Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!

Letnik 2013, november • št. 5



5. jubilejna mednarodna konferenca Dnevi korporativne varnosti

Ljubljana, 19. – 20. marec 2014

Nacionalna varnost je temelj za delovanje države

g. Jože Sironič
Svetovalec za nacionalno varnost

5. mednarodna konferenca

Dnevi korporativne varnosti

1. mednarodna konferenca

Informacijska varnost - danes in jutri

Ljubljana, 19.—20. marec 2014

Plaza hotel Ljubljana

ICS

Institute for Corporative Security Studies

Ujemite popust za zgodnjo prijavo!

Vabimo tudi strokovnjake s področja korporativne in informacijske varnosti, da se konference udeležite s svojim prispevkom.

Več informacij o **programu in prijavi** na spletni strani **www.ics-institut.com**

Soorganizator

Zlati sponzor

Medijski sponzorji



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
dr. Denis Čaleta

Namestnik odgovornega urednika:
Andrej Kovačič

Trženje:
ICS-Ljubljana
info@ics-institut.si
Aljoša Kandžič
aljosa.kan@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
Schwarz print d.o.o.

Datum izida
november 2013

Izvod revije je brezplačen

Naslovnica:
Dreamstime

ISSN 2232-6170

Objavljeni prispevki in njihova vsebina odraža mnenja in stališča avtorjev ter predstavljajo v celoti njihovo odgovornost.

Dinamično varnostno okolje nas vseskozi prebuja iz spanca lažne prepričanosti, da živimo v popolnoma varnem okolju, kjer našim organizacijam ne pretijo nobene nevarnosti. Vendar je realnost še kako drugačna. Že pregovorno velja, da se je bolje učiti iz tujih kakor lastnih napak. Smo res sposobni učenja iz tujih napak? Na žalost realnost pokaže, da moramo v večini primerov prehoditi to trnovo pot in se na lastnih napakah učiti tistih izkušenj, ki bi jih lahko prevzeli od drugih. Trenutna kriza je s stališča očiščenja trga lahko dobrodošla priložnost za spremembe, ki jih v času »debelih krav« nismo bili sposobni ali pa jih nismo želeli narediti. Po ekonomski teoriji chicaške šole je taka situacija nekaj povsem vsakdanjega in zagotavlja, da na trgu preživijo samo tisti, ki so svoje poslovanje sposobni prilagoditi v smeri večje učinkovitosti in racionalnejše porabe resursov, brez vmešavanja države. Če to situacijo prenesemo na področje korporativne varnosti in celovitejšega obvladovanja tveganj bi morali biti uporabniki varnostnih storitev dovolj varnostno ozaveščeni, da bi za svoj vložek zahtevali višjo raven kakovosti varnostnih storitev izvajalcev, ki v naših okoljih izvajajo pogodbeno varovanje. Vendar smo poleg države, ki ni sposobna postaviti ustreznih standardov za opravljanje dejavnosti zasebnega varovanja, ravno mi uporabniki oz. naročniki teh varnostnih storitev največji problem, da konkurenčna tekma in razmere na trgu ne prisilijo slabih ponudnikov k propadu. Še več z dampingškimi cenami, ki so jih naročniki pripravljeni plačati, brez, da bi se zavedali kakšno kvaliteto varnosti dobijo za svoj denar, se je na trgu dogodila ironična situacija, ki načenja poslovno kondicijo tistih zasebno varnostnih podjetij, katera vlagajo v razvoj dejavnosti in usposobljenosti svojih zaposlenih. Nadzorne institucije ne opravljajo svoje predvidene vloge, tudi Zbornica za razvoj zasebnega varovanja nima dovolj moči ali interesa, da iz svojih vrst izključi podjetja, ki na trgu nudijo slabo kvaliteto storitev in le to opravljajo za ceno, ki ne zadošča niti za izplačilo minimalne plače zaposlenega varnostnega osebja. Če je to cena, ki jo bomo morali v tej krizi plačati za svoje nizko varnostno zavedanje, potem se je potrebno temu z vsemi silami javno upreti. Ravno v tem prelomnem zgodovinskem trenutku, ima korporativna varnost, kot profesija ključno vlogo, da se tej apatični situaciji upre z vsemi strokovnimi argumenti. Ravno z argumentiranim pristopom, podprtim z dobro prakso mednarodnega okolja in lastnih izkušenj ter seveda znanstvenih spoznanj je potrebno prepričati strateška vodstva organizacij, da se je treba v procesu izbire zunanjih izvajalcev odpovedati najnižji ceni kot edinemu merilu izbire, temveč je potrebno gledati ekonomsko upravičeno ceno storitve tudi in predvsem skozi kvaliteto storitve, ki jo naročnik dobi od izbranega izvajalca. Seveda mora skozi nadzorne institucije, končno svoj del domače naloge opraviti tudi država, ki se je zaradi neznanja in nezainteresiranosti njenih kadrov v nadzornih institucijah, v tem razmerju pojavila kot ena izmed glavnih odgovornih za trenutno stanje. Vendar pa nam napisano jasno pokaže, da smo ravno korporativno varnostni strokovnjaki tisti potencial, ki ob upoštevanju in zagovarjanju strokovnih stališč lahko bistveno pripomoremo k ustrezni ureditvi stanja na področju zagotavljanja varnosti skozi mehanizme najemanja zasebno varnostnih subjektov.

V tokratni številki revije »Korporativna varnost« smo posvetili pozornost različnim temam, ki so posredno in neposredno povezane z zgoraj izpostavljenim dvigovanjem varnostnega zavedanja naročnikov storitev zasebnega varovanja.

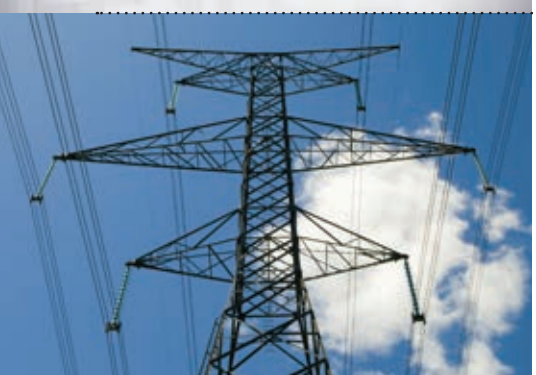
Doc. dr. Denis Čaleta
Glavni urednik



VODSTVENI NADZOR KOT SESTAVNI DEL KORPORATIVNE VARNOSTI

Vodstveni nadzor je sestavni del korporacijskega upravljanja in s tem tudi del korporativne varnosti, kot temelja varnega opravljanja poslovnih procesov.

8



KOLUMNA

PRODAJA DRŽAVNEGA PREMOŽENJA – PASTI IN STRAN POTI DO USPEŠNEGA DELOVANJA NACIONALNE KRITIČNE INFRASTRUKTURE

15



PREDLOGI VLADI REPUBLIKE SLOVENIJE NA PODROČJU NACIONALNE KIBERNETSKE VARNOSTI

Področje kibernetske varnosti v naši državi je vseskozi na zaskrbljujoče nizkem nivoju. Žal odsotnost novega strokovnega kadra s tega področja v javni upravi onemogoča kakršne koli spremembe na bolje.

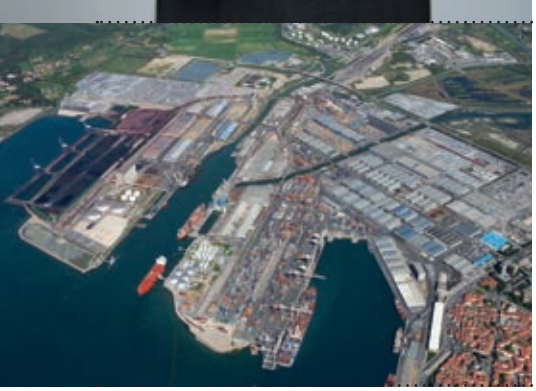
17



NADZOR NAD IZVAJALCI VAROVANJA KOT DEJAVNIK POSLOVNE USPEŠNOSTI NAROČNIKA

Namen prispevka je nakazati nekatere možnosti za izboljšanje varnosti v organizacijah in opozoriti odgovorne, kako pomemben je neodvisni nadzor nad izvajanjem varovanja za poslovno uspešnost organizacije.

27



POMORSKA IN PRISTANIŠKA VARNOST

Pristanišča zaradi svoje kompleksnosti in količine tovora ter potnikov predstavljajo izjemen varnosti izziv, ki pred korporativno varnost postavlja veliko odprtih dilem po učinkovitejšem obvladovanju tveganj.

52

Avtor: Dr. Denis Čaleta / Institut za korporativne varnostne študije*

INTERVJU
g. Jože Sironič
Svetovalec predsednice vlade za nacionalno varnost

NACIONALNA VARNOST JE TEMELJ ZA DELOVANJE DRŽAVE

Vprašanje nacionalne varnosti je za vsako državo zelo občutljivo področje, v katerega so vpeti številni subjekti s svojimi sistemi in podsistemi.

Ali menite, da je Slovenija in njen nacionalno-varnostni sistem ustrezno organiziran za ustrezno preprečevanje asimetričnih groženj, ki jih prinaša dinamično varnostno okolje?

V sodobni družbi se varnosti namenja vse več pozornosti, kajti varnost je sama po sebi vrednota in predpogoj za kakršnokoli blaginjo. Kljub dejstvu, da varnostne politike težko sledijo razvoju novih načinov asimetričnih groženj, med katerimi je terorizem skozi različne pojavne oblike tipičen predstavnik asimetričnega ogrožanja sodobne družbe, smatram, da imamo v Republiki Sloveniji ustrezno organiziran sistem nacionalne varnosti. Zagotavljanje nacionalne varnosti Republike Slovenije temelji na delovanju obrambnega sistema, sistema notranje varnosti ter sistema varstva pred naravnimi in drugimi nesrečami, kot podsistemov sistema nacionalne varnosti, vključuje pa tudi zunanjepolitične, gospodarske, informacijske in druge dejavnosti, ki neposredno vplivajo na nacionalno varnost.

Nacionalno varnostni sistem je sestavljen iz celega spektra procesov in subjektov. Kako bi se po vašem mnenju dalo še dodatno izboljšati na področju koordinacije tega sistema, da bi dosegli večjo učinkovitost?

Zaradi celega spektra procesov in subjektov, ki so vključeni v nacionalno varnostni sistem, je za njegovo učinkovitost nujno dobro sodelovanje vseh akterjev, pravočasna izmenjava informacij in koordinacija delovanja. Zaradi večje učinkovitosti smo celotno koordinacijo delovanja prenesli v Kabinet predsednice vlade, na funkcijo svetovalca za nacionalno varnost, ki preko Sekretariata SNAV operativno usklajuje aktivnosti za delovanje SNAV in skrbi za usklajeno izvedbo stališč SNAV.

Kako vidite nadaljnji razvoj nacionalno-varnostnega sistema v teh zahtevnih gospodarskih in družbenih okoliščinah?

Slovenija se trenutno nahaja v težki, zahtevni gospodarski situaciji in za izhod iz recesije izvaja številne in konkretne ukrepe za uravnoteženje javnih financ. Posledično to vpliva tudi na krčenje proračunskih sredstev in razvoj na vseh področjih delovanja države in njene uprave. Tudi področje nacionalno-varnostnega sistema ni izjema, tako da v trenutnih razmerah o konkretnejših vlaganjih v razvoj sistema ne razmišljamo. Kljub zapletenim gospodarskim razmeram in družbenim okoliščinam sem mnenja, da je Slovenija še vedno varna oaza sredi Evrope.

Svetovalec predsednika vlade za nacionalno varnost ima v večini držav izredno pomembno vlogo pri usklajevanju in koordinaciji aktivnosti na področju nacionalne varnosti. Kakšne so vaše dosedanje izkušnje o vlogi, ki



*avtor je član Slovenskega združenja korporativne varnosti

Za učinkovito zaščito kritične infrastrukture je nujna komunikacija, koordinacija in sodelovanje med vsemi zainteresiranimi stranmi, lastniki in upravljalci, zakonodajno vejo oblasti, strokovnimi telesi in gospodarskimi združenji v sodelovanju z upravnimi ravnmi ter javnostjo.

jo trenutno opravljate pri predsednici Vlade Republike Slovenije?

Vprašanje nacionalne varnosti je za vsako državo zelo občutljivo področje, v katerega so vpeti številni subjekti s svojimi sistemi in podsistemi. Skladno s parlamentarno organiziranostjo državne oblasti v Republiki Sloveniji so v upravljanje in vodenje sistema nacionalne varnosti vključeni organi zakonodajne in izvršilne veje oblasti. Funkcijo svetovalca za nacionalno varnost v Kabinetu predsednice vlade Republike Slovenije sem nastopil pred kratkim, prej pa sem bil preko trideset let zaposlen v Policiji, kjer sem se s tovrstno problematiko profesionalno že srečal. Določeno obdobje sem bil vključen tudi v delo Sekretariata SNAV, kjer sem si nabral pozitivne izkušnje, ki mi pri delu na sedanjem položaju pridejo še kako prav. Pri mojem sedanjem delu gre seveda za bolj široko in kompleksno področje, ki zajema veliko število izmenjav, ocen in vrednotenja informacij, usklajevanja, koordinacije, svetovanja in odločanja.

Kritična infrastruktura je nujna za nemoteno delovanje družbe. Kako ob tej predpostavki organizirati sistem obvladovanja tveganj, ki bo zagotavljal ustrezno varnost za nemoteno delovanje te infrastrukture?

Pojem kritična infrastruktura je relativno nov in je postal aktualen zaradi večjih in odmevnih terorističnih dogodkov. Pred njim se je govorilo zgolj o infrastrukturi. Razlika med njima je predvsem v percepciji ogroženosti posameznika, skupnosti in države kot celote. V preteklosti je bila glavna skrb vodstva usmerjena v razvoj in širjenje proizvodnje, medtem ko v sedanjem času ogroženost izhaja iz terorističnih aktivnosti in drugih oblik asimetričnega ogrožanja sodobne družbe.Tako kot se je pojavila potreba po enotnem definiranju kritične infrastrukture, se je pojavila tudi potreba po metodološkem okvirju za zaščito te infrastrukture. Kljub dejstvu, da je vsak lastnik oziroma upravljalec poskrbel za ustrezno stopnjo zaščite svoje infrastrukture, obstaja nujnost po poenotenju zaščite in ukrepov v primeru različnih vrst ogrožanj. Ob tem je popolnoma razumljivo, da kritične infrastrukture glede na njen obseg in velikost ni možno popolnoma zaščititi. Za učinkovito zaščito kritične infrastrukture je nujna komunikacija, koordinacija in sodelovanje med vsemi zainteresiranimi stranmi, lastniki in upravljalci, zakonodajno vejo oblasti, strokovnimi telesi in gospodarskimi združenji v sodelovanju z upravnimi ravnmi ter javnostjo. Pomembno vlogo na področju kritične infrastrukture ima tudi upravljanje s tveganjem, ki ga sestavljajo potrebni ukrepi za zaščito, ki izhajajo iz načrtov za zmanjšanje tveganja oziroma iz načrtov za čim prejšnjo odpravo posledic.



Vedno višji odstotek upravljalcev kritične infrastrukture prihaja iz zasebnega sektorja. Družbeno stanje na področju dojemanja varnosti v Sloveniji ni na ustreznem nivoju. Kako to varnostno kulturo in zavedanje tako pri posameznikih kakor tudi pri vodilnih strukturah organizacij javnega in zasebnega okolja dvigniti na višji ustreznejši nivo?

Razvoj in uporaba novih tehnoloških sredstev, informacijska družba, gospodarska in finančna soodvisnost v svetu postavljajo lokalne, nacionalne in regionalne skupnosti stalno pred nove izzive in zahtevajo iskanje družbenih dogovorov. Pri tem pa je zelo pomembno sodelovanje vseh akterjev. To velja tudi za področje varnosti, saj je varnost ena izmed temeljnih dobrin družbe. Upoštevaje dejstvo, da je večina kritične infrastrukture v zasebnem lastništvu oziroma upravljanju, je nujno poleg javnega sektorja v to vključiti tudi zasebni sektor. Nesporno je, da je sodobno poslovno okolje izpostavljeno več varnostnim tveganjem, kot se zdi na prvi pogled. Ob tem, posebej pa še v kriznih časih, pogosto pozabljamo na važnost dojemanja varnosti in njenega neprekinjenega izvajanja oziroma delovanja, zaradi česar je varnost zagotovljena zgolj z nekaterimi osnovnimi in najenostavnejšimi ukrepi. Posebej nevarno pa je, če do takšnega stanja prihaja na področju upravljanja s kritično infrastrukturo, kjer so posledice v primeru ogrožanj še toliko hujše. Ob tem gre za nivo dojemanja varnosti oziroma varnostno kulturo, ki

mora pri posameznikih kakor tudi pri vodilnih strukturah organizacij zasebnega in javnega sektorja prevladati nad zgolj finančnimi vidiki in dobičkonosnostjo poslovanja. Pri tem velja opozoriti oziroma izpostaviti pomen korporativne varnosti v organizacijah, ki upravljajo kritično infrastrukturo. Po mojih informacijah se tega pomena premalo zavedajo, čeprav je to ena od možnih variant za dvig varnostne kulture.

Ali lahko govorimo o učinkovitih procesih javno-zasebnega partnerstva na področju varovanja kritične infrastrukture, kot tisti pilotski projekt, ki lahko prinese ustrezne odgovore na tveganja in grožnje, ki jih prinaša dinamično varnostno okolje?

V zadnjem obdobju so vse bolj prisotni in tudi uspešni procesi oziroma projekti javno-zasebnega partnerstva, ki bi bili nedvomno lahko učinkoviti tudi na področju varovanja kritične infrastrukture. S prilagoditvijo pilotskega projekta potrebam dinamičnega varnostnega okolja bi v okviru izvedbe projekta nedvomno lahko poiskali del odgovorov na tveganja in grožnje, ki se pojavljajo v tem okolju.

Razvoj in odvisnost od informacijske tehnologije postavlja kibernetske grožnje v posebno perspektivo. Kateri so po vašem mnenju tisti koraki, ki jih lahko storijo manjše države kot je Slovenija za učinkovito zavarovanje pred temi kompleksnimi grožnjami?

Internet je v komunikacijskem in informacijskem smislu omogočil proces globalizacije in s tem postal glavna infrastruktura, na kateri temelji današnja civilizacija. V tej infrastrukturi za napad ni potrebno tvegati življenj, izvesti pa se ga da na različne načine. Problematika računalniške kriminalitete je v porastu v Sloveniji in v Evropi. Za uspešen boj na tem področju je bistvenega pomena dobro multidisciplinarno ali multiinstitucionalno sodelovanje med različnimi deležniki, ki so zadolženi za preprečevanje, odkrivanje in preiskovanje tovrstne problematike. Za zagotavljanje varnosti je pomembna tudi ustrezna zaščita informacijskih sistemov, poleg tega pa tudi sodelovanje z zasebnim sektorjem in drugimi akterji, ki zaznavajo tovrstno problematiko. Pomembno je tudi samozaščitno ravnanje in obveščanje uporabnikov o varnosti na spletu.

Menite, da lahko znanstveno raziskovalna spoznanja ob njihovem ustreznem prenosu v prakso doprinesejo k kvalitetnejšim rešitvam upravljanja nacionalno-varnostnega sistema?



Posebej nevarno pa je, če do takšnega stanja prihaja na področju upravljanja s kritično infrastrukturo, kjer so posledice v primeru ogrožanj še toliko hujše. Ob tem gre za nivo dojemanja varnosti oziroma varnostno kulturo, ki mora pri posameznikih kakor tudi pri vodilnih strukturah organizacij zasebnega in javnega sektorja prevladati nad zgolj finančnimi vidiki in dobičkonosnostjo poslovanja.

Nacionalno-varnostni sistem Republike Slovenije temelji na političnih, pravnih, gospodarskih, socialno-zdravstvenih, informacijskih, infrastrukturnih, znanstveno-tehnoloških, izobraževalnih in drugih temeljih ter zmogljivostih države. V okviru tako široko utemeljenega koncepta nacionalne varnosti so za njegovo kvalitetno in uspešno upravljanje dobrodošla tudi znanstveno raziskovalna spoznanja.

Strokovna združenja imajo pomembno mesto pri zagotavljanju uveljavljanja posamezne stroke. Menite, da lahko Slovensko združenje korporativne varnosti prinese dodatno kvaliteto pri povezovanju korporativne varnosti v okolje nacionalno-varnostnega sistema?

Podobno velja tudi za strokovna združenja, ki se ukvarjajo z uveljavljanjem posamezne stroke. Naj na koncu še enkrat ponovim, da je za iskanje novih družbenih dogovorov ključno sodelovanje vseh akterjev. ■

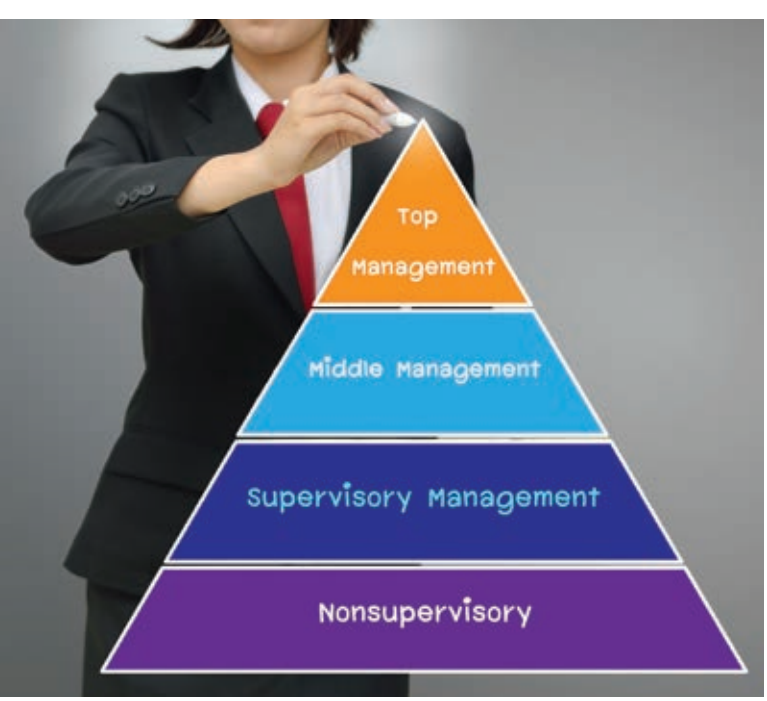
Avtor: Dr. Brane Bertoncelj / Banka Slovenije



VODSTVENI NADZOR KOT SESTAVNI DEL KORPORATIVNE VARNOSTI

Vodstveni nadzor je sestavni del korporacijskega upravljanja in s tem tudi del korporativne varnosti, kot temelja varnega opravljanja poslovnih procesov.

Nedavni škodni dogodki in finančni škandali so vplivali na zaupanje v poštenost poslovnih izkazov organizacij. Manjše število škodnih dogodkov lahko pripišemo poslovnim prevaram in drugim kaznivim dejanjem, večje število pa je bilo, po mojem mnenju, posledica neuspeha poslovodstva v razumevanju dogajanja na trgu in v organizaciji, ki jo vodijo. Menim, da si je preveč organizacij dovolilo preveč presenečenj, tudi zaradi pomanjkljivega vodstvenega nadzora in slabega delovanja sistema notranjih kontrol. Ob tem se postavlja vrsta aktualnih vprašanj, npr.: (1) ali so poslovni procesi v organizaciji transparentni in ustrezno dokumentirani? (2) kakšna je izpostavljenost organizacije raznim vrstam tveganj? (3) ali ima organizacija vzpostavljene ustrezne preventivne in korektivne ukrepe v poslovnih procesih? (4) kako se ocenjuje razmerje med obsegom škodnih dogodkov in višino stroškov varnostnega sistema, zunanjih revizorjev ter notranje kontrole?



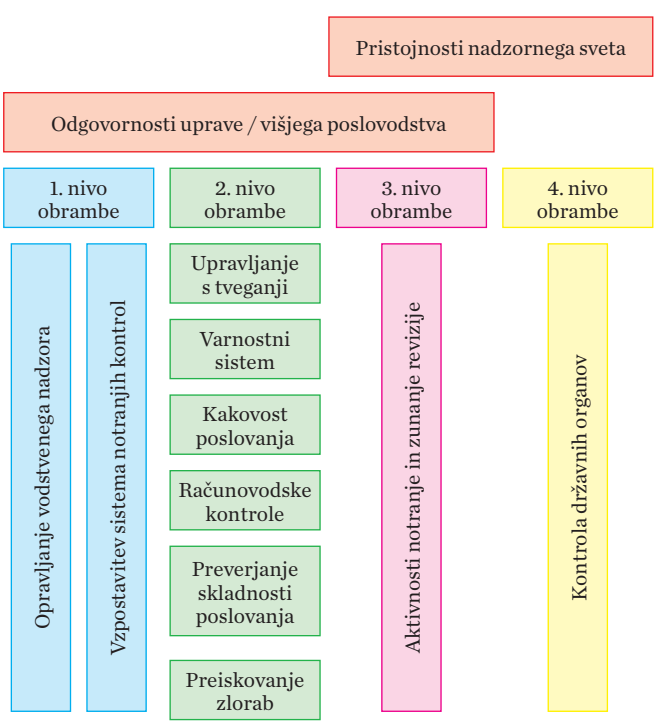
> Vodja ni plačan za to, da »ugaja« podrejenim, ampak, da ustrezno organizira in vodi delo.

Ključni dejavnik, ki v organizaciji odloča, ali se bo tehtnica uspeha poslovanja nagnila k reaktivni pasivnosti ali k proaktivnim dejanjem, je poslovodenje. Tradicionalno pojmujejo poslovodenje kot načrtovanje, usmerjanje in nadzor podrejenih. Sodobna pojmovanja pa vključujejo tudi spodbujanje, mentorstvo, motiviranje in ustvarjanje pozitivnih čustev. Poslovodja se spreminja v vodjo, ki je simbol organizacije, tudi njenega uspeha ali neuspeha. Ta simbolična vloga izhaja iz prepričanja in zahtev poslovanja, da lahko ob okoljskem determinizmu tudi sam pomembno vpliva na dogajanje v organizaciji. Vodja ni plačan za to, da »ugaja« podrejenim, ampak, da ustrezno organizira in vodi delo. Na drugi strani pa je lahko tudi ustrezna tarča za zunanje pritiske (Pfeffer in Salancik, 2003). To seveda ne pomeni, da dober vodja sebi in svojim zaposlenim »natika rožnata očala«, da se vedno smehlja in da se izogiba problemom s ponavljanjem mantre o »pozitivnem mišljenju«. Dober vodja se zna soočiti s tekočimi problemi tako, da pozornost preusmeri od »zaletavanja in ujetosti« v problem proti njegovim možnim rešitvam (Musek, 2006). Vodja ni zgolj »lovec zabušantov«, po Kovaču et al. (2004) so namreč naloge vodje zlasti načrtovanje lastnega dela in zaposlenih, nadziranje, obveščanje in sporazumevanje.

Vodstveni ali managerski nadzor je skupek planiranja in nadziranja opravil (Anthony, 1965). Anthony in Govindarajan (2003) ga razširita v proces, preko katerega vodstvo vpliva na obnašanje zaposlenih organizacije, s ciljem udejanjiti želeno strategijo poslovanja. Skozi čas so se pojavile različne kritike tradicionalnega modela vodstvenega nadzora, saj ta zanemarja dinamične povezave, motiviranost zaposlenih, premalo upošteva dinamično poslovno okolje, kulturo organizacije, inovativnost in mnogo drugih nefinančnih (»mehkih«) dejavnikov uspešnosti. Avtorji so zato sčasoma raz-

širjali tradicionalni vidik vodstvenega nadzora s sociološko - psihološkimi vidiki; vlogo in pomenom okolja, v katerem organizacija posluje, njeno organizacijsko kulturo, kompetentnostjo zaposlenih ipd.

Vodstveni nadzor je sestavni del korporacijskega upravljanja in s tem tudi del korporativne varnosti, kot temelja varnega opravljanja poslovnih procesov. Učinkovit vodstveni nadzor in dobro postavljen sistem notranjih kontrol lahko bistveno pripomoreta k doseganju strateških usmeritev ter planiranih ciljev poslovanja, poleg tega pa zagotavljata poslovanje v skladu s pozitivno zakonodajo, internimi akti in dobro prakso. S tem se zlasti zmanjšujeta dve pomembni tveganji: finančna izguba in zmanjšanje ugleda organizacije. Vodstveni nadzor zagotavlja upravi in nadzornemu svetu, da so tveganja obvladovana in da je korporacijsko upravljanje uspešno ter učinkovito. Sodobna ureditev sistema nadzora ima vsaj štiri »nivoje obrambe« (glej spodnjo sliko). Prvi nivo obrambe predstavljata opravljanje vodstvenega nadzora in sistem notranjih kontrol; drugi nivo obrambe se nanaša na upravljanje s tveganji, delovanje varnostnega sistema, preverjanje kakovosti poslovanja in računovodske kontrole, preverjanje skladnosti poslovanja (compliance) in preiskovanje zlorab; tretji nivo je povezan z aktivnostmi notranje kontrole in zunanjega revizorja; četrti nivo obrambe pa se nanaša na kontrolo pristojnih državnih organov.



Slika: *Sodobna ureditev nadzora*
Vir: prirejeno po SIR (Slovenski inštitut za revizijo)

Vodstveni nadzor je najvišja raven nadzora organizacije. Nanaša se na razumevanje tveganj, ki jih organizacija prevzema, na skrb, da vodstvo sprejema ustrezne ukrepe in na postopke ter aktivnosti za merjenje, spremljanje in kontroliranje teh tveganj. Izhodišča za vodstveni nadzor so:

- pozornost mora biti namenjena le pomembnim ciljem, nalogam in večjim problemom poslovanja,
- največ pozornosti naj bo namenjeno zlasti tistim ciljem, od katerih je odvisno uspešno upravljanje finančnih tveganj in tveganje zmanjšanja ugleda,

Učinkovit vodstveni nadzor in dobro postavljen sistem notranjih kontrol lahko bistveno pripomoreta k doseganju strateških usmeritev ter planiranih ciljev poslovanja, poleg tega pa zagotavljata poslovanje v skladu s pozitivno zakonodajo, internimi akti in dobro prakso.

- vpeljati je potrebno take metode vodstvenega nadzora, ki ne zahtevajo veliko časa, a so kljub temu proaktivne in učinkovite,
- zagotoviti je potrebno učinkovit pretok informacij med vsemi pomembnejšimi sodelavci in
- pomembna je izbira sodelavcev, ki so za delo kompetentni, usposobljeni in motivirani.

Notranji kontrolni sistem je definiran kot dobro delujoč sistem organizacijskih in operativnih kontrol. Sistematično ima vgrajene postopke in metode, ki jih vzpostavi vodstvo, da bi se: (1) pravilno in uspešno opravljali poslovni procesi, (2) zagotovila gospodarna raba sredstev,(3) varovalo premoženje organizacije, (4) zagotovila točnost in zanesljivost evidenc, (5) izdelovali resnični računovodski izkazi in (6) preprečevalo in odkrivalo napake ter prevare v poslovanju.

Obseg teh kontrol je na eni strani odvisen od velikosti organizacije, narave in raznolikosti poslovnih procesov, tveganosti posameznih področij poslovanja, centraliziranosti poslovanja in delegiranja pooblastil, na drugi strani pa od učinkovitosti varnostnega sistema in informacijskega sistema, ki podpirata navedeno poslovanje.

Vodstvo organizacije mora uveljaviti visoka merila etičnosti, morale, lojalnosti in organizacijske zavesti, ki poudarjajo pomen vodstvenega nadzora in notranjih kontrol. Skrbeti mora za primerno ločenost dolžnosti in da zaposleni ne dobivajo nalog z nasprotujočimi se odgovornostmi. Ugotavljati mora kje bi lahko prihajalo do navzkrižja interesov in takšna področja čim bolj zmanjšati ter jih skrbno spremljati. Vsi zaposleni morajo razumeti svojo vlogo v notranjih kontrolnih postopkih in v njih tudi aktivno sodelovati.

Pomembnejša področja vodstvenega nadzora so zlasti: organizacija, politike, postopki, zaposleni, planiranje in poročanje. Na kratko so pojasnjena v nadaljevanju.

1. Organizacija

Struktura vlog, ki so dodeljene zaposlenim, mora zlasti zagotavljati, (1) da so odgovornosti razdeljene na način, da nihče od zaposlenih ne kontrolira vseh faz posla (upoštevati je potrebno tristopenjski princip: pripravil, kontroliral, odobril), (2) da ima vsak vodja organizacijskega dela pristojnost za zmanjšanje ali odvzem pooblastil podrejenim, (3) da je odgovornost zaposlenih vedno jasno določena, da ne bi prišlo do odstopanj ali prekoračitev, (4) da zaposleni, kateremu je bila dodeljena neka odgovornost, realizira naloge brez stalnega neposrednega nadzora, vsaka izjema pa zahteva preveritev pri vodji organizacijskega dela.

2. Politike

Politika je vsako pravilo, ki vodi ali omejuje poslovanje. Politike morajo biti (1) jasno zapisane v obliki poslovnika vodenja kakovosti, pravilnikov, delovnih navodil, zapisov ipd., (2) skladne s pozitivno zakonodajo in konsistentne s strategijo poslovanja organizacije, (3) oblikovane na način, da spodbujajo učinkovito in gospodarno opravljanje poslovnih procesov.

3. Postopki

Postopki so metode za izvedbo aktivnosti v skladu s predpisano politiko. Poleg zahtev iz zgoraj navedene točke je za postopke potrebno (1) da se izvajajo tako, da delo vsakega zaposlenega avtomatično nadzoruje drugi, ko izvaja svoje zadolžitve, kar se izmenjuje in ponavlja, (2) upoštevati, da sta obseg in intenzivnost avtomatičnih kontrol odvisna od stopnje tveganosti in primerjave med stroški ter koristmi, (3) upoštevati, da za neavtomatično delo postopki ne smejo biti tako podrobni in natančni, saj mora obstajati tudi možnost lastne presoje, (4) da so preprosti, kot je le mogoče, ob upoštevanju učinkovitosti in ekonomičnosti, (5) da niso dvomljivi ali nerazumljivi.

4. Zaposleni

Zaposleni morajo biti za delo, ki jim je dodeljeno, ustrezno usposobljeni, motivirani in nadzorovani. Zato je potrebno (1) stalno izobraževanje zaposlenih, tako da ostajajo v profesionalni formi, (2) informirati zaposlene o delu in odgovornosti ostalih, saj to omogoča boljše razumevanje lastnih zadolžitev, (3) spremljanje in občasno preverjanje poslovanja zaposlenih.

5. Planiranje

Planiranje poslovnih aktivnosti se nanaša na pričakovane rezultate poslovanja z upoštevanjem določenih predpostavk. Pri tem je potrebno upoštevati, da zaposleni, ki je odgovoren za doseganje postavljenih ciljev, tudi sodeluje pri pripravi planov aktivnosti.

6. Poročanje

Vodstvo praviloma sprejema odločitve na temelju prejetih poročil. Poročanje mora biti pravočasno, vsebinsko, natančno in ekonomično. Zato je potrebno, da (1) so stroški poročanja manjši od koristi, pridobljenih z uporabo poročil, (2) so poročila enostavna, kot je le mogoče, (3) poročila praviloma vsebujejo primerjave.

Zaključek

Celostni vidik sistema vodstvenega nadzora se je razvil kot odgovor na pomanjkljivosti tradicionalnega modela in pomeni njegovo razširitev. Sistem vodstvenega nadzora kombinira normativno obravnavanje vodstva in njegove aktivnosti na področju nadzora (vključuje cilje, ki jih je potrebno doseči in poti do njih). Učinkovit vodstveni nadzor kot del upravljanja in kot del korporativne varnosti za organizacijo predstavlja tiste aktivnosti, ki se lahko prevesijo v uspeh ali neuspeh poslovanja. Več o tej temi bom predstavil na mednarodni konferenci ICS o korporativni varnosti v letu 2014. ■



Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Dr. Iztok Podbregar
Član uprave Aerodrom Ljubljana d.d.

PRENOS ZNANSTVENIH SPOZNANJ V PRAKSO KOT POMEMBNA PARADIGMA BOLJ UČINKOVITEGA OBVLADOVANJA TVEGANJ

Uravnoteženost razmerja pri uvajanju procesov javno-zasebnega partnerstva na področju zaščite kritične infrastrukture je lahko odgovor na dinamično varnostno okolje.

Kakšno je po vaši oceni delovanje nacionalno-varnostnega sistema v Republiki Sloveniji in predvsem ali je le ta sposoben ustreznega odzivanja na tveganja in grožnje, ki jih prinaša dinamično in nestabilno varnostno okolje?

Nacionalno varnostni sistem v ožjem smislu, tj. predvsem tisti del, ki ga bolj neposredno usmerja Vlada Republike Slovenije, se na grožnje nacionalne varnosti odziva relativno dobro. Posamezni subjekti imajo zakonsko določene pristojnosti, ki jih tudi izvajajo. Problem nastane pri novodobnih grožnjah nacionalne varnosti, kjer se posamezen subjekt nacionalne varnosti takoj ne vidi kot lastnik problema, temveč je grožnja nekje med pristojnostmi dveh ali več subjektov nacionalne varnosti. Takrat je potrebna koordinacija na operativni ravni, kjer se določijo nosilci in sodelujoči pri reševanju posameznega problema. Takšna koordinacija zahteva svoj čas, kar pa je pri nekaterih grožnjah lahko usodno, te lahko medtem prerastejo tudi že v resne krize. Menim, da bo v prihodnosti potrebno nacionalno varnostni sistem prenoviti, verjetno v smeri, da se subjekti nacionalne varnosti, npr. vojska, policija ter zaščita in reševanje, procesno in praktično še bolj tesno povežejo in postanejo še bolj interdisciplinarni. Potrebno bo tudi bolje opredeliti razmerje med poklicnostjo, prostovoljnostjo in profesionalnostjo v sistemu nacionalne varnosti, kjer je problem, ko se v reševanje posameznih groženj vključi tudi ostale subjekte nacionalne varnosti, npr. prostovoljna društva oz. nevladne organizacije.

Ste eden izredno redkih primerov slovenske prakse, ki trenutno deluje na področju korporativne varnosti in ima predhodne izkušnje na najvišjih položajih različnih subjektov nacionalno varnostnega sistema, imate pa neposredne izkušnje tudi iz akademskega področja, kjer ste redni profesor in ste se v svojih raziskavah in proučevanjih neposredno dotikali varnostnih pojavov. Nam lahko zaupate, kako vam te bogate izkušnje pomagajo pri delovanju na trenutnem področju korporativne varnosti?

Družba Aerodrom Ljubljana, d. d., v kateri zasedam mesto člana uprave, je upravljavec mnogih procesov v letališkem mestu, če se lahko tako izrazim. Delo, ki ga opravljam, zahteva interdisciplinarna znanja na strateški in operativni ravni. Moje izkušnje iz letalstva, vodenja kompleksnih sistemov, kot je npr. Slovenska vojska, in večletne izkušnje iz usmerjanja Sveta za nacionalno varnost Republike Slovenije so potrebna podlaga za mojo vlogo v tej družbi. K zadostnosti mojega dela pa brez dvoma prispeva tudi dolgoletno znanstveno in

*avtor je član Slovenskega združenja korporativne varnosti



pedagoško delo na področju varnosti in kriznega menedžmenta na Univerzi, kjer sem s strani radovednih tujih in domačih študentov enostavno motiviran v iskanje vedno novih odgovorov na varnostne probleme. Moja vloga v Aerodromu Ljubljana zahteva sposobnost povezovanja teorije s praktičnimi problemi, kjer so mi nedvomno v pomoč bogate izkušnje.

V Sloveniji se osebe, ki so zadolžene za strateško načrtovanje in izvajanje procesa korporativne varnosti zelo redko nahajajo na prvem nivoju odločanja oz. v njegovi bližini. Primerljiva praksa v mednarodnem okolju pa se kaže ravno v smeri te potrebe saj je zaradi dinamičnosti varnostnega okolja vedno težje zagotavljati ustrezen celovit pristop do obvladovanja tveganj za organizacijo. Menite, da bo to počasi postala praksa tudi v slovenskem prostoru?

Upam, da se bo takšna praksa prenesla tudi v slovenski prostor, saj bo to pomembno prispevalo k zagotavljanju pravih odgovorov v realnem času in reševanju problemov, ki se vsakodnevno postavljajo pred posamezne subjekte. Možnost, da povežem akademsko znanje in izkušnje z zelo izpostavljenim mestom v gospodarstvu, mi predstavlja poseben izziv. Menim, da je večje povezovanje teh dveh vej nujno za hitrejše izhode podjetij iz kriznih stanj. Akumulirano akademsko znanje in s tem povezane analize posameznih problemov v gospodarstvu, ki obstajajo z neke varne akademske distance, morajo sobivati s prakso, saj odločevalci v gospodarski družbi le tako lahko ustvarijo potrebno dodano vrednost. Ocenjujem, da varnostna funkcija postopoma, vsaj v nekaterih večjih slovenskih gospodarskih družbah, že pridobiva pravo mesto med ostalimi poslovnimi funkcijami.

Akumulirano akademsko znanje in s tem povezane analize posameznih problemov v gospodarstvu, ki obstajajo z neke varne akademske distance, morajo sobivati s prakso, saj odločevalci v gospodarski družbi le tako lahko ustvarijo potrebno dodano vrednost.

Aerodrom Ljubljana vsekakor sodi v okvir kritične infrastrukture. Kateri so tisti sistemski ukrepi, ki jih nameravate izvesti za ustrezno varovanje nemotenega delovanja te letališke infrastrukture?

Upravljanje kritične infrastrukture v osnovi urejajo že nekateri standardi in uredbe kritične infrastrukture v EU. V nekaterih gospodarskih subjektih, ki predstavljajo kritično infrastrukturo v Sloveniji, je infrastruktura razdeljena med nosilcem infrastrukture državnega in lokalnega pomena ter upravljalcem oziroma uporabnikom te infrastrukture. Družba Aerodrom Ljubljana, d. d., ima enotno strukturo, ta torej ni razdeljena, z vidika kritične infrastrukture delitev tudi ni potrebna, ne glede na lastništvo družbe. Vsekakor pa mora država z različnimi predpisi zagotoviti nemoteno delovanje letališča v vsaki situaciji. Bojim se, da je zavedanje v posameznih resorjih glede graditve takšnega pristopa še zelo raznoliko in se to stanje sistemsko morda prepočasi izboljšuje. Naloga uprave družbe Aerodrom Ljubljana je opozarjanje vseh nosilcev omenjenih odgovornosti v javni upravi k iskanju rešitev za zagotavljanje največje varnosti pri oskrbi potnikov letališča in tovora ter nemotenega razvoja in rasti družbe.

Menite, da država s svojimi pristojnimi organi dovolj upošteva realno stanje in potrebe upravljalcev kritične infrastrukture ali gre zakonska regulativa v smeri predpisovanja nečesa, kar je v praksi nemogoče zagotavljati?

Menim, da je zavedanje problematike še na dokaj raznoliki ravni in je morda iskanje ustreznih rešitev prepočasno, togo in birokratsko. Res pa je, da gre za procese, v katerih se vsi skupaj neprestano učimo in iščemo najboljše rešitve.

Kakšen je vaš pogled na procese javno-zasebnega partnerstva pri zagotavljanju določenih procesov varovanja kritične infrastrukture? Lahko v Sloveniji sploh govorimo, da smo pravilno razumeli izzive in dileme, ki jih prinašajo ti procesi?



Prepričan sem, da je klasična državna uprava bistveno predraga tudi na področju upravljanja kritične infrastrukture. Brez dvoma je rešitev, ali pa ena od rešitev, v javno zasebnem partnerstvu. Vendar javno zasebno partnerstvo mora biti uravnoteženo kar se tiče pristojnosti in odgovornosti vseh partnerjev in nikakor ne sme biti pri zasebnikih naravnano samo v doseganje finančnih dodanih vrednosti. Vsebovati mora torej elemente socialnega podjetništva. Zato je tudi nujno jasno razmejiti poklicnost, profesionalnost in prostovoljnost pred drugimi odločitvami.

Brez dvoma je rešitev, ali pa ena od rešitev, v javno zasebnem partnerstvu. Vendar javno zasebno partnerstvo mora biti uravnoteženo kar se tiče pristojnosti in odgovornosti vseh partnerjev in nikakor ne sme biti pri zasebnikih naravnano samo v doseganje finančnih dodanih vrednosti.

Za razvoj novih pristopov je nujno potrebno tudi znanstveno-raziskovalno delo, ki je usmerjeno v kasnejšo implementacijo teh spoznanj v neposredno okolje. Boste v upravi družbe pristopili k intenzivnejšemu povezovanju z znanstveno-raziskovalnimi organizacijami pri skupnem nastopanju na mednarodnih projektih, ki bi lahko prinesli nujno potrebna finančna sredstev za razvoj varnostnih procesov in produktov varovanja kritične infrastrukture?

Izjemno sem vesel, da moje novo delovno okolje že dalj časa deluje tako, da v okviru projektov povezuje teoretična, znanstveno raziskovalna spoznanja s prakso. S tem bomo tudi nadaljevali, vendar v okviru zmožnosti in potreb, ki jih moramo obvladovati.

V Sloveniji aktivno deluje Slovensko združenje korporativne varnosti, ki predstavlja visoko strokovno združenje v okviru katerega so med drugimi zbrani skoraj vsi najpomembnejši upravljalci kritične infrastrukture. Menite, da je prišel čas za vključitev Aerodroma Ljubljana v okvir take oblike združevanja, ki omogoča izmenjavo izkušenj in dobrih praks ter predvsem skupno in transparentnejše nastopanje pri zagotavljanju skupnih interesov na področju korporativne varnosti?

Vaša pobuda in spoznanje v zvezi z vključevanjem družbe v širše okolje korporativne varnosti si zasluži resno obravnavo in prepričan sem, da jo bomo v družbi korektno opravili. ■

Slovenian Grand Security Award 2013



Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikov za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti.

Neodvisna komisija ocenjuje in izbira kvaliteto in izvirnost prijavljenih udeležence v naslednjih kategorijah:

Najbolj varno mesto
Najbolj varno podjetje
Zasebno-varnostna služba leta
Korporativno varnostni manager leta
Najboljša knjiga s področja varnosti
Inovativna medijska promocija varnosti.

www.ics-institut.si

Avtor: Doc. dr. Denis Čaleta / Institut za korporativne varnostne študije-ICS, Ljubljana*



KOLUMNA
denis.caleta@ics-institut.si

PRODAJA DRŽAVNEGA PREMOŽENJA – PASTI IN STRAN POTI DO USPEŠNEGA DELOVANJA NACIONALNE KRITIČNE INFRASTRUKTURE

Finančno in gospodarsko stanje Slovenije sili Vlado Republike Slovenije v prodajo določenega dela državnega premoženja, katerega obseg je pred kratkim potrdil tudi Državni zbor. Ne smemo pa pozabiti, da določen del podjetij, ki so predvideni za prodajo, sodi v tako imenovano nacionalno kritično infrastrukturo, ki je zaradi svoje pomembnosti in neprekinjenosti delovanja nujno potrebna za nemoteno delovanje družbene skupnosti. V okviru tega nabora podjetij velja posebej izpostaviti Aerodrom Ljubljana in Telekom Slovenije, Cinkarno Celje pa zaradi posrednih učinkov, ki bi jih lahko imelo njeno slabo upravljanje na širše življenjsko okolje. Praktično si je nemogoče zamišljati, da bo celotna informacijska hrbtenica Telekoma d.d. na kateri je temeljila svoj razvoj celotna državna uprava, prenešena brez ustreznih zavez na novega lastnika ali pa, da bo na območju Aerodroma zasebnik brez posluha za probleme države odločal o razvoju glavne zračne luke za Slovenijo in o možnostih pristajanja vojaških, policijskih in drugih državnih zrakoplovov.

Ta dejstva pa proces priprav v določenem delu skrbniškega pregleda in priprave ustreznih podlag, zavez in zahtev postavi v drugačno, bolj zahtevno situacijo. Postavlja pa se ključno vprašanje ali se odgovorni v tej državi sploh zavedajo pomembnosti tega problema in ali je državna administracija s svojim kadrovskim potencialom sploh sposobna pripravtiti ustrezne podlage, ki bodo zagotovile, da bo kljub spremembi lastništva v teh podjetjih, kritična infrastruktura še naprej neprekinjeno delovala brez večjih posledic za normalno funkcioniranje širše družbene skupnosti.

Samo ustrezna priprava in upoštevanje vseh potrebnih dejavnikov bo omogočilo učinkovito in uspešno prodajo. Potrebno je namreč pripraviti vse potrebne podlage in zahteve, ki bodo umeščene v razpisno dokumentacijo, na podlagi katere se bo kasneje kupec zavezal, da bo tiste dele kupljenih podjetij, ki so pomembni s stališča kritične infrastrukture, vodil in razvijal v tej smeri, da bo zagotavljal neprekinjenost delovanja tiste infrastrukture, ki jo v Sloveniji nujno potrebujemo za svoje delovanje. V tem procesu prenosa lastništva iz javnega na zasebni subjekt, bo potrebno še posebej na področju delovanja kritične infrastrukture, posvetiti pozornost vzpostavitvi ustreznega javno-zasebnega razmerja, ki bo zagotovilo neprekinjenost delovanja te infrastrukture. Privatni lastniki v večini primerov zasledujejo samo finančni vidik svoje naložbe. Vsi ostali vidiki, ki so ključni za državo in s tem širšo družbeno skupnost, pa so potisnjeni v ozadje. S tega stališča se mora Republika Slovenija, skozi zelo jasno podpisane zaveze novega lastnika teh infrastrukturnih zmogljivosti zavarovati, da bo kritična infrastruktura delovala nemoteno in bo zagotavljala neprekinjenost tistih procesov in dejavnosti, ki so ključni za našo družbo.

Na primer na Nizozemskem, kjer se skoraj 80% te infrastrukture nahaja v zasebnih rokah, je javno-zasebno partnerstvo v celoti zaživelo.

*avtor je član Slovenskega združenja korporativne varnosti

Če bomo zamudili vlak in omenjena podjetja prodali brez priprave ustreznih podlag in pogojev, poti nazaj na žalost ne bo več.

V tujini poznamo različne prakse glede obsega nacionalne kritične infrastrukture, ki se nahaja v lastništvu ali upravljanju zasebnih lastnikov. Na primer na Nizozemskem, kjer se skoraj 80% te infrastrukture nahaja v zasebnih rokah, je javno-zasebno partnerstvo v celoti zaživelo. Vsi deležniki v tem razmerju se zavedajo pomembnosti neprekinjenega delovanja te infrastrukture. Tako na eni strani država zaradi posledic, ki bi jih lahko občutila družba, na drugi strani pa lastnik, ki mu neprekinjenost delovanja zagotavlja ustrezen prihodek za uspešno delovanje organizacije. Vendar v naši družbi to zavedanje in vzpostavitev teh razmerij ni mogoča čez noč saj kultura dialoga in sodelovanja ni na ustreznem nivoju. Država namreč s svojo okorelo birokracijo nima posluha za dinamični poslovni razvoj, ki ga potrebujejo lastniki podjetij, tuji lastniki podjetij pa se v večini primerov do svojih naložb v državah v tranziciji obnašajo relativno nesistemsko saj v večini primerov črpajo dobiček in ga prenašajo na matično podjetje v tujini, brez bistvenih vložkov v razvoj teh podjetij. Če to gledamo s stališča razvoja kritične infrastrukture je to lahko še bolj problemtično.

Institut za korporativne varnostne študije, ICS-Ljubljana in Slovensko združenje korporativne varnosti, ki v svojem okviru obsega skoraj vse slovenske organizacije, ki obvladujejo kritično infrastrukturo sta praktično edini organizaciji v širšem regijskem okolju, ki v tem primeru lahko s svojim ekspertnim znanjem znanstvenikov in strokovnjakov na področju procesov zaščite in delovanja kritične infrastrukture nudi pomoč pri pripravi vse potrebne podlage na področju zagotavljanja nemotenega delovanja kritične infrastrukture. To bi zagotovilo uspešno prodajo predvidenih podjetij, s predpostavko zagotovila o neprekinjenosti delovanja kritične infrastrukture tudi z novimi zasebnimi lastniki. Na pereč problem so bili opozorjeni tako predstavniki Vlade Republike Slovenije, nadzorniki in strateško vodstvo Slovenske odškodninske družbe. Če bomo zamudili vlak in omenjena podjetja prodali brez priprave ustreznih podlag in pogojev, poti nazaj na žalost ne bo več. Odgovornost pred generacijami, ki so to premoženje ustvarjale in generacijami, ki jim zapuščamo zahtevno prihodnost te države, je zelo velika. Jutri možnosti izgovorov, da tega nismo vedeli, ne bo več. Treba pa je zadevo pogledati izven zakoreninjenih kalupov in izbrati ustrezno pomoč. ■



Avtor: Blaž Ivanc, mag / ICS Center za informacijsko varnost*



PREDLOGI VLADI REPUBLIKE SLOVENIJE NA PODROČJU NACIONALNE KIBERNETSKE VARNOSTI

Področje kibernetske varnosti v naši državi je vseskozi na zaskrbljujoče nizkem nivoju. Žal odsotnost novega strokovnega kadra s tega področja v javni upravi onemogoča kakršne koli spremembe na bolje.

Na podlagi posnetkov stanj in varnostnih analiz smo v letu 2012 in 2013 na različnih znanstvenoraziskovalnih konferencah in v knjigah predlagali ukrepe za izboljšanje kibernetske varnosti v državi. Žal odsotnost novega strokovnega kadra s tega področja v javni upravi onemogoča kakršne koli spremembe na bolje. Sem lahko prištejemo še brezglavo zapravljanje za v tujini razvite varnostne rešitve. V tem članku so predstavljeni predlogi Vladi Republike Slovenije na področju nacionalne kibernetske varnosti z vidika kritične infrastrukture. Predstavljen je še pomen kompetentnega in motiviranega kadra na področju kibernetske varnosti. Ne glede na obstoječe stanje je potrebno povedati, da ni znano, da bi Slovenija do sedaj že bila tarča dejansko resnih kibernetskih napadov. V isti sapi dodajmo, da izkušnje kažejo, da so naši sistemi varovani zgolj pred ljubiteljskimi izvajalci informacijskih groženj. V kolikor delovni procesi niso moteni, bo po vsej verjetnosti kakršna koli kompromitacija sistemov spregledana. Pri tem še omenimo, da so elementi forenzične pripravljenosti in odziva na incidente omejeni zgolj na nekaj izkušenih posameznikov.

Predlogi z vidika kritične infrastrukture

V marcu 2013 je bila predstavljena varnostna analiza kritične infrastrukture, konkretneje računalniško podprte oskrbe z vodo v Republiki Sloveniji (Ivanc, 2013). Na podlagi posnetka stanja, kjer smo med drugim predstavili številne enostavne poti za kompromitacijo industrijsko-krmilnih sistemov, smo ugotovili, da je z vidika učinka informacijskega napada na kritično infrastrukturo bolje izvesti napad na sistemskega integratorja IKT sistemov kot na samega upravljavca kritične infrastrukture. Hkrati smo v diskusiji izoblikovali tri varnostno kritična vprašanja:

- Ali lahko upravljavec kritične infrastrukture prepreči konkretne informacijske napade, ki izkoriščajo sistemskega integratorja kot vstopno točko?
- Ali lahko upravljavec kritične infrastrukture prepreči varnostni incident, ki je rezultat kompromitacije sistemskih komponent na ravni proizvajalca?
- Je upravljavec kritične infrastrukture sploh upošteval predhodno omenjeni točki pri oceni tveganj in kakšne varnostne protiukrepe je sprejel?

Seveda tudi bralec, ki ni strokovnjak na tem področju, sklepa pravilno, da je odgovor na vsa vprašanja enak: »ne«. Odgovor je pričakovan ter celo upravičen: upravljavec kritične infrastrukture bo težko zagotavljal varnost pred napadi iz kibernetskega prostora, dokler ne bo na ravni države ustanovljena majhna, vendar zares visoko kompetentna ekipa, katere naloge bodo:

- Izvajanje varnostnih presoj sistemskih komponent v kritični infrastrukturi.
- Verifikacija in validacija ustreznosti varnostnih mehanizmov.
- Razvoj standardov in smernic, ki bodo silile domače znanje v mednarodno primerljiv razvoj kibernetske varnosti in od upravljavcev kritične infrastrukture ter sistemskih integratorjev zahtevale zagotovitev strokovnega kadra na obravnavanem področju.

V tem sklopu velja še omeniti, da nekateri upravljavci kritične infrastrukture v Sloveniji, sicer povsem legitimno, pod pretvezo zagotavljanja informacijske varnosti onemogočajo sodelovanje strokovnjakov pri kakršni koli presoji kibernetske varnosti. Kljub vsem referencam in izkušnjam upravljavci kritične infrastrukture ne želijo nikakršne pomoči domačih strokovnjakov in v izgovor po-

*avtor je član Slovenskega združenja korporativne varnosti



nudijo izjavo, da že izvajajo razne ocene tveganj s katerim od zasebnih podjetij. Pri tem velja omeniti, da se takšne stvari bistveno redkeje dogajajo v sosednjih državah pri enako kritičnih objektih. V izogib zakrivanju obstoječega stanja s strani upravljavcev kritične infrastrukture, ki lahko imajo izvor tudi v strahu pred razkritjem neprimerne kibernetske varnosti strokovni javnosti, bi v Sloveniji bilo potrebno sprejeti še sledeče:

- Obvezna uvedba varnostnih standardov na področju industrijsko-krmilnih sistemov in nadzor nad izvajanjem le-teh.
- Določitev nivoja samostojnosti upravljavcev kritične infrastrukture na področju varnosti industrijsko-krmilnih sistemov.
- Takojšnji razvoj smernic s področja forenzične pripravljenosti v industrijskih IT sistemih.

Kot smo svetovali v enem od objavljenih člankov (Ivanc, Klobučar, 2012), bi moral za varnost kritične infrastrukture na ravni upravljavca le-te, skrbeti številčno majhen, specializiran oddelek. Razlogov, zakaj za kibernetsko varnost ne more in ne sme skrbeti sektor splošne ali procesne informatike, je več:

- Za varovanje kritične infrastrukture pred napadi iz kibernetskega prostora morajo biti zadolženi specializirani posamezniki, ki redno spremljajo nove ofenzivne tehnike, taktike in procedure.
- Analize dovršenih kibernetskih napadov v kritični infrastrukturi kažejo, da so napadi, ki izvedejo prikrit kanal, praktično dokaj sorazmerno porazdeljena kombinacija fizičnega in kibernetskega napada, podkrepljenega z izčrpnim obveščevalnim delom.

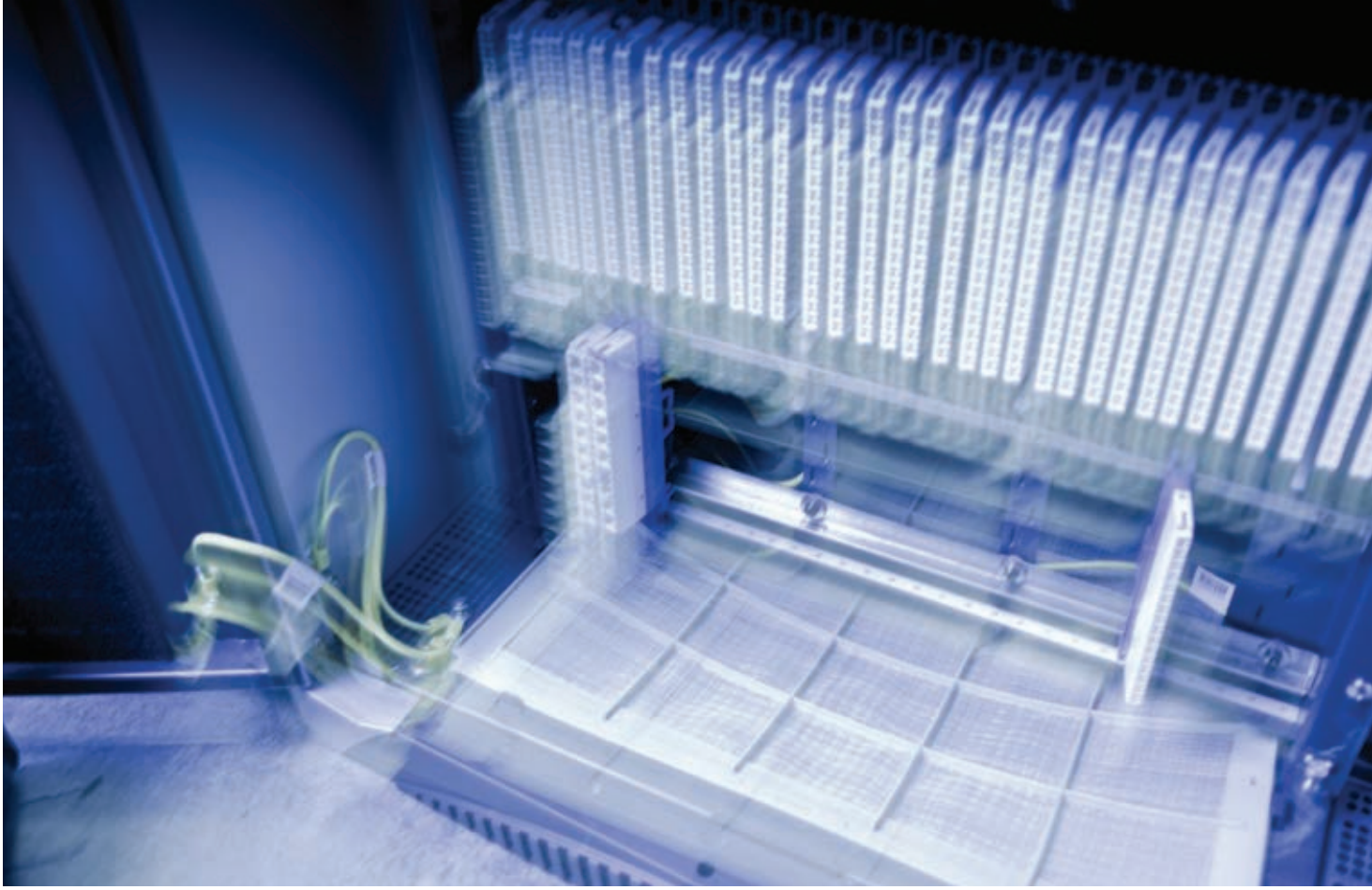
Problemi na področju kibernetske varnosti so posledica nezavedanja strokovnih omejitev. Ne gre spregledati zavzetosti pri pisanju smernic za zavarovanje podatkov v informacijskih sistemih s strani različnih inštitucij, a vendar je vedno znova sama vsebina tako pavšalna, da praktično ne zmanjšuje incidentov.

- Specializiran kader za kibernetsko varnost kritične infrastrukture potrebuje dostop do laboratorijskih sistemov in mora biti sposoben razvoja novih tehnik in izvedb samih kibernetskih napadov.

Pomen kompetentnega in motiviranega kadra

V Sloveniji imamo precej kadra, ki površinsko pozna področje in s tem dobi pravico za upravljanje informacijske varnosti v organizacijah javnega in zasebnega sektorja. Vendar bo taisti kader potrebno obremeniti z vso odgovornostjo za morebitne resne incidente v prihodnosti. Poglejmo si primer trenutnega stanja varovanja podatkov v informacijskih sistemih. Čeprav statistika obravnave incidentov s strani policije tega ne kaže, se organizacije v sklopu javne uprave srečujejo z zelo pogostimi notranjimi zlorabami informacijskih sistemov in preprodajo podatkov. To je eden izmed pokazateljev, da varnost, pa naj si bo pred zunanjimi agenti grožnje ali notranjimi sovražniki, ni predmet obravnave že v fazi zasnove informacijskega sistema.

V prejšnjem odstavku omenjen problem je rezultat slabe prakse razvoja informa-



cijskih sistemov z vidika varnosti, ugotovitve pa znane: Varnostni ukrepi se ne osredotočajo na tveganja, povezana z varovanjem samih operativnih podatkov, saj pogosto manjka premišljena kontrola dostopa pri deljenju podatkov. Politike kontrole dostopa so predstavljene preveč posplošeno in so operativno neuporabne. Sistemi kontrole dostopa ne upoštevajo negotovosti in tveganja pri dostopnih odločitvah. Vprašljivo je testiranje varnostno kritičnih komponent in drugo (Wang et al. (2009), Habib et al. (2008), Shaikh et al. (2011), Zhihong et al. (2011)).

Problemi na področju kibernetske varnosti so posledica nezavedanja strokovnih omejitev. Ne gre spregledati zavzetosti pri pisanju smernic za zavarovanje podatkov v informacijskih sistemih s strani različnih inštitucij, a vendar je vedno znova sama vsebina tako pavšalna, da praktično ne zmanjšuje incidentov. Nadalje se varnostne mehanizme jemlje kot dane, nihče vanje ne dvomi, saj so jih odobrili različni certificirani strokovnjaki. Tako niti ne opazimo, da smo pod vplivom podaljšane roke industrije. Vprašanje pa je, če sploh imamo izbiro, saj je pri nas na obravnavanem področju zgolj nekaj podjetij, ki imajo v resnici lasten razvoj rešitev.

Glede na stanje lahko rečemo, da pri skrbnikih informacijskih sistemov še vedno ne najdemo ustreznega kadra za izvajanje varnostne funkcije. To je rezultat nizkih varnostnih standardov v državi. Tako znova velja poudariti, da v Sloveniji potrebujemo ekspertno skupino, ki bo upravljavcem sistemov v javnem in zasebnem sektorju zagotavljala kompetentne smernice, standarde in okvirna delovna navodila s področja kibernetske varnosti.

Zaključek

Ne pozabimo, da je potrebno varnostna vprašanja presojati z vidika agentov grožnje. Takšna presoja zahteva nabor izvornih znanj, seznanjanje z najnovejšimi dognanji in vrhunsko poznavanje nasprotnika. Čeprav se komu zdi upravljanje informacijske varnosti zabavno in je verjetno zato tako popularno in prepolno »strokovnjakov«, pa v resnici potrebujemo operativno znanje na tem področju. Javna uprava potrebuje svež, kompetenten in motiviran kader, ki bo zmožen prispevati oprijemljive rezultate. Odsotnost zadostnih kompetenc in dvomljiva motivacija predstavljata neposredno grožnjo vitalnim interesom države in varnosti državljanov.

Reference

- Habib, L., Jaume, M. in Morisset, C. (2008). A formal comparison of the Bell & LaPadula and RBAC models. *Fourth International Conference on Information Assurance and Security*. 3–8. Washington, DC: IEEE Computer Society.
- Ivanc, B., Klobučar, T. (2012). Critical Infrastructure Attack Modelling. V: *Elektrotehniški Vestnik*, 79(4), 193–196.
- Ivanc, B. (2013). Techniques and procedures of cyber attacks on critical infrastrutcure. V: Čaleta, D. (ur.), Vršec, M. (ur.), *Management of corporate security : new approaches and future challenges*, 161–171.
- Shaikh, R. A., Adi, K., Logrippo, L. in Mankovski, S. (2011). Risk-based Decision Method for Access Control Systems. V: *Ninth Annual International Conference on Privacy, Security and Trust*. 189–192.
- Wang, X., Wu, X., Wang, Y. in Le, D. P. (2009). The Design and Implementation of a Sensitive Information System. V: *Fourth International Conference on Computer Sciences and Convergence Information Technology*. 1174–1179.
- Zhihong, T., Bailing, W., Ye, Z. in Zhang, H. (2011). The Survey of Information System Security Classified Protection. V: *Lecture Notes in Electrical Engineering*, 98, 975–980. ■

ICS — Center za informacijsko varnost



ICS

Institute for Corporative Security Studies

Delovno področje ICS—Centra za informacijsko varnost:

razvoj sistemov ter rešitev za podporo informacijske varnosti,

izvedba aplikativnih projektov gospodarskih ter pravnih subjektov,

integracija modelov informacijske varnosti z različnimi sistemi kakovosti procesov,

svetovanje pri izgradnji sistema informacijske varnosti gospodarskih ter pravnih subjektov,

izdelava ocen ter preprečevanje tveganj informacijske varnosti gospodarskih ter pravnih subjektov,

vzpostavitev modelov in presoja sistema informacijske varnosti gospodarskih ter pravnih subjektov.

Več na www.ics-institut.si!

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Igor Loborec
korporativno varnostni manager v ELES

KORPORATIVNA VARNOST TEMELJ ZA USPEŠNO UPRAVLJANJE PODJETJA

Glede na število procesov in organizacijskih enot v ELES-u se zavedamo, da je obvladovanje tveganj kompleksna naloga. Zato prav v danem trenutku posodabljamo sistem upravljanja s tveganji, ki bo postal sedmi sistem v okviru »sistemov upravljanja« našega podjetja.

Trenutno opravljate vlogo nosilca procesov korporativne varnosti v podjetju ELES. Nam lahko bolj podrobno opredelite kakšne so strateške naloge vaše službe in njena organizacijska umeščenost?

V ELES-u od 1.1.2013 izvajam funkcijo predstavnika vodstva za Sisteme upravljanja, ki vključuje koordinacijo in organizacijo sistemov vodenja po standardih ISO/IEC 9001, ISO/IEC 14001, ISO/IEC 27001, BS OHSAS 18001 ter sistemov civilne obrambe in zaščite in reševanja. Korporativna varnost zajema samo en del mojih obstoječih nalog in aktivnosti. Korporativna varnost je formalno in strukturno zajeta v organizacijskih predpisih, pravilnikih in navodilih navedenih šestih podsistemov. Izvaja se preko aktivnosti Službe za varnostni sistem in civilno obrambo (SVSCO), ki je organizacijsko umeščena kot ena od štabnih služb vodstva podjetja. Ena od osnovnih nalog SVSCO so načrtovanje in izvajanje ukrepov za potrebe kriznega upravljanja RS, koordiniranje družb elektrogospodarstva na področju kriznega upravljanja, uvajanje zahtev EU pri zaščiti kritične infrastrukture, organiziranje in vodenje fizičnega in tehničnega varovanja ter vzdrževanje in izboljševanje sistema varovanja informacij, če naštejem samo najpomembnejše. Strateške naloge službe so opredeljene v Strateškem poslovnem načrtu kot del strategije podjetja in sicer je še v fazi izvedbe izdelava enotnega načrta kriznega vodenja. ELES je kot podjetje, katerega dejavnost je posebnega pomena za obrambo RS med drugim zavezan (pre)mnogim zakonskim predpisom in uredbam, med katerimi se nekatere izključujejo. Zato izdelujemo načrt, ki bo vključeval vse zahtevane aktivnosti in v primeru izvedbe zagotavljal osnovno poslanstvo ELES-a – kakovosten in zanesljiv prenos električne energije.

ELES predstavlja izredno kompleksno in razvejano organizacijo, ki je že zaradi svojih osnovnih procesov zelo izpostavljena celemu nizu tveganj. Kako se s stališča strateškega korporativno varnostnega managerja spopadate z uravnoteženjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov?

V ELES-u imamo vpeljan procesni model delovanja družbe. Tveganje lahko nastopa samo v posameznem procesu, bodisi na nivoju posamezne aktivnosti ali sredstvu, ki se nahaja v posamezni organizacijski enoti. Glede na število procesov in organizacijskih enot v ELES-u se zavedamo, da je obvladovanje tveganj kompleksna naloga. Tudi na tem podro-



*avtor je član Slovenskega združenja korporativne varnosti

čju je ELES zavezan priporočilom dobre prakse korporativnega upravljanja OECD, Kodeksu upravljanja kapitalskih naložb v družbah v pretežno državni lasti ter nenazadnje tudi Aktu o ustanovitvi družbe javnega podjetja ELES, d.o.o.. Zato prav v danem trenutku posodabljamo sistem upravljanja s tveganji, ki bo postal sedmi sistem v okviru Sistemov upravljanja. Dosedanje ocene in analize tveganj s področja operativno – tehničnih tveganj, tveganj varovanja informacij, tveganj varnosti in zdravja pri delu ter tveganj okoljske problematike se niso sistematično in celostno vodile, zaradi česar so bili tudi ukrepi za zmanjševanje posameznih tveganj nesorazmerni. Nov sistem upravljanja s tveganji bo dano anomalijo odpravil in primerno ovrednotil višino posameznega tveganja.

Kakšno mesto in vlogo ima v hierarhiji strateških dokumentov v ELES varnostna politika organizacije? Ali tak dokument predstavlja strateški pogled in usmeritve za postavitev in delovanje sistema korporativne varnosti v ELES-u?

Varnostne politike nimamo posebej opredeljene, imamo pa poleg kadrovske politike, politike komuniciranja, politike varnosti in zdravja pri delu, opredeljeno politiko varovanja informacij, ki je samo ena od politik delovanja podjetja in, ki v širšem obsegu pokriva varnostno politiko in zajema tudi korporativno varnost. Vse politike imamo opredeljene v Poslovniku sistema upravljanja, ki je javni dokument. Kot sem že povedal imamo strateške cilje opredeljene v posebnem dokumentu – Strateškem poslovnem načrtu, ki deloma zajema – predvsem iz organizacijskega vidika – tudi elemente korporativne varnosti. Predvsem bi pa na tem mestu tudi opozoril na ponekod napačno razumevanje pomena varnostne politike. Sam termin varnostna politika je dobesedno preveden iz anglosaškega sveta kot »Security policy«. Najbližje temu terminu in tudi osnovnemu namenu se približujejo npr. zavarovalne police, ki pa seveda niso politike, temveč jasna navodila za katere primere si zavarovan. Torej govorimo o navodilih in pravilnikih. Politika, tudi varnostna, je širša usmeritev delovanja družbe na varnostnem področju, količinsko lahko zajema od nekaj vrstic do pol strani teksta. Daje nam odgovor na vprašanje »Kaj delamo?«. Za odgovor na vprašanje »Kako delamo?« pa morajo biti za vsak segment posebej napisana jasna, konkretna in nedvoumna navodila, bodisi v obliki organizacijskih predpisov, bodisi v obliki pravilnikov.

Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od slabše uspešnih. Kako se v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Predvsem se zavedamo, da je vsakršna kultura v podjetju povezana z zadovoljstvom zaposlenih ter s primernim usposabljanjem. Samo zadovoljen in primerno usposobljen delavec bo hkrati tudi primerno varnostno ozaveščen. V ta namen skladno s potrebami/zahtevami večkrat letno organiziramo specializirane interne tečaje in seminarje, preko katerih ozaveščamo zaposlene na kakšen način ravnati, da bodo varnostna tveganja kar najmanjša. In tudi o vlogi posameznika v organizaciji, kajti nezadovoljen posameznik je vedno najšibkejši člen v varnostni verigi. Poleg tega nam tudi standardi zapovedujejo določene aktivnosti, ki nam ohranjajo ter zvišujejo varnostno kulturo.

Standardizacija sredstev na področju tehničnega varovanja in varnostnih procesov na splošno je v tako razvejanem sistemu verjetno nujno potrebna. Kakšne so na tem področju vaše izkušnje in kakšne pristope uporabljate v ELES?

Tehnična standardizacija je spričo hitrih tehnoloških sprememb praktično nemogoča. Npr. imeli smo standardizirane nadzorne video kamere glede na število pixlov, vendar je že za časa enega samega javnega naročila tehnologija toliko napredovala, da bi morali kupiti že zastarelo opremo. Zato smo v nekaterih postopkih pristopili k določanju funk-



cionalnosti. Potrebno je namreč vedeti, da ELES kot javno podjetje mora in tudi upošteva vsa določila predpisov o javnem naročanju. To pa tudi pomeni, da se postopki priprave in izbire za večja naročila merijo v mesecih, če ne tudi v letih. V takih časovnih obdobjih se pa tehnika zelo spremeni, še posebej, ker je danes vedno bolj vezana na mikroprocesorje in pripadajočo programsko opremo. In vsi poznamo Moorov zakon, ki trdi, da se približno vsakih 18 mesecev zmogljivost mikroprocesorjev podvoji.

Kakšne so vaše izkušnje pri zagotavljanju določenih segmentov varnosti z uporabo outsorcinga varnostnih storitev?

Zaenkrat dobre. Glede na osnovno poslanstvo in teritorialno razdrobljenost družbe ni gospodarno in ekonomično organizirati lastno službo fizičnega varovanja. Tako imamo npr. podpisane pogodbe z več lokalnimi varnostnimi službami, ki nam zagotavljajo primeren nivo fizičnega varovanja. Za področje varovanja informacij najemamo zunanja podjetja, da nam izvajajo napovedane ali nenapovedane penetracijske teste računalniškega omrežja.

Kritična infrastruktura je nujna za nemoteno delovanje družbe. Kako ob tej predpostavki organizirati sistem obvladovanja tveganj, ki bo zagotavljal ustrezno varnost za nemoteno delovanje infrastrukture? Kakšne so vaše izkušnje sodelovanja z državnimi organi zadolženimi za pripravo sistemskih ukrepov za zaščito te infrastrukture?

O sistemu upravljanja s tveganji sem že odgovoril. Kar se pa tiče sodelovanja z državnimi organi so pa izkušnje mešane. Zaradi prevelike zbirokratiziranosti državnega aparata nekateri postopki potekajo absolutno predolgo. Poleg tega se v okviru države pristojna ministrstva usklajujejo preko medresorskih komisij in na koncu postopka dobimo sicer usklajen dokument, ki pa večinoma le interesno zadovoljuje posamezne akterje. Osnovni cilj pa zaradi tega lahko izgubi na vrednosti. Že prej sem omenil, da imamo kar nekaj načrtov, ki jih zahteva zakonodaja, za vsakim od njih pa stoji določena interesna skupina. Dodana vrednost le teh je za ELES vprašljiva, sem pa prepričan da za interesne skupine dodana vrednost ni vprašljiva. Žal zakonodajo pišejo teoretiki, izvajati jo pa moramo praktiki. Da, želel bi si več sodelovanja oziroma upoštevanja naše dobre prakse v državnih aktih in zakonih.



Razvoj in odvisnost od informacijske tehnologije postavlja kibernetske grožnje v posebno perspektivo. Kateri so po vašem mnenju tisti koraki, ki jih lahko storijo sistemski operaterji za učinkovito zavarovanje pred temi kompleksnimi grožnjami?

Govorimo o stari zgodbi žandarjev in lopovov. In lopovi so vedno korak pred žandarji, še posebej v kibernetskem svetu. Tega dejstva se je potrebno zavedati. Nikoli ne moremo v določenem času vzpostaviti toliko tehničnih varnostnih kontrol, da bomo lahko trdili, da smo kolikor toliko varni. Tehnika ne rešuje, vedno je človek tisti, ki odloča in ukrepa. In zopet smo pri zadovoljnih in varnostno ozaveščenih zaposlenih – poznano je namreč dejstvo, da je 80% kibernetskih incidentov povzročenih s strani zaposlenih. In eden od nujnih korakov je stalno varnostno usposabljanje, opozarjanje na možne posledice nepremišljenih dejanj, primernih notranjih organizacijskih predpisih in navodilih, primerni kulturi in organizacijski klimi. O konkretnih ukrepih pa ne bi govoril – tudi to je lahko del razkrivanja občutljivih poslovnih informacij.

ELES je eden izmed korporativnih članov Slovenskega združenja korporativne varnosti. Kakšen pomen pripisujete stanovskemu združevanju na področju korporativne varnosti? Je to dolgoročno lahko pomemben korak k dvigovanju varnostnega zavedanja in predvsem pomena korporativne varnosti?

V ELES-u pozdravljamo vsako aktivnost, ki pripomore k uveljavljanju stroke v širši družbeni skupnosti. Slovensko združenje korporativne varnosti izvaja takšno aktivnost in s svojim delovanjem pozicionira korporativno varnost na mesto, kamor sodi. Kakor se počasi v Sloveniji uveljavljajo OECD načela in principi korporativnega upravljanja (lastnik – nadzorni svet – odgovorna oseba – organizacija), tako mora temu slediti tudi korporativna varnost. Dandanes je v slovenski družbi žal še vedno prevladujoče in razširjeno mnenje, da se varnost in varovanje nanaša samo na npr. fizično varovanje objektov, kar je seveda daleč od resnice. Govorimo vendar o organizacijskemu sistemu vodenja. Združenje s svojim aktivnim delovanjem razširja pomen korporativne varnosti in dviguje nivo varnostnega zavedanja svojih članov, ki ga nato prenašajo v svoja delovna okolja. Na ta način se bo korporativna varnost sčasoma uveljavila kot nenadomestljiv element vodenja in upravljanja uspešnih slovenskih podjetij. ■

Združenje s svojim aktivnim delovanjem razširja pomen korporativne varnosti in dviguje nivo varnostnega zavedanja svojih članov, ki ga nato prenašajo v svoja delovna okolja. Na ta način se bo korporativna varnost sčasoma uveljavila kot nenadomestljiv element vodenja in upravljanja uspešnih slovenskih podjetij.

Avtor: doc. ddr. Robert Brumnik / ICS Center za informacijsko varnost*



RAZISKOVALNI PRISTOPI, POGLEDI IN MODELI OBRAVNAVE (KIBERNETSKEGA) TERORIZMA

Za razliko od tradicionalnih komunikacijskih medijev, je internet kot najzmogljivejše komunikacijsko sredstvo vse pomembnejši, tudi za komuniciranje in načrtovanje operacij prostorsko in organizacijsko dislociranih terorističnih organizacij.

V obdobju po hladni vojni je terorizem postal eno izmed najpomembnejših varnostno-političnih tem tudi v državah, ki sicer niso bile neposredno ogrožene. Skozi preteklost si strokovnjaki pri splošni obravnavi in definiranju terorizma kot pojava in njihove percepcije, največkrat niso bili enotni (Gamage, 2010). Terorizem je verjetno star kot človeštvo (Barnaby, 2000; Lederberg, 1999). Ne glede na to, da pojem zgodovinsko izvira iz časov francoske revolucije[1], pa večina definicij največkrat izpostavlja uporabo sile ali nasilja, z namenom ustrahovati prebivalstvo in se skozi čas ustrezno prilagaja političnim in tehnološkim spremembam. Etimološko gledano je terorizem koncept, ki izhaja iz samostalnika »teror« in pomeni skrajni strah ali strah v najrazličnejših možnih oblikah. V tem kontekstu je bil izraz »terorizem« na pravnem področju prvič uporabljen l. 1930 v Bruslju na mednarodni konferenci, ki je bila namenjena poenotenju kazenskega prava. Izraz »terorizem« je bil opredeljen kot namerna in sistematična uporaba nasilja za dosego določenih ciljev (Levasseur, 1977). Leta 1934, ko sta bila umorjena jugoslovanski kralj Karađorđević in francoski zunanji minister Barthou, so časopisi vsak dan opominjali na kugo tistega časa: mednarodni terorizem (Estevez, Pavolka in Nižňansky, 2006). Schmidt in Yongman (2005) sta naštela kar 109 različnih definicij terorizma, ki sta jih pridobila v raziskavah vodilnih akademikov tega področja. Iz definicij in opredelitev terorizma so statistično največkrat zastopani naslednji (izolirani) ponavljajoči se elementi:

- nasilje, sila (se je pojavil v 83,5 % definicij),
- politično (65 %),
- strah, groza (51 %),
- grožnje (47 %),
- psihološki učinek in pričakovane reakcije (41,5 %),
- razhajanje med cilji in žrtvami (37,5 %),
- namerno, načrtovano, sistematično, organizirano delovanje (32 %) in
- način boja, strategije, taktike (30,5 %).

Sledijo izsiljevanje, želja po publiciteti, zastraševanje, nedolžnost žrtev ter kriminalni oz. zločinski značaj, pri čemer pa je zanimivo, da pri navedenih elementih raziskave ne zaznamo besed »informacijski«, »informacijska tehnologija«, »elektronski«, »mediji« itd. kar bi nakazovalo na vpliv tehnoloških sprememb ter njihovem prilagajanju v evoluciji terorizma.

Kibernetski terorizem je mogoče opredeliti z uporabo računalnika politično motivirane mednarodne ali sub-nacionalne skupine kot orožje ali kot cilj, za ogrožanje ali povzročitev nasilja in strahu, da bi vplivali na občinstvo, ali povzročili, da neka vlada spremeni svojo politiko (Hutter, 2002).

*avtor je član Slovenskega združenja korporativne varnosti

IKT kot temeljna predpostavka modelov modernega terorizma

Kadar govorimo o terorizmu najprej pomislimo na izvedeno fizično nasilje in marsikdo je mnenja, da je informacijski terorizem predvsem pojavna oblika, katere namen je sejati strah s teroristično grožnjo, saj naj bi bilo nemogoče z informacijskimi tehnologijami fizično ogrožati prebivalstvo. Za lažje razumevanje v nadaljevanju poglejmo nekaj modelov obravnave terorizma.

Kibernetski terorizem[2] je ena izmed najsodobnejših pojavnih oblik terorizma, ki ga nekateri avtorji vključujejo v okvir informacijskega bojevanja (Shahar, 1997), drugi pa menijo, da je informacijsko bojevanje popolno teroristično orožje (Schiller, 2010). Izraz kibernetski terorizem, se nanaša na zbliževanje kibernetskega prostora in terorizma in ga je v 80. letih prejšnjega stoletja prvi uporabil Collin, raziskovalni sodelavec Inštituta za varnost in obveščevalno dejavnost v Kaliforniji (Denning, 1999). O kibernetskem terorizmu govorimo, ko so zaradi terorističnih napadov na kritično informacijsko infrastrukturo fizično ogrožena življenja in premoženje prebivalstva ter moteno normalno delovanje družbe (Quigley, 2008). Kibernetski terorizem pomeni protipravno namerno uporabo ali grožnjo uporabe nasilja, motenj ali interference kibernetskih sistemov, z verjetnostjo, da bi bila takšna uporaba povzročila smrt, poškodbo osebe ali oseb, dejansko škodo fizične lastnine, civilne nemire ali pomembno gospodarsko škodo (Information Warfare Site [IWS], 2011). Denning (2001) kibernetski terorizem definira kot politično motivirano hekersko aktivnost, z namenom, povzročiti resno škodo, smrt ali hudo gospodarsko škodo. Krasavin (2004) trdi, da vsaka namerna uporaba informacijske tehnologije terorističnih skupin in njihovih pripadnikov, z namenom, da škoduje predstavlja kibernetski terorizem. Kibernetski terorizem je mogoče opredeliti z uporabo računalnika politično motivirane mednarodne ali sub-nacionalne skupine kot orožje ali kot cilj, za ogrožanje ali povzročitev nasilja in strahu, da bi vplivali na občinstvo, ali povzročili, da neka vlada spremeni svojo politiko (Hutter, 2002). Ta definicija, združuje več mnenj o kibernetskemu terorizmu in zajema tri načine delovanja: fizični, elektronski, in informacijski, za napade na računalnike (Congressional Research Service [CRS], 2005). Mehka verzija definicije informacijskega terorizma izpostavlja predvsem IKT, ki jih teroristi uporabljajo za izvajanje pritiska in propagando, namenjeno javnosti, in mobiliziranje ter rekrutiranje novih podpornikov (Müller, Wille in Björn, 2004). Od oblike delovanja in želje uničevanja, so namreč posledice zlonamerne uporabe IKT lahko zelo različne. Po Hoffmanu (1999) ima ta nova oblika terorizma tudi večjo ubojnost. Lahko bi rekli, da v primeru kibernetskega terorizma, gre za delovanje, pri katerem sicer neposredno ne pride do poškodovanja lastnine ali ljudi. Samo oškodovanje pri tej obliki kriminala, se največkrat res ne pokaže neposredno, vendar so posredni učinki delovanja lahko katastrofalni tudi za ljudi. Kljub temu pa je kibernetski teorizem po mnenju nekaterih strokovnjakov zapleteno definirati (Murrill, 2011). Teroristične organizacije danes niso hierarhično in centralizirano organizirane, ampak povzemajo sodobne mrežne oblike (celice). Ne glede na različna izhodišča in odprta vprašanja pa ostaja nesporno dejstvo, da so IKT sredstvo in hkrati cilj terorističnega delovanja v 21. stoletju. Glede ustrahovanja pa je seveda jasno, da brez medijev in danes pomembnih interaktivnih IKT, o terorizmu ni mogoče govoriti. Danes imamo tako več splošnih opredelitev kibernetskega terorizma, zato se težave pojavijo, ko je potrebno definicijo praktično uporabiti v sodobnih konfliktih. Medijsko posredovanje in prikaz terorističnih dejanj, omogoča pojavitev občutka strahu in zaznavo ogroženosti, ki je mnogo večja od tiste, ki jo kažejo podatki o številu žrtev ali poškodovanih v napadih.

> Za Slovenijo bi lahko celo trdili, da gre za popolno odsotnost takšnih institucionalnih organov.

EU pristop k boju proti kibernetskemu terorizmu

Širok pristop EU, ki ga sestavljajo štiri glavne prednostne naloge (preprečevanje, zaščito, preganjanje in odzivanje) s katerim je EU v letu 2012 pozvala vse članice k ustanovitvi centrov za zaščito infrastrukture in boj proti kibernetski kriminaliteti, je hvalevredno, ker učinkovito implementira protiteroristične politike. Določa obsežno vizijo in predlaga potrebne ukrepe, ki temeljijo na močni zaščiti in spodbujanju uveljavljanja pravic državljanov, da bo imela EU najvarnejše spletno okolje na svetu. Vendar je za strategijo kibernetske varnosti za Evropsko unijo potrebno veliko več kot pregon in zunanja obramba.
Cilj strategije evropske komisije, sprejete februarja 2013 mora okrepiti prožnost ter varnost omrežja in informacij; znatno zmanjšati kibernetsko kriminaliteto; razviti politiko EU glede kibernetske zaščite; okrepiti industrijske in tehnološke vire za kibernetsko varnost;



spodbujati raziskave in razvoj (R&R) in okrepiti politiko EU glede mednarodnega kibernetskega prostora. Čeprav se priznava krepitev učinkovitega sodelovanja med državami za boj proti kibernetskemu terorizmu, je prav tako potrebno upoštevati, da mora EU okrepiti svoja prizadevanja še za odpravo vrzeli in pomanjkljivosti, ki izhajajo iz institucionalnih in pravnih okvirov protiteroristične in kibernetske politike EU.

Posebni kazenski in zato protiteroristični ukrepi so v pristojnosti držav članic in je zato glavna vloga EU predvsem usklajevanje. Ampak, da bi bili uspešni pri tej nalogi, EU v prvi vrsti potrebuje celovit in skladen institucionalni okvir za boj proti kibernetskemu terorizmu. Namesto tega je bila dosedanja evropska institucionalna arhitektura boja proti terorizmu sestavljena iz preveč akterjev, s podvajanjem in prekrivanjem nalog. Za Slovenijo bi lahko celo trdili, da gre za popolno odsotnost takšnih institucionalnih organov. Takšen način pa kaže na nujno spremembo odnosa do posameznih (varnostnih, obrambnih in zunanjih) politik neke države, ki se mora prilagoditi sodobnim trendom groženj in tveganj, ki se selijo v kibernetski prostor.

Viri

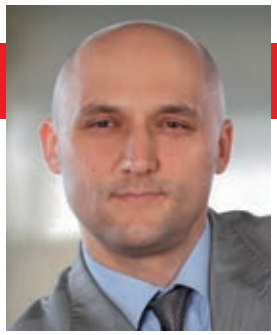
- Gamage, P. (2010). Media, Terrorism and Insurgency in South Asia, http://www.upsam.upeace.org/pdf/Curricula/Gamage/Media%20Terrorism%20and%20Insurgency%20in%20South%20Asia.pdf
- Barnaby, W. (2000). The plague makers: the secret world of biological warfare.
- Lederberg, J. (1999). Arguing that the deliberate use of microorganisms and toxins to harm others has been practiced for centuries, and will likely continue into the future.
- Levasseur, G. (1977). Les aspects repressifs du terrorisme international, Institut des hautes etudes Internationales de Paris, Pedone, str. 62.
- Estevez, M. L.M., Pavolka, D., Nižňansky, J. (2006). European response to terrorism: the cases of Spain and Slovakia http://www.mod.gov.sk/data/files/518.pdf
- Schmidt, P. A.,Yongman, J. A. (2005). Political terrorism. http://books.google.si/books?id=vKyzhXA71jEC&source=gbs_similarbooks_s&cad=1 http://unjobs.org/tags/political-terrorism
- Shahar, Y. (1997). Information warfare. International Policy Institute for Counter-Terrorism. http://www.iwar.org.uk/cyberterror/resources/CIT.htm
- Schiller, J. (2010). Cyber Attacks & Protection, CreateSpace.
- Denning, D. (1999). Information warfare and security. Berkeley, Sidney, Bonn: addison-wesley.
- Quigley, M. (2008). Encyclopedia of information ethics and security, Idea Group Inc. (IGI).
- Information Warfare Site (2011). http://www.iwar.org.uk/cyberterror/
- Denning, D. (2001). "Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, ed., *Networks and Netwars*, (Rand, 2001), str. 241.
- Krasavin, S. (2004). *What is Cyberterrorism?*, Computer Crime Research Center. http://www.crime-research.org/analytics/Krasavin/
- Hutter, R. (2002). Cyber Terror-eine realistische Gefahr? http://www.aksis.de/Cyber-Terror.pdf
- Congressional Research Service (2005). Computer Attack and Cyberterrorism:
- Vulnerabilities and Policy Issues for Congress, http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf
- Müller, W. B. (2004). For our eyes only? Shaping an intelligence community within EU. Occacional paper No.50. Paris. Institute for security Study.
- Murrill, R. (2011). The Question Of Cyber Terrorism. http://articles.forensicfocus.com/2011/07/23/the-question-of-cyber-terrorism/
- Evropska komisija (2013). Sporočilo komisije evropskemu parlamentu in svetu: Drugo poročilo o izvajanju strategije notranje varnosti EU, Bruselj.

[1] Izraz »terorizem« izhaja iz obdobja v letih 1793 in 1794 (med francosko revolucijo). Uporabljali so ga vodje sistematskega odstranjevanja »izdajalcev« med revolucionarnimi odbori, z njim so namreč imenovali najboljšo možnost za ubranitev svobode.

[2] Kibernetski terorizem; Standardizirane definicije računalniške kriminalitete v funkciji terorizma, veljavne na svetovnem nivoju še ni. ■



Avtor: Andrej Kovačič / Inštitut za korporativne varnostne študije*



NADZOR NAD IZVAJALCI VAROVANJA KOT DEJAVNIK POSLOVNE USPEŠNOSTI NAROČNIKA

Namen prispevka je nakazati nekatere možnosti za izboljšanje varnosti v organizacijah in opozoriti odgovorne, kako pomemben je neodvisni nadzor nad izvajanjem varovanja za poslovno uspešnost organizacije.

Da bi bile organizacije pri zagotavljanju varnosti bolj učinkovite in poslovno uspešne, bi morale upoštevati določene varnostne standarde. Neobvladovanje varnostnih in ostalih povezanih tveganj vpliva na stopnjo varnosti in posledično na poslovno uspešnost organizacije.

Pri tem pa se ne moremo izogniti varnosti, kot družbeni odgovornosti, saj so organizacije pogosto vpete v lokalno okolje, kjer živijo ljudje. Organizacije, ki ne obvladujejo varnostnih tveganj so lahko pogosto tarča različnih nevarnosti, kar pri bližnjih prebivalcih lahko povzroča določeno nelagodje in s tem vpliva na kvaliteto njihovega življenja.

Organizacije javnega in zasebnega prava, z namenom zagotavljanja varnosti, najemajo zasebne varnostne družbe ali varnost ljudi in premoženja zagotavljajo z lastnimi varnostniki. Nekatera sledijo varnostnim standardom medtem, ko ostala temu področju posvetijo več pozornosti takrat, če sploh, ko je žal že prepozno. Tako se pogosto slabosti v neustreznem načinu varovanja pokažejo takrat, ko je že bila storjena škoda in ko je odpravljanje te škode veliko dražje, kot bi bilo sicer. Ko govorimo o varnostnih standardih[1] na področju upravljanja varnosti v organizacijah, ne moremo mimo neodvisnega nadzora.

Neodvisni nadzor, kot dodana vrednost za učinkovito zagotavljanje varnosti v organizacijah

Naročniki pričakujejo, da bodo zasebno varnostne družbe profesionalno opravljale naloge varovanja, zato jim s podpisom pogodbe prepustijo celotno varnostno situacijo. V praksi pa se pogosto izkaže, da izvajalci varovanja niso vredni tovrstnega zaupanja. Izvajanje nadzora nad izvajalci varovanja je tako prvi pogoj za obvladovanje tovrstnih tveganj (Gostič, 2006).

Strateško vodstvo s pravilnim pristopom k izboru izvajalca varovanja v prvi fazi ter v nadaljevanju z neodvisnim nadzorom nad njegovim izvajanjem razume svojo odgovornost za varnost v organizaciji. Takšen pristop je značilen za uspešne organizacije, ki imajo sprejeto varnostno politiko in se ravnajo po varnostnih standardih in katerim ni vseeno, kakšno varovanje imajo in kaj dejansko plačujejo.

Neodvisni nadzor je postopek, ki ga izvajajo kompetentni strokovnjaki s področja zasebnega varovanja z izkušnjami na različnih varnostnih področjih. Koristijo ga lahko tako naročniki zasebnega varovanja, kot sami izvajalci. Naročniki z nadzorom pridobijo neodvisno strokovno mnenje o izvajanju varovanja v njihovem poslovnem okolju medtem, ko izvajalci varovanja pridobijo boljše oziroma drugačne vidike v načinu izvajanja varovanja v določenem okolju. Nadzor je tako zbiranje in sporočanje informacij o izvajanju varovanja, ter vrednotenje teh informacij s postavljenimi standardi (Gostič, 2006).

Strateško vodstvo z nadzorom pridobi; (1) neodvisno strokovno mnenje o ustreznosti in kakovosti izvajanja varovanja;

> Učinkovit nadzor pomaga izboljšati varnostne in poslovne zmogljivosti ter finančne prihranke. Z nadzorom se tudi ugotavlja, ali je mogoče z drugačnimi oblikami oz načinom varovanja zadostiti enako ali višjo stopnjo varnosti.

*avtor je član Slovenskega združenja korporativne varnosti



(2) odgovore ali poteka varovanje v skladu s sprejetimi standardi; (3) večji vpliv na upravljanje z varnostjo v organizaciji. Pri tem gre za ugotavljanje ustreznosti, učinkovitosti in skladnosti varovanja s poslovanjem ter njegove finančne perspektive. Preventivno naravnani nadzor temelji na dejavnosti, značilnosti in velikosti organizacije oziroma poslovanja. Ugotavljanje, ali je določen sistem varovanja stroškovno učinkovit, izhaja iz različnih komponent – poslovno okolje, panoga, ocenjevanje varnostnih tveganj, varnostne kulture zaposlenih, obiskovalcev oz kupcev, organizacijske klime, sistema nadzora, informiranja in poročanja, spremljanja varnostne situacije itd. Preventivni nadzor pomembno vpliva na uspešnost zagotavljanja varnosti in na zastavljene poslovne cilje organizacije. Pogoji poslovanja se v teh nenehnih spremembah neprestano spreminjajo, zato je način varovanja potrebno prilagajati danim razmeram sodobnega časa. Prepoznavanje in obravnavanje varnostnih tveganj v določeni dejavnosti, se ne sme prepuščati naključjem. Tudi, ko/če nekdo ''po malem'' prazni skladišče, to pomeni, da varovanje ni učinkovito oz je zaskrbljujoče, če to počnejo tisti, ki varovanje izvajajo.

Nadzor mora vključevati širšo perspektivo, če upoštevamo, da na organizacije vplivajo številne spremenljivke, pogosto zunaj njihovega neposrednega okolja in delovanja. Nadzor je potrebno izvajati in uporabljati kot odgovor na specifična varnostna tveganja, njihove vzroke in posledice. Nadzor se pogosto dojema in obravnava samo kot zahtevo po skladnosti, in ne možnosti za povečanje organizacijske učinkovitosti. Učinkovit nadzor pomaga izboljšati varnostne in poslovne zmogljivosti ter finančne prihranke. Z nadzorom se tudi ugotavlja, ali je mogoče z drugačnimi oblikami oz načinom varovanja zadostiti enako ali višjo stopnjo varnosti. Nadzor je potrebno obravnavati, tudi kot postopek pri obvladovanju tveganj z osredotočanjem na identifikacijo slabosti pri izvajanju varovanja, groženj in nevarnosti. Pri naročnikih nadzora, ki so izvajalci varovanja, neodvisni nadzor pomeni konkurenčno prednost, za naročnike varovanja pa garancijo za boljšo kakovost varovanja in zmanjšanje tovrstnih tveganj. Ali v organizacijah razumejo, kako imajo lahko različna varnostna tveganja skupne vzroke in medsebojno povezanost na uspešnost poslovanja? Obvladovanje varnostnih tveganj in nadzor nad izvajanjem varovanja sta sestavni del učinkovitega sistema upravljanja organizacije. Vključevanje in učinkovito izvajanje nadzora s svojimi ugotovitvami in priporočili izboljša ugled in finančno perspektivo, ovrednoti izmerjeno uspešnost varovanja ter spremlja varnostne izboljšave. Razmere v dinamičnem okolju in v družbi vplivajo na spreminjajoča se varnostna tveganja in na način izvajanja varovanja. Načrtovanje, izvajanje in spremljanje procesa izvajanja varovanja mora biti v skladu s cilji organizacije. Z nezadostno pozornostjo varnostni problematiki, bodo težko doseženi poslovni

Uspešne organizacije dobro vedo, kako izkoristiti možnosti za preprečevanje in zmanjševanje tveganj z učinkovitim izvajanjem nadzora ter z optimiziranjem izvajanja varovanja. Pravočasen in učinkovit nadzor prepoznava varnostno problematiko v zgodnji fazi in vsa dogajanja, ki ogrožajo vitalne točke poslovanja.

cilji. Poročilo o opravljenem nadzoru temelji na konkretnih primerih, kjer določeni postopki izvajanja varovanja niso skladni s poslovanjem, bodisi so pomanjkljivi, se izvajajo neustrezno itd. Vsaka evidentirana ugotovitev mora biti utemeljena s konkretnimi primeri in smernicami za učinkovitejše izvajanje varovanja.

Dileme izvajanja varovanja in prednosti neodvisnega nadzora

Eden izmed učinkovitih obramb pred poslovnim neuspehom zaradi neobvladovanja varnostnih tveganj, kakor tudi pomembno gonilo uspešnosti organizacij, je neodvisni nadzor. V primerih, ko organizacija nima ustrezno urejenega sistema varovanja, ko se dogajajo tatvine (zaposleni, stranke, varnostniki), s tem nastaja škoda v organizaciji in posledično slabše finančno poslovanje. Naj omenimo samo en primer v razmislek o (ne)ustreznosti varovanja, ko imajo varnostniki naloge fizičnega varovanja in hkrati naloge nadzora preko video nadzornega sistema (trgovski centri, trgovine, skladišča ipd). V teh primerih bi nadzor preko video nadzornega sistema morala opravljati bodisi ločena notranja služba v organizaciji ali zunanja služba druge zasebno varnostne družbe.

Zunanji nadzor lahko pokaže na neustrezno izvajanje varovanja, kar seveda zmanjšuje oziroma odpravlja določena tveganja pri naročnikih. Z nadzorom nad izvajanjem varovanja je mogoče obvladovati varnostna in ostala poslovna tveganja ter vplivati na višjo stopnjo varnosti organizacije. Nadzor bi moral biti ključni del dobrega upravljanja organizacije skozi perspektivo obravnavanja varnosti in izvajanja varovanja. Uspešne organizacije dobro vedo, kako izkoristiti možnosti za preprečevanje in zmanjševanje tveganj z učinkovitim izvajanjem nadzora ter z optimiziranjem izvajanja varovanja. Pravočasen in učinkovit nadzor prepoznava varnostno problematiko v zgodnji fazi in vsa dogajanja, ki ogrožajo vitalne točke poslovanja.

Strateško vodstvo, ki razume svojo odgovornost za varnost zaposlenih, strank, premoženja in ostalih vitalnih delov organizacije, se poslužuje neodvisnih nadzorov. Takšne organizacije izpolnjujejo kriterije za višje varnostne standarde. Z neodvisnim nadzorom, glavno vodstvo organizacije pridobi naslednje: (1) Presojo varnostnega stanja, saj neodvisna institucija, ki izvaja nadzor poda oceno o (ne)ustreznosti izvajanja varovanja; (2) Konkretne predloge in priporočila za izboljšanje varnostnega stanja, saj neodvisna institucija na podlagi ugotovitev predlaga nove, lahko tudi finančno ugodnejše rešitve; (3) Finančno ovrednotenje izvajanja varovanja, kar pomaga glavnemu vodstvu pri investicijah v sistem varovanja; (4) Na podlagi ocene stanja in analize varnostnih dogodkov ovrednotenje uspešnosti in učinkovitosti varovanja; (5) Priporočila za odpravo pomanjkljivosti, napak in nepravilnosti pri izvajanju varovanja.

Neodvisni nadzor, bi moral postati standard, ki bi ga podpirali tudi nadzorni sveti oziroma lastniki organizacije.

Zaključek

Posledice neustreznega in slabega izvajanja varovanja so lahko (ne)vidne navzven in imajo vpliv na poslovno uspešnost organizacije. Običajno gre za primere uničenja, poškodovanja ali odvzem premoženja naročnika. Strateško vodstvo, ki je odgovorno za varnost v organizaciji in za obvladovanje varnostnih tveganj, z nadzorom pridobi odgovore na temeljna vprašanja: (1) Ali je izvajanje varovanja ljudi in premoženja v skladu s standardi in cilji organizacije? (2) Ali je varovanje učinkovito? (3) Kakšni so rezultati izvajanja varovanja? (4) Kako in če odmevni varnostni dogodki vplivajo na uspešnost poslovanja? (5) Ali se zaposleni na delovnem mestu počutijo varno? (6) Ali se stranke oz uporabniki počutijo varno? (7) Ali se prebivalci, ki živijo v neposredni bližini počutijo varno oziroma ali varnostne razmere v organizaciji vplivajo na kvaliteto njihovega življenja itd?

Strateško vodstvo mora neodvisni nadzor nad izvajanjem varovanja videti, kot dodano vrednost k poslovni funkciji. Menim, da s tovrstnimi nadzori lahko opozorimo na določeno problematiko pri izvajanju varovanja, kar na kratki rok prinese skrbi in dodatno delo odgovornih, na daljši rok pa boljše varovanje, višjo stopnjo varnosti in s tem boljše poslovanje. V tem kontekstu je potrebno nadzor gledati, kot na investicijo za izboljšanje varnosti in varnostnega sistema. Brez nadzora in presoje o ustreznosti, kakovosti in učinkovitosti izvajanja varovanja s strani neodvisne institucije, težko zadostimo varnostnim standardom, kaj šele varnosti. Organizacije, ki se poslužujejo nadzora, se s tem držijo znanega reka, in sicer, da je zaupanje dobro, nadzor pa še boljši.

Neodvisni nadzor, bi moral postati standard, ki bi ga podpirali tudi nadzorni sveti oziroma lastniki organizacije. Kakovost in uspešnost poslovanja ima veliko skupnega z varnostjo, bodisi da gre za storitveno, proizvodno ali drugo dejavnost. Brez učinkovitega zagotavljanja varnosti imajo organizacije lahko finančne težave. Seveda ni vedno varnost predpogoj za uspešno poslovanje, je pa pogosto pogoj za miren spanec odgovornih. Da bi glavno vodstvo pridobilo popolno sliko o učinkovitosti varovanja in varnostnem stanju v organizaciji, bi moralo vsaj dvakrat letno opraviti neodvisni nadzor nad delom varnostne službe ter merjenje zadovoljstva strank in zaposlenih. Poročilo o izvedenem nadzoru nad delom izvajalcev varovanja in rezultati meritev zadovoljstva, lahko odgovorijo na določena vprašanja ter dajo nove smernice za izboljšanje varnosti v organizaciji. Varnostniki so v prvi liniji v glavnem tudi "prva podoba organizacije" in operativni nosilci varnosti. Ali je v resnici res tako, zagotovo izveste z neodvisnim nadzorom.

Viri

- Gostič, Š., (2012). Zagotavljanje korporativne varnosti s pomočjo standarda ISO 28000:2007 – sistema za upravljanje z varnostjo. Revija Korporativna varnost str. 24-27, ICS Ljubljana.
- Gostič, Š., (2006) Inšpekcijski nadzor na področju zasebnega varovanja. Kriminalni napadi na premoženje gospodarskih subjektov. Pravna fakulteta, Fakulteta za policijsko-varnostne vede.
- Kovačič, A. (2007). Zunanji in notranji nadzor v zasebno-varnostni družbi. Diplomsko delo. Fakulteta za varnostne vede. Ljubljana.
- Sennewald, C. A. (1996), Security Consulting (Second Edition), Butterworth-Heinemann, Boston, Oxford.

[1] Organizacije se lahko poslužujejo različnih standardov, npr. standard ISO 28000:2007 – sistem upravljanja z varnostjo - Security management System ali standarde sprejmejo sami. ■

*avtor je član Slovenskega združenja korporativne varnosti

Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij.
Skozi združenje člani organizirano uresničujejo osebne in poslovne interese na področju korporativne varnosti.

Namen združenja je uresničevanje interesov članstva, ki so:

- združevanje znanja, izkušenj, interesov in razvojnih pogledov,
- pospeševanje razvoja izobraževanja in usposabljanja,
- razvoj mednarodno primerljivih korporativnih varnostnih standardov,
- izboljšanje kakovosti storitev na področju zagotavljanja korporativne varnosti,
- razvoj korporativnega varnostnega managementa,
- razvoj varnosti kot vrednote, ki izboljšuje pogoje dela in dviguje motivacijo.

»Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!«

»Ab uno disce omnes (po enem spoznaj vse)«

Članstvo v združenju je prostovoljno. Združenje ima redne, korporativne in častne člane.

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih strokovnih srečanjih;
- popusti pri nakupu izdanih publikacij ICS, Ljubljana;
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS, Ljubljana;
- brezplačna naročnina na revijo Korporativna varnost;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS-Ljubljana
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij katere so korporacijski člani združenja (korporacijski člani);

Več informacij je dostopnih na spletnih straneh www.ics-institut.si.

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

Avtorja: Gregor Dešman / Pošta Slovenije d.o.o.
Jure Marguč / Pošta Slovenije d.o.o





IZVAJANJE TESTOV INTEGRITETE V POŠTI SLOVENIJE d.o.o

Namen tega članka je predstavitev celovitega varnostnega sistema v Pošti Slovenije s poudarkom na zagotavljanju notranje varnosti in uvedbo testov integritete. V zvezi s tem nas bo zanimala predvsem uporabnost, učinkovitost in smiselnost vpeljave omenjenega testa v delovno okolje.

Celovito obvladovanje področja korporativne varnosti v podjetju poleg ukrepov fizičnega in tehničnega varovanja ljudi in premoženja zahteva tudi druge ukrepe, med katerimi so pomembni predvsem kadrovski in organizacijski ukrepi. Tudi v Pošti Slovenije d.o.o. (v nadaljevanju PS) uporabljamo takšne ukrepe za zagotavljanje varnosti, saj si brez njih celovite varnostne politike ne znamo predstavljati. Za PS sicer velja, da je podvržena različnim vrstam zunanjih in notranjih oblik ogrožanj ter poslovnih in varnostnih tveganj, ki jih lahko s skupnim izrazom imenujemo ogroženost poslovnega sistema.

Kriminalna ogroženost poslovnega sistema je tista, kateri v PS posvečamo še posebno pozornost. Med kaznivimi dejanji izvršenimi s strani tretjih oseb se največkrat pojavljajo ropi in roparske tatvine ter poškodovanja tuje stvari. Med kaznivimi dejanji, ki jih znotraj PS izvajajo zaposleni pa so najpogostejše zatajitve, ponarejanje listin, kršitev tajnosti občil, zloraba položaja in podobno. V zadnjem času v PS beležimo porast slednjih, ki v času nestabilnih družbenih, ekonomskih in gospodarskih razmer dosegajo velik razmah ter predstavljajo resen izziv na področju upravljanja s človeškimi viri. Za reševanje obstoječega stanja in navedene problematike smo v PS pristopili k sistemskemu reševanju nastale situacije, in sicer preko vpeljave različnih kadrovskih in organizacijskih ukrepov z uporabo katerih bi lahko preprečili, zmanjšali in obvladovali tveganja za nastanek škodnih dogodkov in kriminalnih dejanj povzročenih s strani zaposlenih.

Pomemben ukrep za zagotavljanje varnosti premoženja predstavlja uvedba testov integritete, kjer gre za povezanost varnostne in kadrovske funkcije z načini preverjanja integritete posameznika. V ozadju navedenega ukrepa je namreč prepričanost, da se med pomembne segmente varnosti v posameznem podjetju uvršča tudi ustrezna kadrovska politika, saj je iz varnostne perspektive pomemben izbor in spremljanje posameznikove integritete. Posamezniki z visoko stopnjo integritete naj bi namreč imeli dobro izoblikovana moralna in etična načela in so zaradi tega temelj stabilnosti podjetja.

Posamezniki z visoko stopnjo integritete naj bi namreč imeli dobro izoblikovana moralna in etična načela in so zaradi tega temelj stabilnosti podjetja.

Test integritete

Najprej je potrebno vedeti, kaj sploh integriteta je. V definiciji pojma integritete, ki je objavljena na spletni strani Komisije za preprečevanje korupcije je zapisano, da je integriteta celovitost, skladnost, pristnost, poštenost, verodostojnost. Organizacija z integriteto pa je organizacija, ki ima zaposlene osebe z integriteto, obenem pa deluje skladno z etičnimi normami, zapisanimi v etičnih kodeksih organizacij in veljavnim pravom.

Glede na pojasnjen pomen besede integriteta lahko test integritete opredelimo kot izmišljeno situacijo iz vsakdanjega delovnega življenja posameznika, usmerjenega v opazovanje vedenja delavca pri katerem je delavec izpostavljen priložnosti, da v okviru svojega dela in nalog, ki jih opravlja, ravna pravilno, zakonito in etično ali pa zlorabi zaupanje in ravna v nasprotju s pravili, neetično ali krši zakon.

V PS smo se osredotočili predvsem na izvajanje dveh vrst testa integritete, in sicer ciljni test in naključni test. Ciljni test integritete je namenjen točno določenim uslužbencem, ki so osumljeni zlorab. Pomaga potrditi ali ovreči pristnost obtožb oz. sumov o kriminalnem obnašanju posameznika. V primerih, ko

Odločitev o izvajanju testov integritete mora temeljiti na strokovnih in etičnih kriterijih, saj je uporaba slednjih smiselna le v primeru, če je široko sprejeta med zaposlenimi in kadar je cilj podjetja vzpostavitev varnega, prijetnega in poštenega delovnega okolja.

pa celotna enota kaže nagnjenost k odklonskosti pri opravljanju svojega dela, se izvede naključni test integritete. Če je preverjanje izvedeno na ta način in zaposleni z izvedbo testa niso seznanjeni, so lahko zbrani podatki zelo zanesljivi in lahko pomagajo natančno oceniti dejansko razsežnost kriminalnih aktivnosti znotraj izbrane skupine delavcev.

Namen izvedbe testa integritete je tako ugotoviti, ali bo delavec ali skupina delavcev v vnaprej ustvarjeni »fingirani« situaciji ravnal/a v skladu z zakonom in internimi pravili ali pa bo svoje dolžno ravnanje opustil, kršil pogodbo o zaposlitvi, ravnal neprofesionalno ali izvršil kaznivo ravnanje. Njegova uporaba je omejena le v primerih, ko z drugimi tehničnimi, organizacijskimi ali kadrovskimi ukrepi ni mogoče pričakovati zmanjšanja kriminalnih ravnanj. S testi integritete se ugotavljajo tudi dejanska varnostna tveganja pri izvajanju delovnih nalog, pri čemer se posebna pozornost posveča ugotavljanju tveganj za izvršitev kaznivega dejanja.

Teste integritete je potrebno uporabiti v dobri veri in vnaprej onemogočiti kakršnokoli zlorabo rezultatov testiranja predvsem v neetične namene, saj izvajanje slednjih ne sme vplivati na druge cilje korporacije kot je npr. zniževanje morale ali samozavesti zaposlenih. Odločitev o izvajanju testov integritete mora temeljiti na strokovnih in etičnih kriterijih, saj je uporaba slednjih smiselna le v primeru, če je široko sprejeta med zaposlenimi in kadar je cilj podjetja vzpostavitev varnega, prijetnega in poštenega delovnega okolja.



Izvajanje testov integritete v Pošti Slovenije

V področju korporativne varnosti in nadzora smo na podlagi opravljenih analiz podatkov o izginotjih trgovskega blaga v poštnih poslovalnicah, podatkov o izginotjih pisemskih in paketnih pošiljk ugotovili, da so izginotja pisemskih in paketnih pošiljk praktično stalnica, da so le redki primeri uspešno preiskani in da zaznavamo različna dejstva in okoliščine, ki kažejo na to, da so izginotja pošiljk posledica kriminalnih ravnanj zaposlenih. Zaradi navedenih dejstev smo se odločili za uvedbo ukrepa testa integritete, pri čemer smo upoštevali tako pravna kakor tudi etična načela. V zvezi s tem smo iskali širši konsenz znotraj podjetja, kjer smo teste integritete predstavili tako sindikatom kot svetu delavcev in pristopili k izdelavi notranjih aktov, ki določajo ukrepe in postopke s katerimi se ugotavlja pravilnost in zakonitost izvajanja delovnih postopkov. Slednje smo opredelili v Pravilniku o izvajanju testov za ugotavljanje pravilnosti in zakonitosti ravnanja in varnostnem preverjanju z uporabo poligrafske metode zaposlenih v Pošti Slovenije d.o.o. Z objavo Pravilnika v uradnem glasilu PS pa smo o uvedbi ukrepa seznanili celoten kolektiv podjetja.

Primeri uporabe testa integritete v Pošti Slovenije

Kršitev ustavno varovane pravice do tajnosti pisemskih pošiljk – izginotja pisemskih pošiljk.

V tem primeru je šlo za poštno poslovalnico, na kateri je bilo zaznanih več izginotij pisemskih pošiljk v katerih naj bi se po navedbah oškodovanih strank nahajala gotovina. Po zbranih podatkih in informacijah v sklopu notranje preiskave je obstajal sum, da je pismonoša te pošte večkrat storil kaznivo dejanje kršitve tajnosti občil po členu 139/1 in 5 KZ in s tem huje kršil pogodbo o zaposlitvi. Na podlagi rezultatov notranje preiskave in opravljenih analiz podatkov o izginotjih pisemskih pošiljk ter dejstva, da z drugimi tehničnimi, organizacijskimi ali kadrovskimi ukrepi ni bilo mogoče nedvoumno potrditi vpletenosti zaposlene osebe v kriminalno ravnanje oz. njene izločitve, smo se odločili izvesti ciljni test integritete. V skladu s pravili, ki opredeljujejo postopek izpeljave samega testa, smo v poštni promet oddali označeno pošiljko ter jo poslali na naslo-

ve, ki so del dostavnega okraja konkretnega pismonoše. Pri tem smo izključili morebitne dejavnike, ki bi lahko vplivali na dostavo pošiljke. Ker pošiljka ni bila dostavljena naslovniku, smo opravili pogovor s pismonošem z namenom, da se pojasnijo vsa varnostno relevantna dejstva in okoliščine v zvezi z izginotjem pisemske pošiljke. Na podlagi predloženih ugotovitev in dejstev je slednji priznal več odtujitev pisemskih pošiljk. Zoper konkretnega delavca so bili sproženi ustrezni delovno - pravni postopki ter podana kazenska ovadba.



Preverjanje ustreznosti ravnanja poštnih delavcev pri sprejemu gotovine

Uporaba testa integritete je primerna tudi za preverjanje ravnanja zaposlenih v skladu s predpisanimi delovnimi postopki. Na podlagi obvestil o unovčevanju ponarejenih evrskih bankovcev na poštah smo namreč ugotovili, da so v večini primerov ponaredki odkriti šele pri preverjanju pristnosti gotovine v trezorju in ne pri sprejemu na poštnem okencu. V tem primeru smo se odločili izvesti naključni test integritete z namenom ugotavljanja ustreznosti ravnanja poštnih delavcev pri poskusu unovčevanja ponarejenih bankovcev.

V okviru testa integritete smo v sodelovanju s kriminalistično policijo na poštnem okencu s ponarejeno gotovino plačevali blago ali gotovino menjali v menjalnici. Pri tem smo uporabili »očitne ponaredke« in ponarejene bankovce večje kakovosti. Pri izvedbi testa integritete, v katerega sta bili vključeni po dve pošti iz vsake poslovne enote PS, smo ugotovili, da delavci kljub poznavanju pravil, ki določajo postopek preverjanja pristnosti gotovine in ravnanje v primeru, da zaznajo poskus unovčevanja ponarejene gotovine, pri vsakdanjem delu v večini primerov veljavnih navodil niso spoštovali. Po izvedenem testu integritete se je stanje na tem področju občutno izboljšalo. Poleg tega pa so bili na podlagi ugotovitev in priporočil določeni dodatni organizacijski in kontrolni ukrepi.

Sklep

Na spremenjeno varnostno okolje se je morala prilagoditi tudi varnostna politika PS, ki se je tako poleg organizacije fizičnega in tehničnega varovanja ljudi in premoženja, proaktivno lotila tudi ukrepov s področja organizacijskih (notranji nadzor in notranje preiskave) ter kadrovskih ukrepov. Dokazilo o nekaznovanosti, preventivni varnostni razgovor, poligrafsko testiranje, usposabljanje zaposlenih na področju zagotavljanja varnosti premoženja in osebne varnosti so le nekateri izmed primernih ukrepov. Novost pri tem pa zagotovo predstavlja ukrep izvajanja testov integritete. Ena izmed temeljnih pozitivnih lastnosti testiranja integritete je predvsem ta, da se je test integritete v PS pokazal kot učinkovit preventivni ukrep pri zmanjševanju in obvladovanju posameznih tveganj. Že samo vedenje delavcev, da v Pošti Slovenije izvajamo aktivnosti na različnih področjih in segmentih delovnih procesov, preventivno vpliva na potencialno izvrševanje kaznivih dejanj, saj ocenjujemo, da morebitni storilci prav zaradi tega odstopijo od nameravane storitve kaznivega dejanja.

Vsaj pri nekaterih izmed naštetih ukrepov pa se odpirajo vprašanja zakonitosti, primernosti in sorazmernosti pri izvajanju takšnih ukrepov s ciljem, da delodajalec primerno poskrbi za varnost svojega premoženja. Glede strokovnega, pravnega in etičnega kriterija izvedbe testa integritete, pa mogoče kaj več v enem izmed prihodnjih člankov.

Že samo vedenje delavcev, da v Pošti Slovenije izvajamo aktivnosti na različnih področjih in segmentih delovnih procesov, preventivno vpliva na potencialno izvrševanje kaznivih dejanj, saj ocenjujemo, da morebitni storilci prav zaradi tega odstopijo od nameravane storitve kaznivega dejanja.

Viri

- Dobovšek B. (2012). Testi integritete in provokacija. Pridobljeno 31. 1. 2012.
- Interno gradivo Pošte Slovenije d.o.o.
- **Internetni vir**: Internet-1: http://www.kpk-rs.si/sl/korupcija-integriteta-in-etika/integriteta-in-etika ■

Avtor: Jože Grozde / Slovenska vojska*



RAZVOJ ZNANJA IN OBVEŠČEVALNA DEJAVNOST

Značilnost mednarodnega okolja je varnostna nestabilnost, kompleksnost in nepredvidljivost tako na političnem, okoljskem, gospodarskem in finančnem področju, ki se odraža v pestrem spektru kriz.

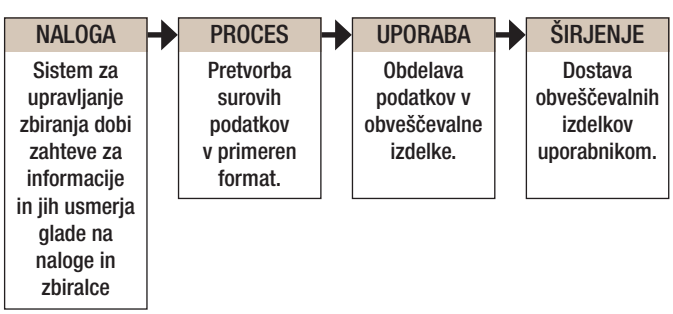
Dinamično globalno in nacionalno okolje narekuje organizacijam (tako v državnem, javnem in zasebnemu sektorju) nenehno prilagajanje nastalim spremembam. Niso dovolj samo organizacijske spremembe, ampak tudi učinkovito upravljanje in ustvarjanje organizacijskega znanja ob uporabi modernih informacijskih tehnologij kar ustvarja pogoje za konkurenčno prednost. Iskanje novih pristopov organizacij pri odzivanju na krizne razmere se odraža tudi pri iskanju novih rešitev pri delovanju obveščevalne dejavnosti. Obveščevalna skupnost je soočena z:

- organizacijskimi izzivi, ki so posledica sprememb v okolju delovanja,
- omejenimi viri (tako kadrovskimi kot finančnimi), ki lahko rušijo ravnovesje med viri in cilji,
- omejenim specialističnim znanjem (tako tehničnim kot družboslovnim),
- racionalizacijo delovanja, ki ustvarja generaliste (»specialiste širokega spektra«), hkrati obstajajo zahteve po kvalitetnih storitvah,
- velikansko množico (»hitro pokvarljivih in nezanesljivih«) podatkov in informacij,
- sodobnimi informacijsko telekomunikacijskimi tehnologijami, ki omogočajo hiter, enostaven in poceni dostop do množice podatkov in informacij,
- zahtevami uporabnikov po hitrem odzivanju na tveganja in obveščevalni podpori v »realnem času«.

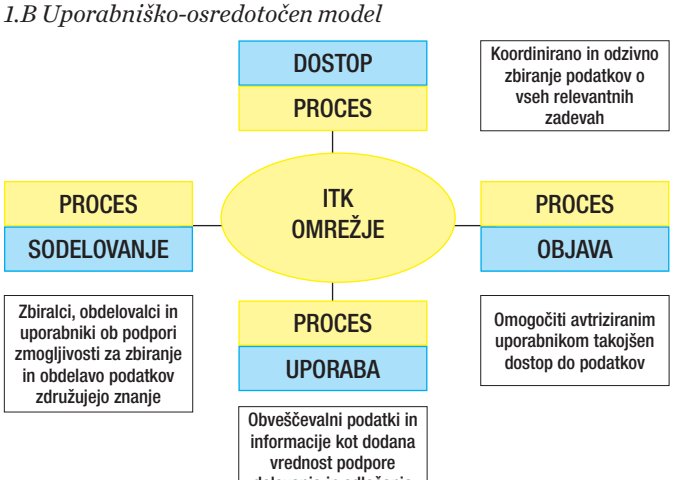
V tradicionalnem, produktno-osredotočenem modelu (zaprta arhitektura) obveščevalnega procesa, so podatki in informacije »v lasti« obveščevalnih organov. Na voljo so samo izbranim naročnikom-uporabnikom (slika 1.A). Uporabniško-osredotočen model (odprta arhitektura) je model prihodnosti, kjer je vloga uporabnika aktivnejša, saj po principu »potrebe po vedenju[1]« uporablja, nadgrajuje ali dopolnjuje obveščevalne produkte (slika 1.B). Ta koncept zahteva celovito upravljanje, sodelovanje in aktivnejše vključevanje tako uporabnikov kot obveščevalnih organov v celotnem procesu od zahteve, naloge, zbiranja, upravljanja vsebin, primerjave, uporabe, združevanja in analize (Herrington v Gutjar, 2005: 153).

Informacije niso znanje
in znanje ni modrost!
Albert Einstein

Slika 1: *Obveščevalni proces*
1.A Produktno-osredotočen model



1.B Uporabniško-osredotočen model

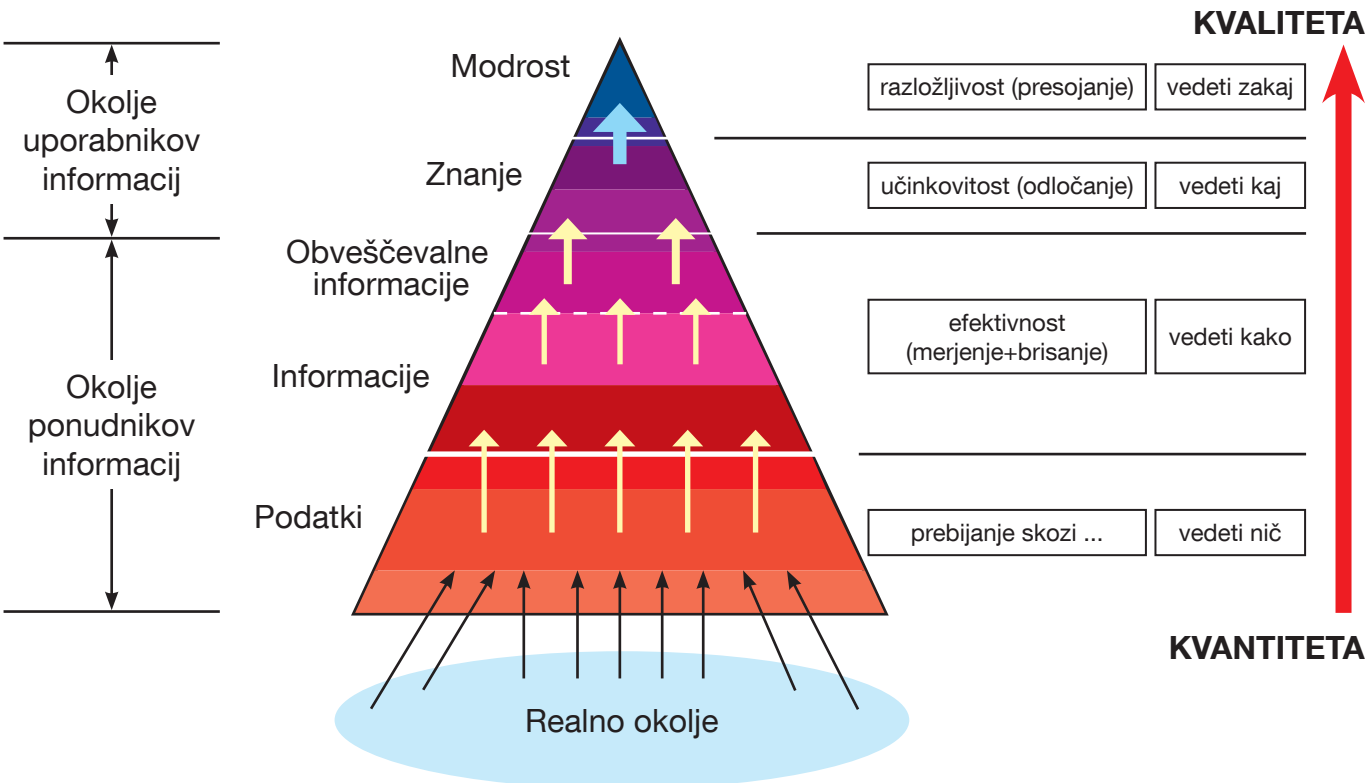


Vir: Herrington(2004 v Gutjar, 2005: 153).

*avtor je član Slovenskega združenja korporativne varnosti

Obstaja dilema ali je obveščevalni izdelek tudi znanje ali samo informacija. Odgovor je v Informacijski piramidi (slika 2), ki prikazuje da je graditev znanja proces zbiranja in obdelovanja množice podatkov v uporabno informacijo, ki uporabnikom pomaga pridobiti ustrezno znanje.

Slika 2: Informacijska piramida



Vir: Grozde, (2011, 59)

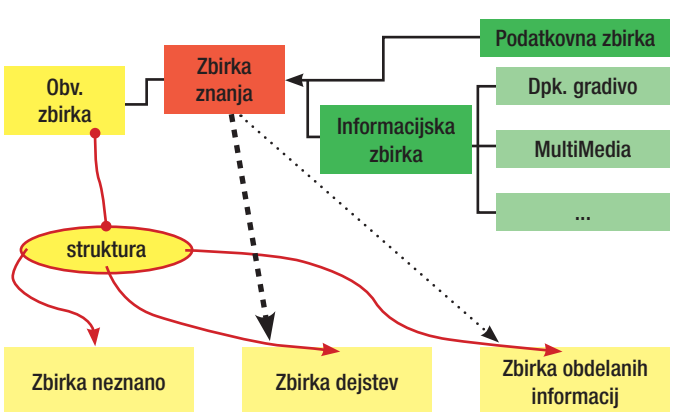
Obveščevalne informacije imajo dodano vrednost, zato so uvrščene v posebno kategorijo. Zeleny (v Grozde 2011, 59) je definiral podatke kot »vedeti nič«, informacije kot »vedeti kako«, znanje kot »vedeti kaj« in modrost kot »vedeti zakaj«.

Podatki, informacije in znanje se ukvarjajo s preteklimi dogodki oziroma sedanjostjo, prepoznavanjem vzročno/posledičnih odnosov, ki vplivajo na delovanje, obveščevalne informacije in modrost (odločanje) pa so usmerjeni v prihodnost z namenom doseganja najboljših odločitev ob najmanjšem varnostnem tveganju.

Na sliki 3 so prikazane povezave med različnimi zbirkami (bazami). Znanje se razvija, dejstva pa ostanejo nespremenjena, zato je pomembno, da jih organizacija hrani v zbirki dejstev, z namenom kasnejše obdelave z nadgrajenim znanjem. Obveščevalni izdelki in informacije so shranjeni v posebni zbirki, tako da je možno tudi kasneje oceniti njihovo vrednost. Enako velja tudi za zbirko znanja.

Pomembno je, da organizacija ve kaj »ve«, kajti le na tak način lahko ugotovi, kaj »ne ve« in kaj »bi rada vedela«. »Zbirka neznano« podpira upravljanje neznanega z namenom pridobiti nove podatke in informacije ter jih pretvoriti v obveščevalne izdelke.

Slika 3: Povezave med zbirkami



Vir: Marc Rabaeyin dr. (2006: 4)

Pomena znanja v procesih odločanja so se zavedali tudi v zvezi Nato, ki uvaja t.i. Celovit pristop načrtovanju operacij v podpori mednarodne skupnosti prireševanju kompleksnih kriz, ki poleg vojaških subjektov upošteva tudi druge udeležence na območju delovanja (ta pristop postopoma uvajajo tudi posamezne članice v svojih procesih odločanja).

Podatki, informacije in znanje se ukvarjajo s preteklimi dogodki oziroma sedanjostjo, prepoznavanjem vzročno/posledičnih odnosov, ki vplivajo na delovanje, obveščevalne informacije in modrost (odločanje) pa so usmerjeni v prihodnost z namenom doseganja najboljših odločitev ob najmanjšem varnostnem tveganju.

Celovit pristop uvaja novo področje »Razvoj znanja« (angl. Knowledge Development, v nadaljevanju RZ), ki pomeni prehod iz tradicionalnega reaktivnega k proaktivnemu pristopu procesu analiz območja delovanja. Proces »Razvoja znanja« vključuje procese zbiranja, analize znanja in dostopa po sistemu »Potisni-Povleci« (angl. Push-Pull), ki uporabnikom omogoči pridobivanje podatkov o vplivih vojaških, političnih, gospodarskih in civilnih dejavnikov na različne akterje ter sisteme na območju delovanja.

Obstaja veliko podobnosti med obveščevalnim procesom in RZ, vendar pa obstaja pomembna razlika v virih in metodah pridobivanja podatkov in informacij ter koraki v procesih dela. Obveščevalni proces ima štiri korake (usmerjanje, zbiranje, obdelava, posredovanje, proces RZ pa tri korake (zbiranje, analiza, dostop).

Tradicionalni pristop obveščevalne zagotovitve je temeljil na združeni obveščevalni pripravi območja delovanja, ki je ocenjeval predvsem njegove vojaške vidike. Obveščevalna dejavnost skozi proces obveščevalne zagotovitve s svojimi zmogljivostmi pridobivanja podatkov in v sodelovanju s partnerskimi organizacijami pripravi obveščevalno informacijo o virih ogrožanja ter tveganjih v določenem času in prostoru.

RZ pridobiva podatke in informacije o ciljnem območju ter njenih družbenih sistemih iz nevojaških virov, predvsem javnih virov in s tem presega področje vojaških obveščevalnih dejavnosti. Sistem analiz družbenih sistemov zahteva analitične sposobnosti, zanesljiv in kakovosten vir informacij, urejeno podatkovno zbirko in interdisciplinarno znanje. Glavni viri so različni civilni strokovnjaki in strokovne organizacije, mednarodne humanitarne organizacije in nevladne organizacije, zasebne in gospodarske ter nevladne organizacije in agencije itd, ki imajo dostop do različnih informacij.

V prispevku je prikazan proces razvoja obveščevalne dejavnosti, ki jih poleg dinamičnih sprememb v globalnem okolju narekuje tudi hiter razvoj informacijske tehnologije. Novost je uvajanje področja Razvoja znanja, ki poleg obveščevalne dejavnosti, postaja vse bolj pomemben element v procesih odločanja pri odzivanju na krize. Predstavljeno povezovanje obveščevalne dejavnosti, znanja in aktivnega uporabnika, je lahko tudi strokovni izziv v razvoju poslovnih procesov korporativne varnosti pri obvladovanju varnostnih tveganj v poslovnem okolju.

Sherman Kent, začetnik sodobne teorije obveščevalne dejavnosti, je že leta 1949 opredelil obveščevalno dejavnost kot znanje, proces in organizacijo (Herman v Grozde 2011:58). Njegova opredelitev je v današnjem času še kako aktualna.

Obveščevalno dejavnost čakajo v prihodnosti veliki strokovni in organizacijski izzivi, ki bi jih strnil v izrek Charlesa Darwina: »Ne preživijo najmočnejši niti najbolj inteligentni, ampak tisti, ki so najbolj dovzetni za spremembe.«

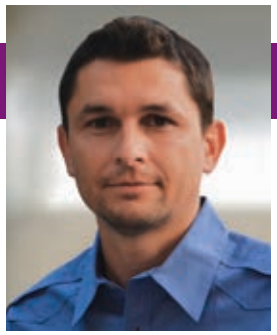
Literatura

- GROZDE, Jože, (2011). Obveščevalno vrednotenje geografskega prostora območij delovanj Slovenske vojske, zaključna naloga, Maribor, Ministrstvo za obrambo, SV, PDRIU, Poveljniško-štabna šola.
- GUTJAHR, Melanie M. H., (2005). The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era. The Joint Military Intelligence College
- RABAEY, Marc, LECLERCQ Jean-Marie, VANDIJCK Eddy, HOFFMAN Ghislain, TIMMERMAN Martin, (2007). Intelligence Base: Strategic Instrument of an Organisation. Bruselj, NATO.

1 Načelo potreba po vedenju ang. »need to know« ■



Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije-ICS, Ljubljana*



REPORTAŽA:
Beograd - mednarodna znanstvena konferenca

»NATIONAL CRITICAL INFRASTRUCTURE PROTECTION«

Institut za korporativne varnostne študije aktivno sodeloval pri soorganizaciji konference v Beogradu

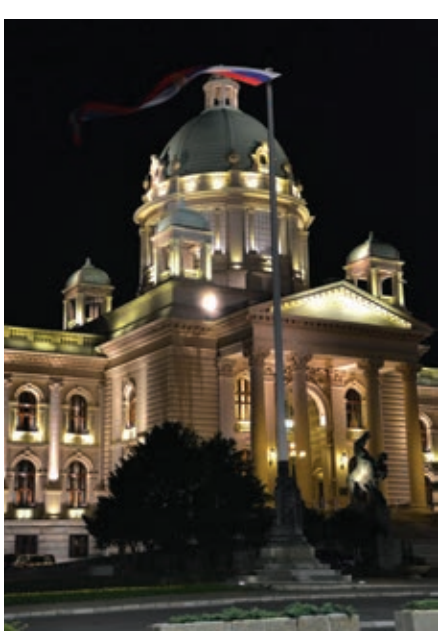
Fakulteta za varnostne vede v Beogradu je v sodelovanju z Gospodarsko zbornico mesta Beograd in ostalimi partnerskimi organizacijami - Inštitutom za korporativne varnostne študije iz Ljubljane, Ministrstvo za šolstvo, znanost in tehnologijo Republike Srbije in NIS Gazprom, 24. oktobra 2013 organizirala mednarodno znanstveno konferenco z naslovom »National Critical Infrastructure Protection – Regional Perspective«.

Zaščita nacionalne kritične infrastrukture (KI) je vedno bolj prepoznavna kot visoko tvegano področje in tako predstavlja eno od osnovnih elementov nacionalne varnosti vsake države. Ta konferenca je bila prva te vrste organizirana na področju Srbije, s ciljem krepitve nacionalnega zavedanja in regionalnega sodelovanja z vidika zaščite KI v državah Jugovzhodne Evrope. Na konferenci se je zbralo preko 100 strokovnjakov iz celotnega regijskega prostora.

Udeležence konference so nagovorili različni pomembni gostje, dr. Radomir Milašinović, dekan Fakultete za varnostne vede, dr. Jovan Bazić, pomočnik ministra za šolstvo, znanost in tehnologijo Republike Srbije, g. Predrag Marić, pomočnik ministra za notranje zadeve (MUP) in načelnik Sektorja za izredne razmere MUP, dr. Milan Janković, predsednik Gospodarske zbornice mesta Beograd, g. Dejan Pavlović, predstavnik Naftne industrije Srbije, dr. Tanja Miščević, glavna pogajalka za vstop Republike Srbije v EU in g. Nebojša Rodić, minister za obrambo RS, ki je odprl konferenco.

> Ta konferenca bi po mnenju ministra Rodića morala prispevati ne le k izmenjavi teoretičnih in praktičnih izkušenj, ampak tudi k spodbujanju sodelovanja med obstoječimi sistemi varovanja ključne nacionalne infrastrukture v Republiki Srbiji in sistemi v širšem regijskem prostoru.

V uvodnem nagovoru je minister Rodić poudaril, da je kritična infrastruktura del sistema, zaščita le te pa ključnega pomena za delovanje družbe. Škoda na kritični infrastrukturi, okvare ali uničenja, naravne nesreče, terorizem in organizirani kriminal ter druge oblike škodljivega vedenja, lahko nepopravljivo negativno vplivajo na varnost države in blaginje državljanov. Tako mora biti eden od glavnih ciljev države zmanjše-



*avtor je član Slovenskega združenja korporativne varnosti



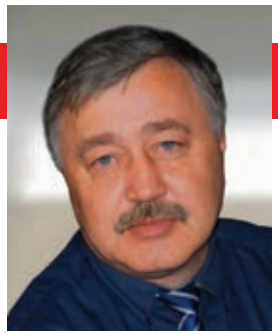
vanje ranljivosti in povečanje odpornosti nacionalne KI, je dejal obrambni minister in dodal, da je Evropa prepoznala vrsto potencialnih groženj in v ta namen pred petimi leti sprejela Direktivo o ugotavljanju in določanju evropske kritične infrastrukture ter oceno za izboljšanje njihove zaščite. Ta konferenca bi po mnenju ministra Rodića morala prispevati ne le k izmenjavi teoretičnih in praktičnih izkušenj, ampak tudi k spodbujanju sodelovanja med obstoječimi sistemi varovanja ključne nacionalne infrastrukture v Republiki Srbiji in sistemi v širšem regijskem prostoru.

Na konferenci so aktivno sodelovali tudi predstavniki Inštituta za korporativne varnostne študije iz Ljubljane (ICS) in člani Slovenskega združenja za korporativno varnost. Imeli so pomembno vlogo, ki je bila usmerjena v prenos dobrih praks in novih spoznanj. Na otvoritveni slovesnosti je udeležencem poleg najvišjih predstavnikov Republike Srbije spregovoril **dr. Denis Čaleta** (predsednik sveta ICS) in posebej izpostavil pomen tovrstnih dogodkov, kot odlično priložnost za tesnejše sodelovanje in izmenjavo novih izkušenj. Posebej je izpostavil slovenske izkušnje, kot dober primer graditve javno-zasebnega partnerstva, kot ključnega dejavnika za zagotovitev ustrezne zaščite KI v posamezni državi in regiji kot celoti. Konferenca je bila razdeljena v dva dela. V prvem so predstavili svoje prispevke strokovnjaki iz področja EU. Profesor dr. Ernst-Peter Döbbeling, University of Applied Sciences, je predstavil programe in trende na področju zaščite KI v EU, g. Khan Jahier je podal pogled na izbrano temo z vidika NATO, g. David Austin, British Standardization Institute pa nam je pokazal, kako vpliva neprekinjeno poslovanje na zaščito KI. V drugem delu so bila oblikovane tri sekcije z delovnimi naslovi: 1) sodobne varnostne grožnje in kritična infrastruktura, 2) kritična infrastruktura in politike, ter možnosti za zaščito in obvladovanje tveganj, ter 3) zaščita kritične infrastrukture s pomočjo kriznega vodenja in neprekinjenega poslovanja. V okviru konferenčne sekcije z naslovom »Contemporary security threats and critical infrastructure« je **g. Aleš Kotnik**, predstavnik Slovenskega združenja korporativne varnosti, predstavil predavanje na temo »Cyber threats and dilemmas of critical infrastructure protection in small states: Comparison between attacks in Georgia and Estonia«. Dr. Denis Čaleta je v nadaljevanju vodil in moderiral sekcijo z naslovom »Critical infrastructure protection through crisis and continuity management«, kjer se je zvrstilo pet zelo vsebinsko aktualnih predavanj.

V zaključku je bilo ugotovljeno, da kljub različnim pristopom k odpravi ali zmanjšanju nevarnosti za KI, obstoja skupni imenovalec v vseh družbenih strukturah nacionalnih in mednarodnih okvirjev. Imenovalec je potreba po sodelovanju, izmenjavi informacij, izkušenj in dobre prakse ter skupnimi usklajevalnimi organi na nacionalni in mednarodni ravni za učinkovitejše soočanje z grožnjami, katere v večini ogrožajo nemoteno delovanja kritične infrastrukture. ■



Avtor: Alojz Cestnik / Univerzitetni Klinični center Ljubljana*



NEKATERI VIDIKI VAROVANJA ZDRAVSTVENE ORGANIZACIJE

Najpomembnejši cilj varovanja je seveda varnost bolnikov, delovnih procesov in lastnine.

1. Načrt varovanja in vloga izvajalcev varovanja

1.1 Sistem upravljanja z odkloni

V zdravstvenih organizacijah se v zadnjem času uvaja sistem upravljanja z odkloni. Tu je pomembna vloga korporativno varnostnega managerja, ki poleg pooblaščenca za varnost pacientov, zaposlenih in drugih predstavlja pomemben člen v procesu zagotavljanja varnosti in vez med strateškim vodstvom ter vodstvom posameznih kliničnih oddelkov, služb itd. Izdelava ocene stopnje tveganja je temelj postavitve učinkovitega sistema varovanja. Varnostniki poleg splošnih nalog s področja varovanja opravljajo tudi in včasih predvsem naloge receptorjev-informatorjev. Kot pri vsakem drugem delu je tudi na področju varovanja zelo pomemben segment nadzora, tako samega dela varnostnikov, še bolj pa celotne varnostne situacije v organizaciji. V organizacijah se uporablja veliko osebnih podatkov, zaščiti katerim je potrebno posvetiti posebno pozornost. In končno se pri izvajanju varovanja pojavijo tudi etični problemi, ki so na področju zdravja še najbolj občutljivi.

Namen sistema je vzpostavitev čim višje stopnje varnostne kulture. Preko sistema upravljanja z odkloni želi organizacija s svojim delovanjem zagotavljati pacientom in njihovim bližnjim, sodelavcem, obiskovalcem in drugim dostojanstvo, kakovost in varnost. Cilj sistema upravljanja z odkloni je, da zaposleni preprečujejo, zaznavajo, prijavljajo, obravnavajo ter spremljajo ustreznost ravnanja v primeru odklona, kar bo doseženo:

- s celovitim obvladovanjem sistema upravljanja z odkloni,
- s spremljanjem vseh odklonov in njihovo obravnavo (strokovni varnostni zapleti, sumi na kaznivo dejanje, nasilje, pritožbe pacientov in njihovih bližnjih),
- z zmanjševanjem pojavnosti odklonov na najmanjšo možno mero s ciljnimi preventivnimi ukrepi, obdobnimi akcijami in sistemskimi rešitvami, ki izhajajo iz primerov dobrih praks.

Strokovno presojo ustreznosti ravnanja udeležencev v odklonih in iskanje sistemskih rešitev za odstranjevanje okoliščin, ki dopuščajo varnostne zaplete izvaja obdobno in v primeru izrednega dogodka takoj, stalna strokovna skupina, sestavljena iz strokovnjakov posameznih strok. Član stalne presojevalne skupine je tudi korporativno varnostni manager. Podatki pridobljeni preko sistema upravljanja z odkloni bistveno vplivajo na izdelavo ocene stopnje tveganja in posledično načrta varovanja.

1.2 Izdelava načrta varovanja zdravstvene organizacije

Pri izdelavi vsakega načrta varovanja zdravstvene organizacije moramo izhajati iz ocene stopnje tveganja. Obsegati mora predvsem razdelano in realno oceno možnih zunanjih in notranjih škodnih pojavov, ki lahko zmanjšajo možnost opravljanja storitev, zmanjšajo kvaliteto dela, povečujejo socialne probleme in krnijo ugled ustanove in posameznih uslužbencev.

Poleg zunanjih imamo tudi notranje škodne pojave, ki tudi lahko bistveno vplivajo na varnost organizacije in z njihovo pravilno oceno tudi na način in obseg organizacije varovanja. Izsledki raziskav, v zvezi s poštenostjo zaposlenih kažejo, da je približno ena tretjina poštena, ena tretjina delno poštena, ena tretjina nepoštena.

Pri izdelavi ocene seveda izhajamo iz vseh možnih škodnih pojavov, ki lahko vplivajo na varnost zdravstvene organizacije. Pri obdelavi jih razvrstimo glede na njihov vpliv, ter rezultatu primerno tudi organiziramo samo varovanje. Poleg možnih škodnih pojavov pa vsekakor ne smemo pozabiti na lokacijske in nekatere notranje elemente (razporeditev prostorov, lokacije skladišč, tehnične in ostale infrastrukture) organizacije. Vodstvo organizacije mora na osnovi svoje ocene stopnje tveganja in svoje poslovne politike sprejeti tudi varnostno politiko svoje organizacije in strategijo razvoja in izpopolnjevanja varnostnega sistema.

1.3 Lokacijska specifičnost izvajanja varovanja.

Objekti so grajeni v zelo različnih mikrolokacijskih razmerah. Navada je, da se novi objekti gradijo v urbanistično urejenih

*avtor je član Slovenskega združenja korporativne varnosti

Preko sistema upravljanja z odkloni želi organizacija s svojim delovanjem zagotavljati pacientom in njihovim bližnjim, sodelavcem, obiskovalcem in drugim dostojanstvo, kakovost in varnost.

okoljih, zunaj strnjenih mestnih jeder, vendar moramo največkrat upoštevati obstoječo lokacijo. Veliko je namreč zdravstvenih ustanov, ki so precej starejšega datuma in jih pač ni mogoče kar preseliti.[1] Pri izdelavi načrta varovanja moramo upoštevati notranjo razdelitev prostorov. Zelo so lahko ogroženi vitalni deli tehničnih postrojenj, ki so običajno locirani v kletnih etažah, ali v neposredni bližini objektov.

1.4 Specifičnosti varovanja zdravstvene ustanove

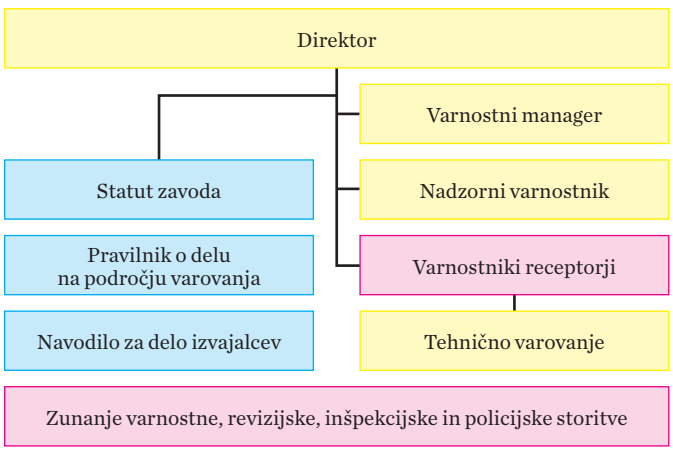
Frekvenca gibanja različnih ljudi je v zdravstvenih organizacijah izredno velika. Specifična je zaposlitvena struktura, od najmanj izobraženih do doktorjev znanosti, prihajajo bolniki z raznovrstnimi potrebami in željami, ter njihovi svojci. Zdravstvene organizacije so kot vse druge javne ustanove večinoma odprtega tipa, pa naj bodo javne ali zasebne. Kdo lahko omeji dostop do izbranega zdravnika ali prepreči občanu zagotovljeno zdravstveno pomoč. To ni varnostnik, ki nikakor ni strokovnjak s področja medicine. Ravno tako ni usposobljen da izvaja triažo torej, da odloča katera poškodba ali indikacija bolezni je nujna in katera ni. To je v domeni medicinske stroke. Vendar se varnostnik v zdravstveni organizaciji pri svojem delu dnevno srečuje s podobnimi primeri.[2] Pomembno je poudariti, da delo v zdravstvenih organizacijah poteka neprekinjeno 24 ur na dan in vse dni v letu, kar pomeni tudi večje tveganje.

1.5 Varnostnik v zdravstveni ustanovi kot varnostnik - informator - receptor

Naloge varnostnika v zdravstveni organizaciji niso okvirjene samo v tipično delo varnostnika, temveč se vsakodnevno srečuje z množico različnih ljudi, ki potrebujejo njegove usluge. Človek, ki prvič ali občasno pride v neko ustanovo se pač obrne na prvo osebo, ki nekako predstavlja ustanovo in od njega pričakuje korektno in popolno informacijo, ki jo želi. Seveda je ta oseba na vhodu običajno varnostnik. Njegove informacije morajo torej biti natančne in popolnoma točne. V kolikor mu niso takoj dostopne se mora potruditi, da ustrezno informacijo pridobi in s tem ustreže stranki. Torej ne predstavlja le človeka, ki varuje objekt, temveč tudi receptorja in predvsem informatorja. Seveda pa varnostnika podajanje različnih informacij ne sme ovirati pri njegovem osnovnem delu - varovanju in s tem zmanjšanju škodnih pojavov.

1.6 Organizacija nadzora izvajanja varovanja

Izvajanje kateregakoli procesa je brez pomena, če ni učinkovitega nadzora. Nadzor mora biti popoln in predvsem korekten. Nadzor je lahko opredeljen kot dvodelni, torej nadzor nad samim fizičnim varovanjem in nadzorom varnostne situacije v sami organizaciji. V največjih primerih je izvajalec fizičnega varovanja zunanja pogodbena organizacija, ki tudi izvaja nadzor nad delom svojih neposrednih izvajalcev, nadzor nad varnostnimi razmerami na posameznih enotah pa mora izvajati notranja kontrola. Delo nadzornega varnostnika ni le varovanje določenega delovnega mesta, temveč obvladovanje celotne varnostne situacije določene institucije. S tem presega običajen nadzor nad delovanjem fizičnega in tehničnega varovanja, ter predstavlja srce in dušo življenja "hiše", v smislu varnosti. Za lažjo predstavo si v skici št. 1. oglejmo primer strukture varnostnega sistema zdravstvene ustanove, ki nam prikaže tudi razmerja med posameznimi nosilci in izvajalci varovanja. Barvno lahko ločimo zaposlene v ustanovi (rumeno) in pogodbene in zunanje sodelavce (rdeče).



Skica 1. *Struktura varnostnega sistema zdravstvene organizacije*

2. Varovanje osebnih podatkov

Velik poudarek pri varovanju zdravstvenih organizacij moramo posvetiti varstvu osebnih in drugih podatkov ter dokumentarnega gradiva. Podatki nastajajo v celotnem procesu zdravljena in z njimi pride v stik veliko zaposlenih od zdravnikov, medicinskih sester, in tudi ostalih uslužbencev. Podatki se hranijo in pošiljajo v pisni obliki ali prek elektronskih medijev. Tako uporabo podatkov pa je potrebno tudi ustrezno zavarovati.

3. Etični problemi

Etika je nauk o tem kaj je dobro in prav. Že v 4. stoletju pred našim štetjem je Hipokrat napisal znano Hipokratovo prisego. V njej so zbrana načela, katerih se morajo zdravniki in drugi zdravstveni delavci držati pri opravljanju svojega poklica. Temeljna načela veljajo še danes. Delati samo po zakonu je v zdravstvenih institucijah premalo. Medicinske sestre in zdravstveni tehniki Slovenije so leta 2010 sprejeli svoj kodeks etike, po katerem so se dolžni ravnati. Nekatere določbe tega kodeksa pa veljajo tudi za ostale delavce v zdravstvu.

4. Zakjuček

Upam, da je pričujoči članek uspel prikazati nekatere specifičnosti varovanja zdravstvene organizacije in bo pripomogel k večji varnosti v našem zdravstvu. Žal na področju varovanja zdravstvenih organizacij v Sloveniji za enkrat še ne obstajajo standardi, ki bi poenotili delovanje. Uredba o obveznem organiziranju varovanja določa le nekaj organizacij, ki so zavezane



k uvedbi varovanja, večina pa je prepuščena iznajdljivosti in dovzetnosti posameznih direktorjev. Za dober in učinkovit se je izkazal sistem upravljanja z odkloni, katerega so uvedli v UKC Ljubljana in že daje posamezne rezultate. Menim, da je nujno zdravstvene organizacije predvsem na sekundarni in terciarni ravni opredeliti tudi kot kritično infrastrukturo, kar bi razširilo krog obveznikov organiziranja varovanja. Pomembno je, da vodilni in odgovorni v zdravstvu spoznajo, da je varovanje v njihovo prid in ne izgubljeni denar.

Viri

- Cestnik A. (2000). Normativna ureditev obveznega organiziranja varovanja. Zbornik posveta Portorož 2000, 181-188
- Kodeks etike medicinskih sester in zdravstvenih tehnikov Slovenije Ur. List RS št. 40/2010
- Vršec M.(1993). Varnost podjetja - tokrat drugače. Ljubljana. Viharnik
- Zakon o varstvu osebnih podatkov Ur. List RS št. 17/2011
- Zakon o zasebnem varovanju Ur. list RS št. 17/2011
- Uredba o obveznem organiziranju varovanja Ur. List RS 80/2012
- Pravilnik o sistemu upravljanja z odkloni v UKC Ljubljana, 2008.

Delo nadzornega varnostnika ni le varovanje določenega delovnega mesta, temveč obvladovanje celotne varnostne situacije določene institucije.

1 Odklon - pomeni odmik od normalnega, pravega, kot so različne oblike nasilja, neželeni dogodek, varnostni zaplet, sum na kaznivo dejanje in drugo.

2 Kot primer lahko navedemo Klinični center Ljubljana, kjer ena glavnih mestnih ulic (Zaloška cesta) poteka skozi središče bolnišnice.

3 Omenjeni primeri so največkrat pojavijo pri varnostnikih na delovnih mestih pri urgentnih blokih, predvsem v primerih, ko so tam postavljene zapornice in je pri svojem vsakdanjem delu prisiljen izvajati laično triažo. ■

Avtor: asist. mag. Simon Starček / Davčna uprava Republike Slovenije



KORPORATIVNA VARNOST NA PODROČJU SPLETNEGA IGRALNIŠTVA

Z razvojem računalništva, sodobnih tehnologij in predvsem svetovnega spleta lahko v zadnjih dveh desetletjih govorimo o revoluciji na področju iger na srečo. Igralniška dejavnost postaja vse bolj prepletena s številnimi drugimi gospodarskimi panogami ali celo usmerja ter vzpodbuja njihovo rast in razvoj.

Igre na srečo, ki predstavljajo sicer posebno vrsto tveganj, so po ugotovitvah raziskav prisotne vse od starih civilizacij izpred več kot šest tisoč let (Schwartz, 2006; Ferentzy in Turner, 2013). Skozi zgodovino so se spreminjale in razvijale oblike organiziranja in vrste iger na srečo, njihovo dojemanje in namen prirejanja (Binde, 2005). V zadnjih 50-tih letih je igralništvo prerastlo v izjemno pomembno gospodarsko panogo. Za to obdobje je značilna vrsta pomembnih sprememb. V sedemdesetih letih prejšnjega stoletja je sprožen val liberalizacije zakonodaje na področju iger na srečo, številne države so sistem prepovedi prirejanja iger na srečo preoblikovale v sistem pridobivanja sredstev za javno dobro (Gainsbury, 2012). Razvijati so se začeli veliki igralniški centri in uporabljati igralne naprave, ki temeljijo na generiranju naključnih števil.

Razvoj in obseg spletnega igralništva

Ponudba iger na srečo se nezadržno širi. Liberalizacija pomembnih trgov v Evropi (Italija, Francija, Španija, Velika Britanija idr.) in svetu ter svetovni splet sta igralniško dejavnost pripeljala domala v sleherni dom. Igralniška ponudba je postala vse bolj prilagodljiva potrebam potrošnikov in hitro izkorišča priložnosti, ki jih ponuja širitev na nove trge sveta (Kitajska, Indija, Afrika, Južna Amerika). Učinkovito izkorišča razvoj novih tehnologij, predvsem mobilne telefonije, pametnih telefonov, tablic in televizije. Številni televizijski kanali in milijone spletnih strani nam vsak dan ponujajo najrazličnejše podatke o dogodkih, na katere je moč staviti oz. z njihovo pomočjo oblikovati strategije igranja. Na voljo so 24 urni televizijski programi za spremljanje igre poker idr.

Izraz »spletne igre na srečo« zajema številne različne igre na srečo. Te vključujejo spletne športne stave, vključno s stavami na konjskih dirkah, igralniške igre, stave na razliko (spread betting), medijske igre, promocijske igre, igre na srečo, ki jih organizirajo priznane dobrodelne in neprofitne organizacije, ter loterije. Svetovni splet (in druge interaktivne tehnološke platforme, kot je mobilno poslovanje ali IPTV) se uporabljajo za nudenje iger na srečo potrošnikom, omogočanje potrošnikom, da stavijo ali igrajo na srečo en proti drugemu (npr. stavne borze ali spletni poker) ali kot tehnika za distribucijo (npr. za nakup loterijskih lističev neposredno prek spleta) (Evropska komisija, 2011; Gainsbury, 2012).

Opredelitev pojma spletne igre na srečo se med posameznimi državami razlikuje. Splošno sprejeta definicija spletne igre na srečo na ravni Evropske unije pravi, da so »spletne igre na srečo vse storitve, ki vključujejo denarne vložke v igre na srečo, vključno z loterijskimi in stavnimi transakcijami, ki se zagotavljajo na daljavo, prek elektronskih sredstev in na posamezno zahtevo prejemnika storitve.« (Evropska komisija, 2011)

Začetek spletnih iger na srečo sega v prvo polovico devetdesetih let prejšnjega stoletja (z vzpostavitvijo spletne strani švicarske loterije Loterie Romande septembra 1993) in sovpada z začetkom hitre rasti uporabe računalnikov, komercializacije in razvoja svetovnega spleta ter spletnih storitev (Girdwood, 2002; Campbell, 2003).

Spletne igre na srečo so v letu 2000 ustvarile 2,2 milijardi dolarjev bruto prihodka, tj. vložek, od katerega se odštejejo nagrade, vendar vključuje bonuse (Gross Gaming Revenues). Leta 2006 je bruto prihodek znašal 15,2 milijardi

dolarjev, v letu 2010 pa že 24,5 milijarde. V letu 2013 se predvideva, da bo bruto prihodek presegel 40 milijard dolarjev, ob napovedani 12 % do 15 % letni rasti prihodkov v prihodnje. Med prihodki je 39 % delež stav, 26 % prispevajo spletni casinoji, spletni poker 14 %, loterije 9%, bingo 8 % in 4 % spretnostne igre. Evropa predstavlja največji trg spletnega igralništva (47 %). Razmerje se ob procesu liberalizacije zakonodaje intenzivno spreminja. Ključni trgi postajajo Severna in Latinska Amerika, Kitajska, Bližnji in Srednji Vzhod. Na razvoj novih trgov pomembno vpliva tudi dostopnost svetovnega spleta, razvitost mobilne tehnologije in varne metode plačevanja (Gainsbury, 2012). Podatki potrjujejo, da je spletna ponudba najhitreje rastoči del trga iger na srečo.

Pomen korporativne varnosti ponudnikov spletnih iger na srečo

Vse večje število sodelujočih v spletnih igrah na srečo, hitra rast prihodkov, vse večja želja po hitrem zaslužku vodi do pojava številnih, tudi novih oblik tveganj tako na strani ponudnikov spletnih iger na srečo, kot udeležencev (igralcev). Ponudniki spletnih iger na srečo v svojem poslovnem modelu zaokrožajo številne kompleksne tehnološke in poslovne procese, povezane z visokimi zahtevami varnosti (varstvo osebnih podatkov, varne finančne transakcije idr.),



Učinkovito orodje za obvladovanje obstoječih in novih tveganj v tovrstnih družbah predstavlja integralni varnostni sistem, ki obsega dejavnosti in medkulturnemu okolju prilagojeno varnostno politiko, načrt varovanja za posamezne poslovne procese, oceno ogroženosti in tveganj, zaščito zaupnih podatkov, informacij in znanja.

neprekinjenega poslovanja, tehnološke združljivosti, družbene odgovornosti, učinkovite obravnave pritožb idr. Pogosto delujejo čezmejno, v različnih zakonodajnih in kulturnih okoljih, s ponudbo svojih storitev 24 ur na dan, 365 dni v letu. Ob tem tovrstna podjetja svoje procese izvajajo s številnimi zunanjimi podpornimi funkcijami (telekomunikacije, marketing, varovanje, nadzor nad dogodki idr.). Domala celoten poslovni model je prilagojen poslovanju na spletu in s tem izpostavljen vrsti sodobnih oblik tveganj. Zato je ustrezna oblika korporativne varnosti oz. varnostnega sistema v podjetju ključnega pomena za učinkovito obvladovanje varnostnih in drugih tveganj ter odzivov na zahteve okolja. Ponudniki spletnih iger na srečo morajo skozi preplet pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov skrbeti za stabilnost in hitro prilagodljivost poslovnega sistema, spoštovanje različne in spremenljive nacionalne zakonodaje v državi, kjer ponujajo svoje storitve, internih predpisov in varnost premoženja podjetja. Učinkovito orodje za obvladovanje obstoječih in novih tveganj v tovrstnih družbah predstavlja integralni varnostni sistem, ki obsega dejavnosti in medkulturnemu okolju prilagojeno varnostno politiko, načrt varovanja za posamezne poslovne procese, oceno ogroženosti in tveganj, zaščito zaupnih podatkov, informacij in znanja. Ob tem mora biti poseben poudarek na učinkovitem upravljanju z informacijsko varnostjo, stalni skrbi za varnostno kulturo ter fizično in tehnično varovanje. Prav varnost in stabilnost poslovanja so v tej hitro rastoči gospodarski panogi ključni dejavnik konkurenčnosti, ki se v pomembni meri zagotavlja skozi ustrezen sistem notranje varnosti.

Podjetja na področju spletnega igralništva zaradi svoje specifične oblike dejavnosti, čezmejnega poslovanja, visoke izpostavljenosti najrazličnejšim oblikam kriminala idr. soočajo z vrsto zunanjih in notranjih tveganj, kot so:

- tehnološka: vdori v igralniški sistem, motnje v delovanju spletnih povezav, nedelovanje finančnih transakcij, nekakovostno preverjanje identitete igralcev idr.;
- človeška: nezadovoljstvo zaposlenih, sabotaže, igralniške in druge goljufije, kraja razvojnih in zaupnih podatkov ter informacij, kraja identitete igralca, prirejanje rezultatov dogodkov;
- naravna: odpovedi športnih dogodkov zaradi vremenskih dejavnikov;
- druga: državna zakonodaja, ekonomsko-finančne in politične razmere, motnje na strani dobaviteljev idr.

V okviru korporativne varnosti mora biti dan poseben poudarek varnosti podatkov, varnosti v procesu izvedbe plačil, varnosti kompetenc zaposlenih in igralcev ter varnosti sklada za dobitke (Mingnan et al, 2012). Pri svojem poslovanju in razvoju tovrstna podjetja uporabljajo najrazličnejša orodja, metode, standarde, priporočila in dobre prakse za učinkovito obvladovanje tveganj, ki izhajajo iz poslovnih okolij tradicionalnega igralništva. Ob tem je pomembno, da poslovne procese obvladujejo v skladu z mednarodnim standardom ISO



9001:2008. Glede na tehnološko zahtevnost poslovnih procesov predstavljajo standardi družine ISO 27000 ustrezno podporo učinkovitemu upravljanju informacijske varnosti. Na področju zagotavljanja neprekinjenega poslovanja se priporoča uporaba mednarodnega standarda ISO 22031:2012 (Societal security – Business continuity management systems), ki spletnim ponudnikom iger na srečo pomaga pri spremljanju, vzdrževanju in nenehnem izboljševanju okolja za obvladovanje incidentov. Ob rasti števila uporabnikov spletnih iger na srečo je ob zagotavljanju varnosti in poštenosti poslovanja, ključna konkurenčna prednost ustrezna podpora igralcem in učinkovita obravnava njihovih pritožb. Podjetja se ob tem naslanjajo na priporočila standarda ISO 10002:2004 (Zadovoljstvo odjemalcev – Smernice za ravnanje s pritožbami v organizacijah). Za prireditelje spletnih iger na srečo so vse pomembnejša tudi priporočila standarda ISO 26000:2010 (Napotki za družbeno odgovornost) na vseh ključnih področjih družbene odgovornosti: organizacijsko upravljanje, človekove pravice, delovne prakse oziroma sodelovanje z zaposlenimi, naravno okolje, poštene prakse poslovanja, odnos do potrošnikov in vključenost v lokalno okolje in njegov razvoj. Na tem temelji tudi certifikat odgovornega igralništva Evropskega loterijskega združenja.

Zaključek

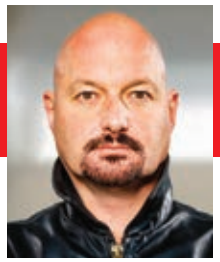
Cilj sodobnih pravnih ureditev je zaščititi potrošnike (pred goljufivimi ponudniki storitev in ponudniki storitev, vključenimi v kazniva dejanja), ponudnike storitev (pred goljufivimi igralci ali združbami igralcev) ter organizatorje prireditev. Zato k uporabi omenjenih orodij prireditelje spletnih iger na srečo spodbujajo ali zavezujejo tudi številne nacionalne zakonodaje. Kot odziv na zahteve sodobnega okolja so reprezentativna združenja (npr. Evropsko in svetovno loterijsko združenje) oblikovala panožne standarde poslovanja. Le-ti slonijo na uveljavljenih mednarodnih standardih, pri čemer še podrobneje opredeljujejo posamezne aktivnosti za učinkovitejši sistem korporativne varnosti in obvladovanja tveganj. WLA-SCS:2012 (Security Control Standard) predstavlja mednarodno priznan standard na področju varnosti v igralništvu. Obravnava področje nadzora varnosti, integritete in notranjih kontrolnih mehanizmov, ki slonijo na zahtevah ISO 27001:2005. Ob tem vsebuje še 90 posebnih zahtev temelječih na najsodobnejših praksah na področju igralniške varnosti.

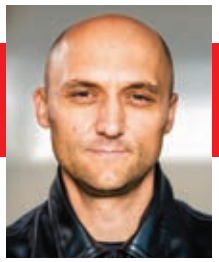
Ob nezadržnem razvoju tehnologije, novih komunikacijskih oblik in poti, rasti števila igralcev, njihovih kompetenc, kibernetske in druge z igralništvom povezane kriminalitete, zahteva od prireditelj ev spletnih iger na srečo, tako vrhnjega vodstva kot ostalih zaposlenih, redno vzdrževanje in posodabljanje varnostnega sistema ter dviga organizacijske kulture, kulture tveganj in varnostne kulture nasploh.

Viri:

- Binde, P. 2005. Gambling, Exchange Systems, and Moralities. Springer: Journal of Gambling Studies, 21 (4): 445–479.
- Campbell, J. 2003. Regulating Internet Gambling: Is It Really a Game of Craps?
- Evropska komisija. 2011. Zelena knjiga o spletnih igrah na srečo na notranjem trgu. SEC(2011) 321 konč. Bruselj: Evropska komisija.
- Ferentzy, P., Turner, N. 2013. The history of problem gambling. Temerance, Substance Abuse, Medicine, and Metaphors. Springer: 174 str.
- Gainsbury, S. 2012. Internet Gambling. Current Research Findings and Implications. Springer: 153 str.
- Girdwood, R. S. 2002. Place Your Bets... on the Keyboard: Are Internet Casinos Legal? Campbell Law Review, 25: 135–150.
- Mingnan Y., Hongliang Z., Lingjun H.. 2012. Research on Security Issues of Internet Lottery Sales V: Affective Computing and Intelligent Interaction, AISC 137. Luo, J. (ur.). Berlin, Heidelberg: Springer-Verlag: 815–821.
- Schwartz, D. (2006). Roll the bones. New York: Gotham Books. ■

Avtorja: Mag. Marko Potokar / ju-jitsu trener*
Andrej Kovačič / inštruktor fitnesa*





FIT ZAPOSLENI - DODANA VREDNOST KORPORATIVNI VARNOSTI V ORGANIZACIJAH

Skrb za varnost in vadbeno aktivnost je v uspešnih organizacijah eno od glavnih načel politike pri njihovem vodenju, ter novost pri njeni korporativni varnosti.

Uvod

Promocija zdravega in aktivnega življenja v poslovnem svetu je pri nas dokaj novo področje. Evolucija je človeka ustvarila za gibanje, zato je za ohranjanje zdravja pomembno, da poskrbimo za osnovne potrebe organizma tudi na delovnem mestu. Negativne posledice za naše počutje in zdravje imajo tudi določeni dejavniki na delovnem mestu. V zadnjem času se organizacije čedalje bolj zavedajo, kako pomembni so zdravi in motivirani zaposleni, zato so že pripravljeni sprejemati določene ukrepe za izboljšanje njihovega psihofizičnega stanja.

Zdravje in dobro počutje zaposlenih imata vpliv na kakovost storitev in izdelkov, varnost in zadovoljstvo strank. Dobra psihofizična kondicija je eden izmed pogojev za učinkovito delo. Redna vadba povečuje intelektualne sposobnosti človeka. Dobra kondicija in boljše zdravje posledično pomeni tudi manj bolniških odsotnosti z dela. Zaposleni, ki izvajajo redno vadbo in vzdržujejo dobro telesno kondicijo so tudi manj občutljivi na negativne posledice stresa. Pri zagotavljanju zdravega in varnega delovnega okolja pa so z vidika varnosti in zdravja pomembne tudi varnostne organizacije. Pri opravljanju varnostnih nalog morajo zaposleni (policisti, pazniki, varnostniki itd) znati poskrbeti tako za lastno varnost, kot za varnost udeležencev v obravnavanih postopkih. V teh strukturah morajo biti zaposleni dodatno ustrezno usposobljeni za opravljanje svojih nalog.

> Organizacije, ki imajo zaposlenega strokovnjaka za varnost oziroma varnostnega managerja, ki je zraven še dodatno usposobljen in licenciran za delo na področju športa (inštruktor, trener ipd), lahko njegova znanja pridejo prav za vzpostavitev sistema za ohranjanje psihofizične kondicije zaposlenih.

Skrb organizacije za psihofizično pripravljenost zaposlenih

Telesna vadba in fitnes programi imajo pomembno vlogo v organizacijah, kjer spodbujajo zaposlene k redni vadbi za doseganje visoke ravni dobrega počutja. Poleg fizičnega izboljšanja, telesna vadba vpliva na zmanjšanje stresa in nosi osebni občutek odgovornosti za zdravje na ostalih področjih življenja, kot so prehrana, nadzor teže itd.

Organizacije, ki imajo zaposlenega strokovnjaka za varnost oziroma varnostnega managerja, ki je zraven še dodatno usposobljen in licenciran za delo na področju športa (inštruktor, trener ipd), lahko njegova znanja pridejo prav za vzpostavitev sistema za ohranjanje psihofizične kondicije zaposlenih. Organizacija lahko ustanovi delovno skupino za promocijo telesne vadbe in zdravja, katere nosilec je varnostni manager. Delovna skupina deluje znotraj organizacije in načrtuje, spremlja, implementira ter vrednoti vse aktivnosti zaposlenih na tem področju. Delovno skupino v glavnem sestavljajo zaposleni, katerim je vadba že način življenja in ti lahko postanejo promotorji znotraj organizacije.

*avtor je član Slovenskega združenja korporativne varnosti

Glede na organizacijo, delo v njej in na želje zaposlenih se lahko omogoči način vadbe po principu vojaškega fitnesa (Military fitness). Gre za skupinsko vadbo, ki vpliva na izgubljanje odvečne maščobe, pridobivanje fizične kondicije in izboljšanje splošnega počutja. Gre za serijo aktivnosti, pri katerih udeleženci med seboj tekmujejo, kdo jih opravi v najkrajšem možnem času oziroma hitreje kot soudeleženec. Pri tej vadbi se krepi skupinski duh in medsebojno sodelovanje pri premagovanju ovir, saj se le-ta lahko izvaja skupinsko.

Zelo koristna je tudi funkcionalna vadba, kjer gre za krepitev celotnega telesa. Vadba se izvaja s pomočjo lastne teže, uteži, elastičnih trakov in ostalih vsakodnevnih pripomočkov. Pri tej vadbi vključimo večje število mišičnih skupin in tako dosežemo visoko porabo kalorij, večjo vzdržljivost ter pospešeno presnovo.

Zaposleni naj imajo organizirane aktivne odmore, namenjene gibanju in izvedbi izbranih telesnih vaj. Tistim, ki so dejavni v tekmovalnem športu je smiselno omogočiti pogoje za specialno izvajanje vadbe. Vsem, ki so redno telesno dejavni, je zaželeno omogočiti nekoliko podaljšan odmor za malico/kosilo, tako da bodo imeli čas za gibanje in zdrav obrok po njem. Organizacija naj vzpostavi sistem nagrajevanja zaposlenih, ki temelji na aktivnostih, ki jih posamezniki pogosto izvajajo, upošteva pa tudi tiste, ki so redno telesno aktivni, ohranjajo fizično kondicijo oziroma z njo napredujejo. Uvede se lahko razglasitev zaposlenega meseca oziroma tistega, ki je najboljši primer dobre prakse v določenem mesecu in razstavi njegovo fotografijo, mu podeli certifikat, denarno nagrado ipd. Posameznikom naj bo dovoljeno, da nekajkrat na mesec vzamejo dodatne pol ure prosto med časom kosila za hojo, tek, plavanje, obisk fitnesa itd. Za spodbujanje zdravega načina življenja naj organizacija zagotovi prostor za fitnes, športno igrišče ali športno dvorano za zaposlene oziroma s popusti pri obiskih zaposlenih v lokalnih športnih klubih.

Psihofizična pripravljenost in znanje borilnih veščin zaposlenih na področju varovanja*

Poseben pomen ima psihofizična pripravljenost za zaposlene, ki opravljajo delo na področju varovanja ljudi in premoženja. Poleg uradnih oseb (policisti, kriminalisti, pazniki itd) in oseb s posebnimi pooblastili (zasebni varnostniki, telesni stražarji, redarji) mednje sodijo tudi vsi zaposleni, ki funkcijo varovanja izvajajo v sklopu svojih rednih delovnih nalog (receptorji, čuvaji) ali občasno (reditelji). Za uspešno in učinkovito, predvsem pa varno izvajanje delovnih nalog, je za njih poleg ustrezne psihofizične pripravljenosti, ključnega pomena tudi visoka delovna usposobljenost. Pri svojem delu so namreč velikokrat izpostavljeni konfliktnim situacijam, ki lahko vodijo tudi v fizični obračun. Nekaterim izmed njih so take situacije pri opravljanju dela skoraj že postale stalnica.

Samo psihofizična pripravljenost (kondicija) pri opravljanju tovrstnih poklicev seveda ni dovolj. Zato se navedeni zaposleni v določenih organizacijah usposabljajo tudi v tehnikah uporabe fizične sile. V varnostnih organih (policija, zasebne varnostne službe) se zelo pogosto poučuje in uporablja borilna veščina *ju-jitsu*.

Pri tem se zastavlja vprašanje ali obvladanje te in podobnih veščin pripomore oziroma ali je znanje teh veščin dovolj





za (zakonsko skladno) izpolnitev delovne naloge recimo varnostnika, ki se je znašel v okoliščinah, ko mora poseči po uporabi fizične sile?

Zavedati se namreč moramo, da jujitsu, karate, judo ipd. kot jih poznamo danes, niso borilne veščine, ampak borilni športi. Šport in vanj umeščene zvrsti temeljijo na pravilih in na kontroliranem izvajanju aktivnosti ter s tem na omejenosti. Iz borilnih športov so izvzete prepovedane tehnike, ki bi lahko pripeljale do težkih poškodb ali smrti udeležencev. To ne pomeni, da je znanje borilnih športov nepomembno, se je pa treba zavedati, da določene tehnike, ki iz njih izhajajo niso uporabne v realni situaciji (obvladanje napadalca, samoobramba). Poleg tega je pot do uporabnega znanja, ki izhaja iz borilnih športov dolga in naporna. Zahteva odrekanje, predanost in naporno treniranje, skratka način življenja. Je pa posledica aktivnega ukvarjanja z borilnimi športi dobra psihofizična pripravljenost in tisti, ki jih trenira, je bolje telesno in duševno pripravljen na konfliktne situacije.

> Obnovitveni nekajurni treningi 'samoobrambe' enkrat na mesec ali redkeje niso dovolj. Pravzaprav so nevarni, saj udeleženci niso kondicijsko in tehnično pripravljeni. Še nevarnejše pa je, da gojijo iluzijo, da so s takim (ne) znanjem sposobni suvereno obvladati konfliktno situacijo oziroma napadalca v realnosti. Organizacije, ki na tak način zavajajo svoje zaposlene izkazujejo svojo neodgovornost in skrajni čas bi bil, da temu področju namenijo večjo pozornost.

Tako lahko odgovorimo na zastavljeno vprašanje: znanje borilnih športov pripomore k uspešnemu opravljanju varnostne funkcije. Ni pa znanje borilnih športov dovolj za učinkovito reševanje konfliktnih situacij, ki zahtevajo uporabo fizične sile.

Razlogov za to je več. Eden izmed njih je, da borilni športi niso namenjeni uporabi v realnem nasilnem spopadu, kjer ni pravil. Prav tako veliko tehnik, ki so značilne za posamezen borilni šport ni primernih oziroma v realni situaciji ne delujejo. Zato je potrebno izbrati in prilagoditi tiste tehnike, ki bodo v dejanski situaciji uporabne. Poleg golega obvladanja tehnik je pomemben tudi način treninga in psihološka priprava na konfliktne situacije. Pri treniranju je potrebno preigravati različne realne situacije, sodelujoče je potrebno ustrezno ozavestiti in izobraziti o fiziologiji telesa in o delovanju človeške psihe v stresnih situacijah. Velik del usposabljanja za realne situacije mora temeljiti na psihološkemu vidiku konfliktov, poudariti je potrebno različne faze konflikta ter načine ravnanja v konfliktni situaciji. Za učinkovito usposobitev in ohranja-



nje usposobljenosti oseb za opravljanje varnostnih nalog, je potrebno zagotoviti dovolj pogosto, specializirano in kvalitetno vadbo.

Žal je v praksi ravno ta del zanemarjen. Obnovitveni nekajurni treningi 'samoobrambe' enkrat na mesec ali redkeje niso dovolj. Pravzaprav so nevarni, saj udeleženci niso kondicijsko in tehnično pripravljeni. Še nevarnejše pa je, da gojijo iluzijo, da so s takim (ne)znanjem sposobni suvereno obvladati konfliktno situacijo oziroma napadalca v realnosti. Organizacije, ki na tak način zavajajo svoje zaposlene izkazujejo svojo neodgovornost in skrajni čas bi bil, da temu področju namenijo večjo pozornost.

Zaključek

Organizacijam naj bo cilj, da promocija zdravja in telesne aktivnosti zaposlenih postane del organizacijske kulture in korporativne varnosti. Dobro zasnovana in strokovno vodena vadba na delovnem mestu ali izven nje, koristi zaposlenim, saj krepi zdravje, dobro počutje in moralo, učinkovitost dela in ne nazadnje koristi organizacijam. Izvajanje programa je seveda potrebno prilagoditi značilnosti organizacije in njene delovne sile, z okoljem, v katerem deluje in s sredstvi, ki so na voljo za to. Programi vadbe morajo potekati pod vodenjem strokovnjakov, ki so usposobljeni za delo na področju športa in ki so pozorni na to, kaj program prispeva, da zadovolji novim potrebam in izzivom organizacije.

Še večji poudarek je na psihofizični pripravljenosti potrebno dati usposabljanju zaposlenih pri opravljanju varnostnih nalog. Ti zaradi specifičnosti dela, ki ga opravljajo, potrebujejo specializirano vadbo, ki mora biti namensko usmerjena in dovolj pogosta ter intenzivna, da ohranja posameznike v funkcionalni kondiciji za opravljanje delovnih nalog. Poleg vrste izbranih tehnik, načina in pogostosti vadbe, je izredno pomembna tudi pravilna psihološka priprava posameznikov na reagiranje v konfliktnih situacijah. Bistveno je, da se tako zaposleni kot delodajalci zavedajo, da je le z ustrezno usposobljenostjo mogoče profesionalno opravljati varnostno funkcijo.

* Vsebina sestavka ne obsega zaposlenih na področju varnostnih funkcij v specializiranih enotah/oddelkih varnostnih organov.

Viri

- Corry, J. (2011). Physical Training and Fitness Programmes: An Organizational Asset, International Labor Organization, Geneva.
- http://www.military-fitness.info/military-fitnessprivilegecardoutlets.htm
- Inštitut za varovanje zdravja RS. Priporočila za promocijo telesne dejavnosti v delovnem okolju (2008).
- Kovačič, A. (2009). Fitnes programi za varnostnike. Interno gradivo, igralnica GCL.
- Potokar, M. (2003). Priprava in izvedba učne ure pri predmetu samoobramba: seminarska naloga pri predmetu didaktika. Filozofska fakulteta, Univerza v Ljubljani. ■

Avtor: Mag. Mirjam Bežnik / Zavod Karnika



VLOGA UČINKOVITEGA KOMUNICIRANJA PRI OBVLADOVANJU POSLOVNIH TVEGANJ

Znanje in poznavanje učinkovite in uspešne komunikacije je v povezavi z drugimi mehanizmi za učinkovito obvladovanje tveganj namreč pomemben pripomoček, s katerim podjetje lahko bodisi prepreči nastanek tveganja ali pa pripomore k zmanjšanju nastanka škode, če vseeno pride do neželene situacije ali dogodka.

Po zaslugi številnih spoznanj, zlasti s področja organizacijskih, psiholoških in komunikoloških znanosti, je danes zapisanega že zelo veliko o medsebojnih odnosih v organizaciji, kot tudi o vrstah, ravneh in zakonitostih komuniciranja v poslovnem okolju.

Skrajni čas je, da smo v naši družbi pričeli v večji meri prepoznavati vlogo, ki jo ima učinkovita komunikacija v sistemu zagotavljanja korporativne varnosti in s tem tudi v sistemu obvladovanja poslovnih tveganj. Prav gotovo pa s tem stanjem ne moremo biti zadovoljni. Še vedno se razmeroma pogosto pojavljajo dvomi, ali je izobraževanje in informiranje v smislu pridobivanja znanj s področja učinkovite korporativne komunikacije v resnici potrebno ali pa ga morda lahko v družbi odložimo za nedoločen čas. Vodstvo podjetja pri planiranju stroškov lahko oceni, da usposabljanja s področja (učinkovite) komunikacije pri poslovnem subjektu morda ne sodijo na lestvico prioritet, saj s tem nastanejo dodatni poslovni stroški. Tovrstna razmišljanja vodstva so realna možnost, zlasti v času krize, ko so mnoga podjetja prisiljena zelo optimizirati poslovne odhodke. Vprašanje pa je ali je dobro varčevati na ta način in s tem povečati tudi tveganja, ki lahko bistveno negativno učinkujejo na razvoj oziroma na poslovanje podjetja.

> Ključno pri vsem procesu vzpostavitve sistema za obvladovanje tveganj je doseči zavedanje, da so za varnost v podjetju odgovorni prav vsi zaposleni.

Vloge in pomena učinkovitega pretoka informacij in učinkovitega komuniciranja se žal nekateri odgovorni zavedo šele tedaj, ko je potrebno v podjetju rešiti zapleteno situacijo ali ob pojavu krize, naravne nesreče in podobno. Malešič (2006)[1] ugotavlja, da je ena najobčutljivejših točk kriznega upravljanja in vodenja komuniciranje, ki se odraža v (ne) uspehu nekaterih drugih prvin tega procesa, kakor so preventiva in pripravljanje na krizo, vodenje in odločanje, pa tudi politično organizacijsko delovanje in konflikt.

Ključno pri vsem procesu vzpostavitve sistema za obvladovanje tveganj je doseči zavedanje, da so za varnost v podjetju odgovorni prav vsi zaposleni. Tudi iz tega razloga je učinkovita komunikacija o tveganjih eden izmed tistih dejavnikov, ki bistveno pripomorejo k dvigu varnostne kulture in uspešnosti podjetja. Zato pa mora biti zasnovana na osnovi procesa medsebojnega sodelovanja med ključnimi deležniki (posamezniki in skupinami) v organizaciji in njenem okolju ter z uporabo ustreznih komunikacijskih kanalov.

V prispevku želim podrobneje osvetliti pomen učinkovitosti komunikacijskega procesa, s ciljem, da se ta spoznanja v čim večji meri vključijo v sistem obvladovanja poslovnih in varnostnih tveganj pri posameznem gospodarskem subjektu. V zadnjem času še posebej izpostavljena poslovna tveganja so poleg varnostnih in informacijskih tudi tržna in prodajna tveganja. Pomembno je, da si vodstvo podjetij za obvladovanje teh tveganj postavi visoke standarde, jih dosledno spoštuje in nenehno nadgrajuje skladno z dobrimi praksami.

Številne organizacijske teorije izražajo množico pogledov na komuniciranje, ki jih avtorji obravnavajo z vidika posameznih teoretskih modelov. Zato povzemam le opredelitev, ki je hkrati tudi najbolj splošna, zajema pa ključne elemente komunikacijskega procesa**.**

Komuniciranje *je sporazumevanje, sistem izmenjevanja simbolov ali informacij med informacijskim virom in sprejemnikom. Strokovni izraz »komuniciranje« se uporablja tako v družboslovju kot humanistiki in tehničnih znanosti, na primer v računalništvu, elektrotehniki ipd. Komunikacija nam omogoča usklajevanje mnenj, doseganje različnih ciljev, pa tudi vzpostavljanje, vzdrževanje in spreminjanje medosebnih odnosov. Čeprav je veščina komuniciranja najpomembnejša izmed vseh, ki jih ljudje sploh imamo, se je le malokdaj načrtno učimo.*[2]

Velja omeniti dve komponenti, ki vplivata na učinkovitost pri komuniciranju, to pa sta: 1) vsebinska raven in 2) odnosna raven. Bodimo torej pazljivi ne le na sam tekst našega sporočila, ki ga posredujemo prejemniku, pač pa tudi na to, kako bomo predali naše sporočilo, da bo prejemnik sporočila oziroma poslušalec pravilno razumel, kaj smo hoteli povedati, sporočiti. Pri pisnem sporočanju uporabimo ustrezno jezikovno zvrst, pri ustnem sporočanju pa seveda upoštevajmo govorico našega (in sogovornikovega) telesa, barvo glasu in obrazno mimiko.

> Izjemnega pomena, tudi z vidika zagotavljanja korporativne varnosti, so povratni informacijski tokovi, ki jih poslovni subjekt prejme bodisi iz notranjega okolja, kot tudi iz okolja, v katerem posluje.

Pri vsem naštetem seveda obstajajo določene izjeme, zlasti v primerih, ko so določeni postopki standardizirani. V tem primeru ima sporočevalec natanko predpisan sistem sporočanja, poleg tega je v teh primerih bistvena vsebina sporočila. To je značilno za sodne ali upravne zadeve.

Vse našteto povezujemo s pojmom učinkovite komunikacije (effective communication), ki jo lahko definiramo kot stopnjo zmanjševanja napačnega razumevanja sporočil ali kot stopnjo, do katere udeleženci komuniciranja pripisujejo sporočilom isti pomen. Učinkovitost komunikacije lahko opišemo tudi kot stopnjo vzajemnega razumevanja med udeleženci. Kot pravita David in Frank Johnson (Johnson in Johnson, 1997)[3] je »učinkovita komunikacija med dvema osebama tista, pri kateri si prejemnik razlaga sporočilo pošiljatelja enako, kot je le–ta želel, da bi si«. Učinkovita komunikacija je torej odvisna od učinkovitega pošiljanja in od učinkovitega prejemanja sporočil.

Zelo preprosto lahko rečemo tudi, da je cilj učinkovite komunikacije dobiti dobre rezultate ob potrošnji primernega časa in sredstev.

Ali lahko učinkovitost v komunikaciji enačimo z uspešnostjo (successful communication) in od česa je odvisna učinkovitost komunikacijskega kanala?

V prvi vrsti je učinkovitost odvisna od zmogljivosti prejemnika sporočila, od psihofizioloških lastnosti prejemnika sporočila (čutila), ne nazadnje tudi od motivacije posameznika za sprejem no-



vih informacij, saj prav motivacija bistveno poveča obseg informacij, ki jih posameznik lahko sprejme. Vse našteto velja tudi za sporočevalca. Učinkovitost je prav tako odvisna od pravilnega izbora komunikacijskega kanala, s čimer se dodatno izognemo entropiji oziroma komunikacijskemu šumu.

Kaj pa uspešnost komunikacije oziroma kdaj lahko rečemo, da je bila neka komunikacija uspešna? Ali je lahko neka komunikacija uspešna, hkrati pa ni učinkovita? Ali lahko pojma uspešnost in učinkovitost v komunikaciji morda celo obravnavamo kot identična?

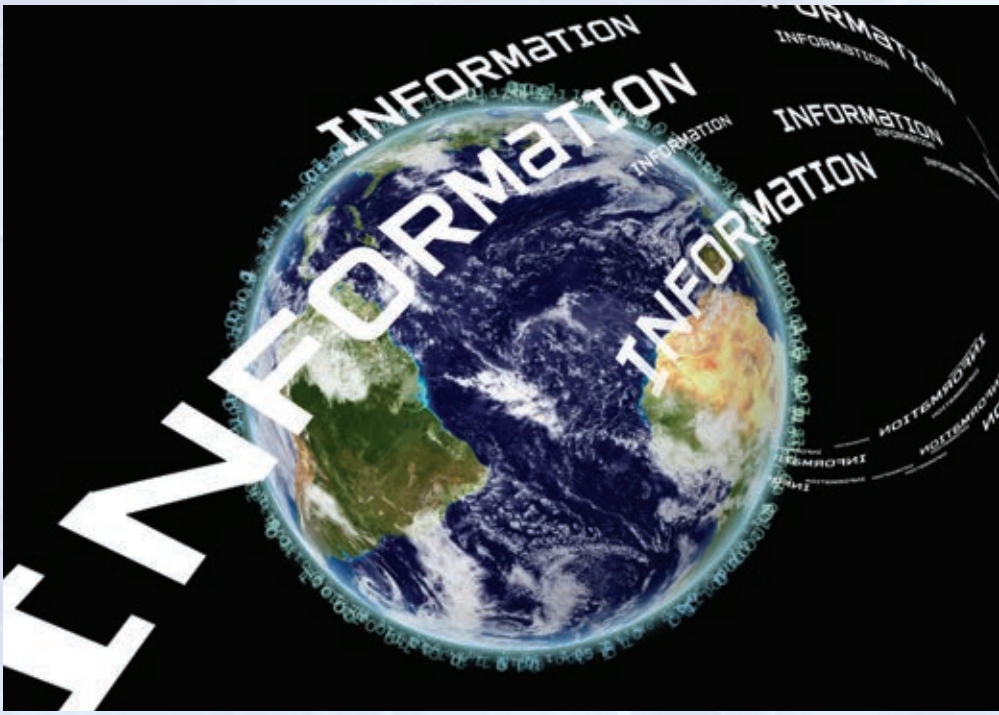
V praksi se mnogokrat celo enačita pojma uspešnost in učinkovitost v komuniciranju, razlikovanje obeh pojmov pa je morda za površnega bralca oziroma poslušalca celo nepomembno. Vendar, če nekoliko podrobneje analiziramo vsebino posameznih prispevkov na to temo, dejansko vidimo, da avtorji v večji meri kot o sami uspešnosti pravzaprav govorijo o učinkovitosti komuniciranja. Vsekakor sta oba pojma med seboj močno povezana in ju ni mogoče v celoti ločiti.

Pri uspešnosti komunikacijskega procesa zasledujemo zlasti vsebinsko tehnični vidik, torej ali :

- smo izbrali ustrezen komunikacijski kanal oziroma ustrezno komunikacijsko strategijo;
- je sporočilo v pravem času prispelo do prejemnika oziroma do prejemnikov le tega;
- je prejemnik sporočilo ustrezno dekodiral oziroma ga je razumel;
- je morda prišlo do motenj v komunikacijskem procesu.

Za razliko od merjenja uspešnosti komuniciranja, kjer je izpostavljen tehnično vsebinski vidik tega procesa, pa pri proučevanju učinkovitosti komunikacijskega procesa poudarjamo odnosni vidik.

Učinkovitost komuniciranja lahko torej presojamo zlasti z vidika posledic oziroma učinka sporočanja na prejemnika oziroma na prejemnike. Naj povedano ponazorim s praktičnim primerom. V situaciji, ko določeni osebi pisno sporočimo informacijo, ki jo prejemnik napačno interpretira, je učinek tega komunikacijskega procesa celo proti našim pričakovanjem. V primeru, ko poslano pismo s pomembnimi informacijami prejemniku ni dostavljeno, tak komunikacijski proces ne more biti niti uspešen niti ne more biti učinkovit.



Od narave poslovnega procesa, strukture zaposlenega osebja, lokacije, kjer se dejavnost odvija, okolja v katerem organizacija posluje, je odvisno, kateri komunikacijski kanali bodo izbrani za interno komuniciranje, kot tudi za komuniciranje organizacije z njenim okoljem. Ni namreč vseeno ali je bila neka komunikacija uspešna, mora biti tudi učinkovita, izpolniti mora svoj namen oziroma cilj, ki ga želi doseči sporočevalec. V nasprotnem primeru je bila lahko komunikacija sicer uspešna, torej sporočilo je pravočasno doseglo vse prejemnike, ki so ga pravilno razumeli, vendar ni bilo pričakovanega učinka.

Pri korporativnem komuniciranju mora vodstveno osebje ves čas spremljati tako uspešnost, kot tudi učinkovitost internega komuniciranja. In ne samo to. Izjemno pomembno je spremljati tudi učinkovitost in uspešnost komuniciranja med organizacijo in njenim okoljem. V primeru neugodnih gibanj je nujen sestanek, da se ugotovijo in odpravijo vzroki. Vse našteto bistveno pripomore k utrjevanju pozitivne podobe organizacije in ugleda podjetja v poslovnem okolju, prispeva k tržnemu uspehu, pri delničarjih in vseh drugih zunanjih deležnikih pa povečuje občutek varnosti. Vse to v končni fazi bistveno pripomore k zmanjšanju stopnje poslovnega tveganja.

Izjemnega pomena, tudi z vidika zagotavljanja korporativne varnosti, so povratni informacijski tokovi, ki jih poslovni subjekt prejme bodisi iz notranjega okolja, kot tudi iz okolja, v katerem posluje. V primeru pritožb, naj si bodo to pritožbe zaposlenih kot tudi morebitne pritožbe drugih subjektov iz okolja, naj bodo določeni tudi postopki in varne poti za sprejemanje le teh.

Vodstvo podjetja, ki si prizadeva pri sodelavcih in tudi v njenem poslovnem okolju zagotoviti vitalno podporo pri razvoju in politiki organizacije nasploh, je dolžno premišljeno izbrati komunikacijsko strategijo ter pravilno izbrati vrsto in obliko sporočanja glede na vsako posamezno konkretno situacijo. Nekatere komunikacijske poti so določene z zakoni in predpisi, prav tako naj bo standardizirano tudi arhiviranje in dostop do informacij. Pri zagotavljanju dostopa do relevantnih poslovnih informacij je upravičencem nujno potrebno zagotoviti pravočasen in enakopraven dostop brez nepotrebnih stroškov. Poleg poslovnih informacij, ki so jih gospodarski subjekti dolžni redno, v predpisanem času, posredovati javnosti, je dobro, da se določi, katere informacije, komu in v kakšni obliki bo družba posredovala periodično, stalno ali pa zgolj občasno.

1 Malešič, M.; Teorija kriznega komuniciranja; http://www.sos112.si/slo/tdocs/ujma/2006/malesic_2.pdf

2 http://sl.wikipedia.org/wiki/Komuniciranje

3 Johnson, David W.,. Johnson, Frank P. 1997. Joining together : group theory and group skills (6th ed.). Boston, Allyn and Bacon ■

Avtor: Boris Kankaraš, mag / Vodja službe za splošno varovanje in varovanje morja, Luka Koper*



POMORSKA IN PRISTANIŠKA VARNOST

Pristanišča zaradi svoje kompleksnosti in količine tovora ter potnikov predstavljajo izjemen varnosti izziv, ki pred korporativno varnost postavlja veliko odprtih dilem po učinkovitejšem obvladovanju tveganj.

Pomorski transport pokriva kar ¾ celotnega svetovnega blagovnega transporta. Ob tem je pomembno tudi dejstvo, da se kot transportna zvrst izjemno hitro razvija tako v tehnološkem kot v kvantitativnem smislu. Temu trendu sledijo tudi pristanišča, če želijo ohraniti oz. povečati svoje tržne deleže in konkurenčnost. V transportno logistični verigi so pristanišča »vmesniki« (interface) med vodnimi in kopenskimi transportnimi potmi.

Z varnostnega vidika plovne poti, plovila in pristanišča predstavljajo atraktivno tarčo oz. objekt za različne posameznike in skupine, ki izvajajo različne vrste kriminalitete. Obenem pa dinamika in obseg te panoge in dejavnosti sama po sebi predstavlja vrsto drugih tveganj (okoljska, poslovna, politična...).

Zaradi opisanih značilnosti in pomena za državo so pristanišča kot objekt deležna posebne skrbi in obravnave in predstavljajo kritično infrastrukturo države.

Razvoj pristaniške varnosti in predpisov

V preteklosti je pomorska varnost obravnavala predvsem varnost plovbe medtem, ko je bila pristaniška varnost v domeni posamezne države. Kljub naporom, ki jih je v standardizacijo (v regulatornem smislu) vlagal IMO (International maritime organization – Mednarodna pomorska organizacija[1]) mednarodna skupnost ni bila sposobna doseči konsenza. Pomemben premik je bil dosežen po terorističnih napadih na ZDA leta 2001. Spoznanje, da terorizem predstavlja resno grožnjo pomorski varnosti je pomembno vplivalo na širšo mednarodno skupnost.

Koprsko pristanišče se na kopenskem delu razteza na 2.720.000 m2 površine, pristaniški akvatorij pa obsega 1.949.095 m2 površine. Kopenski del je ograjen z ograjo v skupni dolžini 6.915 metrov.

Med temeljne akte pomorske varnosti štejemo Mednarodno konvencijo o varstvu človeškega življenja na morju[2] (International Convention for the Safety of Life at Sea - SOLAS). Je najpomembnejša, obenem pa tudi najstarejša konvencija, ki pokriva obsežno področje varnosti na morju. Konvencija je bila sprejeta leta 1914 po tragični nesreči Titanika.

Leta 1974 so bili sprejeti dodatni amandmaji in nekatere spremembe v sami konvenciji. Sprejeta je bila nova konvencija SOLAS (Safety of Life at Sea), ki je stopila v veljavo 25. maja 1980.

Kasneje so konvencijo še nekajkrat modificirali. Dodana sta bila dva protokola, ki določata letni pregled in nadzor tankerjev (1984) in protokol, ki določa usklajen sistem pregleda in certificiranja (2000).

Konvencija je razdeljena na 12 poglavij:
- splošna določila;
- protipožarna oprema;
- sredstva za reševanje;
- radiokomunikacije;
- varnost plovbe;
- prevoz razsutega tovora;
- konstrukcija ladje in stabilnost;
- prevoz nevarnega tovora;
- nuklearne ladje,
- varnostna pravila na hitrih ladjah;
- posebni ukrepi za povečanje varnosti na ladjah in v pristaniščih;[3]
- dodatni varnostni ukrepi za ladje, ki prevažajo razsute tovore.

*avtor je član Slovenskega združenja korporativne varnosti

Konvencija se nanaša na vse ladje, ki plujejo v mednarodnem prometu, in izključuje vojaške ladje, ribiške ladje, ladje brez naftnega pogona, lesene ladje primitivne gradnje in jahte.

Ne glede na to, da konvencija primarno ureja varnost na morju in plovilih, je zelo pomembna tudi za pristaniško varnost. Države podpisnice konvencije so sprejele standarde, ki so enotni in zaradi tega kompatibilni med državami podpisnicami. Od trenutka, ko ladja[4] najavi vplutje v pristanišče, se pričnejo izvajati določeni procesi, ki zagotavljajo varnost in zaščito ladje, posadke ter pristanišča, njegove infrastrukture ter življenja zaposlenih.

Evropska unija je v evropski pravni red implementirala ISPS kodeks, omenjeni amandma SOLAS konvencije z Uredbo o povečanju varnosti na ladjah in v pristaniščih (Regulation on enhancing ship and port facility security (EC) No 725/2004). Razlog je bila implementacija varnostnih ukrepov v evropski pomorski prostor ob upoštevanju, da standardi postajajo mednarodni. Predpis je dal osnovo in temelj za koordinirano in usklajeno interpretacijo, implementacijo in možnost nadzora nad izvajanjem varnostnih ukrepov.

Direktiva o pristaniški varnosti (Directive 2005/65/EC on enhancing port security) zaokrožuje varnostne ukrepe, deloma obravnavane tudi v Uredbi ((EC) 725/2004) in celotno pristanišče obravnava kot enotno območje varnostnega režima.

Inšpekcije Komisije na področju pomorske varnosti[5] (Regulation (EC) 324/2008 on procedures for conducting Commission inspections in the field of maritime security) je predpis, ki obravnava področje nadzora nad izvajanjem varnostno zaščitnih ukrepov na področju pristaniške varnosti. Inšpekcija tako s ciljem spremljanja implementacije ukrepov, zahtevanih v evropski zakonodaji na področju pomorske varnosti, izvaja inšpekcijske nadzore, katerih namen je preverjanje učinkovitosti varnostnih ukrepov za zagotavljanje varnosti ladij in pristanišč.

V nacionalnih strateških dokumentih je pomorstvo in pristanišče opredeljeno kot pomembna panoga in objekt posebnega pomena za obrambo in gospodarstvo Republike Slovenije. Pri tem je zanimivo, da je Republika Slovenija navedene evropske predpise implementirala v Uredbi o izvajanju zaščitnih ukrepov na ladjah in v pristaniščih (Ur.l. RS, št. 64/2004, 41/2007 in 68/2012), ki pa žal ne upošteva specifike koprskega pristanišča, pravno formalnega vidika delovanja državnih organov in varnostne skupnosti in da ni usklajen z drugimi predpisi, ki urejajo področje varnosti in varovanja.

Pomembni so tudi interni predpisi Luke Koper, ki obravnavajo in urejajo notranji red v pristanišču, področje varstva pri delu, varstva okolja, varovanje morja, požarno varnost, krizno upravljanje, varovanje tajnih podatkov in poslovne skrivnosti itd...



foto: Denis Zupan

Koprsko pristanišče

Koprsko pristanišče je last Republike Slovenije, v skladu s koncesijsko pogodbo[6] pa z njim upravlja gospodarska družba Luka Koper, delniška družba. Opredeljeno je kot pristanišče za mednarodni javni promet in izvaja tovorno in potniško dejavnost.

V slovenskem teritorialnem morju se odvija mednarodni potniški promet tudi v pristaniščih Izola in Piran, koprsko pristanišče pa je edino slovensko tovorno pristanišče.

S primerjalnega vidika je pristanišča možno klasificirati z mnogo različnih aspektov. Pristanišča je mogoče klasificirati glede na velikost celotnega pristanišča, kopenskega ali vodnega dela pristanišča, glede na vrsto tovorov, glede na količino pretovorjenega blaga, glede na njegovo specializiranost ali diverziteto, glede na njegove povezave z zaledjem itd...

Koprsko tovorno pristanišče, glede na velikost ter količino pretovorjenega blaga, sodi med srednje velika večnamenska pristanišča[7]. Pristanišče je strukturirano glede na vrste blaga tako, da ga sestavljajo naslednji terminali:

- Kontejnerski in ro-ro terminal
- Avtomobilski terminal
- Terminal za generalne tovore
- Terminal za sadje
- Terminal za les
- Terminal za minerale in rudnine
- Terminal za žitarice in krmila
- Terminal za glinico
- Evropski energetski terminal
- Terminal za tekoče tovore
- Terminal za živino
- Potniški terminal

Koprsko pristanišče se na kopenskem delu razteza na 2.720.000 m2 površine, pristaniški akvatorij pa obsega 1.949.095 m2 površine. Kopenski del je ograjen z ograjo v skupni dolžini 6.915 metrov.

Pristanišče ima:

- 247.000 m2 zaprtih skladiščnih površin;
- 76.000 m2 pokritih skladiščnih površin;
- 900.000 m2 odprtih skladiščnih površin;
- 30 kilometrov železniških tirov;
- 3.283 m operativnih obal;
- 25 priveznih mest;
- maksimalno globino bazenov 18 metrov.

Promet na vhodu v pristanišče	Povprečno število na dan
Tovorni promet	1000
Kombinirana vozila	750
Osebna vozila	800
Fizična oseba	1500
Ladje	2000

Tabela 2: *Pregled dinamike vstopanja na glavnem vhodu v koprsko pristanišče (leto 2011)*

Zagotavljanje varnosti Koprskega pristanišča je poseben izziv ravno zaradi dejavnosti, ki poteka na tem območju z veliko dinamiko, obsegom in sodelovanjem zunanjih deležnikov. Pristanišče mora biti odprto za poslovne partnerje in priložnosti, in hkrati varno za tiste, ki se v njem zadržujejo in izvajajo poslovne procese.

Ob pretovoru različnih vrst blaga je potrebno izpostaviti tudi dejavnost potniškega terminala, ki ima pomen tudi za lokalno skupnost in širšo regijo. V času delovanja terminala, ki je



foto: Mitja Božič



foto: Jaka Jerasa

Zagotavljanje varnosti Koprskega pristanišča je poseben izziv ravno zaradi dejavnosti, ki poteka na tem območju z veliko dinamiko, obsegom in sodelovanjem zunanjih deležnikov. Pristanišče mora biti odprto za poslovne partnerje in priložnosti, in hkrati varno za tiste, ki se v njem zadržujejo in izvajajo poslovne procese.

zaradi svoje specifike[8] povezan z javnimi površinami mesta Koper, je v tem času vzpostavljen poseben varnostni režim, ki mora ustrezati standardom mednarodnega mejnega prehoda, na drugi strani pa zagotavljati varnost in varovanje koprskega pristanišča. Velike križarke prevažajo tudi preko 3000 potnikov in blizu 2000 članov posadke. Večina potnikov se odloča za ogled mesta in drugih znamenitosti Slovenije. Dinamika prehajanja kontrolne točke je zelo visoka zato zahteva dobro organizacijo, ustrezno število osebja ter tehničnih sredstev in opreme. Pri tem je ključnega pomena koordinacija ukrepov in postopkov z varnostnim osebjem ladje.

Kompatibilnost varnostnih postopkov, ukrepov in varnostnih stopenj je pomembna zaradi deležnikov, ki sodelujejo v procesu »vezanja« ladje na operativno obalo pristanišča. Vsaka ladja in pristanišče imata v veljavi določeno varnostno stopnjo[9], ki je odvisna od ocene ogroženosti. Ladja in pristanišče si pred prihodom ladje izmenjata varnostno deklaracijo s katero uskladita varnostne ukrepe. Ukrepi veljajo za čas, ko je ladja v pristanišču. Varnostno stopnjo za koprsko pristanišče določa Policija.

Za varnost koprskega pristanišča skrbi Služba za splošno varovanje in varovanje morja, ki izvaja naloge na podlagi mednarodne in nacionalne zakonodaje. Služba »pokriva« področje varovanja, varovanje morja, požarne varnosti, obrambno načrtovanje in civilno zaščito, varovanje tajnih podatkov in poslovne skrivnosti ter krizno upravljanje. Služba ima lasten VNC, delo pa je organizirano po izmenah. Za zagotavljanje varnosti so na varovanem območju nameščeni različni varnostno tehnični sistemi.

Zaradi potreb po usklajevanju aktivnosti ter izmenjavi informacij v pristanišču deluje varnostna koordinacija. V koordinaciji sodeluje Policija, Uprava Republike Slovenije za pomorstvo, Carina, Slovenska vojska, Slovenska obveščevalno-varnostna agencija SOVA in Obveščevalno-varnostna služba MORS, Luka Koper d.d. ter drugi deležniki, odvisno od obravnavane vsebine.

Zagotavljanje varnosti koprskega pristanišča zahteva hitro, stalno in učinkovito sodelovanje različnih deležnikov, varnostne skupnosti ter pristojnih služb Luke Koper d.d., ki upravlja s koprskim pristaniščem.

1 leta 1948 je OZN s konvencijo ustanovila Mednarodno pomorsko svetovalno organizacijo (Intergovernmental Maritime Consultive Organization – IMCO), predhodnico IMO
2 International Convention for the Safety of Life at Sea.
3 International ship and port security code - ISPS kodeks.
4 Ki izpolnjuje varnostne in tehnične standarde.
5 Tudi varnosti pristanišč.
6 Uredba o upravljanju koprskega tovornega pristanišča, opravljanju pristaniške dejavnosti, podelitvi koncesije za upravljanje, vodenje, razvoj in redno vzdrževanje pristaniške infrastrukture v tem pristanišču (Ur.l. RS, št. 71/2008).
7 Klasifikacija ESPO (European Sea Ports Organization)
8 Prihodi in odhodi potnikov.
9 Varnostne stopnje od 1 do 3 (MarSec level – Maritime Security level). ■

Avtor: Doc. dr. Aleša Svetic / GEA College-Fakulteta za podjetništvo



SOCIALNO VARNOSTNI VIDIK PRI RAVNANJU S TVEGANJI

Pri iskanju ravnotežja med uspešnostjo, učinkovitostjo in etičnostjo poslovanja, se vodstva pogosto odločajo za rešitve, ki so v interesu močnejših partnerjev, najpogosteje lastnikov, zaposleni pa so največkrat prezrti.

Z ignoriranjem socialno varnostnega vidika se tveganja povečujejo, podjetje pa odmika od optimalnih ekonomskih in morda celo etičnih odločitev. Tveganja, ki se nanašajo na sodelavce, kompetentnost vodstva in etičnost odločanja, mobing in podobno so pogosto podcenjena in prezrta, čeprav so lahko usodna za podjetje.

Koncept odgovornega delovanja

Od podjetij na današnji stopnji razvoja se ne pričakuje, da uresničujejo le ekonomske odgovornosti (maksimiranje profita) in pravne odgovornosti (spoštovanje zakonov, pravil ipd.) pač pa tudi obveznosti do socialnega in naravnega okolja ter zlasti etične in človekoljubne odgovornosti kot tudi odgovornosti do novih socialno družbenih trendov, ki se nanašajo na zelo specifične potrebe posameznika.

Praviloma okoli tega, da je temeljna odgovornost vodstva ustvarjanje dodane vrednosti, ni dilem, zaplete pa se pri vprašanju kako to doseči, ali drugače kaj za to žrtvovati, katere interese in pričakovanja prezreti, da vodstva dosežejo želeni izid. Ali so to interesi zaposlenih ali kapitala? Zaposleni za svoje delo pričakujejo pošteno plačilo, varno in zdravju primerno delovno okolje, možnosti za napredovanje in rast in podobno. Če pričakovanj ne uresničijo, se počutijo izigrani, njihova delovna motivacija pade in se to pokaže na njihovih delovnih prispevkih in seveda končnemu rezultatu. Prav tako so še vedno podjetja, ki zaposlenih ne obravnavajo kot dejavnika uspešnosti, pač pa nanje gledajo predvsem z vidika stroškov, stroške pa je v smislu doseganja poslovnega uspeha, potrebno zmanjševati. To pa je neustrezna praksa, ki povečuje socialna tveganja. Nezadovoljni zaposleni lahko ustvarjajo negativno podobo v širši javnosti, kar še dodatno zmanjšuje ugled in dobro ime podjetja v družbi.

Družbeno odgovorno podjetje spoštuje zakonska določila, predpise, davke, prispevke, dajatve, podjetniške pogodbe ipd., spoštuje standarde in druge norme poslovanja, predvsem pa etično in pošteno ravnanja z zaposlenimi, kajti vsi odmiki od navedenih ravnanj predstavljajo tveganje. Žal pa v današnji izrazito potrošniško naravnani družbi, ko je cenjen predvsem uspeh na ekonomskem področju in so temu cilju bolj ali manj podrejena tudi sredstva za njegovo doseganje, postaja kritična presoja posameznikovih dejanj vse redkejša.

Nezadovoljni zaposleni lahko ustvarjajo negativno podobo v širši javnosti, kar še dodatno zmanjšuje ugled in dobro ime podjetja v družbi.

Vprašanje socialne pravičnosti, tranzicije, bogatenja, kratenja človekovih pravic, pravic do dela, vprašanja novih tehnologij, vprašanja varnostnih izzivov in boja proti gospodarski kriminaliteti ter številna druga, so vprašanja, ki pretresajo vsakodnevno poslovno prakso in nas odmikajo od pričakovanih poslovnih rezultatov. Poznano je, da poslovanje v okolju z nižjimi etičnimi standardi, zahteva veliko več previdnosti, preverjanja poslovnih partnerjev in zaposlenih, dodatna zavarovanja plačil ipd. kar povečuje stroške in zmanjšuje učinkovitost delovanja. Nasprotno pa visoki etični standardi ustvarjajo pogoje zaupanja, odgovornega ravnanja in visoke motiviranosti ljudi, da naredijo več in bolje. V takem okolju so tudi medsebojni odnosi dobri, prav tako pa tudi kakovost delovnega življenja ljudi, ki pri delu preživijo velik del življenja.

Etiko je potrebno, enako kot načrtujemo politiko, strategijo ali operativne dejavnosti, načrtovati, in obenem preverjati ali se ta tudi uresničuje. Pri tem pa sta nepogrešljiva zgled in delovanje vodstev. Ti morajo biti etično ozaveščeni in morajo tudi ravnati tako, da se lahko sodelavci oprejo nanje. Če teh kvalitet nimajo, etičnega delovanja v podjetju ne moremo pričakovati, spremembe se običajno zgodijo šele s prihodom novih kompetentnih in zaupanja vrednih lju-

Velikokrat so odločitve vodstev pogojene s kulturo podjetja, ki pa ni nujno povsem skladna z njihovimi osebnimi vrednotami in stališči.

di na ključna delovna mesta. Prav zato je potrebno sposobnosti in osebnostne značilnosti managerja predhodno preveriti, zgolj dvomljiva priporočila ne ustrezajo današnjemu času. Pomembne so zlasti »mehke« veščine, ki temeljijo na poštenosti, obvladovanju odnosov, participaciji in kompetentni in pošteni posamezniki, ki izžarevajo zaupanje in ki lahko zahtevajo spoštovanje in zvestobo sodelavcev, ker se tudi vedejo v skladu s svojim prepričanjem.

Ključna vloga vodstva

Naloga vodstev je, da s strokovno pravilnim in etično sprejemljivim odločanjem usklajujejo interese, pričakovanja in ravnanja različnih interesnih skupin. Velikokrat so odločitve vodstev pogojene s kulturo podjetja, ki pa ni nujno povsem skladna z njihovimi osebnimi vrednotami in stališči. Tu gre zlasti za razlike med podjetniki in managerji večjih podjetij ali delniških družb. Podjetniki odločajo o svoji lastnini in lahko zato v večji meri ravnajo po svojem preudarku, managerji pa so v podjetju predstavniki lastnikov in morajo svoje odločitve upravičiti pred lastniki, za katere pa ne vedo vedno, kaj so njihovi resnični nameni. Prav zato se moramo vedno, ko presojamo določene odločitve, ki so manj skladne z etičnimi standardi in zakonskimi predpisi vprašati, koliko so k temu prispevale osebnostne in značajske lastnosti tistega, ki odloča in koliko zahteve lastnika pred katere so bili postavljeni.

Kako se torej odločati, da so tveganja slabih odločitev čim manjša? Prvo vodilo so zakoni in druga določila, vendar to ni dovolj. Manager je pri odločanju pogosto v dilemah kako zadostiti različnim interesom. Lastniki želijo čim večji dobiček, delavci pa želijo višje plače, večje varstvo pri delu, kar seveda povečuje stroške. Koga naj manager upošteva prednostno, lastnike ali sodelavce, da bo njegovo odločanje pravilno? Primarni cilj je dobiček, vendar pa lahko dobiček tudi negativno vpliva na etičnost, saj lastniki pritiskajo na managerje, da sprejemajo odločitve, ki managerja pogosto omejujejo pri etičnem odločanju. Manager zato potrebuje sodila za etično odločanje (kriterije, standarde, norme). Ker pa se pogosto znajde v situacijah, ko sodil za odločanje na katere bi se z zanesljivostjo oprl primanjkuje, si pomaga z lastno presojo in intuitivnim odločanjem. Za slednje pa potrebuje ustrezne osebnostne lastnosti in vrednote, ki ga usmerjajo.

Kako ravnati z ljudmi za zmanjšanje socialno etičnih tveganj

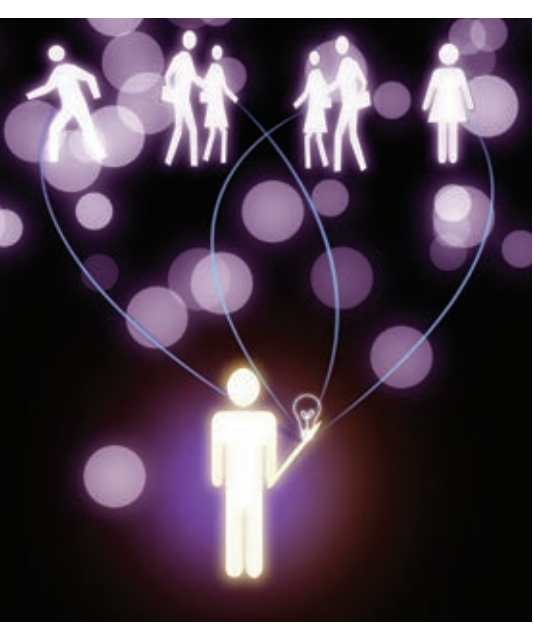
Ljudje so v današnjem času prepoznani kot zanesljiva konkurenčna prednost podjetja, a hkrati tudi največji dejavnik tveganja. Čeprav imajo vodstva nanje omejen vpliv, so od njih močno odvisna. Ljudje so tisti, ki načrtujejo poslovne strategije, jih uresničujejo, se kreativno odločajo, uvajajo nove postopke dela in ustvarjajo lastno znanje. So pa lahko tudi tisti, ki ne dosegajo predvidenih rezultatov dela, niso zavzeti sodelavci in sprejemajo slabe odločitve ter tako škodujejo podjetju.



Ljudje so v današnjem času prepoznani kot zanesljiva konkurenčna prednost podjetja, a hkrati tudi največji dejavnik tveganja.

Kako ravnati s sodelavci, da bodo dali podjetju na razpolago svoje znanje, sposobnosti, pripadnost in čas v zameno za ustrezno plačilo, so vprašanja s katerimi se morajo vodstva poglobljeno ukvarjati. Žal managerji prvenstveno uresničujejo cilje lastnikov, ki pa niso vedno v skladu s pričakovanji sodelavcev. Pogosto pa jim primanjkuje tudi volje in znanj, da bi se s sodelavci poglobljeno ukvarjali, kar je sicer njihova naloga. Negotova ekonomska situacija položaj še poslabšuje, kajti ljudje so zaskrbljeni in so za varnost zaposlitve pripravljeni tudi potrpeti.

Zaposleni danes od vodstev bolj kot ukaze, pričakujejo usmeritve in navdih v zameno za prizadevnost in zavzetost, ki ju sami vlagajo v delo (McManus, 2006). Vodstva pa pospešeno iščejo nove prijeme s katerimi bodo uresničevala poslovne priložnosti in pogosto pozabljajo, da brez ustreznih kadrov poslovni preobrat ne bo mogoč. V prizadevanju po ohranitvi konkurenčnosti, neredko izvajajo dodaten pritisk nad svojimi zaposlenimi, s čimer se povečuje konkurenca tudi med zaposlenimi. Odnosi se zaostrujejo, stres narašča in raziskave kažejo na visoko stopnjo psihičnega nasilja na delovnem mestu. S tem pa se ustvarjajo razmere za socialna tveganja. Čeprav je odgovornost vodstev za ljudi nedvoumno opredeljena, ta skoraj vedno najdejo izgovore za slabo ravnanje s sodelavci. Podjetje, ki sicer spoštuje pravne okvire svojega delovanja, vendar ob tem šikanira zaposlene ter zavrača skrb za njihovo varnost pri delu, ne bo deležno pozitivnega odziva. Podoben primer je pogosto neustrezno razumljena fleksibilnost zaposlovanja.



Ravnanja vodstev s katerimi naj bi minimizirala tveganja socialnih konfliktov so zelo odgovorno in občutljivo področje in zahtevajo sistematično strokovno in etično odločanje na kadrovskem področju. Z veliko pozornosti se morajo vodstva posvetiti kadrom že v procesu načrtovanja in izbire bodočih kandidatov. Zlasti pomembna je izbira vodstvenih kadrov, pa tudi predstavnikov nadzornih teles. Le te postavijo lastniki in prav ti so odgovorni za dobro izbiro, kajti pogosto se v primerih finančne kriminalitete pojavljajo vprašljive vodstvene, strokovne in moralne kompetence zaposlenih na pomembnih položajih. In ponavadi je kriminaliteto lahko prikriti z zapletenim poslovanjem, podprtim s strokovnimi mnenji in tem, da imajo storilci navidezen ugled.

Pomemben del ravnanja s sodelavci je tudi razvoj talentov, bodočih zvezd in nosilcev razvoja. Ti potrebujejo neprimerno večjo pozornost kot problematični kadri, kar pa mnoga vodstva še niso dojela in se zmotno preveč ukvarjajo s prvimi pri tem pa pozabijo, da je izguba talentov eno največjih tveganj za podjetje.

Prav tako je pomembno skrbno načrtovati plačne sisteme in sisteme nagrajevanja ter povezati rezultate dela z ustreznimi motivacijskimi strategijami. Najboljši kadri so vedno prizadeti, če ugotovijo, da za svoje dobre delovne rezultate dobijo enako plačo kot povprečni delavci. Plačna uravnilovka vodi najboljše kadre v pasivizacijo, povprečnost in odhode.

Področje, ki je velikokrat zanemarjeno je tudi skrb za dobre delovne odnose, kulturo, pripadnost, kamor spadajo ukrepi za preprečevanje različnih oblik neprimernih vedenj (mobing), ki so danes pogost spremljevalec delovnih odnosov in razlog za številne bolezenske odsotnosti.

Zaključek

Učinkovito ravnanje s kadri je priložnost s katero vodstvo lahko zmanjša socialna tveganja, tveganja nezadovoljstva zaposlenih, nizke storilnosti in visokih stroškov dela, ki nastajajo kot posledica boleznin, fluktuacije, izostankov z dela, pa tudi tveganja zamujenih poslovnih priložnosti, odtekanja informacij in negativne podobe v javnosti. Da pa se vodstvo odloči za krepitev konkurenčnosti na ta način, pa je seveda odvisno od vrste dejavnikov med katerimi je poleg sposobnosti zavedanja škodljivih posledic naštetih tveganj, še zlasti pomembna igra interesov vseh udeleženih.

Prav zato je pomembno, da se vodstvo vpliva dejavnikov tveganja na socialno družbenem področju zaveda, jih razume kot izziv in novo priložnost, ter vgradi v poslovno strategijo. Ustvarjanje dodane vrednosti in zavezanost etičnim normam, ob istočasni skrbi za kakovost delovnega življenja zaposlenih, njihovih družin in seveda širše družbene skupnosti je namreč danes edini zanesljivi element konkurenčnosti podjetja.

Viri

- Berk A, Peterlin J, Ribarič P. 2005. Obvladovanje tveganj: Skrivnost celovitega pristopa, GV Založba, Ljubljana.
- Bonini, MJ, Mendionca LM, Oppenheimer JM. 2006. When social issues beco me strategic, The McKinsey Quaterly, Vol2.
- Carroll BA in Buchholtz KA. 2000. Etics and Stakeholder management. Cincinnati, South Western College.
- Dimovski, V. et all. 2005. Učeča se organizacija,GV Založba, Ljubljana
- Dubrovski D. 2004. Krizni Management in prenova podjetja. Fakulteta za management, Koper.
- Jolly A. 2003. Managing Business Risk. Kogan Page, London.
- McManus,J. 2006. Leadership: Project and human capital management, Elsevier.
+ Svetic, A. 2009. Vodenje za nove izzive. 28. mednarodna konferenca o razvoju znanosti; Nove tehnologije, novi izzivi, Portorož, 2009. Fakulteta za organizacijaske vede UM, Kranj. ■

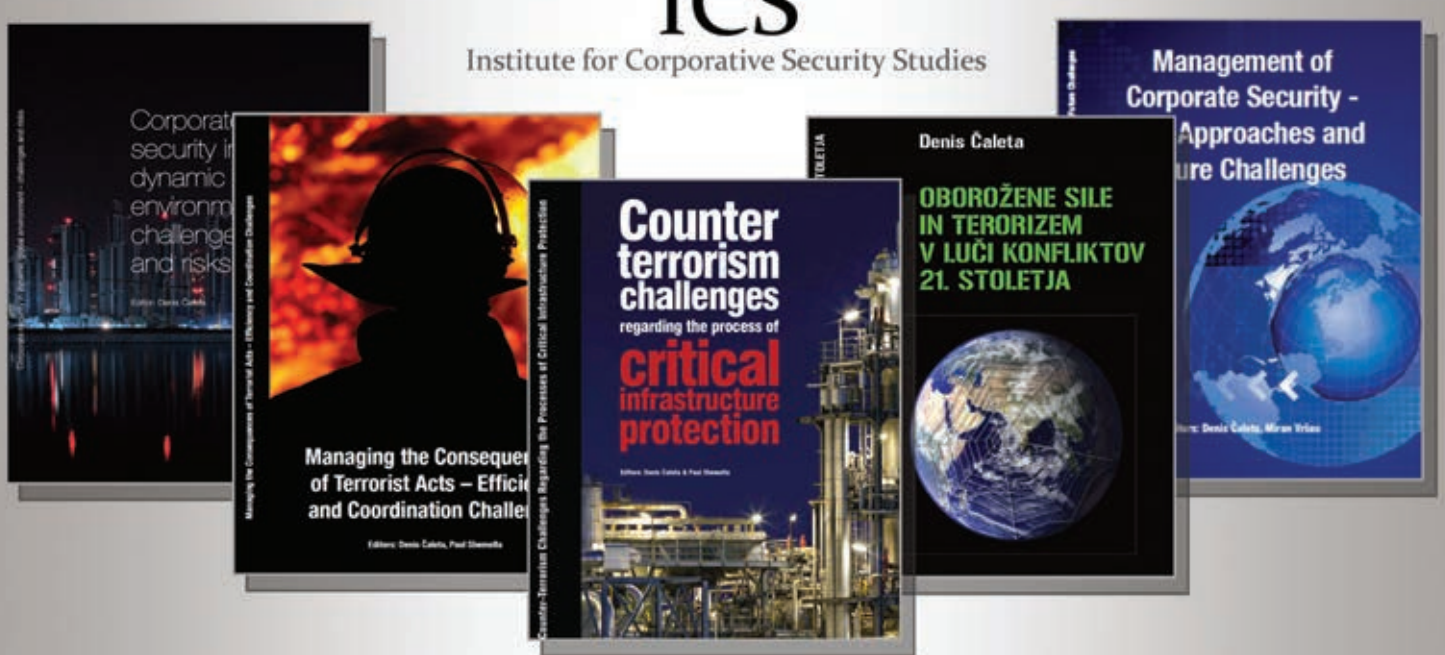


ICS PUBLIKACIJE

www.ics-institut.si

ICS

Institute for Corporative Security Studies





PRENAŠAMO ENERGIJO, OHRANJAMO RAVNOVESJE.

Brez električne energije naš svet udobja ne obstaja. Vsakdanjost, ki jo imamo za samoumevno, je izjemna. Vsak trenutek lahko z električno energijo uresničimo svoje potrebe in želje. Vsak trenutek lahko živimo po svoje. Z zavedanjem, da nekdo 24 ur na dan skrbi za njen zanesljiv, varen in neprekinjen prenos. Ta nekdo je ELES. Smo nosilec slovenske energetske hrbtenice. Kot sistemski operater slovenskega elektroenergetskega sistema ohranjamo ravnovesje znotraj prenosnega omrežja in hkrati skrbimo za njegov razvoj. Strateško, odgovorno in trajnostno načrtujemo, gradimo in vzdržujemo prenosno omrežje Slovenije. Za električno energijo na dosegu roke.

www.eles.si

ELES