov v organizaciji ne bo oziroma se bo možnost incidentov zmanjševala.

VIRI

Bernik, I. (2011). S socialnim inženiringom do sto tisoč evrov. (R. Gorjanc, Izpraševalec). Pridobljeno 14. 11. 2011 iz http://www.siol.net/novice/crna_kronika/2011/10/intervju_bernik_kibernetska_kriminaliteta.aspx

Bernik, I. in Meško, G. (2011). Cybercrime: what are we afraid of? V D. Maver, B. Dobovšek in D. Frangež (Ured.), Criminalistics/criminal investigation in Europe: state of the art and challenges fot the future; conference proceedings, Ljubljana, September 22-23, (str. 85–86). Ljubljana: Faculty of Criminal Justice and Security.

Bernik, I. in Prislan, K. (2011). Information Security in Risk Management Systems: Slovenian Perspective. V Varstvoslovje: Journal of Criminal Justice and Security, year 13, no 2 (str. 208–221). Univerza v Mariboru, Fakulteta za varnostne vede, Slovenija.

Čaleta, D., Rančigaj, K. in Lobnikar, B. (2011). The Nature of Security Culture in a Military Organization: a Case Study of the Slovenian Armed Forces. Journal of Criminal Justice and Security, year 13, no. 2 , str. 222–239.

Felson, M. (2006). HEUNI Paper No. 26 The ecosystem for organized crime. Pridobljeno 16. 11. 2011 iz http://www.heuni.fi:http://www.heuni.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=2rreolo2h.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1266335655741&blo

FIPS, P. 2. (9. 3. 2006). Federal Information Processing Standards Publication: Minimum Security Requirements for Federal Information and Information Systems. Pridobljeno 17. 11. 2011 iz http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Gabor, M. (10. 11 2011). Milan Gabor – etični heker. (V. Ciril Kosednar, Izpraševalec) Pridobljeno 14. 11. 2011 iz http://www.siol.net/novice/lokalne_novice/pomurje/2011/11/eticni_heker.aspx

An Introduction To ISO 27001 (ISO27001). Pridobljeno 19. 11. 2011 iz http://www.27000.org/iso-27001.htm

An Introduction to ISO 27001, ISO 27002....ISO 27008. Pridobljeno 19. 11. 2011 iz http://www.27000.org/index.htm

IT Governance, I. (2006). Information Security Governance: Guidance for Board of Directors and Executive Management 2nd Edition. Rolling Meadows, IL, USA: IT Governance Institute.

Lowenthal, M. M. (2009). Intelligence from secret to policy: fourth edition. Washington: CQ Press.

Markelj, B. in Bernik, I. (2011). Informacijska varnost pri povezovanju mobilnih naprav v oblak. Zbornik Elektrotehniške in računalniške konference ERK (str. 39–42). Ljubljana: Slovenska sekcija IEEE, IEEE Region 8 (Tržaška 25).

Nist. (8. 2009). NIST Special Publication 800-53; Recommended Security Controls for Federal Information Systems. Pridobljeno 17. 11. 2011 iz http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

Novak, V. P. (2011). Prispevek standarda ISO 27001 k informacijski varnosti v slovenskih podjetjih. Ljubljana: Univerza v Ljubljani, Ekonomska fakulteta.

Pfeiffer, M., Avila, M., Backfried, G., Pfannerer, N. in Riedler, J. (7. 3. 2008). Next Generation Data Fusion Open Source Intelligence (OSINT) System Based on MPEG7. Pridobljeno 7. 11. 2011 iz http://www.sail-technology.com/fileadmin/user_upload/pdf/9_Data_fusion.pdf

Podbregar, I. (2008). Nekateri elementi obveščevalne dejavnosti. V I. Podbregar, Vohunska dejavnost in gospodarstvo (str. 21–71). Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.

Podbregar, I. in Ivanuša, T. (2010). Javni viri in analitika v obveščevalni dejavnosti. Revija za kriminalistiko in kriminologijo, april–junij, letnik 61, št. 2 , str. 191–198.

Podbregar, I., Mulej, M., Pečan, S., Podbregar, N. in Ivanuša, T. (2010). Informacije kot "bojna" podpora kriznemu odločanju, krizni komunikaciji in delovanju. Ljubljana: Zavod za varnostne strategije pri Univerzi Maribor.

Rogers, S., Lukens, S. in Lin, S. (2008). Balancing Risk and Performance with an Integrated Finance Organization: The Global CFO Study 2008. Pridobljeno 14. 11. 2011 iz http://www-935.ibm.com/services/us/gbs/bus/html/2008cfostudy.html: http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03037usen/GBE03037USEN.PDF

Sayer, P. in Wailgum, T. (17. 4. 2008). What You Can Learn about Risk Management from Societe Generale. Pridobljeno 14. 11. 2011 iz http://www.cio.com/article/336816/What_You_Can_Learn_about_Risk_Management_from_Societe_Generale?page=2&taxonomyId=3089www.cio.com/article/336816/What_You_Can_Learn_about_Risk_Management_from_Societe_Generale?page=2&taxonomyId=3089

Selan, D. (2011). Management informacijske varnosti na strateškem in operativnem nivoju; magistrsko delo. Ljubljana: Univerza v Mariboru, Fakulteta za varnostne vede.

SI-CERT. Slovenian Computer Emergency Response Team. Pridobljeno 19. 11. 2011 iz http://www.cert.si/

Spencer, J., Aromaa, K., Junninen, M., Markina, A., Saar, J., in Viljanen, T. (2006). HEUNI Paper No. 26 Organised crime, corruption and the movement of people across borders in the new enlarged EU: A case study of Estonia, Finland and the UK. Pridobljeno 16 . 11. 2011 iz http://www.heuni.fi/: http://www.heuni.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=b7n54kjbxblg_1.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1266335655 75

Stefan, S., Heise, D., in Ulrich, F. (14. 5. 2010). RiskM: A multi-perspective modeling method for IT. Pridobljeno 14. 11. 2011 iz http://vir.ukm.si/han/ProQuestTelecomunications/www.springerlink.com/content/j52k6071g4164q82/fulltext.pdf

Sun, C. (2007). Umetnost vojne. Ljubljana: Amalietti & Amalietti.

Symplified and Solstice to Collaborate on Mobile Security for Cloud Applications. (2011). Entertainment Close – Up. Jacksonville (4. 11. 2011). Pridobljeno 4. 11. 2011 iz http://vir.ukm.si/han/DissertationsTheses/proquest.umi.com/pqdweb?index=9&did=2502046901&SrchMode=1&sid=2&Fmt=3&VInst=PROD&VType=PQD&ROT=309&VName=PQD&TS=1320429538&clientId=70262

Von Solms, S. H. in Von Solms, R. (2009). Information Security Governance. New York: Springer Science + Business Media, LLC.

Weill, P. in Ross, W. J. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results (Hardcover). Pridobljeno 14. 11 2011 iz http://hbr.org/product/it-governance-how-top-performers-manage-it-decisio/an/2535-HBK-ENG

Zakon o varstvu javnega reda in miru [ZJRM-1]. (2006). Uradni list RS, (70/06).