Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2013, junij • št. 4



Policija je pomemben partner pri zagotavljanju korporativne varnosti

g. Stanislav Veniger, Generalni direktor Policije

Nov magistrski program

"MANAGEMENT KORPORATIVNE VARNOSTI"

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

Prvim desetim strankam, ki se bodo javile na elektronski naslov: *miran.vrsec@novapanorama.si* ponujamo brezplačno uro varnostnega svetovanja na temo kako optimizirati investicije v varnostni sistem in tekoče stroške financiranja varnostnega sistema?

IZVIRNA MISEL

Profesionalni in celovit varnostni sistem v podjetju odločilno prispeva k povečanju pozitivnih poslovnih izidov ter k dvigu kulture, konkurenčnih prednosti in ugledu podjetja (M. Vršec).

PRAVA IZBIRA

Nova Panorama, d. o. o. je ob sodelovanju vrhunskih varnostnih strokovnjakov usposobljena izvajati varnostni inženiring, to je varnost od A do Ž oziroma t. i. "varnost na ključ". Gre za vzpostavljanje integralnih varnostnih sistemov na projektni način, z integracijo varovanja v sisteme vodenja kakovosti z uvajanjem varnostnih standardov ter z upoštevanjem dobre prakse. Konkretni projektni proizvod je izdelava in implementacija varnostnega elaborata.

Storitve in produkti Nova Panorama, d. o. o. naročniku oziroma uporabniku zagotavljajo uvedbo varnostno in ekonomsko upravičenega varnostnega sistema, ki vzpostavlja ustrezno preventivo, opozorilni sistem in proces obvladovanja ranljivosti, ogroženosti, sprememb, tveganj in izrednih dogodkov.

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

- Načini (oblike) svetovanja
- Posnetek in analiza stanja
- Intervjuji in vprašalniki
- Ocene ogroženosti
- Varnostni elaborati
- Pravilniki, načrti, navodila

Integralni varnostni sistemi (celovito varovanje)

- Varnostna funkcija
- Varnostna politika
- Varnostna strategija
- Pravna podlaga
- Organiziranost in status varovanja
- Področja varnosti
- Civilna zaščita
- Varnostni menedžment
- Varnostni režim
- Alarmni in odzivni sistem
- Strokovni nadzor
- Portfelj zavarovanj

Varovanje oseb in premoženja

- Varovanje ljudi premoženja
- Prevoz in varovanje denarja ter drugih vrednostnih pošiljk
- Varovanje javnih zbiranj
- Izvajanje sistemov tehničnega varovanja

Kakovost in varnost

- Integracija varovanja v ISO 9000:2000
- Varnostni standardi
- Presojevalci kakovosti varovanja

Krizno vodenje (krizni menedžment)

- Objektivna potreba po načrtovanju kriznega vodenja
- Poslovanje na rezervni lokaciji

IZOBRAŽEVANJE

Varnostni menedžment

- Obvladovanje poslovnih in varnostnih tveganj ("risk management")
- Usposabljenje kriznega štaba
- Varnostna služba – usposobljenost varnostnikov za naloge varovanja podjetja
- Varnostna kultura in poslovna etika
- Usposabljanje za nadzornike
- Scenariji obvladovanja izrednih dogodkov



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
junij 2013

Izvod revije je brezplačen

Naslovnica:
123RF Limited

ISSN 2232-6170

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

Slovensko poslovno okolje je še vedno močno v krču gospodarske in finančne krize, ki pušča posledice tudi na področju varnosti. V iskanju rešitev kako organizacijo narediti bolj vitko in predvsem finančno vzdržno, se strateški management vse prevečkrat odloča za drastične reze ravno na področju obvladovanja tveganj v njihovih organizacijah. S predpostavko, da je Slovenija varno okolje se zelo lahkotno odločajo za krčenje razvojnih sredstev, ki so nujno potrebna tudi na področju korporativne varnosti. S tem svoje organizacije potiskajo v situacijo, ko ne bodo sposobne ustreznega zaznavanja tveganj in groženj, katere se pojavljajo v vedno novih modalitetah in imajo lahko za posledico tudi propad marsikatere organizacije, ki ne bo sposobna ustreznega odzivanja. Iluzija varnega okolja se hitro razblini, ko smo dnevno priča devijantnim dogodkom vdorov v plačilne sisteme podjetij, odtujitev ali zloraba ključnih poslovnih informacij, korupcija, namerna poškodovanja lastnine organizacije in mnogo drugih dejanj, ki se realno dogajajo in se v obdobju krize še intenzivirajo. V tem okviru bi tokrat želel izpostaviti dva ključna dejavnika, ki imata še posebej pomemben vpliv na učinkovito delovanje organizacij sedanjosti. Prvi dejavnik predstavljajo zaposleni, ki naj bi, kot večkrat radi uporabimo »oguljeno frazo«, predstavljali največji potencial vsakega poslovnega in drugega organizacijskega sistema. Na žalost se v slovenskem okolju vse premalo zavedamo tega dejstva in na vsak način želimo na kadrovskem potencialu prihraniti znaten del stroškov ali investicij podjetij. Da je ta stvar še bolj kritična se varčuje predvsem na njihovem izobraževanju, to pa ima lahko dolgoročne in nepopravljive posledice. Človek na drugi strani predstavlja tudi najšibkejši člen vsakega varnostnega sistema in, če pogledamo statistiko je s človeškimi ravnanji ali opustitvami povezano več kot 80% vseh varnostnih problemov oziroma devijantnosti v organizacijah. Visoka mobilnost delovne sile v globalnem poslovnem okolju postavlja te procese še v zahtevnejšo obliko, še posebej, če se zavedamo, da je vzpostavitev ustrezne organizacijske in posredno, kar je še pomembneje, varnostne kulture, izredno zahteven proces. Drugi ključen dejavnik v informacijski družbi pa vsekakor predstavlja skoraj usodna odvisnost od informacijsko-komunikacijske tehnologije, ki je vključena skoraj v vsak proces našega življenja in seveda s tem tudi delovanja organizacij. Zatiskanje oči pred tveganji in odprtimi dilemami, ki jih na varnostnem področju prinaša uporaba te tehnologije in s tem povezane grožnje kibernetskega kriminala in kibernetskih napadov na podjetja, med katerimi so še posebej izpostavljena tista organizacijska okolja, ki obvladujejo kritično infrastrukturo, imajo lahko za delovanje naših organizacij nepopravljive posledice. Z neupoštevanjem ustreznih varnostnih ukrepov lahko že s povezavo na omrežje postane naša organizacija ogrožena iz kateregakoli konca zemeljske oble oziroma globalnega medmrežja. Če v ta kontekst dodamo še tveganja, ki jih poleg tega prinaša neusposobljen in apatičen kadrovski potencial, potem se z neupoštevanjem osnovnih varnostnih principov igramo z zelo nevarno eksplozivno mešanico, ki nam zagotovo lahko zamaje temelje normalnega in varnega delovanja naše organizacije.

V tokratni številki revije »Korporativna varnost« smo posvetili pozornost različnim temam, ki so posredno in neposredno povezane z zgornjima izpostavljenima dejavnikoma sistemskega pristopa na področju korporativne varnosti

Doc. dr. Denis Čaleta
Glavni urednik



INTERVJU
g. Stanislav Veniger
generalni direktor Policije

POLICIJA JE POMEMBEN PARTNER PRI ZAGOTAVLJANJU KORPORATIVNE VARNOSTI V ORGANIZACIJAH 5



VOJNA ZA INFORMACIJE – RESNIČNOST ALI FIKCIJA

V globalnem dinamičnem okolju temelječem na razvoju informacijske družbe, je aktualna informacija postala ključna vrednost za prevlado nad konkurenco. 10



NIZKA CENA STORITEV VAROVANJA KOT EDEN POMEMBNIH VIROV TVEGANJA

Misel, da za »Malo denarja dobimo malo muzike«, je praviloma sinonim za tiste produkte in storitve, ki že na prvi pogled kažejo slabšo kakovost, mi pa od njih neupravičeno pričakujemo višjo dodano vrednost, večjo kakovost in delovanje na dolgi rok. 12



FINANČNI VIDIKI OBVLADOVANJA VARNOSTNIH TVEGANJ V IGRALNIŠTVU

Eden izmed osnovnih pogojev za nemoteno poslovanje igralnic in igralnih salonov je vsem udeležencem zagotoviti varno igralniško okolje. 33



JEDRSKA VARNOST V EVROPSKI UNIJI PO FUKUSHIMI

Jedrskih nesreč, ki bi znatno kontaminirale okolje, je relativno malo. Običajno nesreče v jedrskih objektih, če so te sploh povezane z radioaktivno kontaminacijo, povzroče le zelo omejeno kontaminacijo. 52

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

INTERVJU
g. Stanislav Veniger
generalni direktor Policije

POLICIJA JE POMEMBEN PARTNER PRI ZAGOTAVLJANJU KORPORATIVNE VARNOSTI V ORGANIZACIJAH

Ohranjanje visoke ravni in dosedanjih standardov zagotavljanja varnosti spričo pomanjkanja finančnih sredstev za policijo predstavlja zagotovo velik izziv. Prilagoditi se bo treba novim, zahtevnejšim situacijam in okoliščinam. Tesnejše sodelovanje s subjekti, ki zagotavljajo korporativno varnost je lahko pomemben korak pri učinkovitejšem obvladovanju varnostnih tveganj, katere prinaša dinamično gospodarsko okolje.

Kako vidite nadaljnji razvoj policije v teh zahtevnih gospodarskih in družbenih okoliščinah?

Policija je zanesljiva partnerica skupnosti. Naj uvod pričnem z vizijo slovenske policije, ki zaposlenim v policiji skupaj s poslanstvom in vrednotami sporoča, kdo smo in kako želimo biti prepoznavni v širši družbi. S svojim vsakdanjim delom se trudimo, da je ta vizija tudi del naše organizacijske kulture, ne glede na drastične spremembe v družbi. Osebno menim, da so prelomni časi, tudi časi za premislek in priložnost za racionaliziranje in izboljšanje svojega delovanja, tako v družbi kot v organizacijah, ki smo zadolžene za varnost.

Preteklo leto je bilo prelomno za državo kot tudi državljane, soočeni smo bili s posledicami globalne finančne nestabilnosti. Že v začetku preteklega leta nas je javnofinančna kriza s krčenjem sredstev prisilila v določene organizacijske reze in druge težke odločitve, vključno z upokojitvami in poseganjem v že pridobljene pravice zaposlenih. S t. i. projektom Kaskade smo poskušali zmanjšati število uslužbencev, ki opravljajo naloge administrativne narave na državni in regionalni ravni, ter povečati število uslužbencev, ki opravljajo operativne naloge na regionalni in lokalni ravni. Vseskozi pa smo si v vodstvu Policije in v sodelovanju s sindikati aktivno prizadevali, da bi bili varčevalni ukrepi za naše zaposlene čim manj boleči in da bi poiskali rešitve, ki bi bile v danih okvirih čim bolj optimalne. S takšnimi sistemskimi ukrepi smo se prilagajali proračunskim možnostim države, tako da z manjšimi resursi zagotavljamo enako stopnjo varnosti ljudem v naši državi.

Dobre temelje za delo v prihodnosti smo si zagotovo postavili z novo policijsko zakonodajo. Lani smo namreč ob sodelovanju strokovnjakov z notranjega ministrstva dokončali celovito prenovo, začeto že leta 2009, in pridobili trenutno še »sveža« Zakon o nalogah in pooblastilih policije ter Zakon o organiziranosti in delu v policiji. S pomočjo nove policijske zakonodaje, ki policij-

Mogoče bolj kot kdaj koli prej je za našo organizacijo pomembno širjenje integritete in etike v naše delovne strukture, saj sta brez tega tudi vizija in poslanstvo zgolj črki na papirju.

*avtor je član Slovenskega združenja korporativne varnosti

skim upravam in postajam daje več samostojnosti, se bo policija lahko še bolj približala lokalnemu okolju. Med drugim zakona prinašata določene spremembe tudi na področju zagotavljanja javnega reda in miru, zaradi česar bomo, upam, lahko učinkovitejši pri zmanjševanju nasilja in vandalizma na športnih prireditvah. Na področju varovanja državne meje pa se bomo morali prilagoditi predvidenemu vstopu sosednje Hrvaške v Evropsko unijo in ukinitvi carinske kontrole. V zvezi s tem sta se slovenska in hrvaška policija že lani dogovorili za uvedbo skupne mejne kontrole, ki bo pripomogla k intenzivnejšemu čezmejnemu sodelovanju, optimalni izrabi kadrovskih virov, predvsem pa bo prehajanje meje za državljane hitrejše in bolj enostavno. Še boljše storitve prebivalcem naše države pa bomo lahko zagotavljali tudi z nadaljevanjem pilotskega projekta Mobilna policijska postaja in uresničevanjem letos sprejete nove strategije policijskega dela v skupnosti. Zavedamo se, da je treba še naprej krepiti transparentnost delovanja policije in jo odpirati ljudem. Varnost je namreč naša skupna dobrina in svojega dela si ne predstavljamo več brez pomoči in sodelovanja državljanov, tako da bodo pri letnih načrtih dela policijskih postaj vključeni tudi predlogi lokalnih skupnosti.

Opremljenost policije ne sledi potrebam realnega okolja in tempu, ki bi si ga verjetno vsi želeli. Kaj lahko naredimo na področju opremljanja in s tem dvigovanja učinkovitosti dela Policije?

Poudaril bi, da sem izjemno ponosen na zaposlene v Policiji, saj ne glede na varčevalne ukrepe, ki vplivajo tako na nižanje sredstev za materialne stroške, investicije v dotrajano opremo in objekte ter plače in dodatke iz plačnega sistema, so rezultati dela slovenske policije zelo dobri. Iz letnega poročila o delu policije za lansko leto denimo izhaja, da so se znižale pritožbe zoper postopke policistov, teh je bilo za skoraj četrtino manj kot v preteklih letih. A še bolj kot to so zgovorni statistični podatki na glavnih področjih policijskega dela, kot so zagotavljanje prometne varnosti, javnega reda in miru, varovanje meje ter odkrivanje in preprečevanje kriminalitete. Pri slednji je bilo v času vsesplošne krize prioritetno predvsem odkrivanje finančnih malverzacij. Kako pereča so gospodarska kazniva dejanja, pove že podatek, da smo obravnavali skoraj enako število kaznivih dejanj kot leto poprej, pri čemer pa je škoda, ki so jo povzročili njihovi storilci, narasla s 176 (v letu 2011) na kar 449 milijonov evrov (v letu 2012), torej na skoraj pol milijarde evrov! Podatek o povzročeni gospodarski škodi kaže, da je policija na pravi poti v boju proti gospodarski kriminaliteti in bo z njim odločno nadaljevala. Tudi na področju finančnih preiskav so kriminalisti opravili za petino več preiskav. Kot odziv na naraščajoča gospodarska kazniva dejanja smo že konec preteklega leta sprejeli strategijo za obvladovanje gospodarske kriminalitete v državi in resolucijo o nacionalnem programu za preprečevanje in zatiranje kriminalitete do leta 2016. Osnovni cilj resolucije je stalno in dolgotrajno zagotavljanje varnosti vseh prebivalcev v Sloveniji, zato njeno temeljno načelo temelji na preventivnem delovanju, ne na represiji.



Skupaj z ministrstvom za notranje zadeve si bomo tudi v prihodnosti prizadevali za pridobitev sredstev iz evropskih finančnih virov, kar pa je tudi odvisno od zmožnosti proračuna, saj delujejo evropski finančni inštrumenti na osnovi sofinanciranja. V obdobju od 2007 je bilo tako ministrstvu in policiji odobrenih malo preko 50 milijonov evrov iz skladov in drugih finančnih virov EU, predvsem za nakup opreme, usposabljanje in krepitev sodelovanja z drugimi državami. V tem času se pripravlja tudi nova finančna perspektiva EU za obdobje 2014–2020, ki bo tudi v prihodnosti omogočila podporo EU za aktivnosti policij iz t. i. Sklada za notranjo varnost. Partnerstva pri prijavi projektov za sofinanciranje iz evropskih virov, sinergija aktivnosti, ki jih izvajajo podobne organizacije, boljša izraba javno-zasebnega partnerstva so vsekakor ključni inštrumenti oz. ukrepi, ki lahko zapolnijo vrzel, nastalo zaradi zmanjšanih proračunskih virov, in

Glede na ukrepe, ki jih uvajamo, in rezultate ocenjujem, da se je policija zmožna prilagajati novim spremembam in izzivom, tako da bo tudi v prihodnosti zagotavljala visoko stopnjo varnosti v državi.

tako tudi v prihodnje zagotovijo učinkovito delo policije.

Seveda pa bo ohranjanje visoke ravni in dosedanjih standardov zagotavljanja varnosti spričo pomanjkanja finančnih sredstev za policijo zagotovo velik izziv. Prilagoditi se bo treba novim, zahtevnejšim situacijam in okoliščinam. Delovanje slovenske policije bomo zato morali optimizirati. Z razpoložljivimi kadri in sredstvi bomo morali postati še bolj učinkoviti, se pa zavedamo, da z vse manjšimi viri učinkovitosti ni mogoče povečevati v nedogled. Že lani smo veliko truda namenili izboljšanju delovnih procesov in klime v policiji, krepitvi osebnostne in organizacijske integritete ter psihološki pomoči in podpori zaposlenim. Tudi v prihodnje si bomo prizadevali za dobre medsebojne odnose v kolektivih in nadaljevali z zmanjševanjem administrativne obremenjenosti delavcev, z zagotavljanjem zdravja in varnosti pri delu ter z zaščito policistov pred napadi, šikaniranjem, grožnjami, pa tudi z nudenjem pravne pomoči, kadar so v sodnih postopkih. Za učinkovito uporabo virov in usmerjanjem trajnega razvoja, upoštevaje našteto, pripravljamo dolgoročni razvojni program policije do leta 2020, ki bo zagotavljal racionalno načrtovanje porabe sredstev in trajnostni razvoj policije.

Mogoče bolj kot kdaj koli prej je za našo organizacijo pomembno širjenje integritete in etike v naše delovne strukture, saj sta brez tega tudi vizija in poslanstvo zgolj črki na papirju. V policiji se temu področju posvečamo že vrsto let, tako da smo sistemski pristop razvili že na zavidljivo raven. Tako je policija v 2011 ustanovila Odbor za integriteto in etiko, ki je posvetovalno telo generalnega direktorja policije in je namenjeno sistematičnemu preučevanju strateških predlogov, novosti, vprašanj in dilem s področja integritete in etike. Odbor deluje na področju etike, osebnostne in organizacijske integritete, človekovih pravic in svoboščin, enakih možnosti obeh spolov ter na področju upravljanja organizacijskih konfliktov (pomirjanje konfliktov in mediacija). Tako smo za izboljšanje delovnih procesov in organizacijske klime v policiji, na podlagi predloga odbora, vzpostavili kar nekaj projektov. Naj iz projekta Organizacijska klima in podoba policije v javnosti 2012–2015 izpostavim le nekaj ključnih; z namenom izboljšanja medsebojnih odnosov v vseh naših organizacijskih enotah bomo v policiji, v sodelovanju s kompetentnimi notranjimi in zunanjimi strokovnjaki, vključno s predstavniki reprezentativnih sindikatov, v letu 2013 izvedli prvo merjenje organizacijske klime. Merjenje organizacijske klime v letu 2013 bo anonimno in izvedeno s pomočjo elektronske aplikacije. Drugi projekt je pilotski projekt Etični telefon, ki je zamišljen kot orodje za pomoč zaposlenim v policiji, da sprožijo pobude in postavijo vprašanja v zvezi z etičnimi dilemami, ki se nanašajo na delo organa oziroma posameznikov v njem, prav tako pa je izhodišče za nadaljnje izobraževanje in usposabljanje s področja etike in integritete. Temeljni namen projekta je, da se na različne načine omogoči zaposlenim v policiji, da pridejo do informacij in pomoči na tem področju.

Naj zaključim, organizacijske in sistemske spremembe so nujni del kakovostnega upravljanja, impulze, ki zahtevajo prilagajanje novim izzivom, pa mora v pravem času prepoznati vodstvo. Glede na ukrepe, ki jih uvajamo, in rezultate ocenjujem, da se je policija zmožna prilagajati novim spremembam in izzivom, tako da bo tudi v prihodnosti zagotavljala visoko stopnjo varnosti v državi.

Izobraževanje in usposabljanje verjetno tudi naprej ostaja ključna komponenta vložkov v kadrovski potencial Policije. Kakšni so vaši načrti na tem področju?

Pri vprašanju, kako med mladimi zagotoviti ustrezno zanimanje za poklic policista, se je potrebno osredotočiti predvsem na motiv posameznika za opravljanje tega poklica. Za uspešno in učinkovito izvajanje nalog policista je ključno, da je posamezniku na prvem mestu želja po opravljanju tega poklica. Če se nekdo odloči, da se prijavi na razpis samo zaradi ekonomskih razlogov, ker drugje ni mogoče dobiti službe, potem se lahko to odraža tudi pri njegovem delu. Na tem mestu naj omenim tudi novost v izobraževalnem sistemu, ki bi lahko predstavljajo pozitivno motivacijo pri posameznikih, da se odločijo za opravljanje poklica. Po novem se bo v Policiji izvajal nov višješolski študijski program Policist, ki bo udeležencem omogočal pridobitev formalne izobrazbe. Po prejšnjem programu, ki je trajal 18 mesecev, je bil posameznik usposobljen za opravljanje poklica, ni pa pridobil višje stopnje izobrazbe. Razumljivo pa je, da smo glede zaposlovanja trenutno zelo omejeni. Usposabljanje policistov razumemo v policiji kot permanenten način zagotavljanja učinkovitega in kakovostnega dela, zato je področje usposabljanja policistov vključeno v vse letne, srednjeročne in dolgoročne strateške dokumente.

Menite, da je združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti lahko odgovor na obvladovanje zahtevne varnostne situacije in ali so lahko taka združenja ustrezen partner policiji pri zagotavljanju njenega osnovnega poslanstva?

Novi Zakon o organiziranosti in delu v policiji namenja partnerskemu sodelovanju policije z drugimi subjekti za zagotavljanje večje varnosti celotno poglavje in nalaga policiji tudi dolžnost, da jim v okviru svojih pristojnosti in možnosti nudi pomoč. Partnerske oblike sodelovanja policije z organi lokalne skupnosti, drugimi organi, organizacijami in institucijami, civilno družbo ali posamezniki, katerih dejavnost je usmerjena k zagotavljanju večje varnosti, vzpodbujajo k samozaščitnemu ravnanju in varnostnemu samoorganiziranju ter pomoči, vzpodbujajo tudi skupno preprečevanje varnostne problematike, odkrivanje in odstranjevanje vzrokov in pogojev za nastanek kaznivih dejanj. Takšne oblike sodelovanja so bistven element zagotavljanja javne varnosti.

Nasilno izražanje nezadovoljstva na ulicah večjih slovenskih mest je pokazalo, da policija ob množičnih izgredih na različnih koncih Slovenije stežka zagotavlja dovolj sil, ki bi

Sodelovali smo pri varovanju kar 87 protestnih shodov po vsej Sloveniji!

Po raziskavi Eurobarometra že skoraj vsak tretji prebivalec v Evropski uniji ni prepričan o varni uporabi interneta za finančne transakcije in prenos osebnih podatkov, že skoraj vsak deseti uporabnik pa je bil žrtev goljufije, storjene s pomočjo interneta.

poskrbele za javni red in mir. Kako izboljšati komunikacijo med Policijo in odgovornimi v organizacijah za korporativno varnost pri usklajenih aktivnostih zavarovanja premoženja in varnosti na površinah, ki so v neposredni bližini varnostno rizičnih dogodkov?

Seveda ob pogledu na lansko leto ne moremo mimo številnih protestov in množičnih nasilnih izgredov na nekaterih od njih, ko smo se morali v policiji maksimalno angažirati, da smo zagotovili varnost vseh udeležencev. Sodelovali smo pri varovanju kar 87 protestnih shodov po vsej Sloveniji! Lahko rečem, da smo to preizkušnjo uspešno prestali. Vse izgrede smo strokovno, učinkovito in zakonito obvladali, ob tem pa ohranili zaupanje slovenske javnosti. Policisti se namreč niso izneverili pričakovanju ljudi, da bodo tudi v zaostrenih varnostnih situacijah hitro in odločno zavarovali njihova življenja in premoženje. Na ta način smo zagotavljali ustavno pravico državljanov do javnega izražanja, pri čemer sem vesel, da je večina udeležencev na kasnejših shodih že upoštevala naše pozive k strpnemu in mirnemu izražanju stališč. V skladu z novo strategijo v skupnost usmerjenega policijskega dela se bomo preko različnih forumov in oblik partnerskega sodelovanja poskušali še bolj približati posameznikom in organizacijam, odgovornim za varnost, tako da izkoristimo vse potenciale, ki jih takšna sodelovanja lahko nudijo.



So po vašem mnenju procesi centralizacije državne uprave in s tem tudi policijske organizacije pravi korak v smeri zagotavljanja javne varnosti?

Menim, da moramo iskati ravnotežje med centralizacijo in decentralizacijo državne uprave glede na cilje, ki jih je treba doseči. Tako je lahko v nekaterih primerih centralizacija ustrezen odgovor ob iskanju rešitev za bolj racionalne oblike upravljanja, hkrati pa ima ta oblika slabost, da ne prepozna problematike oz. potreb na lokalni ravni, saj ni v neposrednem stiku z uporabniki njenih storitev. V policiji nenehno iščemo to občutljivo ravnovesje. Tako smo sicer zmanjšali število regionalnih policijskih uprav, ne pa tudi števila policijskih postaj na lokalni ravni. Z novo policijsko zakonodajo pa smo začeli tudi proces krepitve decentralizacije in zagotavljanja večje avtonomnosti in samostojnosti policijskih uprav, ki jih bomo tako bolj približali varnostnim problemom, ki so specifični za posamezne lokalne skupnosti.

Pojavljajo se vedno nove oblike groženj, ki v tem dinamičnem okolju zahtevajo kompleksnejši in sistemski pristop za njihovo preprečevanje. Posebej so v tem okviru v zadnjem obdobju izpostavljene grožnje računalniškega kriminala in zlorabe informacijsko komunikacijskih sistemov za napade na organizacije. Kako se policija sooča s temi novimi varnostnimi izzivi?

Poudaril bi, da smo od druge polovice 2012 ugotovili porast števila kaznivih dejanj, ki se nanašajo na vdore v elektronsko bančništvo, nadaljnjih tatvin

Zaradi tesnih zgodovinskih, jezikovnih in kulturnih vezi se člani hudodelskih združb iz regije zahodnega Balkana hitro povezujejo in ustvarjajo združbe, ki ali organizirajo izvedbo kaznivih dejanj ali pa nudijo logistično in podporno dejavnost.

in posledično »pranja denarja«, pridobljenega s kaznivimi dejanji. Takšen trend je zaradi razširjenosti novih tehnoloških informacijskih sistemov in omrežij seveda globalen pojav, tako da to okolje postaja vedno bolj tudi osnovno orodje za zlorabe in kraje identitete, goljufije, kazniva dejanja finančne narave, nedovoljeno trgovino s ponarejenim blagom, zdravili, drogami in orožjem ter zlorab otrok. Po raziskavi Eurobarometra že skoraj vsak tretji prebivalec v Evropski uniji ni prepričan o varni uporabi interneta za finančne transakcije in prenos osebnih podatkov, že skoraj vsak deseti uporabnik pa je bil žrtev goljufije, storjene s pomočjo interneta.

V policiji smo sicer že v 2009 pripravili organizacijske in kadrovske spremembe, tako da smo ustanovili Center za računalniško preiskovanje v Generalni policijski upravi in 4 regionalne centre, prav tako pa krepimo tudi druge službe s strokovnjaki za preiskovanje in računalniško forenziko. Kot sem že navedel, pa sta kibernetska kriminaliteta in tudi odzivanje pristojnih organov globalen izziv. V Evropski uniji smo zaradi tega v začetku leta ustanovili Evropski center za boj proti kibernetski kriminaliteti (imenovan EC3), ki deluje v okviru Europola. Ta center ima nalogo, da podpira države članice pri preiskovanju kaznivih dejanj, prav tako pa tudi, da nudi ekspertna znanja, usposabljanja in programska orodja. Zavedati se moramo, da že programska orodja, ki jih potrebujejo preiskovalci, dosegajo visoke stroške, prav tako pa so vse države omejene s strokovnjaki na tem področju. Zaradi tega je seveda ključno mednarodno sodelovanje, kjer se s podporo Interpola ali posameznih držav zoperstavimo tem izzivom. Kot odličen primer mednarodnega sodelovanja v boju zoper kibernetsko kriminaliteto lahko navedemo medijsko znani primer Mariposa, ki ga je preiskovala slovenska policija v sodelovanju z ameriškim zveznim preiskovalnim uradom (FBI) in španskimi organi odkrivanja in pregona. V Evropski uniji gremo tako v pravo smer, saj je tudi Evropska komisija v začetku aprila predlagala obsežen paket zakonodajnih in drugih ukrepov, ki bodo zagotovili tudi bolj varno prihodnost uporabnikov novih informacijskih sistemov. Ti ukrepi pa se ne nanašajo zgolj na kriminaliteto, temveč na celotno politiko, vključujoč varnost informacijskih omrežij in zaščito kritične infrastrukture, kar bo imelo izrazit vpliv na vse resorje v Sloveniji.

Želim pa še poudariti, da je ključno tudi sodelovanje z drugimi organizacijami v Sloveniji; tako policija že leta uspešno sodeluje z nevladnimi organizacijami, ki skrbijo za varnost in spremljanje nezakonitih vsebin na internetu, kot je npr. SI-CERT (nacionalni center za zaznavanje in spremljanje incidentov v omrežjih) in Spletno oko, ki so za nas ključni partner pri zatiranju kriminalitete.

Katere mednarodne projekte, pri katerih uspešno sodelujete, bi posebej izpostavili in ki pomembno pomagajo pri zmanjševanju tveganj s strani organiziranega kriminala v regiji? S svojim prenosom dobrih praks in izkušenj ste zelo aktivni tudi v mednarodnem sodelovanju. To dokazuje tudi nedavno končana mednarodna konferenca z nazivom »Combating Transnational Organized Crime and Enhencing Border Security Processes«, ki ste jo soorganizirali z George Marshall Centrom in Institutom za korporativne varnostne študije? Kakšna je dodana vrednost takega sodelovanja?

Geografska vpetost Slovenije na stičišču Srednje Evrope, Sredozemlja, Jugozahodne Evrope, dobre prometne povezave in tudi njena velikost vplivajo na povpraševanje in ponudbo nezakonitega blaga in storitev, ki jih nudijo organizirane kriminalne združbe. Območje Slovenije je predvsem tranzitno območje in ne toliko ciljna destinacija za takšne združbe. To potrjuje tudi zadnje Europolovo poročilo, objavljeno v začetku leta, o ogroženosti pred organizirano kriminaliteto in drugimi hudimi oblikami kriminalitete. Zaradi tesnih zgodovinskih, jezikovnih in kulturnih vezi se člani hudodelskih združb iz regije zahodnega Balkana hitro povezujejo in ustvarjajo združbe, ki ali organizirajo izvedbo kaznivih dejanj ali pa nudijo logistično in podporno dejavnost. Slovenija se kot država članica EU tega seveda zaveda, tako da je slovenska policija pomemben segment v evropski varnostni arhitekturi za zagotavljanje notranje varnosti EU. Hkrati pa se naša država zaveda tudi, da je za zagotavljanje stabilnih državnih struktur v državah zahodnega Balkana, ki bodo uspešne pri zatiranju kriminalitete, nujno krepiti njihove zmožnosti. Tako slovenska policija podpira aktivnosti, s katerimi se krepijo oblike sodelovanja v tej regiji. Podlaga za uspešen pregon kaznivih dejanj, ki imajo čezmejno dimenzijo, je seveda skupen pravni okvir in primerljivi standardi za odkrivanje in preiskovanje kaznivih dejanj. Trenutne oblike sodelovanja bodo ravno v maju nadgrajene z novim mednarodnim pravnim okvirjem, saj je Slovenija postala članica držav mednarodne Konvencije o policijskem sodelovanju v jugovzhodni Evropi. Ta bo med drugimi ukrepi omogočala enostavno in hitro vzpostavitev skupnih preiskovalnih skupin z vsemi organi za preiskovanje in pregon držav v regiji, tako da bodo preiskovalci iz različnih držav preiskavo hujših oblik kaznivih dejanj izvajali praktično z ramo ob rami.

Zaradi navedenega lahko razumete, da nam je sodelovanje z različnimi akterji doma in v mednarodnem prostoru zelo pomembno. Konferenca, ki ste jo navedli, je odličen primer združevanja znanja in izkušenj s ciljem, da smo v regiji proaktivni in ohranjamo vlogo pomembnega partnerja za preiskovanje in pregon kriminalitete. Naj izkoristim še priložnost in se za dobro sodelovanje pri izvedbi konference osebno zahvalim Institutu za korporativne varnostne študije. ■

Naj izkoristim še priložnost in se za dobro sodelovanje pri izvedbi konference osebno zahvalim Institutu za korporativne varnostne študije.

Avtor: Andrej Podvršič / korporativno varnostni manager, DuPont de Nemours International*



VOJNA ZA INFORMACIJE – RESNIČNOST ALI FIKCIJA

V globalnem dinamičnem okolju temelječem na razvoju informacijske družbe, je aktualna informacija postala ključna vrednost za prevlado nad konkurenco.

Naše podjetje DuPont de Nemours International je znano širom po svetu kot korporacija, ki se že več kot dve stoletji s svojimi izumi in rešitvami trudi pomagati izboljšati kvaliteto življenja. Vedno s ponosom poudarjamo, da so naši delavci največje bogastvo, ki mu pa zelo tesno sledi naše znanje oziroma naš »know -how«! Zato tudi ne preseneča dejstvo, da na področju naše korporativne varnosti posvečamo največ pozornosti varovanju in zaščiti tema glavnima akterjema naših uspehov.

DuPont je globalna korporacija, prisotna v več kot 93 državah in zaposluje več kot 65 000 delavcev. Seveda kot vse ostale korporacije delujemo v izredno kompetitivnem okolju, ki deluje na legalnih in pa seveda tudi na nelegalnih temeljih. Ti zadnji pa seveda predstavljajo varnostno tveganje, ki ga je potrebno obvladovati. Neizpodbitno dejstvo je, da v realnem okolju že divja 3. svetovna vojna, ki pa se odvija v virtualnem svetu - svetu informacij. Politično in vojaško rivalstvo je nadomestila kruta in neizprosna ekonomska vojna, v kateri tako posamezniki, korporacije kakor tudi države ne izbirajo sredstev za pridobitev ključnih poslovnih, vojaških in ostalih skrivnosti. Po nekaterih podatkih ameriško gospodarstvo zaradi kraje poslovnih skrivnosti letno izgublja več kot 250 milijard $, izguba pa se bo v naslednjih desetih letih najmanj podvojila.

> Danes ni nihče imun na virus, ki bi ga lahko poimenovali »kraja poslovnih skrivnosti«. Slaba novica pa je, da na žalost cepiva za to »bolezen« še dolgo ne bo!

To varnostno tveganje pa je trenutno največji varnostni izziv, s katerim se soočajo tako države (lep primer lahko najdemo že v našem okolju saj je postal pravi nacionalni šport katera politična stranka bo razkrila več skrivnosti, ne glede na nacionalni interes in ugled), kakor tudi vsa podjetja širom po svetu. Danes ni nihče imun na virus, ki bi ga lahko poimenovali »kraja poslovnih skrivnosti«. Slaba novica pa je, da na žalost cepiva za to »bolezen« še dolgo ne bo!

Tudi v okolju naše korporacije smo daljnega leta 2005 doživeli hladen tuš in se zavedli, da imamo kljub naši izredno dobri delovni klimi in medsebojnemu zaupanju problem! Odkrili smo namreč, da je eden izmed naših znanstvenikov ob menjavi službe obenem odtujil tudi številne poslovne skrivnosti.

V preiskavo se je vključil FBI in državni tožilec. Osumljenec je priznal in bil obsojen na daljšo zaporno kazen. Seveda naša korporacija ni osamljena in po podatkih raziskav, je kar 60% anketiranih podjetij izkusilo krajo poslovnih skrivnosti v zadnjih 5 letih, pri čemer so bili izvršilci tatvin povečini zaposleni v podjetju, kar je še vedno prevladujoč trend. Te ugotovitve potrjujejo dejstvo, da so zaposleni, ob neustreznem ravnanju, največje tveganje za organizacijo.

Seveda je ta primer sprožil reakcijo, ki nas je pripeljala na dolgo potovanje, ki bi ga lahko opredelili kot »varovanje poslovnih skrivnosti«. Proces traja še danes in se po mojem mnenju v vsaki resni organizaciji tudi nikoli ne konča.

To seveda ni bil osamljen primer, zato je pričakovati, da dokler bo naše podjetje vlagalo velike vsote sredstev v razvoj novih izdelkov, se bo vedno našel nekdo, ki bo hotel ubrati bližnjico in si pridobiti znanje in informacije na nelegalen način! V primeru korejskega podjetja KO-

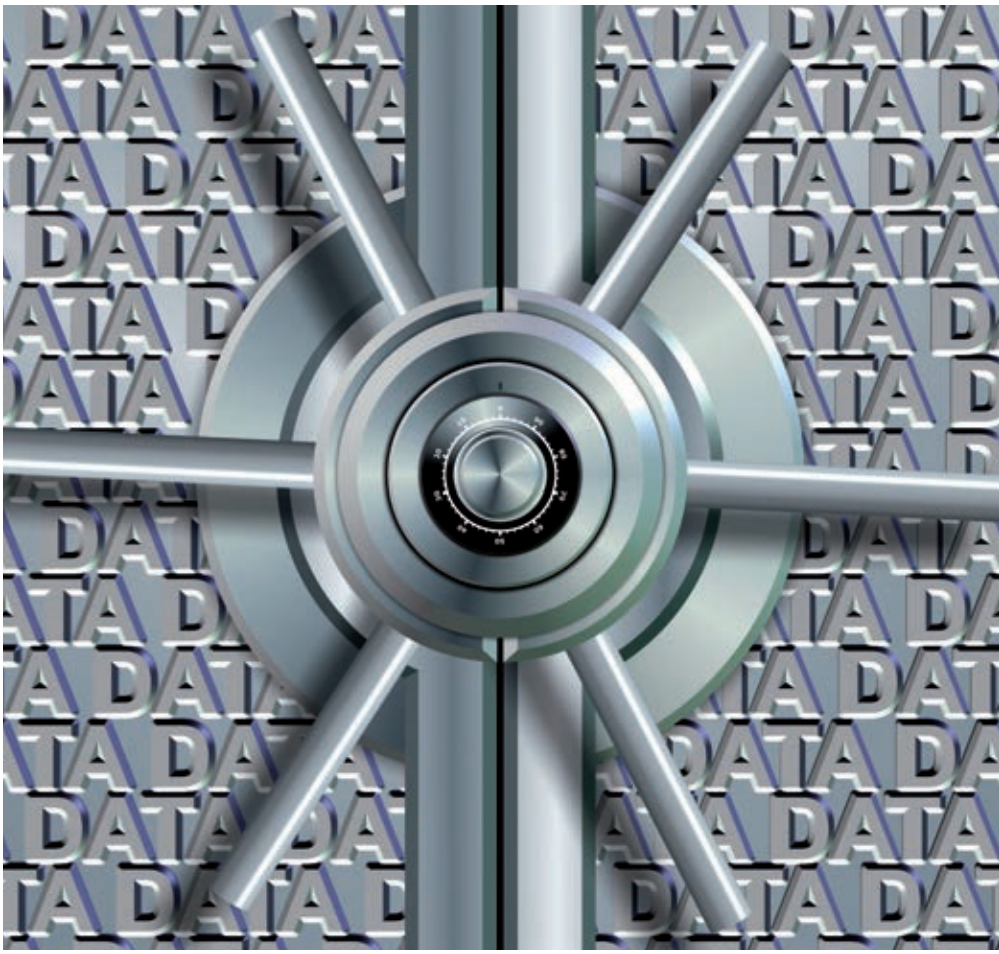
G. Andrej Podvršič je prejemnik nagrade Slovenian Security Award za leto 2012 v kategoriji »korporativno varnostni manager leta«.

*avtor je član Slovenskega združenja korporativne varnosti

LON, ki nam je ukradlo poslovne skrivnosti v zvezi s proizvodnjo posebnih zaščitnih vlaken, ki se uporabljajo za zaščito pred balističnimi izstrelki, nam je bila na sodišču dodeljena ena največjih odškodnin in sicer 900 milijonov $, kar samo potrjuje pravo vrednost poslovnih skrivnosti.

Naše podjetje je temu problemu posvetilo v preteklosti že veliko pozornosti, vendar je bilo potrebno drugače pristopiti k obvladovanju tega varnostnega izziva. Sledil je multidisciplinarni projekt, ki je na novo postavil temelje našega pristopa. Problemu smo pristopili sistematično in sicer:

1. Ustanovili smo multidisciplinarno - projektno skupino, ki je bila odgovorna direktno CEO, kar je zagotavljalo in še danes zagotavlja podporo strateškega managementa. Samo s podporo in sporočilom z vrha korporacije je možna uspešna implementacija obsežnih sprememb na področju varnostne kulture, ki mora potekati od vrha proti bazi in seveda v obratni smeri.
2. Inventura obstoječih poslovnih skrivnosti, ocena varovanja le-teh s konkretnim načrtom izboljšav in dosledno implementacijo ter nadzorom. Glede na velikost naše korporacije, številne lokacije in dinamično okolje v katerem se vrednost in pomen informacije spreminja skoraj vsakodnevno, je tak pristop postala ustaljena praksa.
3. Podrobna analiza pomanjkljivosti (t.i. gap-analiza) obstoječih notranjih prepisov, navodil in ocena implementacije le- teh, s predlogom sprememb in izboljšav. To pa je seveda samo pomemben del celotnega in zelo obsežnega načrta obvladovanja tega varnostnega tveganja.
4. Analiza vseh naših obstoječih primerov in identifikacija potencialnih svarilnih indikatorjev. Pri analizi smo prišli do praktično popolno identičnih ugotovitev glede profila storilcev kot številna druga podjetja. V prvi vrsti gre za nezadovoljne zaposlene, ki so si našli novo zaposlitev in se pri tem čutili upravičene, da s seboj odnesejo še »njihovo znanje«. Tovrstni storilci večinoma delujejo zelo oportunistično in v veliki meri izvršijo samo dejanje v zadnjih dveh mesecih pred odhodom. Drugi, veliko bolj pretkan tip je t.i. machiavelistični tat, ki se ponavadi tudi čuti upravičenega do poslovnih skrivnosti, je pa veliko bolj organiziran in dokaj pogosto tudi pridobi sodelavce, da mu pomagajo. Zadnji tip pa so ekonomski vohuni, ki pa so seveda najbolj nevarni in najtežje odkriti, saj delujejo pod okriljem tujih držav. Ekonomski vohuni leta in leta kot »speci agentje« delujejo v naši organizaciji. Ponavadi so zelo dobri, če ne že nadpovprečni in



v danem trenutku po podrobnih navodilih dotične vlade ukradejo dragocene podatke. Seveda pa so tu še tisti čisto »nevtralni«, ki delujejo pod okriljem organiziranega kriminala in ponujajo informacije/storitve najboljšemu ponudniku.

5. Analiza kadrovskih postopkov (sklenitev in prekinitev delovnega razmerja - intervju, preverke, delovno pravna razmerja s stališča varovanja IP, itd.). Tako smo v mnogih državah, kjer delovna zakonodaja dovoljuje, uvedli klavzulo o varovanju poslovnih skrivnosti kot pogoj za zaposlitev, oziroma če ugotovimo, da je oseba ravnala malomarno ali celo zlonamerno, je to takojšnja odpustitev (v skladu z obstoječo delovno-pravno ureditvijo). Zavedli smo se tudi, da je enakega pomena intervju ob prekinitvi delovnega razmerja kot ga izvajamo ob sami zaposlitvi, saj je to zadnja možnost za pogovor. To nam omogoča, da izvemo še potrebne podatke, okoliščine in razloge za odhod. Omenjeni podatki, pa nam služijo tudi, da iz takih primerov potegnemo določene zaključke in jih kot izkušnje upoštevamo pri izboljšanju našega sistema.
6. Prevetrili smo vsa usposabljanja in uvedli vrsto novih s poudarkom na varovanju poslovnih skrivnosti. Tako mora vsak zaposleni opraviti on- line trening s tega področja in uspešno opraviti preizkus znanja. Ta segment je v današnjem času ekonomske krize še kako pomemben, saj je vsem v organizaciji jasno da ob izgubi »know-how« izgubljamo tudi trg in s tem tudi delovna mesta.
7. Seveda brez nadgradnje obstoječih varovalnih mehanizmov in podatkovnih baz ne gre. To predstavlja konstanten proces, saj se zavedamo, da so storilci teh dejanj »bad guys« vedno korak pred nami. Danes ni podjetja na svetu, ki še ni bilo napadeno s strani hekerjev z jasnim ciljem kraje intelektualne lastnine.

Zaščita poslovnih skrivnosti in procesi kako se primerno zaščititi je del naših vsakodnevnih aktivnosti. Le z ozaveščanjem lahko spreminjamo varnostno kulturo, kar je tudi končni cilj vsakega korporativno varnostnega managerja. Samo korporacije, organizacije in končno tudi države z najvišjo razvito varnostno kulturo in zavedanjem, ki preide v določeni fazi v podzavest zaposlenih (njihov DNK), bodo preživele to na oko neopazno, pa vendar prav tako smrtonosno 3. svetovno vojno. ■

Avtor: Mag. Miran Vršec, Institut za korporativne varnostne študije*



NIZKA CENA STORITEV VAROVANJA KOT EDEN POMEMBNIH VIROV TVEGANJA

Misel, da za »Malo denarja dobimo malo muzike«, je praviloma sinonim za tiste produkte in storitve, ki že na prvi pogled kažejo slabšo kakovost, mi pa od njih neupravičeno pričakujemo višjo dodano vrednost, večjo kakovost in delovanje na dolgi rok. V praksi se seveda pojavljajo tudi izjeme, ki potrjujejo pravilo, pa vendar se je potrebno zavedati, da je za zagotavljanje visoke kakovosti produktov in storitev, ki zagotavljajo neprekinjeno delovanje na dolgi rok, potrebno angažirati več resursov in vlagati več sredstev. To vpliva na dvig njihove lastne cene ter na dvigovanje njihove končne prodajne cene.

V ekonomski krizi se je omenjenega dejstva potrebno še toliko bolj zavedati. Kupna moč podjetij in posameznikov pada, s tem pa se posledično povečujejo pritiski na prodajne cene. Zaradi zmanjšanega povpraševanja in pritiska na cene morajo proizvajalci oziroma ponudniki, s ciljem ohranjanja tržnega deleža in obsega prodaje, prodajne cene zniževati, s tem pa se znižuje dodana vrednost produktom in storitvam, kar sili proizvajalce oziroma ponudnike k zniževanju lastne cene produktov in storitev. Takšen razvoj dogodkov - hote ali nehote – po eni strani negativno vpliva na kakovost produktov in storitev, kar znižuje zadovoljstvo kupcev, po drugi strani pa znižuje dodano vrednost in dobičkonosnost poslovanja podjetij. Ena od bolj perečih pasti ekonomske krize se tako kaže v brezglavem zniževanju stroškov preko razumnih mej, kar sili proizvajalce in ponudnike k improvizacijam, zniževanju kakovosti, opuščanju standardov in kršenju zakonodaje na vseh področjih. Proizvajalci in ponudniki spuščajo svoje lastne cene pod prag rentabilnosti zato zapadajo v vse večje finančne težave, s tem pa povečujejo poslovna tveganja, ki se kažejo predvsem v zmanjševanju dobička, nelikvidnem finančnem poslovanju, povečevanju zamud pri plačevanju obveznosti do dobaviteljev, zmanjševanju plač zaposlenim ipd. Vse to lahko vodi celo do propada podjetja. Te problematike se morajo še posebej zavedati tudi strokovnjaki, ki se ukvarjajo z obvladovanji tveganj, tudi tisti, ki se ukvarjajo s korporativno varnostjo v podjetjih. Na korporativnem varnostnem nivoju si namreč ne smemo privoščiti razmišljanja, da imamo boljšo ali slabšo varnost, kajti varnost imamo, ali pa je nimamo. Slab varnostni sistem namreč ne zagotavlja optimalno obvladovanje tveganj in s tem optimalne varnosti. Lahko torej rečemo, da varnost v tem primeru ni zagotovljena, saj tveganja niso v celoti obvladana.

Nakazana problematika ima še toliko večje razsežnosti, ko govorimo o fizičnem in tehničnem varovanju ljudi in premoženja v organizacijah, ki so zavezanci za javna naročila, organizacijah, ki so v pretežni ali delni lasti države, organizacijah (subjektih), ki so del kritične infrastrukture in organizacijah, ki morajo obvezno organizirati varovanje in so iz varnostnega vidika pomembne za delovanje države v kriznih razmerah. Pri vseh teh organizacijah se zunanji izvajalci praviloma izbirajo na podlagi javnih naročil ali podobnih načinov zbiranja ponudb, ki največkrat za izbor izvajalcev uporabljajo kriterij oziroma merilo najnižje cene. To seveda ne bi bilo problematično, v kolikor bi že sami razpisni pogoji temeljili na dokazovanju kakovosti in strokovnosti, kot temelju za sodelovanje v postopkih izbo-

Najcenejši ponudnik ni nujno najcenejši tudi na dolgi rok, še posebej ko gre za vprašanje varnosti in storitev s področja zasebnega varovanja.

*avtor je član Slovenskega združenja korporativne varnosti



ra ponudnikov. Ugotovitve iz raziskave, ki sem jo izvedel v letu 2010 in je bila usmerjena v pregled razpisnih pogojev več kot deset razpisnih dokumentacij različnih proračunskih porabnikov, žal kažejo drugače in potrjujejo moje ugotovitve iz prakse. Raziskava je namreč pokazala, da je bilo merilo najnižje cene edino merilo za izbor izvajalcev storitev fizičnega varovanja ljudi in premoženja uporabljeno v vseh razpisnih dokumentacijah pri tem pa sta bila kakovost in strokovnost ponudnikov povsem sekundarnega pomena. Potrebno je izpostaviti tudi drugo pomembno ugotovitev, da pri izboru izvajalcev na podlagi cene kot edinega merila, praviloma ne gre za izbor ekonomsko najugodnejšega ponudnika, kar bi moral biti temeljni cilj javnega naročanja, ampak za izbor najcenejšega ponudnika, kar pa velja le na kratek rok. Najcenejši ponudnik ni nujno najcenejši tudi na dolgi rok, še posebej ko gre za vprašanje varnosti in storitev s področja zasebnega varovanja. Tu se moramo vprašati, kje so vzroki za takšno stanje?

Priprava razpisne dokumentacije je precej enostavna, če uporabimo najnižjo ceno kot edino merilo. Razpisna dokumentacija, ki primarno temelji na izboru ekonomsko najugodnejšega ponudnika, torej na ugotavljanju kakovosti, strokovnosti in izgradnji dolgoročnega poslovnega odnosa pa zahteva bistveno več znanja in predvsem poznavanja dejavnosti, ki je predmet razpisa. Pripravljavci razpisnih dokumentacij največkrat teh znanj nimajo ali pa je njihovo poznavanje dejavnosti pomanjkljivo. Tu se zastavi naslednje vprašanje. Zakaj se kljub prizadevanjem Inštituta za korporativne varnostne študije in nekaterih ostalih strokovnjakov, ki stalno opozarjajo odgovorne na omenjeno problematiko, stanje na tem področju ne spreminja na bolje? Morebiti pa takšno stanje nekomu odgovarja, saj omogoča konkuriranje ravno tistim ponudnikom, katerim kakovost in strokovnost nista na prvem mestu? Ima kdo zaradi takšnega stanja tudi osebne koristi?

Zakaj torej izbor zunanjih izvajalcev na podlagi najnižje cene kot edinega merila predstavlja za prej omenjene organizacije tveganje? Na prvi pogled bi lahko celo rekli, da gre za gospodarno ravnanje organizacij saj na ta način dejansko izberejo najcenejšega ponudnika in prihranijo nekaj denarja. Pa ga res? Morebiti na kratek rok da, na dolgi rok pa vsekakor ne. Ugotavljam celo, da gre pri tem lahko za škodljivo ravnanje, ki na dolgi rok povzroča organizacijam nepredvidene stroške in izpade delovanja poslovnih procesov. Še več, vzbuja celo sume kaznivih dejanj zaradi negospodarne porabe sredstev, zaradi ustvarjanja pogojev za delo na črno, omogočanja nelojalne konkurence, korupcije, nepotizma, klientelizma in drugih družbi, organizacijam in posameznikom škodljivih pojavov in nezakonitih ravnanj.

Analiza slovenskih podjetij na področju outsourcinga (Kavčič, K., 2007) je pokazala, da se zunanjim izvajalcem zaupa 66% storitev čiščenja, 55% storitev varovanja, 49% storitev informacijskih tehnologij in 33% pravnih storitev. Vse omenjene storitve bi lahko označili kot osebne storitve, saj zaradi svoje narave



dela posegajo tudi v najintimnejše procese in najintimnejša območja (prostore) podjetij, zato so iz tega vidika še toliko bolj potrebne nadzora. Z najemanjem omenjenih storititev podjetja na stežaj odpirajo vrata zunanjim izvajalcem, s tem pa postajajo bolj ranljiva. Podjetja, ki zaupajo izvajanje storitev zunanjim izvajalcem vse prevečkrat izpostavljajo le koristi, ki jih prinaša outsourcing (nižji stroški poslovanja, večja fleksibilnost, manjše število zaposlenih ipd.), ne prepoznavajo pa tveganj in potencialnih izpostavljenosti, ki jih outsourcing predstavlja za podjetja. Tukaj predvsem mislim na nevarnosti, da podjetja postanejo odvisna od zunanjih izvajalcev ter povečano stopnjo ranljivosti, ki se kaže v manjših učinkih z vidika prihrankov stroškov (skriti stroški in stroški dodatnih storitev), slabši kakovosti najetih storitev, neustreznosti izbora izvajalcev, izgubi strokovnih znanj in ključnih kadrov (npr. prestop k zunanjemu izvajalcu), prevzemu poslovnih partnerjev organizacije ipd. Zato izvajalcev tovrstnih storitve vsekakor ne bi smeli izbirati zgolj na podlagi najnižje cene, kot edinega merila. Pa poglejmo enega od razlogov zakaj ne.

Po hitrem pregledu nekaterih v zadnjem letu zaključenih javnih naročil za izbiro izvajalcev storitev fizičnega varovanja ljudi in premoženja lahko ugotovimo, da je bil v večini primerov izvajalec izbran na podlagi najnižje cene. To niti ne bi bil takšen problem v kolikor ne bi v več kot polovici primerov izbrani izvajalec ponudil ceno storitve za uro varnostnika, ki ne pokriva niti osnovne plače varnostnika. Iz izračuna prikazanega v nadaljevanju so razvidni elementi kalkulacije stroška osnovne plače varnostnika.

Po hitrem pregledu nekaterih v zadnjem letu zaključenih javnih naročil za izbiro izvajalcev storitev fizičnega varovanja ljudi in premoženja lahko ugotovimo, da je bil v večini primerov izvajalec izbran na podlagi najnižje cene. To niti ne bi bil takšen problem v kolikor ne bi v več kot polovici primerov izbrani izvajalec ponudil ceno storitve za uro varnostnika, ki ne pokriva niti osnovne plače varnostnika.

Izračun stroškov dela varnostnika

- Minimalna plača: 556,83 EUR (neto) + bruto I in II = 909,83 EUR / mesec
- Bolniška odsotnost: 29,84 EUR / mesec (povprečje v RS za leto 2012 je 4,1%)
- Prevoz na delo: 37,00 EUR / mesec (Urbana LPP)
- Regres za prehrano: 4,90 EUR/dan x 21 dni = 102,90 EUR / mesec
- Regres za letni dopust bruto: 791,50 EUR/leto : 12 mesecev = 65,96 EUR / mesec
- Letni dopust (20 dni/leto): 909,83 EUR/leto : 12 mesecev = 75,82 EUR / mesec

SKUPAJ: 1.221,35 EUR/mesec : 176 ur/mesec = 6,94 EUR / uro

Izračun torej pokaže, da strošek ure dela varnostnika ob upoštevanju minimalne plače brez dodatkov na plačo, brez upoštevanih ostalih stroškov povezanih z delom varnostnika (stroškov delovne obleke, usposabljanja, nadzora ipd), brez upoštevanih stroškov poslovanja podjetja (režije ipd.) in brez upoštevanega predvidenega dobička znaša 6,94 EUR/uro .

V čem je torej problem? Ugotovitve iz raziskave kažejo, da obstoječa praksa izbora izvajalcev fizičnega varovanja ljudi in premoženja temelji na izboru izvajalcev, ki ponudijo najnižjo ceno, pri tem pa naročnika ne zanima, ali ponudnikova cena pokriva vse stroške izvedbe ponujenih storitev. To pač ni problem naročnika, vsaj tako kaže dejansko stanje in tudi izjave nekaterih naročnikov, ki izjavljajo da je to problem samih ponudnikov, ki so pripravljeni za tako nizko ceno izvajati tako, za naročnika vitalne in pomembne storitve. Pa jih izbrani izvajalci zares lahko tudi zakonito izvajajo? Pri tem ne gre samo za vprašanje zakonitosti izvedbe storitev, ampak gre tudi za vprašanje tveganja poslovanja oziroma sodelovanja s takšnim ponudnikom. To pa je že vprašanje, ki bi moralo še kako skrbeti odgovorne osebe za varnost oziroma poslovodne organe v podjetjih, ki na ta način izbirajo ponudnike. Še posebej bi se morali tveganj nizke cene zavedati odgovorni za varnost v organizacijah, ki so zavezanci za javna naročila, organizacijah, ki so v pretežni ali delni lasti države, organizacijah (subjektih), ki so del kritične infrastrukture in organizacijah, ki morajo obvezno organizirati varovanje in so iz varnostnega vidika pomembne za delovanje države v kriznih razmerah. Pa se jih res zavedajo? Očitno ne vseh, vsaj tako kažejo ugotovitve in dejansko stanje.

Po moji oceni je ključni problem za takšno stanje v odgovornosti oziroma neodgovornosti. Ugotovitve namreč kažejo, da za takšno stanje pač nihče ne odgovarja. Ne odgovarjajo poslovodni organi, ker se izgovarjajo na člane razpisnih komisij in pomanjkljivo oziroma nejasno zakonodajo, ki jo tolmačijo po svoje oziroma v svojo korist. Ne odgovarjajo niti člani razpisnih komisij, ki se izgovarjajo na poslovodne organe in enačijo pojem izbora ekonomsko najugodnejšega ponudnika z najnižjo ceno. Ne odgovarjajo niti ponudniki, ker ni ustreznih oziroma učinkovitih zakonskih in nadzornih mehanizmov s katerimi bi preprečevali oziroma odkrivali nelojalno konkurenco, delo na črno in druga podobna nezakonita ravnanja.



Kje je rešitev problema? Inštitut za korporativne varnostne študije že dlje časa opozarja na obravnavano problematiko. Prvo rešitev vidim v spremembi zakonodaje na področju javnega naročanja, ki bi na področju varovanja bolj natančno določala način izbora izvajalcev, predvsem pa bi zagotavljala večjo transparentnost javnega naročanja na tem področju. Prav tako bi bilo potrebno zakonsko opredeliti kazensko in materialno odgovornost članov razpisnih komisij, ki pripravljajo razpisne dokumentacije in so udeleženi pri izboru izvajalcev. Drugo rešitev vidim v tem, da naročniki v razpisne komisije vključijo strokovnjake Inštituta za korporativne varnostne študije, ki bi jim s svojimi znanji in izkušnjami pomagali pri pripravi vsebinsko popolnih razpisnih dokumentacij na podlagi katerih bi naročniki izbrali ekonomsko najugodnejše in najkakovostnejše izvajalce. Tretjo rešitev vidim v vzpostavitvi sistemskega nadzora. Tudi na tem področju je Inštitut za korporativne varnostne študije razvil celovito rešitev, ki naročnikom zagotavlja popoln pregled nad skladnostjo izvedenih storitev in pogodbenimi obveznostmi in zahtevami naročnika. In četrto rešitev vidim v vzpostavljanju partnerskih poslovnih odnosov med naročniki in izvajalci. Na ta način bi na dolgi rok zagotavljali kakovostne varnostne rešitve in optimalno obvladovanje tveganj.

Naj za zaključek izpostavim še vse bolj pomemben in aktualen vidik družbene odgovornosti podjetij. Podjetja, ki izbirajo izvajalce na podlagi najnižje cene kot edinega merila, po moji oceni vsekakor niso družbeno odgovorno naravnana podjetja. Z uvajanjem predlaganih rešitev lahko tudi na tem področju za podjetja naredimo velik korak naprej. ■

Pri tem ne gre samo za vprašanje zakonitosti izvedbe storitev, ampak gre tudi za vprašanje tveganja poslovanja oziroma sodelovanja s takšnim ponudnikom.

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

INTERVJU
Matjaž Klarič, mag. jav. upr.
Častni poveljnik Gasilske zveze Slovenije

POŽARNA VARNOST KLJUČNI TEMELJ KORPORATIVNE VARNOSTI

Ustrezno načrtovan sistem požarne varnosti je za korporativno varnost v organizacijah izrednega pomena. Zanemarjanje tega dejstva ima lahko za posledico izgubo človeških življenj in uničenje materialnih zmogljivosti, ki so ključne za delovanje organizacije.

Kako vidite nadaljnji razvoj GZS v teh zahtevnih gospodarskih in družbenih okoliščinah?

Slovensko gasilstvo temelji na prostovoljstvu, le v večjih mestih imamo tudi poklicne gasilske enote. Skozi dolgoletno zgodovino je slovenska gasilska organizacija prevzela vedno več nalog, tako da je danes postala osrednja sila v sistemu varstva pred naravnimi in drugimi nesrečami, ki ukrepa praktično pri vseh nesrečah, ki nas v Sloveniji lahko doletijo. S prehodom na tržni sistem gospodarstva smo gasilci v veliki meri zaznali tudi problem odsotnosti gasilcev z dela, zato se – skupaj z državnimi organi – zavzemamo za reševanje statusa prostovoljnega gasilca, ki se nanaša predvsem na odsotnost gasilcev z dela. Državni zbor je sprejel nacionalni program *Varstva pred naravnimi in drugimi nesrečami do leta 2015*, v katerem se načrtuje ureditev odsotnosti prostovoljnih gasilcev z dela. Na podlagi Nacionalnega programa je bila sprejeta tudi *Novela Zakona o varstvu pred naravnimi in drugimi nesrečami,* v kateri se ureja predvsem odsotnost gasilcev z dela zaradi opravljanja nalog javne gasilske službe. Zakon delodajalcem vrača nekatere stroške, nastale zaradi odsotnosti gasilcev z dela. Zagotavlja jim tudi pokrivanje stroškov, ki nastanejo zaradi bolniške odsotnosti gasilcev, ki so se poškodovali na gasilskih intervencijah. Sicer pa v gasilski organizaciji – kljub kriznim časom in veliki brezposelnosti – beležimo rast članstva. Leta 1998 – na Kongresu v Sežani – smo imeli 118.000 članov, na Kongresu leta 2003 na Bledu 123.000, pet let pozneje v Krškem pa že 133.000. Ob letošnjem Kongresu v Kopru pa pričakujemo preko 150.000 članov.

Varčevanje zaradi recesije se običajno najprej začne na področju varnosti, kar posledično povzroči rast števila zahtevnih industrijskih požarov in drugih nesreč. Zato se moramo vsi skupaj – z odgovornimi državnimi organi – zavzemati za ohranjanje gasilske organizacije kot najmočnejše sile na področju varstva pred naravnimi in drugimi nesrečami, ki bo sposobna ukrepati v primeru požarov ter naravnih in drugih nesrečah.

Kakšen je vaš pogled na odprta vprašanja, ki jih prinašajo procesi prostovoljnosti, profesionalnosti in poklicnosti v gasilski organizaciji?

V Sloveniji gasilstvo temelji na prostovoljni gasilski organizaciji. Le v 13 večjih mestih imamo organizirane tudi poklicne gasilske enote. V teh mestih prostovoljni in poklicni gasilci skupaj opravljajo javno gasilsko službo. Način organiziranja gasilstva – poklicno ali prostovoljno – ne sme vplivati na uspešnost izvajanja javne gasilske službe, saj jo morajo oboji vedno opravljati profesionalno.

Slovensko prostovoljno gasilstvo je nacionalno bogastvo, ki ga moramo ohranjati tudi v prihodnje in mu zagotavljati takšne pogoje dela, ki bodo zagotavljali uspešno opravljanje javne gasilske službe, saj pomeni najracionalnejše zagotavljanje varnosti na področju naravnih in drugih nesreč.

*avtor je član Slovenskega združenja korporativne varnosti

Organiziranost prostovoljnega gasilstva v Sloveniji zagotavlja uspešno opravljanje javne gasilske službe tudi v sredinah, kjer poklicnih gasilcev ni. Predvsem pa je pomembna operativna moč prostovoljnega gasilstva pri naravnih in drugih nesrečah, kot so požari v naravi, poplave, plazovi in drugo, kjer na intervencijah sodeluje večje število gasilcev. Na požarih na Krasu je leta 2006 sodelovalo preko 2.800 gasilcev, pri odpravljanju posledic poplav leta 2010 pa kar 20.000 gasilcev. Slovensko prostovoljno gasilstvo je nacionalno bogastvo, ki ga moramo ohranjati tudi v prihodnje in mu zagotavljati takšne pogoje dela, ki bodo zagotavljali uspešno opravljanje javne gasilske službe, saj pomeni najracionalnejše zagotavljanje varnosti na področju naravnih in drugih nesreč.

Izobraževanje in usposabljanje verjetno tudi naprej ostaja ključna komponenta vložkov v kadrovski potencial gasilske organizacije. Kakšni so vaši načrti na tem področju?

Poklicni gasilci se usposabljajo v šoli za poklicne gasilce, kjer si pridobijo poklic gasilca, prostovoljni pa se usposabljajo na tečajih, ki potekajo na nivoju gasilskih društev, gasilskih zvez in regij, ter na nivoju Gasilske zveze Slovenije. Usposabljanje prostovoljnih gasilcev poteka za osnovna znanja, na katerih gasilci dobijo čine – gasilec, nižji gasilski častnik, gasilski častnik in višji ter visoki gasilski častnik. Dopolnilno pa se gasilci usposabljajo tudi za nazive specialnosti, kot so nosilec izolirnega dihalnega aparata, gašenje notranjih požarov, nevarne snovi, tehnično reševanje, predavatelj, inštruktor, mentor..., kjer si tečajniki dobijo še dodatno znanje za opravljanje posameznih nalog. Po opravljenem usposabljanju imajo poklicni in prostovoljni gasilci podoben nivo znanja, kljub temu pa imamo zakonsko nalogo, da se učni programi poklicnih in prostovoljnih gasilcev poenotijo do leta 2013. Tako nas v prihodnje čaka prenova in posodobitev učnih programov, velik poudarek pa bomo dali tudi možnosti e-izobraževanju. Veliko bomo delali na poenotenju in nadgradnji znanja predavateljev in inštruktorjev, ter pripravi ustreznega učnega gradiva in pripomočkov.

Uspešnost slovenskega gasilstva se izraža tudi skozi visoko usposobljenost gasilcev, ki uspešno vsakodnevno opravljajo zahtevne intervencije. Kako se v ta sistem izobraževanja vključuje projekt Višje Gasilske šole?

V Sloveniji primanjkuje možnost gasilskega izobraževanja na višji in visoki stopnji. Zato so se številne generacije gasilcev – v želji po višji izobrazbi – odločile za izobraževanje na drugih, sorodnih izobraževalnih inštitucijah, ki so jim dale ustrezno splošno predznanje, znanja s področja gasilske stroke pa niso dobili. Zato smo se dolga leta zavzemali za ustanovitev višje gasilske šole z verificiranimi programi. Žal se je zaradi kadrovskih problemov zataknilo pri zagotavljanju ustreznih kadrov, zato si gasilci še naprej prizadevamo, za dokončanje projekta, saj bodo kadri, ki nam jih bo dala ta šola, pomemben prispevek h gasilski stroki v Sloveniji.

Kako med mladimi zagotoviti ustrezno zanimanje za poklic gasilca?

Zanimanje za poklic gasilca je v Sloveniji zelo veliko. To se kaže pri velikem številu prijav na razpise poklicnih gasilskih enot za nova delovna mesta. Je pa ta zaposlitev specifična, saj mora imeti kandidat za gasilca V. stopnjo splošne šolske izobrazbe, narediti mora zahteven zdravstveni pregled za gasilca in opraviti praktični preizkus psihofizičnih sposobnosti. Gasilci, sprejeti na ta delovna mesta, morajo v določenem času opraviti tudi šolo za poklicne gasilce.

Pri prostovoljnem gasilstvu s kadrovanjem začnemo že praktično v osnovni



šoli, kjer mlade povabimo k sodelovanju v gasilska društva in jih skozi programe, ki jih izvajajo usposobljeni mladinski mentorji, skušamo zadržati v gasilski organizaciji do prehoda v operativno gasilsko enoto, kjer kot operativni gasilci opravljajo javno gasilsko službo. Na tej poti – od vstopa mladega gasilca v gasilsko društvo do vstopa v operativno enoto – imamo običajno zelo velik upad, ki sega včasih do 80 in več odstotkov. Zato je zelo pomembno kadrovanje in delo z mladimi, saj morajo mladi gasilci skozi program postati del gasilske organizacije. Biti prostovoljni gasilec preprosto postane največkrat način življenja gasilcev, ki zahteva veliko odrekanja, solidarnosti ter poseben čut za humanitarnost in prostovoljstvo.

So po vašem mnenju procesi centralizacije državne uprave in s tem tudi dejavnosti kriznega upravljanja, ki jih združuje Uprava RS za zaščito in reševanje pravi korak v smeri zagotavljanja hitrega odzivanja na naravne in druge nesreče?

Gasilstvo je – po slovenski in najpogosteje tudi evropski zakonodaji – stvar lokalne skupnosti, ki je dolžna zagotavljati organiziranost in pogoje za delovanje gasilstva v občini. Le nekatere naloge delno sofinancira država. Te naloge so povezane z opravljanjem nalog zaščite in reševanja v primeru prometnih nesreč, nesreč z nevarnimi snovmi, ter nesreč v predorih in na rekah, opravljajo pa jih gasilske enote, s katerimi je Uprava RS za zaščito in reševanje podpisala pogodbo o opravljanju in sofinanciranju teh nalog. Na nivoju države je sprejet *Državni načrt zaščite in reševanja ob velikih požarih v naravi*, ki se smiselno uporablja tudi pri drugih velikih nesrečah. Načrt predvideva sodelovanje gasilskih enot izven domačih lokalnih skupnosti in celo iz drugih regij ali delov države.

Biti prostovoljni gasilec preprosto postane največkrat način življenja gasilcev, ki zahteva veliko odrekanja, solidarnosti ter poseben čut za humanitarnost in prostovoljstvo.



Ureja tudi vodenje gasilskih intervencij ter sodelovanje različnih enot zaščite in reševanja. V tem primeru je koordinacijska naloga štabov CZ, ki skrbijo za logistiko ter medsebojno sodelovanje različnih organizacij zelo koristno in se je ob velikih nesrečah uspešno izkazalo.

Opremljenost gasilcev ne sledi potrebam realnega okolja in tempu, ki bi si ga verjetno vsi želeli. Kaj lahko naredimo na področju opremljanja in s tem dvigovanja učinkovitosti dela profesionalnih gasilskih enot?

Opremljanje gasilskih enot se izvaja na nivoju lokalnih skupnosti. Potrebno je poudariti, da je to v preteklosti potekalo primerno in v skladu z uredbo, nekoliko več težav pa je nastajalo pri manjših lokalnih skupnostih. Pri nabavi gasilske zaščitne in reševalne opreme ima pomembno vlogo sofinanciranje, ki ga je država predpisala po uvedbi DDV-ja. V lanskem letu so se ta sredstva skoraj prepolovila, kar je – skupaj z zmanjšanjem sredstev zaradi recesije – pomembno vplivalo na možnost nabave gasilske zaščitne in reševalne opreme. Velik delež pri opremljanju prostovoljnih gasilskih enot nosimo gasilci sami, saj z različnimi delovnimi akcijami in prispevki občanov zberemo tudi do 50 in več odstotkov potrebnih sredstev. Pri ukrepih varčevanja gasilci odgovorne opozarjamo, da se varčevanje zaradi recesije najpogosteje začne pri varnosti, kar pomeni, da je čez nekaj let pričakovati porast števila požarov v industriji, katerih gašenje je posebej zahtevno ter zahteva sodobno opremljene in usposobljene gasilske enote. Varčevanja na račun usposobljenosti in opremljenost gasilskih enot bi se lahko v prihodnosti zelo maščevalo – pokazalo bi se v zmanjšani varnosti občanov in njihovega imetja.

Nam lahko zaupate vizijo nadaljnjega razvoja gasilstva na področju večjih industrijskih obratov.

Po slovenski zakonodaji si morajo gospodarske družbe, zavodi in druge organizacije v primeru povečane požarne ogroženosti prvenstveno same zagotoviti gasilsko službo. Zakon dopušča možnost, da podjetje podpiše pogodbo o opravljanju gasilske službe tudi z gasilsko enoto, ki operativno pokriva teritorij, na katerem se nahajajo objekti in premoženje gospodarske družbe. Industrijsko področje vpliva tudi na višino kategorije gasilske enote, ki posledično zahteva večje število operativnih gasilcev in težjo ter zahtevnejšo gasilsko zaščitno in reševalno opremo enote, ki to področje pokriva. V primeru velikih intervencij se tudi pri industrijskih intervencijah aktiviranje gasilskih enot in

njihova medsebojna pomoč izvajajo v smislu državnega načrta za gašenje velikih požarov.

Menite, da je združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti lahko odgovor na obvladovanje zahtevne varnostne situacije in ali so lahko taka združenja ustrezen partner Gasilski zvezi Slovenije pri zagotavljanju njenega osnovnega poslanstva, predvsem v industrijskih okoljih ali okoljih delovanja kritične infrastrukture?

Povezovanje in združevanje znanja, spoznanj in izkušenj je vedno koristno in pomeni napredek, ki ga želimo s pridom izkoristiti tudi v gasilki organizaciji. Zavedamo se, da se pri opravljanju javne gasilske službe gasilci srečujemo z nalogami, katerih uspešno opravljanje zahteva znanje različnih znanstvenih področij in organizacij, ki se ukvarjajo z varnostjo. Gasilska organizacija je vedno odprta za sodelovanje s sorodnimi organizacijami na področju varstva pred naravnimi in drugimi nesrečami.

Nam lahko za konec postrežete še z nekaj statističnimi podatki o obsegu gasilske organizacije v Sloveniji?

Nekaj statističnih podatkov, ki smo jih zbrali pred XVI. kongresom Gasilske zveze Slovenije, ki bo 25. maja 2013 v Kopru:

120 gasilskih zvez
1299 teritorialnih gasilskih društev
49 industrijskih gasilskih društev
151.156 članov
45.227 operativnih članov ■

Število požarov po vrstah požarov

VRSTA POŽARA / LETO	2008	2009	2010	2011	2012	SKUPAJ
Požari v objektih	1.948	2.179	1.911	2.256	2.199	10.493
Požari na prometnih sredstvih	552	487	436	449	403	2.327
Požari v naravi oziroma na prostem	1.370	1.840	1.036	1.922	2.439	8.607
Požari v komunalnih in drugih zabojnikih	556	552	400	583	523	2.614
Vsi požari	4.426	5.058	3.783	5.210	5.564	24.041

Vir: Spin - URSZR



gea college
Fakulteta za podjetništvo

ICS
Institut za korporativne varnostne študije

Management korporativne varnosti

Magistrski študijski program 2. stopnje

Predstavitev programa

Cilj magistrskega programa Management korporativne varnosti je izobraževanje in usposabljanje podjetnikov in managerjev za obvladovanje poslovno varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Z magistrskim študijem Management korporativne varnosti omogočamo študentom poglobljeno podiplomsko izobraževanje, v katerem bodo pridobili teoretična in aplikativna znanja s področja managementa in vsebine, ki so značilne za korporativno varnost: geostrateški in politični vidiki varnostnih tveganj, varnostni standardi v poslovnih procesih, upravljanje varnostnih tveganj, načrtovanje in razvoj korporativne varnosti, procesi nadzora, zavarovalništvo, gospodarsko poizvedovanje, ekološki vidiki itd.

Razpisane smeri	Trajanje študija in strokovni naslov
Korporativni varnostni manager Korporativni varnostni manager – podjetnik	2 leti; magister/magistrica managementa korporativne varnosti

Kaj omogoča študij Managementa korporativne varnosti

Pridobiti ustrezna multidisciplinarna znanja, ki temeljijo na znanstveno raziskovalnem delu in praktičnih izkušnjah ter dobrih praksah v nacionalnem in mednarodnem korporativnem okolju. Diplomanti bodo pridobili znanja za vodenje organizacijskih struktur na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah. V ta okvir še posebej sodi tudi delovanje v organizacijah, ki obvladujejo kritično infrastrukturo. Poleg navedenega bodo diplomanti pridobili vsa potrebna znanja in kompetence, ki so potrebne za delovanje v podjetniškem okolju in sicer kot samostojni podjetniki, ki bodo drugim organizacijam nudili tovrstne strokovne storitve s področja načrtovanja korporativne varnosti.

Partnerji programa

ICS – Inštitut za korporativne varnostne študije
Slovensko združenje korporativne varnosti (SZKV)
Mednarodna asociacija SE European Corporate Security Association (SECSA)



»Varnost je pojem, s katerim se srečamo že v naših rosnih letih in ima velik pomen za uspešno rast, razvoj in delovanje vsakega posameznika v vseh obdobjih njegovega življenja in ustvarjanja. Korporativna varnost pa je, podobno kot varnost pri posameznikih za razvoj in uspešno delovanje, pomembna predvsem v organizacijah. Kakršnihkoli – v velikih ali malih, pri globalnih mednarodnih korporacijah ali zgolj lokalnem samostojnem podjetniku, in sicer ne glede na to, na katerem področju ustvarja in razvija svoje ideje oziroma poslovne rešitve. Pri tem je pomembno, da se ne omejimo zgolj na osnovno varnost ljudi, premoženja ali informacijsko varnost, saj je izrednega pomena, da znamo pravočasno in pravilno prepoznati vsa možna dejanska in potencialna tveganja ter nevarnosti, ki lahko nastopijo v kateremkoli procesu delovanja naše organizacije. V današnjem hitro razvijajočem, naprednem in hkrati zelo konkurenčnem okolju so pravilna strateška usmeritev korporativne varnosti, njena učinkovita preventivna dejavnost ter strokovno načrtovano ukrepanje in delovanje ključnega pomena za uspešnost organizacije. Našteto lahko dosežemo le prek ustreznega strokovnega izobraževanja, ki bo pripomoglo k dvigu omenjene stroke in zadovoljilo vse bolj naraščajoče potrebe po znanjih s tega področja. Slednja so namreč izrazitega pomena za učinkovitejše obvladovanje varnostnih tveganj v organizacijskih okoljih.«
mag. Boris Novak, generalni direktor Pošte Slovenije

Cilji študija

Ključni cilj programa je izobraziti in usposobiti managerje in strokovnjake s področja korporativne varnosti, ki imajo široko poslovno znanje in perspektivo ter dobro razumevanje globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja. Bistvo spremljanje trendov zagotavljanja integriranih varnostnih rešitev v gospodarskem in poslovnem okolju ter okolju javne uprave.

V tem kontekstu bodo diplomanti pridobili naslednje ključne kompetence:

- Razumevanje delovanja institucij formalnega in neformalnega družbenega nadzorstva
- Znanje s področja globalnih družbenih, ekonomskih in političnih vidikov
- Proučevanje varnostnih pojavov, izdelava varnostnih elaboratov ter evalvacija analiz in ocen ranljivosti, groženj in tveganj v nacionalnem in mednarodnem korporacijskem okolju.
- Pridobljena strokovna znanja za uvajanje integralnih varnostnih sistemov, ki obsegajo varovanje ljudi in premoženja, zaščito podatkov, informacij in poslovnih skrivnosti, benchmarking, poslovno poizvedovanje, varne delovne pogoje, okoljske vidike, sistem zaščite in reševanja v procesih obvladovanja izrednih dogodkov ter evalvacijo geopolitičnih varnostnih dejavnikov.
- Poznavanje metodologij za obvladovanje procesov korporacijske varnosti v smislu trženja, oblikovanja cen varnostnih storitev, načrtovanja investicij v varnostne izboljšave, stroškov, zavarovanja tveganj, zagotavljanja poslovne odličnosti in pravilnega razumevanja postopkov javnih in drugih razpisov ter naročanja storitev zagotavljanja korporacijske varnosti.
- Razumevanje delovanja institucij formalnega in neformalnega družbenega nadzorstva.

Predmetnik

PREDMET	IZBIRNI PREDMETI
1. semester	
Management korporativne varnosti – obvezni predmet	Varnostni standardi v poslovnih *
Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju – obvezni predmet	Upravljanje varnostnih tveganj *
Pravni vidiki korporativne varnosti – obvezni predmet	Načrtovanje in razvoj korporativne varnosti *
2. semester	Trženje/Marketing **
Ekonomika obvladovanja tveganj v poslovnem okolju – obvezni predmet	Finance **
Obvezni usmeritveni predmet*	Procesi nadzorstva v korporativnem varnostnem okolju **
Študijski praktikum	Management človeških virov
3. semester	Okoljski vidiki korporativne varnosti
Obvezni usmeritveni predmet	Metode raziskovanja varnostnih pojavov
Obvezni usmeritveni predmet	Zavarovalništvo v procesih zagotavljanja gospodarske varnosti
Izbirni predmet 1	Gospodarsko poizvedovanje in varovanje poslovnih informacij
Študijski praktikum	Informacijska varnost
4. semester	
Izbirni predmet 2	
Študijski praktikum	
Magistrsko delo	

*obvezni usmeritveni predmet za modul Korporativni varnostni manager

** obvezni usmeritveni predmet za modul Korporativni varnostni manager - podjetnik

" Če smo še včeraj čas merili v letih, mesecih in dnevih, ga danes merimo v urah, minutah in sekundah, saj se svet okoli nas spreminja s tako naglico, da mu enostavno ne moremo več slediti! Seveda pa so te spremembe tako pozitivne kakor negativne narave, ki se lahko pojavijo tudi v obliki varnostnih tveganj in izzivov. Samo holistično izobražen korporativno varnostni manager, ki bo svoje teoretično pridobljeno znanje lahko oplemenitil z ustrezno prakso pod skrbnim mentorstvom izkušenih korporativnih varnostnih managerjev, se bo lahko uspešno kosal s tovrstnimi izzivi! Magistrski študij »Management korporativne varnosti« predstavlja pomemben mejnik v izobraževanju in usposabljanju korporativno varnostnih managerjev, saj zajema tako teorijo kakor tudi prakso!"
Andrej Podvršič, EMEA Director of Security DuPont de Nemours International Sàrl



Avtor: Doc. dr. Denis Čaleta / Institut za korporativno varnostne študije *



KOLUMNA
denis.caleta@ics-institut.si

ALI JE KRIZA LAHKO PRILOŽNOST?

To je osnovno vprašanje, ki si ga strokovna javnost v poslovnem svetu vseskozi postavlja. Seveda je ta dilema vedno aktualnejša v času, ko gospodarska rast upada in se v poslovnem okolju pojavljajo trendi upadanja obsega proizvodnje, zmanjšanja investicij in nenazadnje zmanšanja dobička od poslovanja ter s tem preživetij mnogih podjetij. Na trenutno družbeno gospodarsko stanje je več pogledov, vse od tistih, ki trenutno finančno in gospodarsko krizo primerjajo z velikimi gospodarskimi krizami, ki smo jim bili priča v različnih obdobjih prejšnjega stoletja, do tistih z neoliberalističnimi gospodarskimi pogledi, ki trenutno stanje na trgu pojmujejo kot del čisto normalnega procesa grobe globalne konkurenčne tekme, kjer uspejo preživeti samo najmočnejši in najbolj pripravljeni hitrega prilagajanja na dinamične spremembe v okolju. Različnost pogledov je vsekakor dobrodošla in ponuja več možnosti za spremembo dojemanja o potrebnosti sprememb predvsem na področju novih pristopov poslovanja, ki bodo temeljili na zdravih in razvojno učinkovitih temeljih. Dejstvo je naslednje, da s takimi pristopi poslovanja, ki smo jih dosedaj gojili in razvijali v slovenskem poslovnem okolju ne bo mogoče izvesti prepotrebne spremembe miselnosti, ki bo zagotovila usmerjenost v nov razvoj in zagon gospodarstva. Seveda pa se je potrebno zavedati, da država, s svojo birokratsko okostenelo miselnostjo, prežeto s političnimi interesi lobijev, ki preko koruptivnih povezav ne pustijo prodora novih svežih idej in pristopov v gospodarstvo, nosi veliko breme odgovornosti na svojih plečih.

Pa vendarle uberimo pozitivistični pristop in pogled na dilemo »Ali je kriza lahko priložnost?«. Kriza je vsekakor lahko priložnost, da se streznimo in dojamemo dejstvo, da bo za nov uspeh potrebno korenito spremeniti filozofijo pristopov k poslovanju naših podjetij in tudi organizacij javnega okolja. Tradicionalne vzorce klientelizma bo potrebno zamenjati z novim svežim dinamičnim pristopom, ki bo predvsem temeljil na realnih ocenah in neizmerni energiji usmerjeni v družbeno odgovorno poslovanje, kjer uspešnost podjetja ne bo imela merilo samo v kratkoročnih finančnih dobičkih, vendar se bo odražala v zmerni konstantni rasti podjetij s pripadnimi zaposlenimi in zadovoljnimi uporabniki storitev in produktov, ki jih proizvaja tako podjetje. Če v ta kontekst vpletemo še zavedanje o pomenu poštenosti poslovanja, predvsem v smislu plačilne discipline, potem lahko hitro ocenimo, da so to tisti zdravi temelji na katerih je potrebno graditi nadaljnji razvoj. Država pa mora biti tisto prvo okolje, ki s svojimi ravnanji nudi zgled in seveda preko svojih pristojnih institucij sankcionira in procesira vse tiste, ki ne upoštevajo zakonsko opredeljenih normativov.

Dejstvo je naslednje, da s takimi pristopi poslovanja, ki smo jih dosedaj gojili in razvijali v slovenskem poslovnem okolju ne bo mogoče izvesti prepotrebne spremembe miselnosti, ki bo zagotovila usmerjenost v nov razvoj in zagon gospodarstva.

Lahko bi nekdo hitro zaključil in omenjeno stanje opisal kot preveč idealistično ter s tem nerelano v njegovi izvedbi. Seveda idelanega stanja ni in ga tudi na področju varnosti poslovanja naših organizacij ni mogoče pričakovati. Zato moramo biti sposobni ustrezno ocenjevati in analizirati grožnje in tveganja, katerim so izpostavljena naša podjetja in organizacije ter z zmanjševanjem ranljivosti skozi uporabo celovitih in integralnih pristopov zagotavljati varnost poslovanja. Vendar je pomemben nov in drugačen pristop in energija, ki ju bomo vložili v spremembo temeljev delovanja v našem organizacijskem okolju. Dolgoročno je, ravno na področju obvladovanja tveganj in groženj, katerim so izpostavljena naša podjetja, eden od temeljnih principov sprememba dojemanja dinamičnega okolja, ki nas obdaja. Ravno kriza je priložnost, da se prisilimo k celoviti spremembi in opustitvi vzorcev v podjetju, ki ne prinašajo uspeha, še več, ki so postali pomemben obremenjujoč dejavnik za nadaljnji razvoj. Tudi in predvsem pri zagotavljanju dovolj velike prožnosti naše organizacije, kadar govorimo o prilagajanju vsem tveganjem, ki stojijo pred podjetjem, je pomembno, da k obvladovanju le teh pristopimo z novimi pristopi temelječimi na proaktivnem delovanju. Potrebno bo namreč dokončno dojeti, da so tveganja portfelja naše družbe neposredno povezana z načinom poslovanja. To pa pomeni, da ima varnost kot proces v naših organizacijah neprimerno večji pomen, kot pa smo mu priča pri trenutnem dojemanju strateškega managementa v slovenskih podjetjih. Na-

*avtor je član Slovenskega združenja korporativne varnosti



loge in predvsem proces korporativne varnosti so se iz represivno temelječega pristopa, ki je bil usmerjen v statično obliko varovanja objektov in oseb v podjetjih, močno razširile na celo vrsto področij med katerimi bi posebej želel izpostaviti varovanje ugleda blagovne znamke, korporativno upravljanje, zagotavljanje varnosti ključnih informacij, patentov in produktov ter zagotavljanja varnosti ključnega kadrovskega potenciala. Procesi zagotavljanja korporativne varnosti so postali nedeljiva celota krovnega modela upravljanja korporacij, ki se izraža skozi korporativno upravljanje in korporativno družbeno odgovornost. Seveda je ključno ravno dojemanje novega pristopa, kjer varnost podjetja temelji predvsem na zagotavljanju sprememb v procesu upravljanja in ne več na represiji, kot smo jo bili navajeni v našem okolju. Procesi korporativne varnosti so v temelju novega pristopa »na čelu novega poslovnega razvoja«, kar pomeni, da skozi te procese zagotavljamo podjetju sprejemati tveganja na obvladljivo raven. V tem procesu je pomembna determinanta ravno konstantnost, ki zagotavlja neprestano odzivanje na nova poslovna tveganja. Pristopi popolnega odpravljanja tveganj in groženj so že dalj časa iluzija saj popolne varnosti ni mogoče zagotoviti, še posebno pa ne v tako dinamičnem poslovnem okolju, kateremu smo priča v sedanjosti. V večini podjetij je vloga korporativne varnosti vse bolj povezana z zagotavljanjem splošne odpornosti podjetja na vse spremembe, ki se v okolju poslovanja neprestano dogajajo, kakor pa z zagotavljanjem »tradicionalne« varnosti, kot smo jo in jo na žalost v slovenskem okolju še poznamo. Zagotavljanje korporativne varnosti pa v novem pristopu ne temelji več na moči temveč pridobiva svojo legitimnost na podlagi strokovnega znanja, poslovnih spretnosti ter človeških sposobnosti vodenja in komuniciranja v organizaciji. V tem okviru niso mišljeni samo korporativno varnostni managerji temveč so ta znanja nujno potrebna tudi strateškemu managementu vsake organizacije, da je na tej podlagi sposobno učinkovito načrtovati razvoj svoje organizacije in nenazadnje učinkovito uporabljati vse vzvode, ki mu jih ponuja proces korporativne varnosti.

Če na hitro ocenimo in analiziramo stanje v Sloveniji lahko zelo hitro povlečemo zaključke, da je stanje daleč od zadovoljivega. To pomeni, da razen nekaj svetlih izjem, ki so bili zaradi poslovanja v mednarodnem okolju in lastništva tujega kapitala primorani svojo filozofijo poslovanja in obvladovanja tveganj postaviti popolnoma v novo perspektivo, je stanje katastrofalno. Nezavedanje realnega okolja in nojevska politika tiščanja glave v pesek s splošno znano krilatico »nam se pa res nič ne more pripetiti« je slovenska podjetja pripeljala v zelo nezavidljiv položaj izpostavljenosti na vplive dinamičnega okolja na katere niso bili pripravljeni. Posebej iz tega zornega kota je kriza še kako velika priložnost, da se končno zbudimo in svoje pristope vodenja naših organizacij postavimo na popolnoma nove dimenzije, ki bodo pomenili grobi rez s staro prakso in navadami klientelizma na eni strani ter odsotnosti zavedanja, da so grožnje in tveganja del našega vsakdanjika s katerimi moramo živeti in se jim ves čas prilagajati. Čas je da vrhunskemu znanju in novim pristopom dopustimo prosto pot, kar se bo vsekakor odrazilo v kvaliteti in uspešnosti poslovanja naših organizacij. ■

Procesi korporativne varnosti so v temelju novega pristopa »na čelu novega poslovnega razvoja«, kar pomeni, da skozi te procese zagotavljamo podjetju sprejemati tveganja na obvladljivo raven.

Avtor: Karmen Čaleta, / Institut za korporativne varnostne študije*



MEDNARODNA KONFERENCA »DNEVI KORPORATIVNE VARNOSTI« POTRDILA SLOVES NAJVEČJEGA KORPORATIVNO VARNOSTNEGA DOGODKA V REGIJI

Institut za korporativne varnostne študije je ob soorganizaciji Slovenskega združenja korporativne varnosti in SE European Corporate Security Association (SECSA) v mesecu marcu organiziral že četrto mednarodno konferenco z nazivom »Dnevi korporativne varnosti«. Udeležba več kot 100 udeležencev in visokih gostov iz širšega regijskega prostora je ponovno dokazala, da je dogodek nedvomno postal najkvalitetnejši regijski dogodek na področju korporativne varnosti.

Pomen dogodka so s svojo prisotnostjo in svečanimi nagovori potrdili g. Mitja Bervar, predsednik Državnega sveta Republike Slovenije, ga. Nataša Pirc Musar, Informacijska pooblaščenka Republike Slovenije, g. Stanislav Veniger, Generalni direktor Slovenske policije, ga. Medeja Lončar, direktorica Siemens Slovenija in drugi pomembni gostje iz Slovenije, Hrvaške, Bosne in Hercegovine, Srbije, Makedonije, Avstrije, Velike Britanije, Črne Gore in Ukrajine.

V okviru uvodnega dela konference in šestih panelov se je zvrstilo 25 odličnih predstavitev, ki so z različnih zornih kotov obravnavale osrednjo tematiko konference, ki je bila posvečena temi »Management of Corporate Security – New Approaches and Future Challenges«. Tematika, ki so jo predstavili predavatelji se je v osnovi nanašala na poudarjanje pomena zavedanja o potrebnosti obvladovanja varnostnih tveganj, katerim so izpostavljene organizacije pri svojem delovanju v dinamičnem globalnem okolju. Glavni izzivi, ki stojijo pred strokovnjaki na področju korporativne varnosti se odražajo v dejstvu, da je proces zagotavljanja korporativne varnosti danes postal tako kompleksen in prepletajoč skoraj z vsemi procesi v organizaciji. To pred korporativno varnostne strokovnjake in posredno tudi pred strateški management organizacij postavlja zahtevno dilemo, kako pridobiti ustrezne strokovnjake, ki so sposobni ustreznega in fleksibilnega nadgrajevanja svojih znanj in s tem ustreznega odzivanja na grožnje, katerim so izpostavljene organizacije.V okviru konference je potekala tudi zelo odmevna okrogla miza, kjer so vabljeni gostje razpravljali o »Dilemah in izzivih izobraževanja strokovnjakov korporativne varnosti«. V svojih zaključkih so se vsi razpravljalci strinjali, da velika večina strokovnjakov prihaja v korporativna varnostna okolja iz struktur nacionalno-varnostnih organov, kot so policija, vojska, obveščevalno-varnostne službe. Njihovo znanje temelji predvsem na represivnih pristopih, ki niso usmerjeni v razumevanje poslovnega procesa in vlogo, ki jo ima korporativna varnost pri zagotavljanju podpore delovanja tega procesa, ki je ključno za normalno funkcioniranje organizacije v zahtevnem konkurenčnem poslovnem okolju. Nadaljevanje izobra-

*avtor je član Slovenskega združenja korporativne varnosti



ževanja je nujno za uspešno razumevanje in obvladovanje procesa korporativne varnosti. S tega stališča so interdisciplinarni izobraževalni programi s področja korporativne varnosti nujni in ključni za uspešno graditev korporativne varnosti, kot profesije, ki je podprta z dinamičnim znanstveno-raziskovalnim procesom usmerjenim v stalno interakcijo novih znanj in dobrih praks z realnim okoljem. S tega stališča je novi program »Management korporativne varnosti«, ki se bo v jesenskem semestru začel izvajati v sodelovanju Fakultete za podjeništvo/GEA College in Instituta za korporativne varnostne študije izredno pomemben korak za okrepitev profesije na področju korporativne varnosti. Prof. Dr. Jaka Vadnjal, Dekan GEA College je v okviru mednarodne konference podrobno predstavil omenjeni program, ki je zasnovan izrazito interdisciplinarno in bo diplomantom ponudil celoten spekter znanj, ki so potrebna za ustrezno izvajanje nalog v zahtevnem korporativnem okolju na področju korporativne varnosti in obvladovanja varnostnih tveganj.

Na konferenci je razprava tekla tudi na področjih kot so vpliv asimetričnih groženj na delovanje korporativnega okolja, novih inovativnih pristopov pri razvijanju procesov, ki omogočajo učinkovitejše obvladovanje tveganj na področju korporativne varnosti, zagotavljanju neprekinjenosti poslovanja in obvladovanje informacijskih tveganj, ki so danes v informacijski družbi postala eden izmed ključnih dejavnikov upravljanja tveganj na področju korporativne varnosti.

»Slovenian Grand Security Award«

Na otvoritvi mednarodne konference je potekala tudi prva podelitev Slovenian Grand Security Award za leto 2012, ki za slovenski prostor predstavlja zgodovinski dogodek.

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

Namen nagrade

Nagrada je namenjena procesom dvigovanja splošnega zavedanja in varnostne kulture v širši družbeni skupnosti, ki vsebuje poslovna in druga okolja. V šestih kategorijah neodvisna komisija izbira tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev. To kvaliteto nagrajujemo z uglednim priznanjem, ki je bila tokrat podeljena za dosežke na področju varnosti v letu 2012. Nagrajenci so bili tokrat izbrani v vseh šestih kategorijah in sicer:

- najbolj varno podjetje
- korporativno varnostni manager leta
- zasebno varnostna služba leta
- najbolj varno mesto
- najboljša knjiga s področja varnosti
- inovativna medijska promocija varnosti

Najbolj varno podjetje v letu 2012 je bilo po mnenju komisije podjetje Gorenje d.d.

Nadaljevanje izobraževanja je nujno za uspešno razumevanje in obvladovanje procesa korporativne varnosti. S tega stališča so interdisciplinarni izobraževalni programi s področja korporativne varnosti nujni in ključni za uspešno graditev korporativne varnosti, kot profesije, ki je podprta z dinamičnim znanstveno-raziskovalnim procesom usmerjenim v stalno interakcijo novih znanj in dobrih praks z realnim okoljem.



Obrazložitev:
»Gorenje je globalno multinacionalno podjetje, ki poleg svoje osnovne lokacije v Velenju izvaja svoje proizvodnje in prodajne procese na skoraj vseh svetovnih kontinentih. To je predvsem s stališča zagotavljanja ustrezne varnosti samim poslovnim procesom izredno zahtevna naloga, ki pa jo z ustrezno varnostno politiko in vzvodi korporativne varnosti učinkovito obvladuje. Posebej velja omeniti svojstvene pristope, ki jih podjetje Gorenje izvaja na področju zagotavljanja korporativne varnosti in obvladovanja varnostnih tveganj. V svojem okviru ima ustanovljeno področje korporativne varnosti, ki poleg tega, da zagotavlja učinkovitost delovanja integralnega varnostnega sistema znotraj korporacije, varnostne storitve in dobre prakse prenaša tudi na širše tržišče na področju zasebnega varovanja. Z uvajanjem vseh ključnih standardov zagotavlja, da so procesi obvladovanja varnostnih tveganj pregledni, nadzorovani, primerljivi z mednarodnim okoljem in predvsem ustrezno obvladljivi. Svojo visoko varnostno zavedanje in pripravljenost prenašati svoje izkušnje v širši slovenski in mednarodni prostor kažejo tudi s tem, da so eden izmed ustanovitvenih korporativnih članov Slovenskega združenja korporativne varnosti.«

Nagrado za Korporativno varnostnega managerja leta 2012 je po mnenju komisije prejel g. Andrej Podvršič, DuPont

Obrazložitev:
»G.Andrej Podvršič je direktor področja korporativne varnosti, ki v okviru mednarodne korporacije DuPont pokriva področje Evrope, Srednjega Vzhoda in Afrike. DuPont je globalno prisoten v 93 državah sveta, zaposluje 65 000 ljudi, ki so pripadniki 97 različnih nacionalnosti, njegovo področje odgovornosti pa vsebuje 18.000 zaposlenih, prisotnih v več kot 50 državah delujočih na več kot 300 lokacijah. Njegove bogate strokovne izkušnje temeljijo tudi na najodgovornejših funkcijah v nacionalno-varnostnem okolju. V mednarodnem korporativnem okolju je zaključil mnoge oblike izobraževanj povezane s procesi korporativne varnosti in kriznega vodenja. G. Podvršič je prvi slovenski diplomant na Akademiji FBI v **ZDA** in član mnogih mednarodnih strokovnih združenj.Ob vsem naštetem pa je aktivni član Slovenskega združenja korporativne varnosti, ki deluje v okviru Instituta za korporativne varnostne študije. Kljub številnim obveznostim je vedno pripravljen aktivno sodelovati pri prenosu njegovih bogatih znanj na ostale kolege v združenju in tudi kot predavatelj se aktivno udeležuje mednarodnih dogodkov v organizaciji ICS-Ljubljana. Prav tako v okviru ostalih dogodkov in združenj aktivno promovira ideje in kvalitete slovenskega znanja na področju korporativne varnosti. Je eden od glavnih promotorjev novega magistrskega programa **Management korporativne varnosti**, ki ga bo ICS-Ljubljana skupaj z GEA College/Fakulteto za podjetništvo letos začel izvajati. S svojimi bogatimi izkušnjami je bistveno pripomogel k pripravi odličnih programov in pomagal odpreti mnoga vrata, ki bodo omogočala študentom opravljanje praktičnega izobraževanja v okviru mednarodnega okolja. Če pogledamo enega izmed temeljnih izrekov Slovenskega združenja korporativne varnosti »**Ab uno disce omnes« (po enem spoznaj vse)**, potem je g. Podvršič dokaz visoke kvalitete vseh članov združenja.«

Nagrado za Zasebno-varnostno službo leta v letu 2012 je po mnenju komisije prejela Nova Panorama d.o.o.

Obrazložitev:
»Nova panorama je družba za integrirano varovanje, ki ima v svojem portfelju celoten spekter dejavnosti, ki zaokrožajo celovito ponudbo procesov pomembnih za zagotavljanje integralnih varnostnih rešitev. Te dejavnosti obsegajo poslovno varnostno svetovanje, vzpostavitev integralnega varnostnega sistema, varovanje oseb in premoženja, kakovost in varnost, krizno vodenje in izobraževanje. Po oceni naročnikov varnostnih storitev v podjetju Nova Panorama z inovativnimi pristopi omogočajo uveljavljati osnovno zavedanje pri naročnikih, da je investicija v zagotavljanje integralnega varnostnega sistema tista investicija, ki prinaša dolgoročne rezultate poslovanja. Njihov pristop je vedno usmerjen v to, kako naročniku zagotoviti, da bo za najbolj opti-

malne vložke v zagotavljanje varnosti dobil najvišjo dodano vrednost in kvaliteto. V tem pristopu in filozofiji se bistveno razlikujejo od ostalih ponudnikov varnostnih storitev. Na posebej pomemben indikator kaže tudi dejstvo, da je kljub slabemu stanju na trgu zasebno varnostnih storitev, dampinškimi cenami, drobljenjem dejavnosti zasebnega varovanja, ki uničujejo kvaliteto, uspelo nadaljevati nudenje kvalitetnih storitev s postavljanjem zadovoljstva naročnika, kot tistega najvišjega normativa, ki na dolgi rok prinaša tudi ustrezne poslovne rezultate. Vlaganje v znanje zaposlenih je temelj na katerem podjetje gradi poslovno uspešnost.«

Nagrado za najbolj varno mesto v letu 2012 je na podlagi odločitve komisije prejela mestna občina Koper

Obrazložitev:
»Odgovornost vseh nas je, da s svojim ravnanjem in varnostno kulturo pripomoremo k čim višji stopnji varnosti v slovenski družbi. V Institutu za korporativne varnostne študije in Slovenskem združenju korporativne varnosti se zavedamo, kako pomembno je, ne samo varno poslovno okolje, temveč tudi okolje v katerem živimo. V ta namen želimo z izborom najbolj varnega mesta spodbuditi mestne in občinske uprave, da izkoristijo nove in inovativne pristope oz.načine, s katerimi bi pripomogle k zmanjševanju kriminalitete in k zagotavljanju čim višje stopnje varnosti v lokalnem okolju.

V izbor za naziv *Najbolj varno mesto v RS za 2012* je bilo zajetih 11 mestnih občin. Pri izboru so bili upoštevani *kriteriji*; kot so število kaznivih dejanj, ki kakorkoli vplivajo na varnost občanov ter na kakovost njihovega bivanja v lokalnem okolju ter nacionalna raziskava, ki je odgovorila na določena vprašanja in sicer, kaj naredijo mestne uprave za varnost svojih občanov; kako in če delujejo varnostni sosveti; ali so v njih vključeni predstavniki mladih; koliko denarja namenjajo za varnostno področje, za delovanje varnostnih subjektov, za osveščanje občanov o samozaščitnem ravnanju in varnostni kulturi; ali imajo zaposlenega strokovnjaka za varnost, katerega naloga je povezovanje civilne družbe oziroma občanov v prizadevanjih za preprečevanje kriminalitete v lokalni skupnosti.

Mestna občina Koper je leta 2012 med vsemi ostalimi mestnimi občinami, za varnostno področje namenila enega višjih odstotkov svojega letnega proračuna in sicer od 3 do 4 %. Zavedajo se pomena varnostnih sosvetov, saj ti lahko zelo pripomorejo k boljši varnostni sliki na lokalnem nivoju. Poudarek namenjajo tudi vlogi mladih in njihovemu vključevanju v delovanje varnostnih sosvetov. Prisoten je proaktiven pristop, kjer skozi različne mehanizme osveščanja spodbujajo prebivalce k izvajanju preventivnih ukrepov za preprečevanje kriminalitete in drugih negativnih varnostnih dejavnikov.«

Nagrado za Najboljšo knjigo s področja varnosti je na podlagi odločitve komisije prejel doc. dr. Milan Vršec

Obrazložitev:
»Neodvisna komisija se je odločila, da zaradi dejstva, da se omenjena nagrada v kategoriji »Najboljša knjiga s področja varnosti« v Republiki Sloveniji podeljuje prvič, so bila v ocenjevalni izbor vključena vsa knjižna dela, ki so na področju varnosti nastala od leta 1991. Temeljno študijsko gradivo na področju korporativne varnosti še vedno predstavlja knjiga **doc. dr. Milana Vršca** z naslovom „**Varnost podjetja – tokrat drugače**", ki je bila leta 1993 izdana pri založbi Viharnik iz Ljubljane. Vsebine knjige so kljub časovni odmaknjenosti še danes aktualne in izražajo dejanskost stanja procesov, ki jih je za celovito obvladovanje varnostnih tveganj potrebno izvajati v organizacijskih okoljih naših podjetij. Ta dejstva dokazujejo vizionarsko strokovnost cenjenega kolega Vršca, ki je za večino veliko prezgodaj začel raziskovati procese, ki jih je sodobno dinamično okolje prineslo v spremenjenih gospodarskih okoliščinah družbenega sistema, v katerega smo prešli po osamosvojitvi Republike Slovenije. Mnogokrat nerazumljen v svojih dognanjih s strani vodilnega managementa v slovenskih organizacijskih in akademskih okoljih, je bil v širšem regijskem mednarodnem okolju priznan kot eden vodilnih akademikov na področju korporativne varnosti. Tako so tudi njegova dela predstavljala osnovni študijski temelj za bodoče strokovnjake s področja korporativne varnosti. Vendar je knjiga z naslovom „Varnost podjetja – tokrat drugače", kmalu postala osnovni temelj za nadaljnje raziskave in aplikativne projekte, ki jih je **doc. Dr. Vršec** izvajal v vseh segmentih Slovenskega gospodarstva.«

Nagrado za Inovativno medijsko promocijo varnosti je na podlagi odločitve komisije prejelo podjetje PRO Plus.

Obrazložitev:
»PRO PLUS je vodilna medijska hiša, ki je v 17 letih delovanja pomembno oblikovala razvoj slovenskega medijskega prostora. Prispevki v programskem okolju televizijskih kanalov **POP TV** in **Kanal A** vsebujejo ustrezne informativne vsebine povezane s širšim področjem varnosti in obvladovanjem varnostnih tveganj v javnih in gospodarskih okoljih. Poročanje je ustrezno neodvisno in z vabljenimi strokovnimi gosti zagotavlja učinkovit prenos informacij v širšo družbeno skupnost. Informativni spletni portal **24 ur.com** ravno tako zagotavlja spekter kvalitetnih informacij, ki se dotikajo vsebin povezanih z varnostjo. Z inovativnim, fleksibilnim in ustvarjalnim pristopom do medijskih vsebin ter s pomočjo uvajanja najnaprednejših multimedijskih tehnologij predstavlja zelo pomemben dejavnik za dvigovanje varnostne kulture in splošnega zavedanja o pomenu varnosti v vseh okoljih delovanja naše družbe.

Poleg navedega podjetje **PRO Plus** tudi s svojim zgledom obvladovanja varnostnih tveganj znotraj svojega organizacijskega okolja pristopa inovativno in s svojimi pristopi močno odstopa od ostalih organizacij, ki delujejo v slovenskem poslovnem okolju. Poleg finančne racionalnosti projektov so ti usmerjeni v zagotavljanje kvalitete varnostnih storitev, ki zagotavljajo nemoten potek osnovnega poslovnega procesa.«

Glede na dejstvo, da je za izmenjavo izkušenj in sklepanje novih strokovnih kontaktov potrebno tudi ustrezno družabno okolje so organizatorji poskrbeli, da so se udeleženci počutili prijetno tudi ob družabnih dogodkih, ki ga je popestrila degustacija vinske kleti Graben, kjer je vinar Šekoranja predstavil vrhunska vina.

Ob konferenci je izšla tudi znanstvena monografija z naslovom »Management of corporate security – New Approaches and Future Challenges« urednikov dr. Denisa Čalete in mag. Mirana Vršca. ■

Ob konferenci je izšla tudi znanstvena monografija z naslovom »Management of corporate security – New Approaches and Future Challenges« urednikov dr. Denisa Čalete in mag. Mirana Vršca.

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: Doc. ddr. Robert Brumnik / Institut za korporativne varnostne študije
Center za informacijsko varnost*



SODOBNA OBVEŠČEVALNA DEJAVNOST IN GOSPODARSTVO (Bussines Inteligence)

Po koncu hladne vojne so obveščevalne službe vse bolj preusmerile delovanje z vojaško-političnega področja na področje gospodarstva. Nacionalna varnost je namreč danes bistveno bolj odvisna od gospodarske kot vojaške moči države, zato je postalo pridobivanje informacij gospodarskega področja, prioriteta vseh sodobnih držav. V globalnem svetu informacijske dobe so tako postale informacije, poleg naravnih virov, delovne sile in kapitala, eden izmed ključnih dejavnikov podjetja.

Uvod

Razvoj Informacijsko Telekomunikacijske Tehnologije (nadalje v besedilu IKT) daje delu obveščevalno varnostnih agencij popolnoma nove razsežnosti. Koriščenje IKT in hekerstva[1] v sodobnem mednarodnem okolju zahteva uporabo IKT, tudi v boju proti gospodarski kriminaliteti. Hekerske metode s tem niso omejene samo na teroristično in protiteroristično delovanje, ampak se uporabljajo tudi v obveščevalne namene na gospodarskem področju in diplomaciji.

Eden izmed prvih primerov[2] obveščevalno motiviranega hekanja je potekal leta 1987 v vzhodnem Berlinu. Uporaba hekerskih metod v obveščevalne namene je bila nadalje dokazana leta 1997 v ZDA, ko je NSA[3] izvedla vojaško simulacijo "Operation Eligible Receiver"[4]. Kiber napadi z obveščevalnim ozadjem so dokazljivo potekali tudi iz kitajskih strežnikov. Tako so v Južni Koreji sredi l.2004 zaznali 211 uspešnih vdorov v računalnike desetih državnih ustanov, med drugim tudi južnokorejskega parlamenta, inštituta za obrambne študije, univerz in zasebnih podjetij. Za napade naj bi bila odgovorna Severna Koreja, potekali pa so preko Kitajske. Severna Koreja naj bi imela tudi posebno izobraževalno ustanovo Mirrim College[5], kjer se načrtno šolajo računalniški strokovnjaki in hekerji.

Nadaljni razvoj IKT, bo prispeval k še večji disperziji ekstremnih skupin in posameznikov, saj omogoča njihovo online povezanost in vsled tega hitrejše in učinkovitejše delovanje. NIC[6] je mnenja, da se bo v naslednjih 15 letih povečalo število storilcev, vključno s teroristi, ki bodo usposobljeni tudi za kiberteroristične napade na vozlišča svetovne informacijske infrastrukture. Ta pa vključuje internet, telekomunikacijska omrežja in računalniške sisteme za upravljanje električnih mrež, rafinerij ipd. Glavno področje obveščevalne dejavnosti bodo v prihodnje informacije računalniških sistemov kritične infrastrukture, ki so nemalokrat dragocenejše in ranljivejše kot fizični sistemi.

Analiza tveganj se z razvojem informacijsko komunikacijske tehnologije vse bolj seli tudi v virtualni svet.

Zagotavljanje varnosti v sodobnem gospodarskem okolju

V okviru nacionalno varnostne strategije imajo obveščevalne službe posebno vlogo pri zagotavljanju informacijskega temelja delovanja sistema nacionalne

*avtor je član Slovenskega združenja korporativne varnosti

Nacionalna varnost je namreč danes bistveno bolj odvisna od gospodarske kot vojaške moči države, zato je postalo pridobivanje informacij gospodarskega področja, prioriteta vseh sodobnih držav.

varnosti. Sistem varnosti predstavljajo predvsem informacije, ki se nanašajo na prepoznavanje in analiziranje tveganj za nacionalno varnost. Analiza tveganj se z razvojem informacijsko komunikacijske tehnologije vse bolj seli tudi v virtualni svet. Pridobljene informacije se zagotavljajo vsem organom in službam, ki skrbijo za nacionalno varnost. V takem sistemu obveščevalne agencije nastopajo kot prejemnice, predvsem pa kot posredovalke obogatenih informacij ključnim dejavnikom odločanja v državi. Soočamo se z dinamično globalizacijo informacijskih družb, ki v povezavi s tehnološkimi izboljšavami (npr. lokalne brezžične povezave) povečuje možnosti medsebojnega povezovanja. Množično širjenje storitev in uporabnikov pa povečuje tudi ranljivost in ogroženost, ki se je večina med njimi sploh ne zaveda. V poročilu[7] ameriškega sveta za znanost in tehnologijo, so tako opredelili naslednje tehnološke trende, ki povzročajo skrbi in povečujejo ranljivost informacijske infrastrukture:

- Vse večja kompleksnost informacijskih sistemov predstavlja varnostni izziv za razvijalce in uporabnike.
- Razvoj telekomunikacijske infrastrukture, pri čemer se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo.
- Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop (securing the perimer) ni učinkovit, saj nimamo fizičnega nadzora nad uporabniki in napravami.
- Vse večja prepletenost in dostopnost na računalnikih temelječih sistemov, ki postajajo kritični oz. ključnega pomena za ekonomijo, logistiko, razširjanje dobrin in storitev.
- Globalnost IKT povečuje število nasprotnikov za uporabnike v domačem in mednarodnem prostoru.

Ob zagotavljanju varnosti kritične infrastrukture v operativnem smislu, je potrebno upoštevati tudi zakonodajo, ki opredeljuje pravico do komunikacijske zasebnosti[8]. Pravica do komunikacijske zasebnosti seveda ni absolutna. Na podlagi ustave RS lahko zakon določi, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.

Gospodarska obveščevalna dejavnost[9] (Business Intelligence)

Temeljna značilnost obveščevalno-varnostne dejavnosti je tajnost delovanja, kar jo zelo jasno loči od drugih dejavnosti. V prvi vrsti se tajnost kaže v načinu pridobivanja praviloma tajnih podatkov, ki mora biti tajen. Globalne spremembe v svetu, zlasti v Evropi in vedno nove grožnje varnosti namreč narekujejo učinkovito mednarodno povezovanje za zagotavljanje varnosti in stabilnosti.

Po koncu hladne vojne so obveščevalne službe vse bolj preusmerile delovanje z vojaško-političnega področja na področje gospodarstva. Nacionalna varnost je namreč danes bistveno bolj odvisna od gospodarske kot vojaške moči države, zato je postalo pridobivanje informacij gospodarskega področja, prioriteta vseh sodobnih držav. Tako kot varnost in stabilnost države tudi varnost in uspešnost gospodarskih podjetij temelji na njihovi sposobnosti pridobiti informacije ter z njihovo pomočjo pravočasno oblikovati ustrezne strateške odločitve. V globalnem svetu informacijske dobe so tako postale informacije, poleg naravnih virov, delovne sile in kapitala, eden izmed ključnih dejavnikov podjetja.

V poročilu CETISME[10], ki je bil izveden v okviru Inovacijskega programa pri Evropski Uniji, zajema gospodarska obveščevalna dejavnost zbir orodij, metod in konceptov, ki združujejo vse koordinacijske aktivnosti raziskave, pridobivanja, obdelave, shranjevanja in razširjanja informacij, pomembnih za podjetja ali organizacije pri oblikovanju strategije. Ti procesi so nepretrgani, zaporedni in vzajemni ter tvorijo obveščevalni cikel gospodarske obveščevalne dejavnosti (Economic Intelligence-a guide for beginners and practitioners, 2002).

Pridobivanje podatkov s tehničnimi viri

Osnovna dejavnost obveščevalno varnostnih služb je usmerjena na uresničevanje poslanstva in neposredno operativno izvajanje nalog. Obveščevalne službe v ta namen uporabljajo vse vire pridobivanja podatkov. S hitrim razvojem ITK ter pričakovanim nadaljnim trendom razvoja, je uporaba le teh pridobila na vrednosti, saj omogoča hitrejše in stroškovno ugodnejše zbiranje podatkov.



Vsekakor velja, da sta nadzor ter pridobivanje in obdelava informacij tesno povezana s tehnologijo, predvsem z informacijsko komunikacijsko tehnologijo. Moč nadzorovanja s sodobno informacijsko tehnologijo se kaže tudi v tem, da le ta omogoča tudi povezovanje zbranih podatkov. S povezavo razpršenih podatkov in njihovo obdelavo lahko pridemo do novih pomembnih podatkov in informacij. Nove razsežnosti nadzora pa vzpostavljajo tudi napredne statistične tehnike, npr. tehnike izkopavanja podatkov[11] (ang. data mining) in sisteme umetne inteligence[12]. S tem se dogaja preskok na novo raven, preventive in predvidevanja. Sodobna panoptična tehnologija[13] tako ne čaka, da se nekaj zgodi, temveč ukrepa že vnaprej na podlagi zbranih podatkov in ocenjenih predvidevanj (Whitaker, 1999).

Vendar pa sodobna računalniška tehnologija ni namenjena samo spremljanju posameznikovih dejavnosti, temveč lahko celo tehnično omeji[14] določena ravnanja posameznikov in jim tako fizično omeji možnosti (napačnega) delovanja. Numerični jezik se sestoji iz šifer, ki omogočijo dostop ali zavrnitev dostopa do informacije (Deleuze, 2002). Ne gre torej za to, da bi oblast s prepovedjo, ukazom posamezniku omejila dostop, gre za to, da posameznika opremi z geslom, ki mu dostop omogoča ali pa ga zavrne.

Računalnik oziroma IKT se torej vzpostavlja kot osrednja tehnologija v obveščevalni dejavnosti, saj se tehnologija za nadzorovanje neprestano razvija in krepi tržni segment. Ne samo, da omogoča nadzor, temveč ga tudi olajšuje, saj je že v osnovi zasnovana za zbiranje in hranjenje podatkov. Gre za medij, ki je globalen, multimedialen, na njem pa prihaja tudi do konvergence med različnimi tehnologijami, saj se v internet danes ne povezujemo samo z računalniki, temveč tudi z mobilnimi telefoni in celo drugimi napravami (npr. nadzornimi kamerami ("NannyCam", Wi-Fi kamere itd., televizorji in celo hladilniki). Poleg tega se sprožajo potrebe po novih in novih tehnoloških inovacijah, kar s seboj prinaša nove tehnologije shranjevanja podatkov, povečanja zmogljivosti pomnilniških sistemov pa ustvarjajo možnosti za še bolj izpopolnjene in intenzivne metode zbiranja podatkov.

Nove elektronske nadzorne tehnologije so nevidne[15] oziroma težko opazne, neprostovoljne (oziroma posameznik nima možnosti, da bi se jim izognil), so kapitalsko kot delovno intenzivne (zaradi česar so tudi razmeroma poceni in ekonomične) in niso usmerjene k obravnavi točno določenega posameznika, temveč h kategoriji posameznikov (Lyon, 1994). *Za pridobivanje podatkov se lahko uporabljajo precej preproste naprave[16], ki recimo zaznavajo, kaj pišemo po tipkovnici. Podatki se shranjujejo v napravi kot recimo v ključu USB, lahko pa ta tudi odda podatke prek omrežja (TEMPEST).*

Drugi od preprostejših načinov je prestrezanje podatkov. Prek spleta se podatki praviloma prenašajo nešifrirano, to velja tudi za prenos elektronske pošte. Obstajajo programi za šifriranje elektronske pošte, toda težava je v tem, da ga morata imeti nameščenega oba, pošiljatelj in prejemnik sporočila. Tudi za Skype in sorodne programe ter za internetno telefonijo že obstajajo programi za šifriranje, toda enak program mora imeti tudi sogovornik, kar pa oteži komunikacijo. Nekoliko večji občutek varnosti ponuja govor po spletu oziroma VoIP-telefonija, ki je morda za prisluškovalce še vedno manjša neznanka. Toda tudi tu zasebnost nima več velike prihodnosti. Med drugimi so progami, kot je VoIP-analizator, s katerimi se prestrezajo in analizirajo podatki, že na voljo.

Prestrezanje podatkov je sploh priljubljena dejavnost tajnih služb. Podatke, ki niso šifrirani, je mogoče enostavno prestrezati, šifrirane podatke pa je treba analizirati s kriptoanalizo oziroma dešifrirati. Mogoče pa je izpeljati tudi t.i. napad s posrednikom[17]. V ZDA so sprožili sodni proces[18] proti telekomunikacijskemu velikanu AT&T, ki obvladuje tretjino ameriškega trga in je sodeloval z NSA. V Sloveniji je potrjen sum, da naj bi bili pripadniki SOVE in policije uporabljali prenosno napravo in s tem nepooblaščeno prisluškovali nekaterim osebam. V ZDA to počnejo bistveno bolj prefinjeno, saj lahko na daljavo[19] aktivirajo mikrofone celo ugasnjenih mobilnih telefonov. Telefon naj bi bil povsem ugasnjen šele, ko se iz njega odstrani baterija. Pojavilo se je vprašanje; Kakšna je ta naprava; gre za strojno ali programsko napravo?

Drugi, precej klasičen način dostopa do gesel, so klasični vdori v računalnik, če ta ni opremljen s primerno zaščito. Vendar včasih tudi to ni nujno, v kolikor uporabniki uporabljajo ista gesla za dostop do različnih storitev. Nekdo ima tako za dostop do elektronske pošte lahko tudi 10-mestno geslo, a mu to ne pomaga, če potem uporablja isto geslo še za sodelovanje na forumih. Napadalec namreč lahko vdre v manj zaščiten spletni forum, pridobi geslo in potem dostopa do elektronske pošte uporabnika. Pravemu uporabniku pa verjetno ni jasno, kako so lahko uganili 10-mestno geslo.



Zaključek ("NetSpy" ali sodobno vohunjenje v prihodnosti)

Večplastni in večdimenzionalni varnostni izzivi, tveganja in grožnje v regiji, Evropi in svetu povzročajo številne negotovosti pri zagotavljanju nacionalne in mednarodne varnosti. Za pravočasno načrtovanje in izvajanje ukrepov za ohranjanje in krepitev tako nacionalne kot tudi mednarodne varnosti je potrebno vzpostaviti učinkovit sistem zgodnjega odkrivanja in opozarjanja na potencialna tveganja in grožnje. V skladu z navedenim morajo biti vzpostavljeni organizacijski, kadrovski in materialni temelji za sodelovanje in izmenjavo obveščevalnih in varnostnih podatkov na nacionalni ravni (po potrebi tudi institucionalizirani) v okviru dvostranskega sodelovanja ter v okviru zavezništev.
V tehničnem smislu nas seveda zanima, ali je s stališča varovanja informacij bolje komunicirati z internetno telefonijo oziroma s tako imenovano VoIP-telefonijo? Je delo z različnimi komunikacijskimi programi, kot so priljubljeni Skype, MSN in Yahoo Messenger varno? Je komunikacija prek računalnika in spleta varnejša kot z mobilnimi ali navadnimi telefoni? Seveda je z nekaterimi razumnimi ukrepi mogoče povečati varnost, toda če povprečni uporabnik naleti na motiviranega hekerja ali kriminalno združbo, najbrž nima veliko možnosti. Lahko zaščitimo računalnike s požarnimi zidovi, s protivirusnimi programi, lahko pošiljamo sporočila, kodirana s šifrirnimi programi, kot je program PGP[20],

lahko anonimno brskamo po spletu s programom Tor[21], toda nikoli ni izključena možnost, da bo kakšen poznavalec, kiberkriminalec ali tajna služba s sofisticirano opremo našla varnostno luknjo ali dekodirala sporočila. Sodobne obveščevalne službe in policija uporabljajo učinkovitejše in še bolj sofisticirane načine nadzora, kot smo jih navedli v prispevku. Ob tem pa je potrebno izpostaviti, da je pravna in zakonodajna podlaga v večini držav na tem področju še na trhlih in nedorečenih temeljih.

Viri:

- Council of Europe, (2003). Additional Protocol to the Convention on Cybercrime,
- Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed
- Deleuze, G., (2002). "Družba nadzora". V Filozofski vestnik, št. 3, letnik XXIII, Ljubljana: Filozofski inštitut ZRC SAZU.
- Hager, N., (2001). Secret Power - New Zealand's Role in the International Spy Network, Craig Potton Publishing
- Hutter, R., (2002). Cyber Terror-eine realistische Gefahr? URL: http://www.aksis.de/Cyber-Terror.pdf (09. 05. 2008).
- Lyon, D., (1994). The Electronic Eye. Cambridge: Polity Press.
- Podbregar, I., Slapar, M., (2006). Razsežnosti gospodarskega vohunstva v 21. Stoletju-primer gospodarskega vohunstva s pomočjo trojanskega konja, Bled, Dnevi varstvoslovja.
- Potter, E. H., (1998). Economic Intelligenc and national security. Ottawa: Carleton Uiversity press.
- Trampuž, M., (2002). "Izguba skrivnosti z nadzorovanjem": Bentham in nove tehnologije nadzorovanja. Magisterska naloga, Ljubljana.
- Whitaker, R., (1999). The End of Privacy. New York: The New Press.

[1] **Hekanje** je priključevanje v računalniška omrežja brez dovoljenja z izkoriščanjem uporabniških imen in gesel drugih uporabnikov, ki ni dovoljeno in je kaznivo. Kazniv je tudi vdor v računalniška omrežja, če se razbijejo ali zaobidejo vstopne kontrole URL: http://hekanje.googlepages.com/ (22.04.2008). Eden najbolj znanih hekerjev je Mitnick, po katerem so posneli tudi film. Med drugim je vdrl v sistem podjetja Digital Equipment Corporation. Metodologija klasičnega hekerskega napada vsebuje naslednje stopnje: 1.Pridobivanje informacij, 2.Preizkušanje, 3.Napad, 4.Prodor oz.širjenje napada na sosednje sisteme, 5.Infiltracija/Extrakcija.

[2] **Prvi znan primer obveščevalno motiviranega hekanja**; Skupina zahodnonemških hekerjev je stopila v stik s sovjetsko tajno službo KGB, in v zameno za 18.000 dolarjev ter kokain, Sovjetom posredovala ukradene podatke. Hkrati jim je posredovala tudi znanje o vdiranju in slabostih računalniških sistemov URL: http://slo-tech.com/script/forum/izpisitemo.php?threadID=198884 (21.04.2008).

[3] **National Security Agency**; ameriška agencija za nacionalno varnost URL: http://www.nsa.gov/ (24.04.2008).

[4] **Operation Eligible Receiver**; V tej operaciji je 35 računalniških strokovnjakov NSA poskušalo in tudi uspelo vdreti v določene vojaške in civilne računalnike, ki so nadzorovali ključne infrastrukturne sisteme. Hekerjem uspelo pridobiti »root« dostop v 36-ih od 40.000 omrežij obrambnega ministrstva. Napad je med drugimi povzročil izklop elektro-energetskega sistema in številke 911 za nujne klice v okrožju Washington. Hekerjem je uspelo prodreti celo v računalniški sistem ene izmed bojnih ladij, ki je bila v tistem času na pohodu. URL: http://www.cdi.org/terrorism/cyberdefense-pr.cfm (21.04.2008)

[5] **Mirrim College;** Obrambni minister Južne Koreje pa je oktobra 2004 v poročilu parlamentarnemu odboru za obrambo navedel, da je po obveščevalnih podatkih Severna Koreja izšolala okrog 600 hekerjev, ki so zadolženi za izvajanje obveščevalnih dejavnosti proti Južni Koreji, Japonski in ZDA URL: http://www.securityfocus.com/news/9649 (21.04.2008).

[6] **NIC** (National Intelligence Council); Mnenja so pridobljena iz za obdobje do 2015, URL: http://www.dni.gov/nic/NIC_redirect.html (21.04.2008).

[7] **Poročilo;** Federal Plan for Cyber Security and Information Assurance Research and Development URL: http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf (24.04.2008)

[8] **Pravica do komunikacijske zasebnosti**; zagotavlja varstvo posameznikovega interesa, da se država ali nepovabljeni tretji ne seznanijo z vsebino sporočila, ki ga posreduje preko katerega koli sredstva, ki omogoča izmenjavo ali posredovanje informacij na daljavo URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:SL:NOT (24.04.2008).

[9] **Gospodarska obveščevalna dejavnost** (Business Intelligence ali Economic Intelligence), označuje pridobivanje poslovno pomembnih gospodarskih informacij, vključno s tehnološkimi podatki, finančnimi, komercialnimi, lastninskimi in vladnimi informacijami, katerih pridobitev s strani tujih interisenrov, neposredno ali posredno pripomore k relavantnemu povečanju produktivnosti ali izboljšanju konkurenčnega stanja gospodarstva države iz katere izhaja organizacija ali podjetje, ki tovrstne informacije pridobiva (Potter, 1998)

[10] **CETISME**; Cooperation to promote Economic and Technical Intelligence in Small and Medium-sized Enterprises URL: http://www.sail-eu.net/research_and_development/projects/CETISME_30/ (07.05.2008).

[11] **Izkopavanja podatkov** je interaktiven in ponavljajoč se proces, kjer je potrebna uporabiti tako ekspertizo problemskega področja, kot tudi naprednih tehnologij za ugotavljanje prekritih povezav in značilnosti podatkov. Najbolj poznan je program SPSS, ki je razširjen tudi v Sloveniji. SPSS eno vodilnih podjetij na področju analitičnih orodij za izkopavanje podatkov URL: http://www-ai.ijs.si/MarkoGrobelnik/awamida99/clementine.doc (25.04.2006). Na področju statistike in metodologije pa so poznana še druga analitična orodja; npr.: AnswerTree, DecisionTime, Clementine.

[12] **Sistemi umetne intelligence;** Dolgoročni cilj raziskav strojnega učenja, ki je zaenkrat seveda nedosegljiv, je ustvariti umetni sistem, ki bi z učenjem dosegel ali celo presegel človekovo inteligenco. Širše področje raziskav, ki ima isti končni cilj, se imenuje umetna inteligenca (artificial intelligence) URL: http://www.fri.uni-lj.si/si/katedre_in_laboratoriji/umetna_inteligenca/lab_umetna_inteligenca/ (09.05.2008).

[13] **Panoptična tehnologija,** moderna tehnologija stalnega nadzora, pri čemer ne vemo, da smo nadzorovani URL: http://www.surveillance-and-society.org/articles1(3)/camera.pdf (24.04.2008). Panoptikon pa omogoča nadzorniku, da gleda, ne da bi bil viden, torej ima atribute: vsevidnost, vsevednost in vsemogočnost (Foucalt, 1991).

[14] Omejitev dostopa lahko dosežemo z biometričnimi napravami ter tako preprečimo delovanje v realnem ali virtualnem prostoru.

[15] **Elektronski panoptikum (Superpanoptikum)**; Danes je nadzorovanje dosti bolj nevidno in nevarno, dosti manj javno in na splošno, težko se mu je izogniti (Trampuž, 2002).

[16] **Z napravo za zaznavanje tipkanja** se pride do gesel uporabnika tipkovnice, napravo pa uporabljajo tudi lastniki podjetij za nadzor, kaj počnejo zaposleni med delovnim časom. »Za naprave, namenjene prestrezanju tipkanja, so načrti na spletu ali pa se nabavijo za 150 dolarjev. Prestrezajo vse, kar kdo tipka. Namestijo se na kabel ob priklopu tipkovnice v računalnik.

[17] **Napade s posrednikom**, napadalci pogosto uporabljajo za preusmeritev uporabnikov, na primer elektronskega bančništva, na lažno spletno stran in tako skušajo pridobiti geslo, je pa napade s posrednikom mogoče uporabiti tudi pri uporabi drugih spletnih storitev.

[18] **Sodni proces** proti AT&T, kjer ga tožijo, ker je ameriški tajni službi NSA dovolil, da je nezakonito namestila svojo opremo na njegove glavne usmerjevalnike in pregledovala ves promet. Telekomunikacijsko podjetje pač tožijo, ker je ta pot lažja in uspešnejša, kot če bi tožili tajno službo URL: http://slo-tech.com/script/forum/izpisitemo.php?threadID=296188 (09.05.2008).

[19] Lani konec leta je prišlo na dan, da je FBI nekemu osumljencu na mobilni telefon namestil prisluškovalno napravo. FBI je na mobilni telefon osumljenca naložil programsko opremo, ki mu je omogočila vklop mikrofona in poslušanje pogovorov. Programska oprema pa se naloži kar prek GSM omrežja.

[20] **Program PGP** (Pretty Good Privacy), se uporablja za zaščito elektronske pošte in podatkovnih datotek. Omogoča komuniciranje, ne da bi potrebovali varen kanal. URL: http://www1.fov.uni-mb.si/Studentske_strani/seminarske/pgp/default.html (24.04.2008).

[21] **Tor** je sistem (projekt), ki nastaja pod pokroviteljstvom organizacije Electronic Frontier Foundation. Trenutno gre za razvojno različico zbirke orodij, ki omogočajo anonimno brskanje po spletnih straneh, objavljanje vsebin, anonimno uporabo programov za neposredno sporočanje IM, IRC in SSH in drugih programov, ki slonijo na protokolu TCP. Sistem Tor zmanjša možnost, da bi vas našli, saj preusmeri promet prek večjega števila naključno izbranih strežnikov v omrežju, kar metodo analize prometa močno oteži, če ne celo prepreči. url: www.eff.org (23.04.2008) ■

Avtorja: Mag. Simon Starček, Davčna uprava Republike Slovenije
Andrej Kovačič, Institut za korporativne varnostne študije*





FINANČNI VIDIKI OBVLADOVANJA VARNOSTNIH TVEGANJ V IGRALNIŠTVU

Eden izmed osnovnih pogojev za nemoteno poslovanje igralnic in igralnih salonov je vsem udeležencem zagotoviti varno igralniško okolje.

Neustrezen pristop ter zmanjševanje finančnih sredstev na račun obvladovanja varnostnih tveganj, ima lahko vidne posledice.

Gospodarska in finančna kriza, razvoj konkurence in njihov čezmejni vpliv, visoke davčne in koncesijske obremenitve, ter pomanjkanje ustrezne igralniške strategije, vplivajo na poslovanje igralniških družb[1] v Sloveniji. Drugače je na drugi strani, kjer ''ljubitelji tujega denarja'' izkoriščajo vse mogoče načine, da bi se v neustrezno varovanih igralniških družbah, čim bolje okoristili. Igralništvo je z varnostnega vidika specifična dejavnost, zato so zelo pomembni interni[2] in državni nadzorni mehanizmi. Neustrezen pristop ter zmanjševanje finančnih sredstev na račun obvladovanja varnostnih tveganj, ima lahko vidne posledice. Tako se ne moremo izogniti potrebnim investicijam v učinkovit varnostni sistem za obvladovanje varnostnih tveganj igralniških družb. Najvišje vodstvo je odgovorno za varnostno politiko in strateško odločanje, za kar potrebuje dokument za celovito zagotavljanje varnosti in s tem povezanih tveganj. Informacije o učinkih in uresničenih strategijah na področju korporativne varnosti ter o potrebnih virih za njihovo uresničevanje, so ključna podlaga za strateško razmišljanje in odločanje. Pogosto se pokaže, da je prav uresničevanje strategij, tudi na področju varnosti, najzahtevnejše v procesu strateškega menedžmenta. Namen prispevka je nakazati pristope za boljše razumevanje varnostnih tveganj v igralniških družbah in o potrebnih investicijah za učinkovit sistem zagotavljanja korporativne varnosti.

Zagotavljanje korporativne varnosti za nemoteno poslovanje igralnic in igralnih salonov

Eden izmed osnovnih pogojev za nemoteno poslovanje igralnic in igralnih salonov je zagotoviti varno igralniško okolje vsem udeležencem. Za zagotavljanje splošne varnosti v igralniških družbah skrbi interna ali zunanja varnostna služba. V procesu zagotavljanja celovite varnosti, ima ob interni službi za videonadzor in službi za informacijsko varnost pomembno vlogo tudi vodja skladnosti poslovanja (Chief Compliance Officer). Vidno vlogo v tem procesu ima tudi varnostna kultura vseh udeležencev, čeprav lahko vplivamo nanjo neposredno le pri zaposlenih. Naloga vodstva je, da preko odgovorne osebe za varnost[3] z internimi usposabljanji in drugimi aktivnostmi pripomore k dvigu varnostne kulture. Na ta način zaposleni pridobijo potrebna znanja za boljše razumevanje varnostne problematike v igralništvu in področne zakonodaje ter se seznanijo z internimi varnostnimi pravili. Zaposleni se tako usposabljajo tudi za ustrezna ravnanja s tveganimi obiskovalci ter da s svojim ravnanjem ne povzročijo incidentov. Namen usposabljanja je tudi dvig splošne kulture tveganj ter učinkovit sistem upravljanja in obvladovanja varnostnih tveganj.

Varnostni in škodni primeri ter vzroki zanj pogosto ''niso vidni očem'', tako da je za pristojne službe zelo pomembna

Razmerje med dejanskimi oziroma ugotovljenimi in uspešno rešenimi varnostnimi in škodnimi primeri, je pokazatelj učinkovitosti služb, ki skrbijo za varnost.

*avtor je član Slovenskega združenja korporativne varnosti



Arhiv: Petra Vidmar

njihova vzročna in pripravljalna aktivnost. Za pravočasno ukrepanje in preprečevanje dogodkov, ki bi lahko vplivali na poslovanje, je zato potrebno razvijati strategijo proaktivnega delovanja. Razmerje med dejanskimi oziroma ugotovljenimi in uspešno rešenimi varnostnimi in škodnimi primeri, je pokazatelj učinkovitosti služb, ki skrbijo za varnost. Zelo pomembno je njihovo proaktivno, ciljno in usklajeno delovanje. Naloga odgovorne osebe za varnost je predlaganje varnostnih rešitev, ki pa so lahko učinkovite, če temeljijo na poznavanju igralniških procesov in dobrih praksah. Pri tem je v pomoč tako imenovani igralniški varnostni model[4], ki je za vodstvo družbe osnovni dokument in podlaga pri odločanju o investicijah v sistem obvladovanja varnostnih tveganj. Igralniški varnostni model je prav tako potreben pri izdelavi letnega elaborata »varnostnega projekta« in vsebuje:

- finančne vidike zmogljivosti zagotavljanja celovite varnosti;
- analizo varnostnih tveganj in obstoječega stanja v igralniški družbi;
- analizo varnostnih dogodkov in vzrokih zanj;
- analizo ugotovljenih nepravilnosti na igralnih mizah ter ugotovljenih škodnih dogodkih;
- raziskavo med zaposlenimi o občutenju varnosti v delovnem okolju ter vpliv na njihovo delo;
- analizo obravnavanih varnostnih pritožb obiskovalcev, opozoril gostom ter zaposlenim.

Finančni vidiki zagotavljanja korporativne varnosti igralnic in igralnih salonov

Pri uresničevanju strategij je že nekaj desetletij nepogrešljiv projektni menedžment, ki predstavlja zelo učinkovit in uspešen način pretvorbe strateških ciljev in strategij v dejanja in učinke. Vsaka igralniška družba potrebuje projekt »Obvladovanje varnostnih tveganj«. Projekt je zaporedje enkratnih, kompleksnih in med seboj povezanih dejavnosti, usmerjenih k doseganju skupno opredeljenega strateškega cilja organizacije na področju varnosti. Je časovno in proračunsko omejen v sklopu strateškega oziroma letnega poslovnega načrta organizacije (Wysocky, McGary, 2003). Za letni poslovni načrt igralniške družbe je potrebno izdelati zagonski elaborat za »varnostni projekt«. V sklopu projekta, mora družba določiti (Aver, Pustatičnik, 2006):

- namenske cilje »varnostnega projekta« - kot pričakovani ekonomsko neposredni, posredni in drugi učinki;
- objektne cilje kot načrtovane projektne rezultate;
- dokument formalnega zagona izvajanja »varnostnega projekta«;
- vsebino, taktiko in načrt projekta »Obvladovanje varnostnih tveganj« ter projektno organizacijo;
- matriko kompetenc in odgovornosti;
- analizo vplivnih dejavnikov in načrt ukrepanja;
- analizo rizika in načrt obvladovanja rizika;
- organizacijo obvladovanja sprememb;
- vodenje projektne dokumentacije;
- projektno komunikacijo.

Pri pripravi zagonskega elaborata »varnostnega projekta« gre tako za celostni načrt projekta. Elaborat pripravlja vodja projekta, ki je odgovorna oseba za varnost ter je zadolžena za dosledno evidentiranje stroškov projekta. Ko je zagonski elaborat projekta izdelan, ga preuči vodstvo in se odloči, ali ga bo umestilo v letni poslovni načrt, pri čemer upošteva:

- prispevek in nujnost predvidenih rezultatov (učinkov) projekta zagotavljanja varnosti k doseganju strateških ciljev;
- predvidene potrebne vire za projekt obvladovanja varnostnih tveganj v igralniški družbi in
- predvideno potrebno sodelovanje in pripravljenost subjektov iz zunanjega okolja pri izvajanju projekta.

Učinki projekta »Obvladovanje varnostnih tveganj« so lahko naslednji:

- obvladovanje oziroma preprečitev morebitnih odhodkov za škode v primeru namernega oškodovanja premoženja, goljufij in drugih operativnih tveganj;

- večji ugled igralnice, višja stopnja varnosti obiskovalcev in zaposlenih in s tem povečanega števila obiskovalcev, zaradi medijskih objav o konkurenčnih igralniških družbah, ki imajo težave z zagotavljanjem varnosti. Medijska objava o namerni povzročeni škodi, se lahko odraža skozi finančne in nefinančne kazalnike, zmanjšanje števila obiskovalcev, upad vrednosti delnic, zmanjšanje prihodkov idr.«[5];
- obvladovanje varnosti ali izboljšanje varnosti poslovanja in upravljanje vseh vrst tveganj družbe;
- izboljšanje kompetentnosti sodelavcev in menedžmenta;
- večja učinkovitost in uspešnost izvajanja procesov ter informacijske podpore.

V sklopu zagonskega elaborata projekta se stroški projekta načrtujejo na ravni projekta kot celote. Načrtuje se vse neposredne stroške, ki jih je mogoče načrtovati ob zagonu projekta za boljše obvladovanje varnosti. Posebej se načrtujejo še pričakovani investicijski stroški v varnostno opremo in stroški sodelovanja zunanjih izvajalcev. Ko uprava potrdi omenjeni varnostni projekt, pomeni formalen začetek projekta. Med uresničevanjem projekt postopno dobiva jasnejšo podobo, pojavljajo se lahko spremembe in odstopanja od načrta, kar zahteva njegovo občasno revidiranje.

Za uspešno uresničevanje varnostne strategije igralniške družbe, zahteva izpeljava omenjenega projekta s stroški, ki omogočajo ustrezno zagotavljanje varnosti, s čim krajšim obdobjem vračanja vloženih finančnih virov. Že en odmeven varnostni ali škodni dogodek, ima lahko pomemben vpliv na znižanje prihodkov igralniške družbe. Ob tem ima lahko leta negativne posledice še v nadaljnjih letih. Za ustrezen sistem[6] obvladovanja varnostnih tveganj v igralništvu je potrebno namenjati vsaj 1 do 2 % letnih prihodkov igralnih salonov in vsaj 3 do 4 % letnih prihodkov igralnic.

Vodja varnostnega projekta mora uspešno delovati v vseh fazah, od njegove strateške opredelitve, do začetka koriščenja rezultatov in preverjanja doseženih učinkov projekta v rednem poslovanju. Za nadzor nad projektom skrbijo menedžment in vodja projekta. Informacije o projektnih dejavnostih za menedžment projekta se zbirajo prek rednih mesečnih poročil v predpisani obliki. Večje nepredvideno povečanje finančnih in drugih virov med projektom zahteva, da se ponovno odloča o ciljih projekta, o nadaljevanju dela ali celo o spremembah v organizaciji vodenja in izvedbe projekta. Vložene vire v omenjeni projekt morajo utemeljiti tudi ustrezni projektni učinki, ki so lahko ekonomsko neposredni ali posredni. Pri tem je treba upoštevati, da se učinki običajno le delno pojavljajo že ob koncu projekta. Praviloma se pojavijo pozneje, v fazi koriščenja rezultatov projekta.



Že en odmeven varnostni ali škodni dogodek, ima lahko pomemben vpliv na znižanje prihodkov igralniške družbe.

Zaključek

Prirejanje iger na srečo je specifična dejavnost, ki ni prepuščena svobodni gospodarski pobudi. Zakon o igrah na srečo v Sloveniji ureja, da te potekajo v urejenem in nadzorovanem okolju, da se preprečijo pranje denarja, goljufije in druga kazniva dejanja in ravnanja v nasprotju z javnim redom ter, da se zagotovi varnost vsem udeležencem iger na srečo. Igralniške družbe zato potrebujejo učinkovit varnostni sistem, ki bo celovito obvladoval varnostna tveganja. Oseba odgovorna za varnost skrbi za celoviti pristop obvladovanja korporativne varnostne problematike. Obvladovanje varnostnih tveganj je načrtovano skladno s Strateškim razvojnim programom igralniške družbe za določeno obdobje. Projekt je načrtovan v skladu s Pravilnikom



o projektnem vodenju in Metodološkem priročniku o vodenju projektov. V Poslovnem načrtu igralniške družbe vodja projekta »Obvladovanje varnostnih tveganj«, opredeli varnostni projekt na predpisan način, pri čemer si pomaga z varnostnim modelom. Učinkovitost vlaganja denarnih sredstev v varnostni sistem igralniške družbe se tako nanaša na porabo virov, ki jih potrebuje, da dosega zastavljene cilje na področju korporativne varnosti. Gre predvsem za odnos med vlaganji v varnostni sistem in rezultati - učinki. Učinkovitost pri zagotavljanju varnosti pa je vsekakor potrebna, vendar ne tudi zadostna za uspešnost poslovanja igralniške družbe.

Viri:

- Aver, B., Pustatičnik, J.. Projektni menedžment v Vzajemni d.v.z. *Proj. mreža Slov.*, jun. 2006, let. 9, št. 2, str. 25-29.
- Wysocky, K.R., McGary, R.: Effective Project Management, 3. izdaja, John Wiley & Sons, Inc., 2003.
- Kovačič, A., Stroškovni vidiki fizičnega varovanja v igralnici GCL. Projektno delo, 2008.

[1] Igralnice in igralni saloni.

[2] Varnostna služba, služba za videonadzor, služba za informacijsko varnost, oddelek za skladnost poslovanja, inšpektorji iger.

[3] Odgovorna oseba za igralniško varnost ali korporativni varnostni manager.

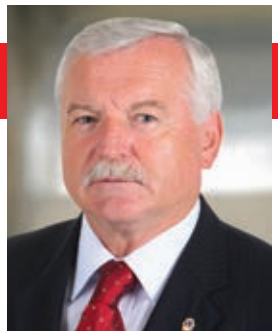
[4] Igralniški varnostni model je dokument, na podlagi katerega se vodstvo odloča o investicijah v sistem za obvladovanje varnostnih tveganj in za delovanje pristojnih služb, ki skrbijo za varnost v igralniški družbi.

[5] Povečanje ali zmanjšanje prihodkov oz. sprememba števila obiskovalcev so temeljni kazalniki, ki kažejo na določene učinke tveganj. "Povečanje prihodkov" je načeloma enostavno izmeriti, težje izmerimo, ali je dvig/padec prihodkov neposredna posledica povečanega/zmanjšanega ugleda igralnice ali igralnega salona.

[6] Za delovanje varnostnega sistema, plače varnostnega osebja oz osebja, ki delujejo na varnostnem področju, usposabljanje, vzdrževanje tehničnih naprav in ostale opreme, zunanji izvajalci itd.

"Mnenja in pogledi, predstavljeni v besedilu, izražajo osebna stališča avtorja in ne odražajo stališč institucije, iz katere avtor izhaja." ■

Avtor: Doc. dr. Boris Žnidarič[1] / Slovensko združenje korporativne varnosti*



PREVENTIVNO DELOVANJE SLOVENSKIH ZAVAROVALNIC

Zavarovalništvo je v sodobnem svetu pomembna gospodarska dejavnost za zagotavljane socialne, zdravstvene, ekonomske, gospodarske in drugih oblik varnosti. Po svoji naravi in načinu opravljanja temeljnega poslovanja ter uradni klasifikaciji dejavnosti nudijo zavarovalnice v sodobni družbi svoje storitve, zato sodijo v t. i. storitveno ali neproizvodno dejavnost.

Tako kot na drugih področjih je tudi na tem bilo potrebno veliko otipljivih razlogov za to, da danes ljudje vidijo v zavarovanju svojo korist. Zavarovalništvo je v veliki meri partner države in družbe kot celote na področju uresničevanja kolektivne in individualne socialne varnosti ljudi (Brask, 1991:479). V bistvu gre za gospodarsko dejavnost, ki se ukvarja z organiziranjem zaščite pred različnimi nevarnostmi, s čimer se zadovoljuje ekonomska (in druge) potreba po varnosti (Ivanjko, 1999:19). Rečeno tudi drugače, zavarovalnice zagotavljajo svojim klientom (zavarovancem) socialno, ekonomsko in gospodarsko varnost, v obsegu in na način, kot je določena z zavarovalno pogodbo.

V tem prispevku bom obravnaval zavarovalniško dejavnost z vidika tistih aktivnosti in opravil, ki bi jih lahko razvrstili med preventivne, pri čemer bom opozoril na dve temeljni dilemi, ki izhajata iz sedanjega stanja in prakse ter možnosti za takšno delovanje v prihodnje. Seveda pa se ni možno izogniti vprašanju kaj imata skupnega zavarovalništvo in preventivna dejavnost (prevencija) oziroma ali je zavarovalništvo dolžno razvijati preventivno dejavnost?

Zavarovalništvo in preventivna dejavnost

Vprašati se je treba kaj imata skupnega zavarovalništvo in preventivna dejavnost (prevencija) in nadalje, ali je zavarovalništvo dolžno razvijati preventivno dejavnost? Zavarovalna prevencija, kakor jo je poimenoval Boncelj (1983:112), je že sama po sebi pomembna za vsako zavarovalnico, saj se z uspešnim delovanjem zmanjšujejo objektivne in subjektivne okoliščine, ki vplivajo na nastanek škodnih primerov. Seveda pa pri tem ni možno poenostavljati in šteti zavarovanje za preventivno dejavnost samo po sebi. Zavarovanje je konkreten pravni posel za zagotavljanje ekonomske, gospodarske, materialne in socialne varnosti, ki poleg preventivne dejavnosti vključuje tudi zavarovanje. Vsekakor pa imata preventivna dejavnost in zavarovanje skupno izhodišče obstoja in družbene vloge, to je obstoj nevarnosti. Obe si jo prizadevata z določenimi ukrepi odpraviti oziroma v primeru nastanka nekega negotovega dogodka vzpostaviti prejšnje stanje. Če ne bi obstajale nevarnosti, potem ne bi bilo potrebe po preventivi in ne po zavarovanju. S preventivno dejavnostjo skušamo odpraviti nevarnost tako, da z izvajanjem dogovorjenih ukrepov neposredno vplivamo na objektivni položaj v zunanjem svetu, iz katerega izvira. Idealne podobe ni. Preventiva na številnih področjih ni mogoča, ker preventivnega sredstva še ni ali je v nesorazmerju s pretečo nevarnostjo, bodisi zaradi samega stroška, bodisi zaradi obsega nevarnosti. Z organiziranim preventivnim delovanjem vplivamo na objektivno stanje v okolju, s čimer zmanjšujemo možnost nastopa tistih pojavov in dogodkov, ki bi lahko ogrozili varovane objekte in dobrine. Absolutne učinkovitosti preventive ni. Lahko govorimo le o relativnih uspehih preventivnega dela v zavarovalništvu, predvsem pa moramo pojmovno ločiti samo preventivo kot del zavarovalniške dejavnosti od zavarovanj.

Vsekakor pa imata preventivna dejavnost in zavarovanje skupno izhodišče obstoja in družbene vloge, to je obstoj nevarnosti. Obe si jo prizadevata z določenimi ukrepi odpraviti oziroma v primeru nastanka nekega negotovega dogodka vzpostaviti prejšnje stanje. Če ne bi obstajale nevarnosti, potem ne bi bilo potrebe po preventivi in ne po zavarovanju.

[1] Doktor družbenih znanosti, habilitiran visokošolski učitelj.

Izvajanje preventivne dejavnosti v zavarovalništvu

Zavarovalnica lahko sama neposredno izvaja preventivne akcije v okviru izvajanja zavarovanj, in sicer z:
- individualizacijo zavarovalnih premij (pred sklenitvijo ali v času trajanja zavarovanja),
- izvajanjem svetovalne dejavnosti (pred sklenitvijo ali v času trajanja zavarovanja),
- zagotavljanjem pripomočkov in naprav manjše vrednosti ter širše namembnosti za izboljšanje varnosti zavarovanega premoženja in oseb (praviloma po sklenjenem zavarovanju).

Pri izvajanju preventivne dejavnosti lahko zavarovalnica sodeluje z zavarovanci in organizacijami, ki opravljajo preventivno in represivno dejavnost za preprečevanje vzrokov nastajanja nevarnosti in škod. Zavarovalnica lahko s sredstvi preventivnega sklada sama ali z drugimi zavarovalnimi organizacijami ustanovi podjetja ali druge organizacije (zavode, inštitute ipd.) za proučevanje, projektiranje in izdelavo naprav na področju preventivnega varstva premoženja in oseb ter za druge storitve na področju preventive. Za načrtno preventivno dejavnost, predvsem za zagotovitev potrebnih sredstev za poslovno leto lahko zavarovalnica vodi ustrezne preglede in evidence podatkov, ki so podlaga za analize in ocene (154. člen ZZavar) ter programske usmeritve in finančni plan. Izdatke za preventivno dejavnost delimo glede na način in oblike financiranja v dve osnovni skupini, in sicer:
- namenska posojila za preventivno dejavnost (štejejo za naložbe zavarovalnice, za posojilojemalca pa posojila pod ugodnejšimi pogoji),
- neposredni izdatki, ki bremenijo tekočo funkcionalno premijo.

Seveda ne gre zanemariti vloge in pomena prispevka slovenskega zavarovalstva na področju zbiranja sredstev za preventivno dejavnost, in sicer v okviru požarne takse, ki jo določa zakon (Zakon o požarni varnosti, 58. in 59. člen) in natančneje ureja uredba vlade (Uredba o požarni taksi, 5. člen).

Vidiki neposrednega preventivnega delovanja

Splošni pogoji in premijski sistemi za posamezne zavarovalne podvrste (zavarovanja) premoženjskih zavarovanj predvidevajo in v posameznih primerih tudi zahtevajo preventivno ravnanje zavarovanca oz. lastnika zavarovanega objekta. Tako npr. požarno zavarovanje ne krije škode, ki je nastala na stvari, če je le-ta pregorela, se osmodila ali ožgala zaradi cigarete, žerjavice, svetilke, peči ipd. To pomeni, da so škode, ki nastanejo zaradi navedenih okoliščin, ki jih je povzročil lastnik ali uporabnik zavarovanega objekta zaradi malomarnega ravnanja ali drugih razlogov (vinjenost, stanje pod vplivom psihotropnih sredstev ipd.) izvzete iz kritja, kar pomeni, da lahko zavarovalnica zavrne izplačilo nastale škode. Prav tako ni krita škoda, ki nastane na zgradbi, ki ni bila zgrajena na način, kot je običajno v kraju in po projektih (upoštevajoč krajevne vremenske in druge okoliščine), ali je slabo vzdrževana ali dotrajana. Podobnih izključitev odgovornosti zavarovalnice je v zavarovalnih pogojih še več. Njihov namen je spodbuditi zavarovance, da bodo s svojimi ravnanji in posegi v zavarovane objekte (posodobitve, preventivna sredstva in naprave) zmanjševali možnosti nastanka škod, po drugi strani pa se zavarovalnica na ta način izogne svoji odgovornosti. Zavarovalnica pa v celoti povrne nujne stroške za ukrepe, ki naj bi odvrnili ali zmanjšali škodo in ki so po nastanku zavarovalnega primera storjeni po nalogu zavarovalnice.

Pri zavarovanju nekaterih, še posebej nevarnih objektov in naprav, zavarovalnica kot pogoj za sklenitev zavarovanja zahteva dodatno preventivno ravnanje zavarovanca. Tako npr. morajo, pri zavarovanju naprav za kurjenje s plinom in gorilnim oljem, lastniki oziroma upravljavci dokazati, da naprave ustrezajo standardom in predpisom. Zavarovanec pa je dolžan dati naprave za kurjenje in kotel redno – najmanj enkrat letno – tehnično pregledati in sproti odpravljati morebitne ugotovljene pomanjkljivosti. Če zavarovanec prekrši eno od obveznosti, navedeni v tej klavzuli in zaradi tega nastane škoda, zavarovalnica lahko odkloni izplačilo odškodnine. Zavarovanec je dolžan storiti vse potrebno za preprečitev ali zmanjšanje škode in v celoti upoštevati navodila zavarovalnice pri tem. V nasprotnem lahko v celoti ali delno izgubi pravico do odškodnine, pri čemer se presoja vpliv njegovega ravnanja oz. obseg opustitve naloženih preventivnih ukrepov.

Zavarovalnice pa so vgradile v svoje cenike popuste na zavarovalne premije in uvedle druge ugodnosti za tiste zavarovance, ki so svoje zavarovalne objekte dodatno zaščitili s sredstvi za odkrivanje in gašenje požara, opremili z alarmnimi napravami oz. organizirali varnostno službo ipd. Varnostne naprave in sistemi morajo ustrezati tehničnim predpisom in standardom in morajo biti redno vzdrževani. Sicer pa je splošno znan način spodbujanja zavarovancev s sistemom bonus – malus, ki omogoča dodatne ugodnosti, predvsem pa nižje zavarovalne premije tistim zavarovancem, ki niso v določenem časovnem obdobju (praviloma v enem letu – zavarovalno leto) imeli škod oz. so bile izplačane škode mnogo nižje od vplačane zavarovalne premije (bonus - ugoden škodni rezultat). In nasprotno.

Vidiki posrednega preventivnega delovanja zavarovalnic

Pri izvajanju preventivne dejavnosti na različnih področjih zavarovalnice sodelujejo z drugimi subjekti v okolju na državni ravni in na ožjih (regionalnih in lokalnih) ravneh. Na državni ravni sodeluje v preventivnih akcijah v imenu vseh svojih članic (zavarovalnic) Slovensko zavarovalno združenje z nosilci oz. izvajalci akcij, in sicer največkrat z vlogo financiranja. Tako je Slovensko zavarovalno združenje že vrsto let uspešno sodelovalo s Svetom za preventivo in vzgojo v cestnem prometu Republike Slovenije (Danes je Svet za preventivo in vzgojo ena od štirih notranjih organizacijskih enot Javne agencije Republike Slovenije za varnost prometa, ki je pričela s svojim delom 1. septembra 2010.). Udeležba Slovenskega zavarovalnega združenja in posameznih zavarovalnic na lokalni ravni je pomembna zaradi zagotavljanja finančnih sredstev in nakupa takšnih naprav, ki lahko vplivajo na učinkovito preventivno delo. Tako je znano, da so zavarovalnice v preteklosti nabavljale določeno opremo za osnovne šole in njihove učence – predvsem prvošolčke (kolesa, opremo za kolesarske poligone, rumene rutice, kresničke, odsevne trakove, odsevne brezrokavnike ipd.), policijo (merilce hitrosti, naprave za ugotavljanje prisotnosti alkohola v izdihanem zraku, kolesa, drugo opremo za opravljanje preventivnega dela), svete za preventivo in vzgojo v cestnem prometu (nakup določene prezentacijske opreme, sofinanciranje publicistične dejavnosti, delno financiranje materialnih stroškov za izvedbo preventivnih usposabljanj ipd.) in druge.

Nekatere dileme in pogled v prihodnost

Kljub znatnim finančnim sredstvom, ki jih posamezne zavarovalnice in Slovensko zavarovalno združenje namenjajo preventivni dejavnosti (neposredni in



posredni), ocenjujemo, da bi bilo potrebno to vprašanje enotneje urediti na ravni posameznih delniških družb in na ravni združenja. Bilo bi potrebno jasneje ločiti namene in načine financiranja preventivnih dejavnosti od komercialnih, čeprav imata obe skupini dejavnosti navidezno isti cilj, pa vendarle vsebinsko zelo različen. Pri preventivni dejavnosti je cilj ozaveščanje širše množice zainteresiranih za to, da lažje prepoznajo vire ogrožanja, njihove negativne učinke in predvsem način obrambe. Če pa že konkretna nevarnost nastopi in s tem tudi škodljive posledice, pa je cilj usposobiti ljudi za preprečevanje nastanka še hujših posledic. Iz takšne akcije zavarovalnice ne morejo pričakovati neposredne koristi. Pri komercialnih akcijah zavarovalnice prav tako opozarjajo na nevarnosti, ki grozijo v okolju in s tem neposredno ozaveščajo svoje komintente oziroma pridobivajo nove (nagovarjanje zavarovancev in pridobivanje novih), s prikazovanjem koristi, ki so jih deležni tisti, ki sklenejo zavarovanja določene vrste. Logično je, da si zavarovalnice iz takšnih akcij obetajo neposredne koristi. Sredstva za izvajanje obeh skupin dejavnosti so lahko ista (denar) ali podobna (različni materialni proizvodi).

Menim, da bi razen teh že utečenih oblik in načinov izvajanja preventivne dejavnosti zavarovalnice morale skrbeti za svoj ugled še na nekoliko zahtevnejši način. Zavarovalnice bi morale razvijati nove in času in krajevnim razmeram aktualnejše oblike preventivnega dela, s poudarjeno vzgojno komponento in ustrezno materialno (finančno) stimulacijo. Kot izhodišče za širšo strokovno in sicersnjo mobilizacijo vseh znanstvenih in strokovnih resursov v naši družbi, bi lahko bila rastoča statistika kaznivih dejanj zoper premoženje (vlomi v stanovanja in druge zaprte prostore ter druge oblike ogrožanj) ter premoženjske interese. Zaradi rastočih stroškov odpravljanja posledic takšnih dejanj bi morali zavarovalnice, policija, varnostni inštituti in varnostne agencije, zasebna varnostna podjetja, proizvajalci varnostnih sistemov in naprav združiti svoje moči, znanje in napore za skupni nastop. Ni dovolj občasen parcialni nastop na razstavi Varnost – Security. Ljubljana kot glavno in največje mesto v naši državi, ki žal slovi tudi z več kot 49,6 % vse slovenske kriminalitete, potrebuje stalno brezplačno varnostno posvetovalnico. Zainteresiranim bi svetovali, kaj storiti za boljšo osebno varnost in varnost premoženja, pokazali in prikazali delovanje najnovejših proizvodov na področju varovanja in zaščite, delili bi brezplačna varnostna opozorila in navodila, propagandni material uveljavljenih in certificiranih proizvajalcev te opreme oziroma naprav in podobno. Večjo skrb kot doslej bi morali posvetiti varovanju okolja.

Zopet se postavlja vprašanje, kako doseči želeno sodelovanje in usklajeno delovanje, predvsem s skupnim nastopom vseh že omenjenih subjektov. Ker bi to lahko bil nacionalni program, bi morale vodilno vlogo prevzeti zbornice oziroma združenja. V tem projektu bi lahko policija odigrala ključno vlogo zaradi strokovnega potenciala, ki ga ima, in zaradi analitičnega spremljanja vseh oblik ogrožanj in napadov na objekte varova-

Zavarovalnice bi morale razvijati nove in času in krajevnim razmeram aktualnejše oblike preventivnega dela, s poudarjeno vzgojno komponento in ustrezno materialno (finančno) stimulacijo.



nja. Tak skupni nastop bi bil dobrodošel in koristen ne samo za tiste, ki jim je namenjen, temveč tudi za vse sodelujoče. To bi bil konkreten in merljiv prispevek k individualni, kolektivni in korporativni varnosti.

Sklep

V prispevku sem kritično obravnaval preventivno dejavnost v zavarovalništvu predvsem v okviru potrebe za oblikovanje poslovne politike in planskega pristopa v Sloveniji. Praksa slovenskega zavarovalništva kaže, da bi bilo potrebno zagotoviti tudi večjo udeležbo zavarovalnic na področju raziskovalne dejavnosti, analitičnega spremljanja in preučevanja vzrokov škodnih primerov ter spodbujanja raziskovalne in inovatorske sfere. Predvsem je utemeljeno pričakovanje, da bi zavarovalnice z večjim vložkom v preventivno dejavnost (raziskovanje, predstavitev raziskovalnih dosežkov in patentov, ozaveščanje prebivalstva vseh starostnih kategorij, uvajanje novih materialov in tehnologij, spremembe v ravnanjih itd.) zmanjšale možnosti nastankov škodnih primerov in s tem škodljivih posledic pri ljudeh in premoženju. To bi bilo možno doseči z dolgoročnim sodelovanjem z raziskovalnimi organizacijami, inštituti, posameznimi članicami univerz, projektantskimi in razvojnimi organizacijami ter drugimi.

Tako na področju neposredne, kakor tudi na področju posredne preventivne dejavnosti so mnoge priložnosti za izboljšave.

Prispevek lahko sklenem s spoznanjem, da je preventivna dejavnost nepogrešljivo potrebna sestavina delovanja zavarovalnic na Slovenskem, potrebno pa je v takšne projekte vključiti tudi znanstveno-raziskovalne zavode in inštitute. Poslovno sodelovanje Slovenskega zavarovalnega združenja in posameznih zavarovalnic z znanstveno-raziskovalnimi organizacijami in inštituti pa je zanesljivo vzvod za dvig ugleda v okolju, česar slovensko zavarovalstvo ne bi smelo prezreti.

Viri:

- Boncelj. J. (1983). Zavarovalna ekonomika. Maribor, Založba Obzorja Maribor.
- Brask. G. (1991. Eine reinprivatkapitalistische Tätigkeit oder ein wichtiger Teil des sizialen Netzes, v: Vesicherungen in Europa, heute und morgen, Karlsruhe.
- Ivanjko. Š. (1999). Uvod v zavarovalno pravo. Maribor. Pravna fakulteta, Univerza v Mariboru.

Predpisi:

- Zakon o varstvu pred požarom, Uradni list RS., št. 71/93, 22/01, 87/01, 110/02.
- Zakon o zavarovalništvu, Uradni list RS, št. 13/2000.
- Uredba o požarni taksi, Uradni list RS., št. 22/94, 11/97. ■

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.

Avtor: Andrej Kovačič / Institut za korporativne varnostne študije*



NACIONALNA RAZISKAVA Z NASLOVOM »VLOGA MESTNIH IN OBČINSKIH UPRAV PRI ZAGOTAVLJANJU LOKALNE VARNOSTI IN PREPREČEVANJU KRIMINALITETE«

Ustrezno varnostno okolje na lokalni ravni je nujno za nemoteno delovanje organizacij in ima na njihovo učinkovitost pomemben vpliv. S tega stališča je Institut za korporativne varnostne študije decembra 2012 začel z nacionalno raziskavo, ki bi lahko predstavljala izhodišče za razmislek o novih pristopih na področju varnosti v mestnih in občinskih upravah.

Varnost je skupna dobrina, ki je zelo povezana z družbenim vključevanjem oziroma socialno integracijo. Kriminal, kot družbeni pojav, v vseh svojih oblikah grozi nad življenjskim ravnovesjem ljudi in poslovnih organizacij. Pri zagotavljanju varnosti v lokalnem okolju imajo pomembno vlogo mestne in občinske uprave, ki s svojimi strokovnimi službami, lahko bistveno pripomorejo k višji stopnji varnosti. Pomembno vlogo imajo predvsem pri osveščanju, izobraževanju in povezovanju občanov, da se aktivno pridružijo in da sodelujejo pri preprečevanju kriminalitete na lokalnem nivoju. Prisluhniti občanom in njihovim potrebam, daje osnovno izhodišče za skupno sodelovanje tudi na področju varnosti, ki je ena osnovnih potreb v bivalnih okoljih. Ustrezno varnostno okolje na lokalni ravni je tudi nujno potrebno za nemoteno delovanje organizacij in ima na njihovo poslovanje pomemben vpliv. Ker je varno okolje predpogoj za kvalitetno bivanje in nemoteno delovanje organizacij, smo se v Inštitutu za korporativne varnostne študije, decembra 2012 odločili za raziskavo. Rezultati raziskave bi lahko predstavljali izhodišče za razmislek o novih pristopih na področju varnosti v mestnih in občinskih upravah. Občane je potrebno spodbujati pri preprečevanju kriminalitete, pritegniti k sodelovanju in izobraževanju o samozaščiti, osebni varnosti in varnosti njihovega premoženja, o samoorganiziranju in svetovanju pri tem, o varnostni kulturi in njeni vlogi v vsakdanjem življenju, varnem sobivanju ter povezovanju. Namen raziskave je bil ugotoviti, kaj dejansko naredijo mestne in občinske uprave za višjo stopnjo varnosti svojih občanov.

Vprašalnik je bil poslan na naslove 43 občin, ki so bile izbrane glede na število prebivalcev in na število zaposlenih v mestnih oziroma občinskih upravah. Razumljivo je, da si manjše občine z manjšim številom zaposlenih težje privoščijo, da bi zaposlile strokovnjaka, ki bi se celovito ukvarjal s področjem varnosti.

Pozitivno se je odzvalo 56 % občinskih uprav, kar pomeni, da je bilo vrnjenih 24 vprašalnikov.

Ugotovljeno je bilo, da 62 % občinskih uprav, ki so odgovorile na vprašalnik nima strokovnjaka za varnost, ki bi se na lokalnem nivoju celovito ukvarjal z varnostno problematiko, kot je to že v nekaterih podjetjih, kjer gre za korporativnega varnostnega managerja. Pri odgovorih smo naredili izjemo in upoštevali nazive oseb, ki se ukvarjajo z lokalno varnostno problematiko in sicer, podžupan, strokovni sodelavec - višji svetova-

*avtor je član Slovenskega združenja korporativne varnosti

lec, predstojnik Medobčinskega inšpektorata in redarstva, vodja mestnega redarstva in vodja referata za promet.

Po mnenju občinskih uprav je v 100 % prav, da se z lokalno varnostno problematiko občanov in s področjem preprečevanja lokalne kriminalitete še vedno in v prvi vrsti ukvarja policija, na drugem mestu in zraven policije še mestno redarstvo v 82 % in v nekaj manjših primerih zraven prvih dveh še strokovnjaki za varnost v 33 %, zasebne varnostne službe 25 % ter drugo v 5 %, kot so nevladne organizacije in varnostni sosveti.

Ugotovitve kažejo, da je pri možnih več odgovorih za spodbujanje občanov k čim večjem sodelovanju pri preprečevanju kriminalitete v prvi vrsti naloga policije in sicer 96 %, sledi mestno redarstvo v 50 %, potem občanov samih oziroma društev ali združenj v 46 %, sledijo strokovnjaki za varnost v občinskih upravah ter drugo, kot so občinske uprave preko medijev, županov, varnostnih sosvetov, svetov za preventivo in vzgojo v cestnem prometu, zasebnih varnostnih služb v 40 %.

Ugotovljeno je bilo, da so v 75 % občin organizirani varnostni sosveti in, da se jih večina sestaja po potrebi medtem, ko so tudi primeri, kjer se sestajajo 5-krat oziroma 8-krat na leto. V teh pozitivnih pristopih daleč izstopa občina Slovenska Bistrica, ki bi gledano na celotno raziskavo, lahko bila za zgled ostalim, tudi mestnim občinam. Po aktivnostih varnostnih sosvetov ji sledita Mestni občini Slovenj Gradec in Ptuj.

V 63 % uprav so mnenja, da varnostni sosveti pripomorejo k boljši varnosti v lokalni skupnosti, zato jih imajo tudi organizirane. Mladi so v varnostnih sosvetih preko predstavnikov osnovnih in srednjih šol oziroma drugih, zastopani v 61 % občin, ki imajo varnostne sosvete.

Večina občinskih uprav osvešča občane o pomenu varnosti in samozaščitnem ravnanju z lokalnimi oziroma občinskimi glasili, sledi lokalni radio ter z organiziranjem strokovnih posvetov za občane. Samo v dveh primerih imata občini odprto varnostno pisarno oziroma posvetovalnico za občane.

Ugotovitve kažejo, da v večini primerov ni podatka oziroma, da ne deluje društvo, organizacija ali skupina, ki bi se prostovoljno in celovito ukvarjala s preprečevanjem kriminalitete v občini. V redkih primerih obstajajo aktivnosti, kot so lokalna akcijska skupina; Društvo, ki se ukvarja s področjem razvrednotenja naravnega in življenjskega okolja; Društvo za nenasilno komunikacijo ter Društvo za preprečevanje prestopništva.

Podatki kažejo, da občinske uprave v glavnem občanov ne spodbujajo v smeri, da bi prišlo do organiziranja društva ali združenja, ki bi se prostovoljno ukvarjalo s preprečevanjem kriminalitete, kot je to praksa v nekaterih tujih državah. V nekaj primerih bi pa uprave nudile pomoč, če bi prišlo do takšnega organiziranja.

Občinske uprave z namenom preprečevanja kriminalitete oziroma zmanjšanje kriminala policiji in mestnemu redarstvu večkrat predlagajo varnostne rešitve. V glavnem pa menijo, da je to naloga policije in mestnega redarstva.

Rezultati kažejo, da ima polovica občin, ki so v raziskavi sodelovale, uvedene občasne mešane patrulje občinskih redarjev in policistov, pri varnostni problematiki sodelujejo z zasebnimi varnostnimi službami, izvajajo skupne akcije za nadzor nad psi na javnih površinah z občinskim redarstvom, veterinarsko inšpekcijo, veterinarji in policijo, uvedba videonadzora, fizični nadzori občinskega redarstva. Poteka tudi sodelova-



nje upravljavcev posameznih javnih objektov v občinski lasti (športne dvorane, športni parki) z občinskim redarstvom. Pri drugi polovici občin pa v glavnem ni bilo navedenega podatka.

Ugotovljeno je bilo, da uprave na področju varnostne problematike v glavnem sodelujejo z ostalimi slovenskimi občinami.

Podatki kažejo, da uprave za svoje občane redko organizirajo strokovne posvete na teme, kako skrbeti za lastno varnost, varnost svojega premoženja, samozaščitna ravnanja itd.

Ugotovitve kažejo, da je v letu 2012 za reševanje varnostne problematike v občini, za delovanje mestnega redarstva in varnostnih sosvetov, za osveščanje občanov o samozaščitnem ravnanju, za delovanje varnostne pisarne itd, največ občin namenilo od 1 do 2 % letnega občinskega proračuna. So tudi primeri, ko je ta odstotek manjši od 1 % medtem, ko se v dveh primerih ta odstotek giblje med 3 in 4 % in sicer pri Mestni občini Koper in Ptuj.

Na podlagi raziskave je mogoče ugotoviti, da občinske uprave v večini primerov še vedno glavno in edino skrb za varnost občanov prepuščajo policiji in mestnem redarstvu. Pri tem se pogreša predvsem njihova aktivna vloga pri osveščanju, izobraževanju in angažiranju občanov za boljšo varnost. Občinske uprave nimajo strokovnjakov za varnost, ki bi se na civilnem[1] nivoju in celovito ukvarjali z lokalno varnostno problematiko, na terenu med ljudmi, v soseskah itd. Za vzdrževanje reda, zagotavljanja splošne varnosti in preprečevanja kriminalitete potrebujemo represivne organe, vendar v povezovalnem pogledu njihova vloga težje krepi neposredno participacijo ljudi, ki živijo v soseskah. Menimo, da je čas za pristope, ki temeljijo na motivaciji in vključevanju ljudi v neposredno soodločanje o preprečevanju varnostnih problemov, ki lahko

Na podlagi raziskave je mogoče ugotoviti, da občinske uprave v večini primerov še vedno glavno in edino skrb za varnost občanov prepuščajo policiji in mestnem redarstvu.

prinesejo ustrezne rezultate v smeri dvigovanja varnosti in bolj varnega življenjskega okolja. Občinske uprave imajo možnost, da s svojimi strokovnjaki za varnost, ki bi imeli strokovne, svetovalne in povezovalne naloge stopijo v soseske ter z organiziranjem strokovnih posvetov privabijo čim večje število občanov k sodelovanju za skupno varnost. Na ta način bi se dvignila lokalna varnostna kultura, okrepil socialni kapital in s tem medsebojno zaupanje, kar bi posledično pozitivno vplivalo na bolj varno življenjsko okolje. Prav gotovo pa ne smemo pozabiti na povezovanje občinskih uprav s pristojnimi institucijami s poudarkom na vključevanju lokalnih prebivalcev in promocijo njihovega angažiranja preko združenj. V tem okviru imajo svojo vlogo in odgovornost tudi poslovne organizacije, ki ravno skozi pristope javno-zasebnega partnerstva in družbene odgovornosti igrajo pomembno vlogo pri podpori občanov v višjem zavedanju pomena varnosti. Pri tem gre za varnost kot stanje, ki se dolgoročno vrača podjetju v zmanjšanju groženj in tveganj za njegovo poslovanje in premoženje v lokalni skupnosti.

[1] Strokovnjaki za varnost v mestnih in občinskih upravah, ki ne bi imeli represivnih nalog, temveč preventivne, izobraževalne in posvetovalne naloge za občane. ■



Avtor: Dr. Andreja Lavrič, uni. dipl. pred. in prof. soc.



PSIHOLOŠKA PRIPRAVA NA IZREDNE DOGODKE KOT DEL KORPORATIVNE VARNOSTI

Upravljanje korporativne varnosti vodi k zmanjševanju ranljivosti in ogroženosti premoženja in ljudi. Z učinkovitim upravljanjem se v organizacijah bolje pripravimo na izredne dogodke. V razsežnostih integralne varnosti je ključno tudi vodenje v kriznih razmerah in pripravljenost ljudi na ravnanje med in po kriznem dogodku.

Za organizacije so krize lahko zelo različne od npr. naravnih, delovnih in drugih nesreč, do odtujitve npr. intelektualne ali fizične lastnine.
Krizni dogodek ima lahko vpliv na posameznika, skupino ali celotno organizacijo. Takšen dogodek je nenaden, redek in vznemirjajoč oziroma stresen za večino ljudi. Vključuje grožnjo ali doživetje izgube osebe, stvari ali vrednosti pomembnih za posameznika ali skupino. Ljudje imajo občutek, da ne morejo sami obvladati krize s svojimi običajnimi mehanizmi soočanja. Izgubljen je nadzor nad situacijo pri čemer zahteve odziva praviloma presegajo razpoložljive vire (Arambašić, 2000).

Naše odločanje v krizi je različno, saj so reakcije posameznikov usmerjene na čustva oziroma doživljaje ali na problem. Usmerjenost na čustva in doživljanje vodi predvsem k pasivnemu soočanju, usmerjenost na problem pa bolj k aktivnemu. Aktiven način prinaša boljše rezultate, saj povečuje občutek nadzora nad situacijo in pripomore k hitrejšemu zbiranju misli za možnost izhoda iz krize.

Kako se oseba odzove na krizni oziroma travmatski dogodek kot je npr. delovna nesreča ali rop poslovalnice je odvisno od več dejavnikov med katerimi imajo poseben vpliv osebnosti posameznika, dimenzij travme in socialnega okolja (Mikuš Kos in Slodnjak, 2000). Odziv na kritični dogodek je pri posamezniku odvisen od njegovih osebnih lastnosti, spola, odpornosti, preteklih izkušenj, kognitivnih stališč in drugega. Na odziv vpliva tudi vrsta, trajanja in bližina dogodka. Ključnega pomena pa so tudi značilnosti socialnega okolja: opora pri sodelavcih, prijateljih, družini in strokovnjakih, družbeno sprejemljivih načinih odzivanja, ritualih žalovanja in izražanja čustev ter stališč družbe do takšnega kritičnega dogodka.

Vrsta kriznega dogodka vpliva na to kakšni simptomi se posamezniku pojavijo po njem. Drugače dojemamo dogodek, če je npr. posledica naravne nesreče ali nasilnega kriminala. Zaposleni v podjetju bodo manj travmatično dojemali, če je zaradi neurja poslopju odneslo streho ali je bila poplavljena tovarniška hala, kot pa, če je ropar napadel bančnega uslužbenca ali kupec v poslovalnici posilil prodajalko. Naravne nesreče dojemamo namreč drugače kot tiste, ki jih povzroči človek (Lahad in Doron, 2010). Do naravnih nesreč smo bolj tolerantni in jih jemljemo kot »dejanje Boga« ali narave. Ne vidimo jih, kot da nas je nekdo želel poškodovati in nam povzročiti bolečino.

Nasprotno pa je pri nesrečah, ki jih povzroči človek. Kriminalno nasilje, teroristični napad ali posilstvo jemljemo kot da nam je želel napadalec nanesti bolečino, trpljenje in se počutimo izdane. Zaradi tega so njihovi simptomi kot je npr. depresija, uporaba opojnih substanc, nočne more mnogo pogostejše (Lahad in Doron, 2010). Raziskovalci psihičnih motenj ugota-

Za organizacijo je pomembno, da ima čim več zaposlenih s tovrstnimi znanji, saj ji to omogoča ustrezno soočanje na čustveni in kognitivni ravni s kritičnimi dogodki.
K še dodatnemu osebnostnemu napredku pa organizacija lahko spodbudi svoje zaposlene z dodatnimi usposabljanji.



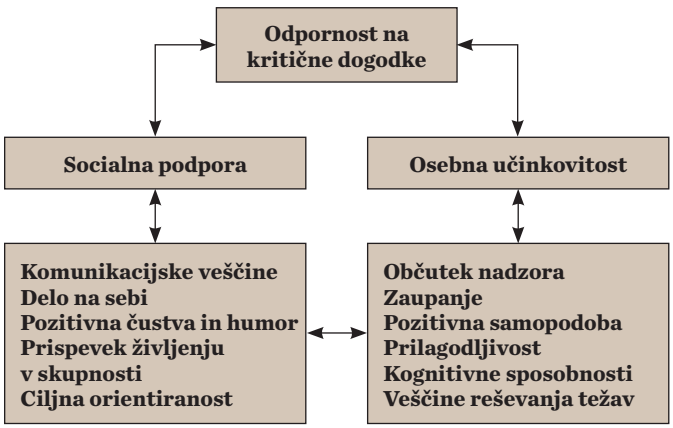
vljajo, da le 3.5 – 4 odstotkov žrtev orkana razvije potravmatično motnjo, medtem ko 60 odstotkov posiljenih trpi za to motnjo (prav tam).

Travmatični dogodek, kot je rop banke ali posilstvo trgovke je za podjetje še toliko hujši, saj travmatično poleg direktne žrtve vpliva tudi na druge prisotne npr. sodelavce ali stranke. Vpliva tudi na tiste, katerim je žrtev blizu: sorodniki, prijatelji ali sodelavci.

Četudi krizni dogodek v podjetju vpliva na več zaposlenih, ne bodo vsi čutili posledic enako. Med njimi jih bo imelo posledice kakih 9 odstotkov in čutili bodo posledice travmatskega dogodka morda celo več mesecev (Erzar, 2007). Dobra čustvena odpornost delavcev pripomore k blažjim posledicam.

Raziskovalci (Schaap in drugi, 2007) ugotavljajo, da na našo čustveno odpornost po kriznem dogodku vplivajo: dobri odnosi z drugimi ljudmi in zmožnost sprejemanja pomoči s strani drugih; dobre kognitivne in komunikacijske veščine; pozitivna samopodoba, učinkovitost in upanje; ciljna orientiranost oz. videti smisel; vera ali občutek, da nekomu pripadamo; prispevek življenju v skupnosti; delo na sebi; pozitivna čustva in humor; občutek nadzora; zaupanje; prilagodljivost oz. zmožnost prilagajanja spremembam; aktivno reševanje težav; veščine reševanja težav primerno situaciji in osebam; prepričanje, da lahko stres krepi človeka (npr. slovenski pregovor: Kar nas ne ubije, nas okrepi.); videti stresno situacijo kot priložnost; sprejemanje negativnih čustev oz. prepričanje, da rastemo s pomočjo negativnih izkušenj; dostop in uporaba preventivnih procesov.

Navedeni faktorji so med seboj interaktivni, kot na primer dobre komunikacijske veščine vodijo k večji socialni mreži. Naštete faktorje lahko strnemo v dve kategoriji: socialno podporo in osebno učinkovitost.



Slika: *Faktorji odpornosti na kritične dogodke (Schaap in drugi, 2007)*

Z vidika korporativne varnosti se lahko na krizni dogodek organizacija pripravi, kakor tudi posamezniki, ki delajo v njej. Posameznik lahko pristopi k učenju novih veščin, ki vodijo k aktivnemu reševanju krize ali sprejemanju situacije takšne kot je, pozitivnemu mišljenju ob krizi, izražanju čustev in upravljanju jeze ob kritičnem dogodku. Ob kriznem dogodku je priporočljivo poleg učinkovitega upravljanja čustev, tudi učinkovito nadziranje oziroma zaustavljanja negativnih mislih, kot je npr. misel, ta dogodek bo pokopal moje podjetje, kar nam omogoča poznavanje kognitivnih tehnik.

Za organizacijo je pomembno, da ima čim več zaposlenih s tovrstnimi znanji, saj ji to omogoča ustrezno soočanje na čustveni in kognitivni ravni s kritičnimi dogodki. K še dodatnemu osebnostnemu napredku pa organizacija lahko spodbudi svoje zaposlene z dodatnimi usposabljanji.

Pri obvladovanju stresa ob kriznih dogodkih ima pomembno vlogo podpora socialnega okolja, predvsem najbližjih ljudi v okviru družine in prijateljev. Poznamo različne oblike socialne opore, in sicer oporo v obliki koristnih informacij, otipljivo oporo v obliki konkretnih aktivnosti drugih, čustveno oporo, oporo v smislu potrditev posameznikovih prepričanj in občutkov ter socialno vključenost. Raziskave torej potrjujejo pomen medosebnih stikov za posameznikovo občutenje sprejetosti, ljubljenosti, potrjenosti in njihovo zaščitno vlogo med boleznijo in njenimi posledicami (Svetina, 2007). Tako je pomembno, da se zaposleni in njihova organizacija tega zavedajo in že pred krizo aktivno delujejo na svoji socialni mreži. Po kritičnem dogodku se lahko uspešno oprejo nanjo, če jo imajo predhodno že izgrajeno. Organizacije to lahko spodbujajo z različnimi ukrepi kot je npr. projekt družini prijazno podjetje.

Poleg socialne opore je pomembno tudi preventivno delovanje v obliki sproščanja. To omogoča učinkovito zmanjšanje delovanja simpatičnega živčnega sistema, organizem poživi in poveča sposobnost zbranosti ter spodbuja spomin in ustvarjalnost (Svetina, 2007). Za sproščanja uporabljmo različne tehnike kot so dihalne tehnike, različne oblike samosugestije, metoda mišične progresivne relaksacije, meditacije ter avtogeni trening in druge. Tehnik se posamezniki naučijo in jih pri tem lahko spodbujajo tudi organizacije, ki dajejo temu poudarek tudi z izvedbo usposabljanj za izvajanje tehnik že pred kriznim dogodkom.

Pomembno je tudi, da se oseba po kriznem dogodku sprošča tudi z drugimi aktivnosmi, kot so hobiji in šport. Vrtnarjenje, skrb za domačo žival, izdelovanje maket idr. so aktivnosti s katerimi se razbremenimo po kriznem dogodku, kakor tudi šport npr. lahen tek, sprehodi ali partija tenisa s prijateljem. Po kriznih dogodkih moramo znati poskrbeti za sprostitev, česar se moramo naučiti že pred krizo. Za sprotitev moramo znanti poskrbeti tudi sicer v vsakdanjem življenju, saj se le tako uspešno kosamo s stresom.

S predhodnimi fizičnimi vajami tudi krepimo fizično pripravljenost za delovanje med kriznim dogodkom ali po njem (npr. pri sanaciji proizvodne hale po poplavi ali ubranitvi pri fizičnem napadu v poslovalnici). Spodbujanje delodajalca zaposlenih k športu z različnimi prireditvami, udeležbo na tekmovanjih, športnih dnevih v podjetju je vsekakor tudi v njihovem interesu.

Zaposleni reagiranjo na krizni dogodek uspešneje, v kolikor imajo vnaprej izvedene priprave nanj. Organizacija se na to pripravi z različnimi možnimi scenariji, ki so kot krizni dogodki najboj verjetni, in se z usposabljanji in vajami nanje pripravijo. Več ko je usposabljanj in vaj oz. simuliranih situacij za ravnanje ob kriznem dogodku, bolj so zaposleni usposobljeni ali celo izurjeni, kako ravnati v primeru nesreče, npr. pri požaru kako izvesti evakuacijo in druge ukrepe ali kako pri ropu banke ravnati samoobrambno in po operativnih postopkih, ki so predpisani za takšne primere.

K obvladovanju stresa in poznavanju zaščitnega vedenja veliko pripomorejo torej tudi usposabljanja, ki sodijo v stvarno odločanje ob kritičnem dogodku. Pri usposabljanju vodij npr. to pomeni, da ne gre več za spoznavanje nekih teoretičnih izhodišč o kriznem vodenju, temveč oblikovanje in reševanje problemov pri dejanskem izvajanju.

Ob navedenih in še drugih preventivnih ukrepih korporativne varnosti so zaposleni in vodstva organizacij opremljena z znanji in veščinami ter spodbujena k osebnostnim spremembam, ki vodijo k uspešni rešitvi krize. Tudi psihološka priprava na izredne dogodke je pomemben del korporativne varnosti.

Viri:

- Arambašić, L. (urednica), 2000. Psihološke krizne intervencije: psihološka prva pomoć nakon kriznih događaja. Društvo za psihološku pomoć, Zagreb.
- Erzar, T., 2007. Duševne motnje. Celjska Mohorjeva družba, Celje.
- Lahad, M. in Doro M., 2010. Protocol for Treatment of Post Traumatic Stress Disorder, IOS Press, Amsterdam.
- Mikuš Kos, A., in Slodnjak, V., 2000. Nesreče, travmatski dogodki in šola. DZS, Ljubljana.
- Selič, P., 1999. Psihologija bolezni našega časa. Znanstveno in publicistično središče, Ljubljana.
- Schaap, I. A. in drugi. 2007. Resilience. Impact, Amsterdam.
- Svetina, M., 2007. Zaključno poročilo o rezultatih opravljenega raziskovalnega dela na projektu v okviru ciljnega raziskovalnega programa (CRP) Znanje za varnost in mir 2006–2010, Filozofska fakulteta Univerze v Ljubljani, Ljubljana. ■



Slovenian Grand Security Award 2013



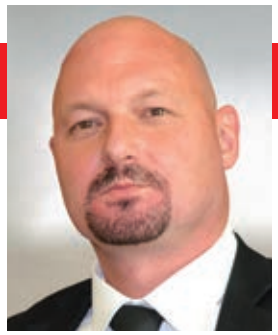
Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikov za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne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



SMO (ŽE) POSTALI DRUŽBA NADZORA? II.

Glavni problem sodobnega nadzora s pomočjo tehničnih sredstev je, da je le-ta vseprisoten, neopazen, avtomatiziran in brezoseben. Nikoli ne počiva in nikoli ne spi.

Družba nadzora je družba v kateri se zbirajo informacije o posamezniku, o njegovem gibanju in aktivnostih s strani vladnih in nevladnih organizacij. Za zbiranje in nadaljnjo obdelavo informacij se v modernih družbah uporablja informacijska tehnologija. Tako pridobljene in obdelane informacije so podlaga za sprejemanje odločitev, ki vplivajo na način življenja posameznikov in njihovih dobrobiti: od dodatnih ugodnosti pri uporabi raznih storitev, do dodatnih možnosti pri iskanju zaposlitve. Po drugi strani pa nadzor ustvarja atmosfero sumničavosti. Delodajalci, ki v službena vozila nameščajo GPS in druge sledilne naprave, na računalnike zaposlenih pa programe, ki beležijo vnose s tipkovnice in aplikacije za zajem zaslonskih slik, slednjim sporočajo, da jim ne zaupajo. Enako sporočilo oddajajo starši, ki na domači računalnik namestijo orodje za spremljanje aktivnosti, ki jih njihov mladi nadobudnež izvaja na socialnem omrežju. Glede na pomembnost vloge, ki jo ima v današnji družbi informacijska tehnologija, si bomo v nadaljevanju ogledali enega izmed pojavov, ki ga je le-ta povzročila in napredek, ki nam ga v tem desetletju na nekaterih področjih IT obeta znanost.

Socialna omrežja

Ljudje se združujemo iz različnih razlogov, tako danes kot skozi zgodovino. Dejstvo je, da obstajajo najdbe iz prazgodovine, ki kažejo, da je človek živel v skupinah. Obstaja več definicij skupine. V organizacijskem smislu skupino sestavljata dva ali več posameznikov, ki medsebojno delujejo interaktivno na tak način, da je obnašanje in/ali opravljanje nalog enega člana pod vplivom obnašanja in/ali opravljanja nalog drugih članov. Skupina ima vedno skupni cilj, neko skupno idejo, s katero želi nekaj doseči.

Dve pomembnejši karakteristiki, po katerih se skupine med seboj razlikujejo sta strukturiranost in velikost skupine. Za nestrukturirane skupine je značilno, da njihovo delovanje ni organizirano. Take skupine obstajajo kratek čas. V njih ni strukture, ni razdelitve vlog in položajev. Nestrukturirane skupine nastajajo na osnovi prostorske bližine članov in podobnih (a ne skupnih) ciljev. V strukturiranih skupinah pa obstaja poleg individualnih tudi skupni cilj, ki se uresničuje ob usklajeni in povezani aktivnosti vseh članov skupine. Za strukturirano skupino je značilna neposredna interakcija in komunikacija med člani, skupni cilji, medsebojna odvisnost in vpliv, skupna aktivnost, pripadnost skupini, norme, statusi (položaj in vloga), ki regulirajo vedenje v skupini, stabilni odnosi itd. Posameznik v skupini zadovoljuje svoje interese in potrebe (varnost, sprejetost, pripadnost, uveljavljanje, sodelovanje ipd.). Preko socialne interakcije pa skupina vpliva na stališča, aktivnost in vedenje članov.

On-line skupnosti

Poleg klasičnih socialnih skupnosti, poznamo tudi skupine ljudi, katerih interakcija v osnovi poteka preko komunikacijskih medijev kot so pisma, telefon, elektronska pošta. Takim skupnostim pravimo *virtualne*, *spletne* oziroma *e-skupnosti*. Z razvojem interneta iz sistema za izmenjavo datotek in iskanja informacij v svet storitev na področju zabave, trgovanja in komunikacije pa se pojavijo t.i. *on-line skupnosti*. Za njih je značilno, da interakcija med člani skupnosti poteka s pomočjo interneta in njegovih storitev. Z razvojem svetovnega spleta (*World Wide Web*) v *web 2.0*, ki ga mnogi označujejo kot družbeni medij (*social media*) s storitvami za razširjanje znanja, združevanje in komunikacijo posameznikov ter socialnih omrežij, postane internet medij za povezovanje posameznikov, kot ga v zgodovini še ni bilo.

Seveda pa poleg množice dobrih stvari, ki jih omogoča internet, v njegovem svetu obstajajo tudi manj prijetne in celo nevarne stvari: otroška pornografija, sovražni govor in teroristična propaganda so le nekatere izmed njih, ki vplivajo na odnose in dinamiko on-line skupnosti. Kakšen je pojav internetnih protestov

Seveda pa poleg množice dobrih stvari, ki jih omogoča internet, v njegovem svetu obstajajo tudi manj prijetne in celo nevarne stvari: otroška pornografija, sovražni govor in teroristična propaganda so le nekatere izmed njih, ki vplivajo na odnose in dinamiko on-line skupnosti.

*avtor je član Slovenskega združenja korporativne varnosti



(*Cyberprotests*), pozitiven ali negativen, pa je odvisno od pogledov posameznih socialnih skupnosti. Hkrati se moramo zavedati, da na spletu z vsakim korakom puščamo (elektronske) sledi. Na spletu obstajajo različni programi, ki pregledujejo spletne strani in komunikacijske poti, lovijo informacije o tem s kom, kdaj, kje pa tudi kaj smo komunicirali, posebni programi imenovani *e-mail extractorji* omogočajo pridobivanje e-naslovov iz poljubnih virov in so le ena vrsta *spletnih žanjcev*, programov-pajkov, ki pregledujejo in zbirajo informacije s spletnih strani, forumov, socialnih omrežij ipd. Pri tem je z vidika zasebnosti popolnoma vseeno ali so tovrstna orodja in njihova uporaba v rokah posameznikov, zasebnih ali pa vladnih organizacij. Popolnoma naša odločitev je, kaj in komu bomo zaupali v našem virtualnem življenju na spletu. Za svojo varnost (in zasebnost) smo, kot vemo, na prvem mestu odgovorni sami!

Informacijska družba

Najbrž se kar strinjamo, da se je večina izmed nas oddahnila, ko je zaključila (uspešno ali pa ne) določeno stopnjo formalnega izobraževanja. S tem je namreč tudi zaključila z določenimi nepriljubljenimi predmeti. Recimo z matematiko. Je že tako, da je ta veda normalnemu človeškemu bitju pravzaprav nerazumljiva; pri tem ne mislim na matematiko učenja poštevanke in izračuna mesečne porabe s kreditno kartico ali pa na risanje tlorisa novega stanovanja. Matematika je veliko bolj abstraktna in nedoumljiva in za nekatere kraljica znanosti (fiziki, oprostite mi izrečeno kleveto). Pa matematika ni edina 'težka' veda, saj med drugim obstaja njena podmnožica, ki se ji je včasih reklo računalništvo. No, iz nje izhaja informacijska znanost, ali po domače informatika in njej pripadajoča informacijska tehnologija in tehnika. In prav zaradi informatike in njenega vpliva na družbo in odnose v njej, danes govorimo o *informacijski družbi*.

Ena največjih revolucij v svetu iznajdb človeške vrste je področje digitalnega procesiranja informacij in s tem računalništva. Slovar slovenskega knjižnega jezika računalnike definira kot 'elektronske naprave za reševanje nalog na osnovi vloženega programa'. S povezovanjem računalnikov v računalniška omrežja pa le-ti postanejo več kot samo naprave za izvajanje računskih operacij; pripomorejo namreč k razvoju informacijske družbe, katere člani s(m)o vse bolj odvisni od računalniških programov in zmogljivosti računalnikov. Od njih, ali bolje rečeno, od internetnih tehnologij, postajamo vse bolj odvisni tudi v zasebnem življenju. Kakšna prihodnost se nam v tem desetletju obeta na področju internetnih storitev, računalništva in telekomunikacij?

Internet

Kot vemo, je bil internet prvotno načrtovan kot računalniško omrežje, namenjeno poveljevanju v primeru vojne, splet je nastal zaradi potrebe jedrskih fizikov po izmenjavi dokumentov v internetnem računalniškem omrežju, socialno omrežje (npr. *Facebook*) pa zaradi potreb študentov po izmenjavi osebnih informacij in komunikaciji znotraj univerzitetnega omrežja. Danes sta internet in vsa internetna tehnologija prevladujoče komunikacijsko, poslovno in vsebinsko orodje, ki ga uporablja tretjina prebivalstva našega planeta (po zadnjih statističnih podatkih ima internet 2,5 milijarde uporabnikov). Pričakovati je, da se bo internet razvijal in širil po vsej zemeljski obli in opravljal nalogo množičnega medija za prenos znanja, informacij in multimedijskih vsebin. Poleg tega bo upravljal tudi druga svetovna omrežja (t.i. *kritično infrastrukturo*): prometna, energetska, vodovodna, naftovodna in plinovodna. Zagotavljal bo veliko storitev, ki počasi romajo v naše domove, ustanove in prostor, ki nas obkroža. Internet bo postal resnično mobilen, dostopen od vsepovsod, izbira uporabniških naprav pa pestra. Internetno omrežje bo povezovalo ne le uporabnike, ampak tudi druge naprave in orodja (*internet of things*). Z internetno infrastrukturo povezana senzorska omrežja bodo zagotavljala inteligentne storitve in skrbela za dobro počutje in potrebe uporabnikov, zlasti bolnih in starejših. Omogočale bodo življenje in delo v tako imenovanih pametnih mestih z optimiziranimi komunalnimi storitvami. No, osebno mnenje pisca je, da bomo pred dosego zapisanega morali predhodno ustrezno modificirati socialno in zdravstveno politiko.

Poseben izziv pa predstavljata internetna varnost in varnost uporabnikov novih internetnih storitev. Kibernetska kriminaliteta postaja ključen in dolgotrajen izziv raziskovalcev pri preprečevanju groženj in varnostnih incidentov v internetu, ki v svetu eksponentno naraščajo. Nastaja nova veda: znanost o kibernetski kriminaliteti, ki ima za podlago znanost o kriminaliteti in informacijsko tehnologijo. Raziskovalni izzivi v novi vedi so izjemni in zahtevni. Zahtevajo namreč rešitve, ki so hkrati zakonite, operativne in tehnično sprejemljive. Te rešitve obsegajo upravljanje in zaščito identitete, hkrati pa tudi transparentnost podatkov in ustrezno zaščito zasebnosti.

Kibernetska kriminaliteta postaja ključen in dolgotrajen izziv raziskovalcev pri preprečevanju groženj in varnostnih incidentov v internetu, ki v svetu eksponentno naraščajo.



Računalništvo in umetna inteligenca

Po napovedih enega izmed slovenskih računalniških strokovnjakov, se bo računalništvo še najmanj deset let razvijalo po Moorovem zakonu, torej eksponentno. Pri tem se lahko vprašamo, kaj bo, ko bomo trčili ob fizikalne omejitve, ki vsekakor obstajajo. Nas bodo pri tem (začasno) res rešila dognanja kvantne fizike? Določene napovedi se že uresničujejo: vse manj se bodo pojavljali stacionarni in prenosni računalniki, vse več bo računalnikov v obliki tablic, mobilnih telefonov, zapestnih ur, oblek itd. Z računalniki bomo lahko komunicirali kot z ljudmi, v naravnih jezikih. Pojavili se bodo prvi uporabni prototipi kvantnih računalnikov, nadaljevale se bodo raziskave naravnega računanja (bioračunanje), realnost pa bodo postale tudi sanje o robotih, ki delajo za nas ne le v industriji, temveč tudi doma, v zasebnem življenju. Večje naprave, kot so avtomobili, bodo vsebovale na desetine in stotine procesorjev, tako da bodo podobno kot računalniki sposobne samostojnega vzdrževanja in avtonomnega delovanja (drugo je vprašanje, kako močno si tega želijo proizvajalci – op.p.).

Strokovnjaki tudi napovedujejo, da bodo ljudje v tem desetletju z umetnimi očmi in ušesi čedalje bolje videli in slišali. Vse več delov telesa bo mogoče nadomestiti z umetnimi, elektronsko upravljanimi. Umetno nogo bomo npr. krmilili prek živcev ali s pomočjo misli. Na voljo bodo tudi možganski vmesniki za komunikacijo z vsajenim oziroma nošenim pomnilniškim diskom in seveda internetom. Spremenil se bo tudi način vodenja držav in podjetij. Ko bo v prihodnosti nekdo predlagal nov ukrep, tehnični, ekonomski, socialni ali politični, bo običajna praksa, da bodo razni strokovnjaki z inteligentnimi orodji simulirali in analizirali pozitivne in negativne učinke. Že samo s tem bo človeška družba prestopila na višjo civilizacijsko raven.

Zaključek

Glavni problem sodobnega nadzora s pomočjo tehničnih sredstev je, da je leta vseprisoten, neopazen, avtomatiziran in brezoseben. Nikoli ne počiva in nikoli ne spi. Je neviden in anonimen. Pojavlja se povsod v vsakdanjem življenju, pri nakupovanju in sprehajanju, obisku kulturnih in športnih prireditev, nadzorovani smo ko telefoniramo ali deskamo po internetu, ko uporabljamo GPS ali ko s seboj nosimo mobilni telefon. Smo v borbi proti kriminalu, terorizmu, poneverbam in ostalim problemom družbe res postali tako slepi, da vidimo in iščemo rešitev le v visoko tehnoloških rešitvah, brez da bi se vprašali, katere od teh so sploh primerne in ali morda ne obstajajo druge, manj nasilne metode? Najhuje pri vsem skupaj je, da se nadzoru nimamo več kam umakniti. ■

Avtor: Dr. Helena Janžekovič / Višja inšpektorica svetnica za jedrsko in sevalno varnost
Uprava RS za jedrsko varnost



JEDRSKA VARNOST V EVROPSKI UNIJI PO FUKUSHIMI

Jedrskih nesreč, ki bi znatno kontaminirale okolje, je relativno malo. Običajno nesreče v jedrskih objektih, če so te sploh povezane z radioaktivno kontaminacijo, povzroče le zelo omejeno kontaminacijo.

Uvod

Po nesreči v Fukushimi so se razmahnile razprave o zagotavljanju jedrske varnosti v svetu ter tudi v Evropi. Ta nesreča je, tako kot že nesreča v Černobilu 1986, ponovno izpostavila problematiko čezmejnega vpliva jedrskih nesreč. Razprave se ne omejujejo le na nekatere elektrarne, ki so v Evropi postavljene blizu državnih mej, saj je Evropa geografsko relativno majhno področje in bi jedrska nesreča v eni državi lahko prizadela velik del Evrope. V državah EU deluje 132 jedrskih elektrarn, največ v Franciji. Dejstvo je tudi, da ima Švica, ki ni članica EU, pet takšnih elektrarn, Ukrajina in Rusija pa v Evropi skupaj 43.

Države EU so se na nesrečo sicer zelo različno odzvale. Tako bodo na primer v Nemčiji postopno zapirali elektrarne, vendar bo njihova razgradnja trajala še desetletja, v Italiji so opustili načrte za gradnjo novih, medtem ko se na gradnjo novih pripravlja Poljska. Francija ni spremenila svoje jedrske usmeritve. Ne glede na trenutne odločitve posameznih držav, pa je na ozemlju EU potrebno dolgoročno zagotavljati jedrsko varnost.



Jedrska varnost ni usmerjena le na delujoče elektrarne, temveč zajema bistveno širše področje. Delovanje elektrarne je le en del celotnega življenjskega cikla jedrskega objekta. To pomeni, da je potrebno nadzorovati med drugim že izbiro lokacije objekta, gradnjo, vzdrževanje, obnovo in razgradnjo elektrarn, ravnanje z radioaktivnim materialom od njegovega pridobivanja v rudnikih dalje, izdelovanje goriva, hrambo izrabljenega goriva, prevoz, ravnanje z radioaktivnimi odpadki in njihovo odlaganje itd. Bistvo varnosti je zagotavljanje zaščite ljudi pred škodljivimi vplivi sevanja ter zagotavljanje zaščite okolja. Zagotavljanje varnosti pa se seveda ne omejuje le na proizvodnjo električne energije s pomočjo jedrskih reaktorjev, torej na jedrske elektrarne, temveč je potrebno upoštevati dejstvo, da se viri sevanja uporabljajo na številnih drugih področjih. Nekateri jedrski reaktorji so namenjeni raziskavam in komercialni dejavnosti, kot je na primer produkcija radioizotopov, ki se uporabljajo v medicini. Jedrska varnost skupaj z varstvom pred ionizirajočim sevanjem je tako zelo široko in razvejano področje.



»Stresni testi« jedrskih elektrarn v EU po Fukushimi

Po nesreči v Fukushimi so vse članice EU, ki imajo jedrske elektrarne, izvedle dodatne varnostne preglede svojih jedrskih elektrarn, t.i. »stresne teste«. Način pregledovanja je pripravila Visoka skupina predstavnikov za jedrsko varnost (European Nuclear Safety Regulator Group - ENSREG). Rezultate testov je mogoče strniti v dve ugotovitvi in sicer, da ni potrebno nobene jedrske elektrarne v EU z vidika jedrske varnosti zapreti ter da je v številnih elektrarnah nujno potrebno izboljšati varnost. Ocenjena vlaganja v varnost znašajo do 25 milijard EUR. Na podlagi priporočil so države pripravile načrte o nadgradnji varnosti. Rezultati testov kot tudi načrti so javno dostopni. Pregledovanje varnosti elektrarn po nesreči v Fukushimi pa ni potekalo le v Evropi temveč po vsem svetu. Mednarodna agencija za atomsko energijo (International Atomic Energy Agency - IAEA) je pripravila poseben akcijski načrt, kako nadgraditi jedrsko varnost.

Nesreči v Černobilu in Fukushimi

Jedrskih nesreč, ki bi znatno kontaminirale okolje, je relativno malo. Običajno nesreče v jedrskih objektih, če so te sploh povezane z radioaktivno kontaminacijo, povzroče le zelo omejeno kontaminacijo. Upoštevati je potrebno tudi, da so bile v preteklosti nekatere jedrske nesreče povezane z vojaškimi programi, zato so dostopne informacije o njih redke. Jedrska nesreča ob trku dveh letal leta 1996 nad Španijo, je tako redko opisana. Iskanje jedrskih bomb je potekalo nekaj mesecev, dekontaminacija pa bo zaključena leta 2014. Danes je informacijsko blokado težje doseči, saj obstajajo mreže detektorskih sistemov, ki omogočajo ugotavljanje, da je prišlo do nesreče z radioaktivnim materialom. Ena izmed takšnih mrež z 80 postajami po vsem svetu deluje v okviru Pogodbe o celoviti prepovedi jedrskih poskusov. Po Mednarodni lestvici jedrskih in radioloških nesreč sta v najresnejšo stopnjo na njej uvrščeni le nesreča v Černobilu in v Fukushimi.

Najbolj odmevna je nesreča v Černobilu v Ukrajini. Tedaj so operaterji reaktorja ob izvedbi poskusa izklopili varnostne sisteme. Prišlo je do izgube nadzora nad reaktorjem. Veliko radioaktivnega materiala je odneslo v zrak ob dveh eksplozijah. Kontaminacijo so zaznali predvsem na S polobli. Sledila je tudi evakuacija prebivalcev ter vzpostavitev kontroliranega področja, ki obsega 2600 km^2. Nadzor nad kontaminacijo je ponekod še vedno potreben. Tako bo nadzor nad uvozom hrane in krme iz potencialno kontaminiranih področij v EU veljal vsaj do leta 2020.

Nesreča je povzročila ne le tehnološke izboljšave, temveč v nekaterih državah tudi vzpostavitev novih nadzornih organov za jedrsko varnost. Države so po nesreči vzpostavile režim obveščanja in ukrepanja ob jedrskih nesrečah. V EU je bil tako vzpostavljen 24-urni sistem obveščanja. Razmahnilo se je mednarodno sodelovanje, kot je na primer priprava varnostnih standardov IAEA. Leta 1996 je bila sprejeta Konvencija o jedrski varnosti, ki omogoča redno in sistematično izmenjavo informacij s področja varnosti.

Nesreča v Černobilu pa je tudi povzročila, da so se nekatere države odločile opustiti uporabo jedrskih elektrarn. Ponekod je nesreča za dolgo zavrla njihovo gradnjo, kot na primer v ZDA. Po približno 20 letih pa se je v energetiki nakazovala t.i. »jedrska renesansa«, saj so ponekod začeli s pripravami na gradnjo jedr-

Po Mednarodni lestvici jedrskih in radioloških nesreč sta v najresnejšo stopnjo na njej uvrščeni le nesreča v Černobilu in v Fukushimi.

Nesreči v Černobilu je botrovala napačna inženirska presoja ter neustrezen sistem nadzora. Nesreča v Fukushimi pa je pokazala, da lahko tudi visoko razvita država ni ustrezno pripravljena in ter, da niz napak vodi do katastrofalnih posledic.

skih elektrarn. Jedrska nesreča v Fukushimi je nekatere načrte prekrižala.

Nesreča v japonski jedrski elektrarni Fukushima Dai-ichi ob Pacifiškem oceanu pušča globoke posledice v jedrski stroki po vsem svetu. Opustošenje na lokaciji elektrarne s šestimi reaktorji je povzročil 11.04.2011 tsunami, ki je bil posledica uničujočega potresa. Prvi val je zalil elektrarno v manj kot eni uri po potresu. Poplava je onesposobila elektrarno do te mere, da so operaterji v veliki meri izgubili nadzor nad štirimi reaktorji, kar je vodilo do puščanja radioaktivnih snovi v zrak ter v ocean. Zaradi kontaminacije je bila potrebna evakuacija prebivalcev, nadzor nad kontaminacijo hrane in vode ter postavitev posebnih varnostnih režimov v bližini elektrarne. Tudi danes operaterji, ki sanirajo stanje v elektrarni, delajo v težkih razmerah ob obsežni kontaminaciji. Predvsem želijo zagotoviti varno stanje, tako da ob morebitni ponovni nesreči ne bi prišlo do izpustov.

Nesreči v Černobilu je botrovala napačna inženirska presoja ter neustrezen sistem nadzora. Nesreča v Fukushimi pa je pokazala, da lahko tudi visoko razvita država ni ustrezno pripravljena in ter, da niz napak vodi do katastrofalnih posledic. Pokazala je tudi, da kljub številnim mednarodnim aktivnostim, te ne jamčijo, da je država pripravljena na jedrsko nesrečo. Države, ki imajo jedrski program ter mednarodne organizacije zato iščejo skupno pot, kako nadgraditi jedrsko varnost.

Jedrska varnost v EU

Jedrsko varnost v EU urejajo članice EU same. V EU je bila leta 2009 sprejeta Direktiva o jedrski varnosti ter kasneje tudi direktiva, ki ureja ravnanje z radioaktivnimi odpadki in izrabljenim jedrskim gorivom. Obe temeljita na Pogodbi o ustanovitvi Evropske skupnosti za atomsko energijo. Ta je bila podpisana že leta 1957, ko je bila jedrska energija izjemno obetajoča smer v energetiki. Tedaj je na tem področju prednjačila tedanja ZSSR s prvo jedrsko elektrarno, ki je začela delovati že leta 1954.

Omenjena pogodba je med drugim usmerjena k pospeševanju znanosti, nadzoru nad jedrskim materialom kot tudi k zagotavljanju varnostnih standardov. Tako na primer v skladu s pogodbo inšpektorji EU nadzorujejo jedrski material v državah članicah, Evropska komisija podaja mnenje o načrtih za odlagališča radioaktivnih odpadkov, sprejema investicijske načrte za nove jedrske objekte in izvaja nadzor nad monitoringom radioaktivnosti zraka, vode in zemlje. V EU so sprejeti tudi zakonski akti, ki se nanašajo na zaščito ljudi pred škodljivimi vplivi ionizirajočega sevanja.

Po Fukushimi Evropska komisija pripravlja novo različico Direktive o jedrski varnosti. Možnosti, kako celovito urejati jedrsko varnost v Evropi, je več. Nadzor je lahko centraliziran ali ne. Lahko temelji na merljivih, torej predpisanih parametrih, lahko pa temelji na predpisanih ciljih. Pri tem mora komisija upoštevati, da ima vsaka izmed 14 držav članic, ki ima jedrsko elektrarno, unikaten razvoj tako na področju tehnologije kot tudi na področju same organiziranosti operaterjev, upravnih organov, agencij in ekspertnih skupin. Ponekod temelji uporaba jedrskih tehnologij na domači tehnologiji, drugod je tehnologija uvožena. Zato tudi ne preseneča, da uporaba standardov IAEA v EU ni enoten.

Poenotenost in standardizacija seveda lahko vodita k izboljšanju varnosti. Nujna uvedba pa je povezana tudi z vprašanjem centraliziranega nadzora v EU. Misel, da bi v EU ustanovili nekakšno centralno agencijo ali centralni upravni organ, ki bi nato bedel nad delovanjem posameznih nacionalnih upravnih organov ali skrbel za usklajeno delovanje tam, kjer je to potrebno, je bila v razpravah jedrskih strokovnjakov že večkrat omenjena. Trenutne razprave v EU pa kažejo, da ni velike naklonjenosti tej ideji.

V EU pa poteka po Fukushimi tudi obsežen pregled pripravljenosti članic na nesrečo. Države sicer same načrtujejo ukrepe, kot je na primer evakuacija, vendar so nekateri ukrepi takšni, da jih je smiselno uskladiti vsaj na nivoju sosednjih držav.

Same države ali operaterji elektrarn izvajajo po Fukushimi številne izboljšave, tako na primer francoski operater pripravlja specializirano enoto s posebno opremo za nujna posredovanja ob resnih nesrečah.

Zaključek

Pri razvoju jedrske varnosti v Evropi je potrebno upoštevati čezmejen vpliv jedrskih nesreč ter časovno dimenzijo jedrskih objektov. Evropa s številnimi jedrskimi objekti na ozemlju držav EU ali v svoji neposredni bližini se vprašanju urejanja jedrske varnosti ne more izogniti. Nekaj novih jedrskih objektov je v državah EU načrtovanih, prav tako tudi v neposredni bližini, na primer ruska elektrarna blizu Kalinigrada ali elektrarne v Turčiji. Nekateri objekti v državah EU so v procesu razgradnje. Nobena država se torej vprašanjem jedrske varnosti ne more izogniti, tudi če sama sploh nima jedrskega objekta, saj je vpliv resnih nesreč čezmejen.

Glede na uporabo jedrskega objekta, ki se običajno raztega preko nekaj desetletij, nato pa sledi razgradnja, ki prav tako lahko traja nekaj desetletij, je pri urejanju jedrske varnosti potrebno upoštevati, da ena ali dve generaciji običajno objekt načrtujeta, gradita in uporabljata, nato pa druge generacije izvedejo razgradnjo objekta. Še dolgoročnejša je skrb za radioaktivne odpadke.

Izkušenj pri nadzoru objektov, ki zahtevajo tako dolgotrajen nadzor in imajo lahko tako velik vpliv, če pride do resne nesreče, pravzaprav ni. Zato mora vsaka država vestno načrtovati, da ima dovolj strokovnjakov s področja jedrske varnosti ter, da ima vzpostavljen učinkovit nadzor in sistem ukrepanja, če do nesreče pride. ■



SITI BESED

SEPTEMBER 2013



Pridružimo se pobudi, da v slovenskih šolah od septembra 2013 ne bo več lačnih otrok.

www.sitibesed.si
Fb: Siti besed

Sredstva za prehrano šolskih otrok lahko nakažete na: **Zveza prijateljev mladine Slovenije, Miklošičeva 16, 1000 Ljubljana, št. računa: SI56 6100 0000 3512 232, BIC: HDELSI22, sklic: 00 07-2401, koda namena: CHAR (namen SITI BESED, dodajte oznako AN, če želite ostati anonimni).**

DOŽIVITE LJUBLJANO DRUGAČE

ZAPELJITE SE Z LADJICO EMONA II

Privoščite si čas za zabavo in sprostitev v družbi poslovnih partnerjev, sodelavcev ali prijateljev (pikniki, poslovna srečanja, team building). Ob dobri hrani in pijači boste zapluli z ladjo EMONA II skozi prestolnico in njeno prelepo okolico.









Plovba lahko poteka od ene do pet ur.
Sprejemamo skupine od 15 do 50 oseb.
Vozimo lahko skozi vse leto, ladijca je ob hladnem vremenu zaprta, ogrevana in ima urejene sanitarije.

Preverite našo ponudbo na naši spletni strani

www.ljubljanica.eu









Informacije in rezervacije:

gsm: 041 770 508 / 031 829 870 , tel.: 05/996-78-55
e -mail: sasomr@gmail.com, ladjica.emona2@gmail.com

Avtor: Jelenko Vidic / Slovensko združenje korporativne varnosti



RAVNANJE S TVEGANJI – III DEL

Proces ravnanja s tveganji je postal pomemben temelj za normalno delovanje organizacij v dinamičnem okolju in njihovo pripravljenost na soočanje s stalnimi spremembami.

»Dosedanja praksa je pokazala, da bo v prihodnosti treba uporabljati bolj eksaktne metode ocenjevanja tveganj, in ne pavšalne, kot so se do sedaj« (Keković, 2013).

Ti zaključki mednarodne konference »Dnevi korporativne varnosti«, so potrdile tudi moje ugotovitve iz prakse, opravljenih raziskav in razmišljanja o tem. Na področju ravnanja s tveganji (analiziranje, ocenjevanje, vrednotenje, itd.) ravnamo dokaj lahkotno, poenostavljamo in sprejemamo pavšalne ocene. Posledica tega so tudi pavšalne odločitve o ukrepanju za obvladovanje tveganj ter iz tega izvedene rešitve. Predvsem je moteče to, da se tako ravna tudi v zvezi z varovanjem in zaščito ključnih nacionalnih objektov in subjektov kritične infrastrukture. Ker sem se v svoji delovni praksi pogosto srečeval s podobnimi težavami, bom v nadaljevanju predstavil moje videnje problema.

Opis problema - izhodišče

Kot pravi Vršec (2012), je prvi (strateški) nivo upravljanja korporativne varnosti izdelava, razprava, sprejem (izdaja) in skrb za implementacijo krovne varnostne politike v poslovne procese, notranjo integriteto, projekte, logistiko, outsourcing, odnose s poslovnimi partnerji in družbeno odgovornostjo. Temeljna izhodišča za pripravo krovne varnostne politike so, poleg nacionalno varnostne politike in veljavne zakonodaje, analiza ranljivosti, analiza ogroženosti, analiza tveganj, ter drugi elementi. Tukaj se v osnovi pojavi že prva resna težava, saj so bile ocene ogroženosti na nacionalni ravni izdelane brez ustrezne enotne metodologije. Država s svojim strokovnim potencialom torej ni bila sposobna izvesti ustrezne strateške analize (Čaleta, 2012). Ja, kako pa naj to potem ustrezno izvedejo v korporacijah, ki nimajo takšnega strokovnega potenciala? Poleg tega pa ni poenotene terminološke opredelitve obravnavanih pojmov, niti ne usmeritev za izbor ustrezne metodologije.

Dejstvo je, da le dobra terminološka opredelitev pojmov področja ravnanja s tveganji omogoča kakovostno strokovno razpravo in poglobljeno izmenjavo znanj različnih strokovnjakov na tem interdisciplinarnem področju.

Temeljna izhodišča za pripravo krovne varnostne politike so, poleg nacionalno varnostne politike in veljavne zakonodaje, analiza ranljivosti, analiza ogroženosti, analiza tveganj, ter drugi elementi.

Repetita iuvant – Repetitio est mater studiorum

Žal je v zvezi obravnavanega treba nekatere stvari ponoviti. Sicer pa ponavljanje koristi in je mati učenja, kot pravita zgornja latinska pregovora (Banič, 1990:270). Dejstvo je, da le dobra terminološka opredelitev pojmov področja ravnanja s tveganji omogoča kakovostno strokovno razpravo in poglobljeno izmenjavo znanj različnih strokovnjakov na tem interdisciplinarnem področju. Problem postane pereč zlasti pri prenosu strokovnih znanj iz tujih govornih področij ter usklajevanje definicij z domačim razpoložljivim izrazjem (Štupar, 2008). To mnogokrat povzroča težave[1] pri izvajanju potrebnih dejavnosti in aktivnosti, saj se v literaturi v zvezi obravnavanega pojavlja množica definicij in opredelitev. V zvezi s tem tudi Keković (2013) opozarja na dosledno uporabo semantike[2]. Predvsem pri prevajanju mednarodnih standardov je to nuja, saj multikorporacijsko in transnacionalno okolje narekujeta potrebo po poenotenju izrazoslovja. Oglejmo si nekaj osnovnih opredelitev, saj vseh tukaj ne moremo opisati.



Terminološka obravnava definicij pojmov

Kot opisuje Štupar (2008), je bil poskus ureditve izrazja s tega področja narejen leta 1982, ko je UNDRO (United Nations Disaster Relief Organization; zdaj UN-DHA - United Nations Department of Humanitarian Affairs) razmejila termin nevarnost od termina tveganje z definicijama, ki sta bili mišljeni za univerzalno uporabo, a se je njuna narava žal izkazala za ne dovolj splošno, saj so si bili avtorji še vedno prisiljeni uporabiti lastne definicije.

Glede na množico definicij o analizi tveganj in enačb, ki izhajajo iz njih, lahko vzamemo za izhodišče definicije pojmov kot jih je postavila UNDRO. S ciljem poenotenja izrazov v slovenščini jih je povzel tudi Lapajne (1987):

- **Nevarnost** *(hazard)* je (naravna ali druga ustrezna) danost za katerikoli neugoden pojav, ki je povezan z možno nesrečo in lahko povzroči neugodne učinke. Govorimo o potresni, poplavni, požarni in drugih nevarnostih. Nevarnost je verjetnostni pojem in jo opredeljujemo z »verjetnostjo prekoračitve«, torej z vrednostmi med 0 in 1.
- **Ogroženost** *(risk)* so možne družbene in ekonomske posledice bodočih nesreč. Govorimo o potresni, poplavni, požarni itd. ogroženosti. Ogroženost je verjetnostni pojem in jo lahko opredelimo z »verjetnostjo prekoračitve«. Odvisna je od nevarnosti, ranljivosti in od časa izpostavljanja. Določujejo jo vrednosti med 0 in 1.
- **Ranljivost** *(vulnerability)* je pričakovana stopnja izgub (ali poškodb) danega ogroženca ali skupine ogroženčev ob morebitni nesreči. Govorimo o potresni, poplavni, požarni in drugi ranljivosti. Ocenjujemo jo navadno z vrednostmi med 0 in1.
- **Tveganje** *(acceptable risk)* je tista ogroženost, ki jo zavestno sprejmemo kot sprejemljivo. Natančneje je to tista »verjetnost prekoračitve«, ki jo jemljemo kot osnovo za določitev projektnih zahtev v graditeljstvu ali pri družbeno ekonomskih posegih.
- **Ogroženci** *(elements at risk)* so vse sestavine življenjskega prostora, npr. prebivalstvo, družbena in zasebna lastnina, družbene in ekonomske aktivnosti, ki so ogrožene na danem območju.
- **Ogrožena vrednost** *(value at risk)* so možne ekonomske izgube na danem območju.
- **Verjetnost prekoračitve** *(exceedance probability)* je verjetnost, da bo v danem obdobju na danem mestu ali območju prekoračena določena vrednost neke značilne fizikalne oz. geofizikalne (lahko tudi statistične) količine, ki za dane potrebe sprejemljivo količinsko opredeljuje nesrečo, ali verjetnost, da bodo presežene določene družbene in ekonomske posledice nesreče. Ima vrednost med 0 in 1.
- **Čas izpostavljanja** *(exposure time)* je doba, ki jo upoštevamo pri oceni nevarnosti ali ogroženosti.
- **Škoda** *(damage)* obsega ekonomske izgube, ocenjene po nesreči.

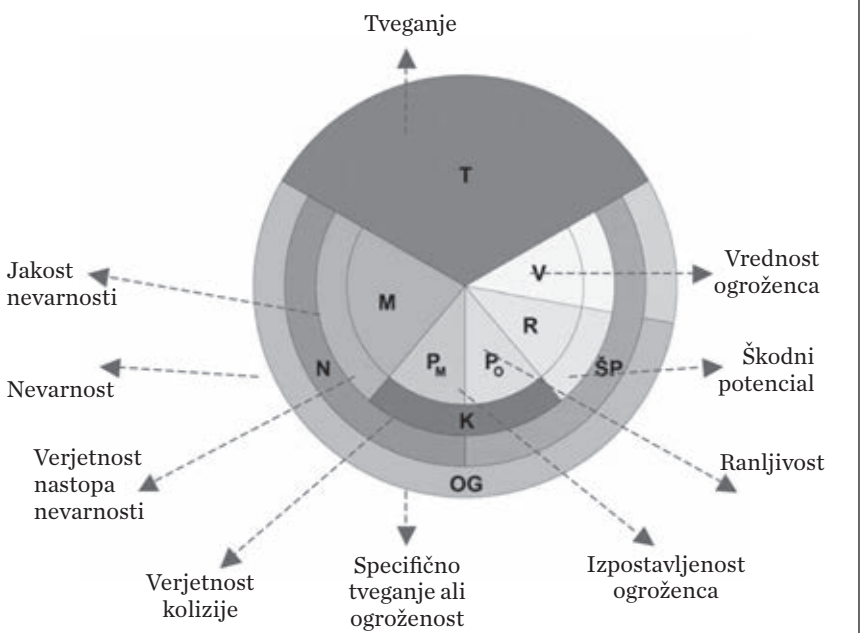
Čarobne formule ocenjevanja - vrednotenja

Da bi lahko presodili in kvantitativno ocenili ter ovrednotili tveganja, je treba uporabiti ustrezno enačbo za vrednotenje. Oglejmo si nekatere konkretne različice:

UNDRO je uvedel kvantitativno definicijo tveganja z množenjem verjetnosti nastopa nevarnosti (H), ranljivosti (V) in socialnih elementov E, torej: tveganje $_t$ = soc.elementi *(nevarnost * ranljivost). Precej splošno razširjeni sta tudi opredelitvi tveganj, ki jo je podal UNESCO (United Nations Educational, Scientific and Cultural Organization): tveganje = nevarnost * ranljivost * potencialna izguba in bolj standardna, ki jo je podal USDOE (US Department Of Energy in USNRC, US Nuclear Regulatory Commission), kjer nastopa tveganost scenarija: tveganost scenarija = verjetnost * posledice.

Zanimiva je še splošna enačba UNDMTP (United Nations Disaster Management Training Programme) za izračun specifičnega tveganja: tveganje $_{ij}$ = nevarnost $_j$ x ranljivost $_{ij}$ ($R_{ij} = H_j \times V_{ij}$). Omenimo še enačbo, ki jo podaja CENAT (2004, v Đurović in Mikoš, 2006), kjer pravijo, da je tveganje odvisno od treh dejavnikov: nevarnosti, ranljivosti in vrednosti ogroženca: tveganje = nevarnost * ranljivost * vrednost.

Pri operiranju z navedenimi parametri analize tveganja, pa je pri ocenjevanju treba dosledno upoštevati njihove odnose, kot jih prikazuje slika 1 (Đurović, Mikoš, 2006).



Slika: *Odnosi med parametri analize tveganja (prirejeno po Đurović in Mikoš, 2006:159)*

Primer uporabe pojmov

Za boljše razumevanje obravnavanih pojmov ponovno uporabimo Flakerjevo (1994) ugotovitev, da je analiza tveganja postopek, ki ga počnemo v vsakdanjem življenju tako rekoč neprenehoma, čeprav se tega ne zavedamo vedno. Za primer vzemimo vsakodnevno vožnjo z avtomobilom.

Ko pričnemo z vožnjo avtomobila in se vključimo iz neprometnih na prometne površine, postanemo prometni udeleženec. Vožnjo izvajamo kot vsakodnevno rutinsko opravilo pri katerem kaj dosti ne razmišljamo, kako to opravljamo. Sedaj pretvorimo primer v strokovni jezik obravnavane teme in pri tem smiselno uporabimo pojme v zvezi s tveganjem, ki jih navaja Lapajne (1987, v CRP, 2004):
Na cesti je prometna nevarnost, ki je odvisna od kakovosti ceste, vremena, dnevnega časa, drugih udeležencev, gostote prometa, predmetov na cesti, ...Ko zapeljemo na cesto postanemo prometni ogroženci. Našo prometno ogroženost določa poleg nevarnosti še prometna ranljivost, ki je odvisna od tehničnega stanja vozila, voznikovih sposobnosti, načina vožnje, ...Ko se podajamo na pot, sprejmemo prometno tveganje. Vrednost vozila, predmetov in potnikov v njem je ogrožena vrednost. Čas, ki ga prebijemo na vožnji je čas izpostavljanja (daljši čas = večja ogroženost). Verjetnost prekoračitve določenega odstotka nesreč na leto na dani cesti daje oceno prometne nevarnosti. Če pride do nesreče, nastane prometna škoda.

Zgornji primer rabe pojmov je potrebno prirediti v skladu z izrazjem in opredelitvami. Torej:
Na cesti je prometna nevarnost, ki je sestavljena iz več dejavnikov nevarnosti (kakovosti ceste, vremena, dnevnega časa, drugih udeležencev, gostote prometa, predmetov na cesti, ...) z določenimi verjetnostmi nastopa in magnitudami. Ko zapeljemo na cesto (območje nevarnosti) postanemo vložek. Izpostavljenost je verjetnost, da se nahajamo v območju nevarnosti. Skupaj tvorijo prometno ogroženost. Našo prometno tveganost, ki jo sprejmemo ob podajanju na cesto (in s tem izrabimo prometno priložnost), določa poleg prometne ogroženosti še prometna ranljivost vložka, ki je odvisna od tehničnega stanja vozila, voznikovih sposobnosti, načina vožnje, ... Vrednost vozila, predmetov in potnikov v njem je vrednost vložka. Skupaj tvorijo škodni potencial. Vseh šest dejavnikov skupaj tvori prometno tveganost za določen vložek.

Zaključek

Z okrnjenim prispevkom sem želel le opozoriti na nekatere težave in probleme s katerimi se je potrebno ukvarjati v operativnem okolju različnih korporacij. V teh okoljih ni takšnega strokovnega potenciala, ki bi lahko z lahkoto prevajal strokovne in znanstvene definicije ter operiral z uporabo enačb za analiziranje, ocenjevanje ter vrednotenje ranljivosti, ogroženosti in tveganj. Že iz opisanega enostavnega vsakodnevnega opravila – vožnje z vozilom – izhaja, da to ni enostavno opravilo, če ga prevedemo v strokovni jezik obravnavanega področja. Zadeva se enostavno že tu zakomplicira, kaj šele pri izvedbi nekih resnejših analiz za zagotavljanje korporativne varnosti. Skratka, še se bo treba učiti in ponavljati ter obnavljati pridobljena znanja.

Viri:

- Banič, S. (1990). Latinski pregovori, izreki in izrazi. Državna založba Slovenije, Ljubljana 1990.
- CENAT (2004). Coping with risks due to natural hazards in the 21st century. Monte Veritŕ Workshop 2004, 28. 11.–3. 12. 2004. http://www.cenat.ch (2.2.2006).
- CRP (2004): »Metodologija za določanje ogroženih območij in način razvrščanja zemljišč v razrede ogroženosti zaradi zemeljskih plazov - končno poročilo«, UL FGG, Poročilo KSH d-78, Ljubljana, maj 2004.
- Čaleta, D. (2012). Ali država zamuja priložnost za racionalizacijo stroškov varovanja objektov v njeni lasti?, Korporativna varnost, št.2, letnik 2012, Institut za korporativne varnostne študije, ICS-Ljubljana.
- Đurović, B. in Mikoš, M. (2006). Pojmi in izrazje teorije tveganj zaradi naravnih, geološko in geografsko pogojenih nevarnosti. Geologija 49/1. Pridobljeno 2008 na: http://www.geo-zs.si/publikacije_arhiv/Clanki/Geologija_49_1/Durovic%20&%20Mikos.pdf
- Flaker, V. (1994). Analiza tveganja. Socialno delo, let. 34, št.4.
- Keković, Z. (2013). Standardization and accreditation of corporate security. MANAGEMENT of corporate security: new approaches and future challenges/ [editorial Denis Čaleta, and Miran Vršec].- Ljubljana: Institute for Corporative Security Studies, 2013
- Lapajne, J. (1987): Strokovna beseda. – Ujma *1*, 94, Ljubljana.
- Prezelj, I. (2005). Nacionalni sistemi kriznega menedžmenta. Fakulteta za družbene vede, Ljubljana.
- Vršec, M. (2012). Varnostna politika kot krovni dokument upravljanja korporativne varnosti. Korporativna varnost, št.2, letnik 2012, Institut za korporativne varnostne študije, ICS-Ljubljana.
- Slovar slovenskega knjižnega jezika. ASP-pregledovalnik podatkovnih zbirk, v1. 40, http://www.amebis.si.
- Štupar, B. (2008). Ali smo ogroženi, kadar tvegamo? Pridobljeno 21.05.2008 na: http://www.gore-ljudje.net/novosti/36119/

[1] Kaplanova teorema komunikacije pravita, da: 50% težav v svetu nastaja, ker se uporabljajo *isti izrazi za različne vsebine* in da drugih 50% težav nastaja, ker se uporabljajo *različni izrazi za iste vsebine.*

[2] SSKJ: nauk o pomenu besed, pomenoslovje. ■



ICS PUBLIKACIJE

www.ics-institut.si

ICS

Institute for Corporative Security Studies



5. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 19.—20. marec 2014



ICS

Institut za korporativne varnostne študije

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

www.ics-institut.si