Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2013, marec • št. 3



Bančni sektor in vloga učinkovitega sistema obvladovanja operativnih tveganj

Dr. Brane Bertoncelj, Banka Slovenije

4. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 20.-21. marec 2013

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
marec 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.

Revija »Korporativna varnost« si je v celoti zagotovila ustrezen medijski prostor in obseg zainteresiranega bralstva, kar je zaznati iz izredno pozitivnih odzivov, ki prihajajo iz različnih družbenih okolij. Z odpiranjem aktualnih vsebin in novih spoznanj nameravamo v uredništvu nadaljevati z nezmanjšano hitrostjo.

Krepitev zavedanja o potrebnosti celovitega obvladovanja tveganj in integralnih rešitev na področju varnosti je tista nujno potrebna komponenta, ki bo naše organizacije naredila prožnejše in bolje pripravljene na dinamično varnostno okolje. Da stanje korporativne varnosti v percepciji slovenskega strateškega managementa ni ustrezno pozicionirano kažejo nešteti primeri deviantnosti, katerim smo priča v javnem in poslovnem okolju. Odsotnost ustrezne stopnje varnostnega zavedanja in kulture se odraža že pri lastnikih, ki bi prvi morali imeti interes, da je stanje njihovega premoženja varno in obvladljivo. Ti vzorci se logično nadaljujejo tudi preko struktur, ki strateško upravljajo organizacije in se v nizkem stanju odražajo v vseh delih organizacij. Temu posledično se procesom korporativne varnosti in struktur, ki so zadolžene za upravljanje korporativne varnosti ne posveča ustrezna pozornost. Njihova organizacijska umeščenost na četrti in peti nivo upravljanja brez ustrezne povezave do strateških struktur odločanja, največkrat v praksi pomeni, da na področju obvladovanja tveganj ni sistemskega pristopa načrtovanja in so rešitve v večini primerov vzpodbujene kot odziv na izredne dogodke. Pristopi preventivnih ukrepov imajo za sistemsko delovanje organizacije neprimerno boljši učinek, kot ukrepi odpravljanja že storjenih posledic. Zahteve izrednih situacij vplivajo na izvajanje naših aktivnosti in v realnosti največkrat sami nimamo ustreznih možnosti pomembnejšega vplivanja po storjenem dogodku. Tudi vloženi finančni in drugi resursi v takih primerih ne dajejo zadostnih rezultatov, saj so zaradi nesistemskega pristopa največkrat neučinkovito uporabljeni. Določen del odgovornosti za stanje korporativne varnosti vsekakor nosijo tudi neposredni izvajalci teh procesov, ki največkrat prihajajo iz različnih struktur, kateri so samo posredno povezani s to profesijo. Ti strokovnjaki pa so brez novih znanj s področja korporativne varnosti neprimerni in v določenem primeru s svojim nepoznavanjem osnovnih poslovnih procesov v organizacijah negativno vplivajo na zagotavljanje korporativne varnosti in posledično tudi ugleda te dejavnosti oz. stroke. Nov magistrski program »Management korporativne varnosti«, ki ga bo letos začela izvajati Fakulteta za podjetništvo-GEA College v sodelovanju z Institutom za korporativne varnostne študije je tisti nujno potreben korak, ki bo zagotavljal višjo kvaliteto in predvsem višji ugled poklica korporativno varnostnega managerja v širši družbi.

Novim pristopom in znanju posvečamo veliko pozornosti tudi v tretji številki revije, kjer je možno poseči po kvalitetnih vsebinah, ki so vse posredno in neposredno povezane z znanji, ki jih za učinkovito delovanje potrebuje strokovna javnost. Aktualni intervjuji in prispevki omogočajo osnovni temelj za dvigovanje splošnega zavedanja o potrebnosti celovitega obvladovanja tveganj v naših organizacijah.

V zaključku mi dovolite, da vas še enkrat povabim na mednarodno konferenco »**Dnevi korporativne varnosti**«, ki bo v mesecu marcu potekala v Ljubljani s tokratno rdečo nitjo posvečeno »**Upravljanju korporativne varnosti – novim pristopom in izzivom prihodnosti**«. Korporativno varnostni manager, ki se zaveda, da pot večje prepoznavnosti in ugleda njegove dejavnosti vodi samo preko pridobivanja novih znanj in dobrih praks, nikakor ne sme manjkati na omenjenem dogodku.

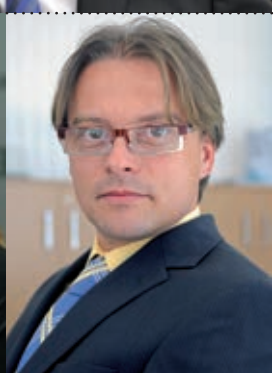
Doc. dr. Denis Čaleta
Glavni urednik



INTERVJU
Dr. Brane Bertoncelj
Direktor oddelka gotovinskega poslovanja v Banki Slovenije

BANČNI SEKTOR IN VLOGA UČINKOVITEGA SISTEMA OBVLADOVANJA OPERATIVNIH TVEGANJ 5





INTERVJU
ga. Medeja Lončar, direktorica in
mag. Igor Kulašič, vodja divizije tehnične opreme objektov, Siemens d.o.o.

NOVA SPOZNANJA IN PREVERJENE REŠITVE NAM OMOGOČAJO VAREN RAZVOJ NAŠIH ORGANIZACIJ 12



INTERVJU
g. Gregor Majcen
direktor Urada Republike Slovenije za varovanje tajnih podatkov

USTREZEN SISTEM VAROVANJA TAJNOSTI KLJUČ ZA USPEŠNO DELOVANJE ORGANIZACIJE 19



INTERNI NADZOR IN NADZOR NAROČNIKOV ZASEBNEGA VAROVANJA NAD DELOM VARNOSTNIH SLUŽB

Zasebno varovanje ima v slovenskem prostoru poseben pomen, zato mora biti nadzor nad njegovim izvajanjem profesionalen, zakonit in dosleden. Poseben pomen gre pripisovati zato, ker s svojim delovanjem prispeva k zagotavljanju notranje varnosti države. 35



SMO (ŽE) POSTALI DRUŽBA NADZORA? I. DEL

Današnji svet je prežet s tehniko in brez nje si ga kar ne moremo več predstavljati. 43

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

INTERVJU
Dr. Brane Bertoncelj
Direktor oddelka gotovinskega poslovanja v Banki Slovenije

BANČNI SEKTOR IN VLOGA UČINKOVITEGA SISTEMA OBVLADOVANJA OPERATIVNIH TVEGANJ

Učinkovito delovanje bančnega sistema je zelo močno povezano z ustreznim obvladovanjem tveganj med katerimi imajo operativna tveganja posebno mesto.

1. Celovito obvladovanje varnostnih tveganj je v bančnem sistemu še posebej pomembno. Kateri so tisti segmenti obvladovanja tveganj, ki jim v Banki Slovenije posvečate še posebno pozornost?

V Banki Slovenije posebno pozornost namenjamo finančnim tveganjem, ki so opredeljena v Zakonu o bančništvu ter v Sklepu o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, in so pomembna za nemoteno delovanje Banke Slovenije ter slovenskega finančnega sistema. Sam se predvsem ukvarjam z operativnimi tveganji na področju poslovanja z gotovino, za katera je pomembno, kot za vsa druga tveganja, da so ustrezno identificirana, ocenjevana, spremljana in obvladovana.

2. Glede na dejstvo, da ste v Sloveniji vodili verjetno enega izmed najbolj zahtevnih varnostnih projektov in sicer zagotovitev gotovinskega poslovanja ob uvedbi Evra, bi vas prosil, da nam z vidika strateškega načrtovanja obvladovanja tveganj zaupate tiste bistvene dobre prakse, ki bi bile lahko uporabne tudi pri drugih večjih varnostnih projektih.

Uporabili smo model strateškega načrtovanja, ki so že obstajali v teoriji in praksi kot dobra praksa in so obsegali naslednje med seboj povezane odločitve, in sicer: (i) definiranje želenih ciljev (kaj smo, kdo smo, zakaj smo), na podlagi kreativnega in dinamičnega procesa odločanja; (ii) določitev vlog udeležencev v gotovinskem ciklusu in oskrbi države z gotovino (kje smo, zakaj smo tam, kam gremo), upoštevajoč pri tem priložnosti in nevarnosti iz zunanjega in notranjega okolja ter sposobnosti in možne slabosti (kot tudi potencialna ogrožanja); (iii) oblikovanje funkcionalnih strategij in operativnih aktivnosti za vse ključne aktivnosti projekta; (iv) alociranje omejenih resursov za uresničitev zastavljenih ciljev, in sicer tako materialnih kot tudi nematerialnih ter kontrola in evalvacija izvedbe. Prevzem evra je bil, tako za zaposlene v finančnem sistemu kot tudi zame, »projekt življenja«, v katerem ni bilo prostora za razna presenečenja. Temelj za dobro strateško pripravo projekta prevzema gotovine v RS je bila ustrezna koordinacija vseh aktivnosti med njenimi posameznimi izvajalci in proaktivnost s predvidevanjem možnih odklonov od želenega stanja ter priprava rezervnih postopkov za primer dejanskih odklonov. Pri tem smo uporabljali izkušnje iz predhodnih zamenjav valut na ozemlju Slovenije (v zadnjih sto letih je bila zamenjana na različne načine devetkrat) in dobro bančno prakso drugih držav pri prevzemu evra. Posebnost projekta je bila na področju načrtovanja pred prevzemom evra tudi izvedba simulacije vseh pomembnih aktivnosti,

Prevzem evra je bil, tako za zaposlene v finančnem sistemu kot tudi zame, »projekt življenja«, v katerem ni bilo prostora za razna presenečenja.

*avtor je član Slovenskega združenja korporativne varnosti

od pred dobave in dobave evrov, umiku tolarske gotovine in njenem uničenju. Pri tem smo smiselno uporabili simulacijski program Ministrstva za obrambo. Ugotovitve simulacije smo vključili v operativni načrt izvedbe, kar je omogočilo tekoči prevzem evra. Osnovo za dobro predpripravo strateškega načrtovanja je bil vzpostavljen dober pretok informacij, varovanje občutljivih informacij in ustrezen vodstven nadzor. Pri aktivnostih nismo želeli presenečenj ali naključij. Že delno pomanjkanje gotovine, nedelovanje nekaterih bančnih avtomatov, ne obvladovanje konic poslovanja ali neugodne vremenske razmere, bi lahko vplivali na uspešno izvedbo projekta, možni škodni dogodki zaradi kriminalnih dejanj pa so več mesecev »viseli v zraku«.

3. Ali Banka Slovenije poleg fiskalne regulative izdaja tudi ukrepe in priporočila na področju neposredne varnosti bančnega sistema?

Banka Slovenije je sodelovala pri pripravi Minimalnih priporočil za varnost bančnega poslovanja na področju varovanja oseb in premoženja, ki jih je pripravilo Združenje bank Slovenije za potrebe slovenskih poslovnih bank. Prav tako Banka Slovenije opravlja preglede na podlagi Zakona o bančništvu in Sklepa o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, kjer se tudi oceni fizično in tehnično varnost pregledane banke. Prav tako mora poslovna banka zagotoviti, da tretja neodvisna oseba najmanj enkrat na dve leti in ob spremembah varnostnega sistema, izvede nadzor nad izvajalcem zasebnega varovanja, ki opravlja storitve v poslovnih bankah.

4. V zadnjem obdobju smo bili priča povečanju frekvence pojavljanja roparskih napadov na subjekte bančnega sistema. Kaj po vaši osebni strokovni oceni lahko naredijo banke za zmanjšanje roparskih napadov na njihove poslovalnice oz. prevoze gotovine?

Slovenija je varna država (kar dokazujejo domače in tuje raziskave), na žalost pa nove nevarnosti (kriminalna mobilnost, gospodarska kriza, socialna negotovost, droge, terorizem, javni protesti ipd.) vse bolj grozijo poslovanju. Latinski pregovor pravi, da nikomur ni prepovedano delati sebi v korist, dokler ne škoduje drugim. Vse več je »prijateljev tujega denarja«, zato morajo banke za povečanje varnosti posvetiti posebno pozornost načrtovanju delovnega okolja banke (ustrezno planiranje, organiziranje, kadrovanje in kontroling), obvladovanju operativnih tveganj (zlasti finančnih tveganj in tveganje izgube ugleda banke), zmanjšanju verjetnosti za škodni dogodek (povečanje tveganja za izvedbo, zmanjšanje dobička), zelo učinkovito je tudi obarvanje gotovine. Pomembno je, da zaposlene izobražujejo, kako ravnati v primeru nenormalne situacije, zlasti pripravljenost na najtežje situacije in vadbi teh scenarijev (vključujejo naj tudi »cepljenje« proti stresu!). Posebna pozornost naj bo tudi na opazovanju okolice in spremljanje posebnosti pri poslovanju, zlasti pol ure po odprtju in pol ure pred zaprtjem poslovalnice, saj se precej ropov zgodi v tem času. Glede prevozov gotovine je pomembno, da se izvajajo v skladu s predpisi. Res je, da večjih ropov transportov vrednostnih pošiljk na srečo v Sloveniji še ni bilo, vendar moramo delovati proaktivno. Izvajalci prevozov se morajo zavedati, da z morebitnim poenostavljanjem poslovnih procesov pri prevozu po nepotreb-



Človek je vsakodnevno izpostavljen različnim vplivom, ki ga bolj ali manj ogrožajo in predstavljajo stalno tveganje za njihovo varnost. V tem kontekstu lahko sodobno družbo primerjam s »hišo strahov«!

nem ogrožajo lastno življenje, ustvarjajo pogoje za možno finančno škodo in negativno vplivajo na ugled podjetja. K večji varnosti prevozov lahko pomembno prispevajo tudi najemniki storitev, ki naj bolj aktivno vključijo v celotno organizacijo prevoza. Razmišljanje, da se tveganja prevoza prenese šele v točki prevzema/predaje je ozko. Nadzor nad opravljanjem storitve, ki je bila zaupana zunanjemu izvajalcu, mora biti stalen in ne prepuščen naključju.

5. Človek je verjetno tisti dejavnik, ki v sistemu zagotavljanja varnosti predstavlja pomembno kategorijo tveganja. Kateri so po vaši oceni tisti ukrepi strateškega managementa vsake organizacije, ki bi tveganja, katera prinaša kadrovski potencial naredila bolj obvladljiva.

Zagotavljanje varnosti človeka je v današnjem globalnem svetu dinamičen proces. V varnostnem okolju se razmere stalno spreminjajo, spreminjajo se oblike in vrste ogrožanj. Varnost človeka obravnavajo različne teorije s področja družbenih, psiholoških in varnostnih študij različno, v ospredje je ta varnost postavljena tudi v konceptu humane varnosti, kot so ga razvili v okviru OZN. Koncept varnosti se v zadnjem času povezuje tudi s koncepti človekovih pravic in svoboščin, ki jih nekateri obravnavajo kot pokazatelje stanja individualne družbene varnosti. Človek je vsakodnevno izpostavljen različnim vplivom, ki ga bolj ali manj ogrožajo in predstavljajo stalno tveganje za njihovo varnost. V tem kontekstu lahko sodobno družbo primerjam s »hišo strahov«!

Človek (z vsemi svojimi potrebami, motivi, stališči in notranjimi osebnostnimi faktorji) pomeni ključni in kritični člen varnostnega sistema, ker vstopa v interakcije s sistemom, zaznava in nadzira nevarnosti, dela napake in popravlja napake. Zlonamerna napaka je odločitev človeka in je iz varnostnega sistema ne moremo izločiti, lahko pa s preventivnimi ukrepi in postopki zmanjšamo njen škodljivi učinek.

6. Varnostna kultura in s tem varnostno zavedanje je na splošno v širši družbeni skupnosti potisnjeno v ozadje. Kako po vaši oceni varnostno kulturo predstaviti kot pomembno vrednoto v posamezni organizaciji in seveda s tem tudi širšem družbenem okolju?

Menim, da varnostno zavedanje ne bo nikoli popolno (kot tudi ni popolne varnosti), saj sta zaznava ogrožanj in varnosti izrazito subjektivno pogojena, z ustreznim usposabljanjem pa se varnostno zavedanje lahko bistveno izboljša. Posebna značilnost varnostnega zavedanja je sorazmerna nepredvidljivost možnega ogrožanja, bolj ali manj verjetnost, ki ne dopušča stalne pripravljeno-



Trenutno stanje na področju korporativne varnosti je boljše kot pred nekaj leti, ko je bila obravnava tega pomembnega področja družbenega življenja bolj v zametkih in razdrobljena po različnih segmentih dejavnosti posamezne organizacije.

sti. Menim, da človek razmišlja o nenormalni situaciji kot o negotovem dogodku nizke verjetnostne narave. Pri tem je pomembno dejstvo, da presoja verjetnosti te situacije vpliva tudi na njegovo vedenje. Osnovni temelj je seznanitev zaposlenih, kaj je varnostna kultura in kaj se od zaposlenih pričakuje. To pomeni, da je potrebno vzpostaviti tako organizacijsko kulturo organizacije, kjer zaposleni intuitivno razumejo usmeritve vodstva o možnih ogrožanjih in tveganjih ter ciljih in koristi, ki naj bi jih prineslo njegovo obvladovanje. Pomemben je formalni sprejem politike upravljanja tveganj v organizaciji (kot norma pričakovanega vedenja), dalje vzpostavitev interne komunikacije za prepoznavo tveganj in sprejemanje ustreznih proaktivnih ukrepov ter postopkov za njihovo upravljanje, razkrivanje glavnih zaznanih tveganj in načinov njihovega obvladovanja lastnikom ter drugim ključnim interesnim skupinam organizacije in vključitev izobraževanja o tveganjih v programe usposabljanja zaposlenih. Z vztrajnostjo se daleč pride, spremembe na tem področju pa ne bodo prišle čez noč, prav tako je to živ, spreminjajoč se proces, ki se neprekinjeno dograjuje in dopolnjuje.

7. V Sloveniji veljate za enega izmed najbolj priznanih in uveljavljenih varnostnih strokovnjakov. Kakšno je po vaši oceni trenutno stanje korporativno varnostnega managementa v Sloveniji?

Hvala za prijazno mnenje. Trenutno stanje na področju korporativne varnosti je boljše kot pred nekaj leti, ko je bila obravnava tega pomembnega področja družbenega življenja bolj v zametkih in razdrobljena po različnih segmentih dejavnosti posamezne organizacije. Sedaj se organizacije pomena korporativne varnosti vse bolj zavedajo in ustanavljajo posebne službe ali zadolžijo zaposlene, da se strokovno ukvarjajo s tem področjem. Pomen varnosti je zelo širok, znanje pa je razpršeno po organizacijskih enotah in večkrat ni koordinacije aktivnosti ter dobrega pregleda nad obstoječim stanjem organizacije ter aktivnostmi za upravljanje tveganj. Trenutno stanje še vedno ni idealno oz. še ni doseglo primerne kvalitete, a se stanje hitro izboljšuje in v bližnji prihodnosti pričakujem, da bo stanje ozaveščenosti glede korporativne varnosti doseglo ustrezen nivo, ko bodo pokrita vsa področja in se bo znanje nadgrajevalo. Gre za izrazit interdisciplinarni strokovni pristop, z uporabo širokega spektra znanj in sposobnosti s področja ekonomije, prava, varnosti, IT, logistike in psihologije. Postati uspešen varnostni manager zahteva čas in kompetentno osebnost.

8. Kaj so po vaši oceni tisti dejavniki, ki so ključni, da bo varnostni management ustrezno prepoznan v organizaciji, kot ključni nedeljiv del glavnega procesa v organizaciji?

Eden od ključnih dejavnikov je naklonjenost vodstva organizacije za obravnavo varnostnih vprašanj in upravljanje tveganj. Vodstvo je zavezano, da prepozna varnost poslovanja kot enega izmed ključnih področij in poveže delovanje varnostnega sistema s poslovnimi cilji organizacije, vse s ciljem, da se tveganja zmanjšajo na sprejemljivo raven. Vpliv na naklonjenost vodstva pa imajo lahko tudi lastniki in/ali posamezni zaposleni, ki se zavedajo pomembnosti tega področja in znajo vodstvu svetovati na prodoren ter učinkovit način. Organizacije se običajno ustrašijo visokih stroškov, ki bi bili lahko povezani z vlaganjem v varnost, vendar se ne zavedajo, kako je na dolgi rok škodljivo, če se na navedenem področju naredi premalo ali celo nič (enkrat bo potrebno plačati, ali proaktivno ali po škodnem dogodku). Seveda tudi druga skrajnost ni priporočljiva, da se varnosti daje prevelik pomen. Skratka, vsakokrat je potrebno pretehtati, kaj določena stopnja varnosti doprinese organizaciji pri njenem osnovnem poslanstvu in kaj želi organizacija doseči (odpira se vprašanje varnosti kot poslovnega stroška). Napaka je tudi, da se poslovne procese gleda kot samostojne enote, kar ni res. So živi procesi, ki se spreminjajo in vplivajo na druge procese, povezljivost mora biti znana in definirana, prav tako morajo biti pomožne storitve definirane in vključene kot pomoč za nemoteno poslovanje organizacije. Kot dobra pomoč služijo obstoječi standardi na področju kakovosti poslovnih procesov in varnosti, ki lahko veliko doprinesejo k razumevanju celovite slike organizacije.

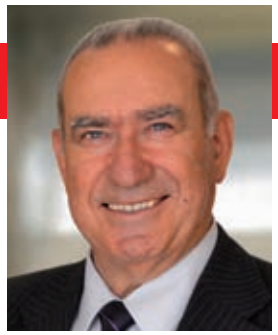
9. Menite, da lahko k dvigovanju strokovne kvalitete in ugleda korporativno-varnostnega managementa svoj del prispevajo stanovska združenja, kot na primer Slovensko združenje za korporativno varnost?

Vsak posameznik ali organizacija, ki se s tem področjem profesionalno ukvarja, lahko doprinese k dvigovanju strokovne kvalitete in ugleda korporativno-varnostnega managementa. Pozitiven pomen delovanja združenja je v tem, da združuje in povezuje organizacije ter posameznike, ki se s tem področjem ukvarjajo. Različnih mnenj in znanja ni nikoli preveč, združenje pa je dobro izhodišče za pospešeno nadgradnjo korporativno-varnostnega managementa, vzgajanje mladih managerjev in pridobivanje novega znanja. Tudi razne strokovne dileme se rešujejo hitreje, če se managerji med seboj poznajo in skupaj rešujejo strokovne težave (kot primer dobre prakse). Že drugačen pogled na težavo/problem lahko prihrani čas, stroške in lahko prispeva k ustrezni rešitvi. Menim, da »skrivanje« znanj in izkušenj ni dobro, ker morajo podatki in informacije čim bolj krožiti, z namenom nadgradnje in izboljševanja varnosti organizacije.

10. Pred kratkim je bil s strani Nacionalne agencije za kakovost v visokem šolstvu dokončno akreditiran nov magistrski program »Management korporativne varnosti«. Menite, da lahko tak program prinese dodatno kvaliteto na področje izobraževanja varnostnih strokovnjakov in s tem tudi njihovo močnejše uveljavljanje v družbi?

Seveda lahko ta program doprinese dodatno kvaliteto. Dobro je, da so izbrani predavatelji tudi iz vrst managerjev, ki se v praksi stalno srečujejo s konkretno problematiko. Teorija in praksa morata iti z roko v roki in ena brez druge ne moreta dajati popolne kvalitete študiju managementa korporativne varnosti. Sam tukaj vidim povezavo v sodelovanju študentov pri projektu kakšnega večjega slovenskega podjetja na področju nadgradnje varnostnega sistema. Študentje morajo v programu videti priložnost za zaposlitev in dodano vrednost novega znanja po uspešno zaključenem programu za organizacijo. Slušatelj programa mora biti sposoben navedeno znanje operativno uporabiti. Več prodornega in samostojnega razmišljanja pa ni nikoli dovolj! ■

Avtor: doc. dr. Milan Vršec / Institut za korporativne varnostne študije*



VAROVANJE POSLOVNEGA INFORMACIJSKEGA SISTEMA NA OSNOVI POLITIKE VAROVANJA INFORMACIJ

Varovanje informacij je že vrsto let top svetovna tema. Pa ne vseh informacij – da se razumemo - temveč samo tistih, ki prinašajo dodano vrednost, razvoj, premagovanje konkurence in poslovno stanje, da si korak pred drugimi.

Gre torej za varovanje poslovnih skrivnosti, varstvo osebnih in tajnih podatkov, zaupne razvojne projekte, zaupne poslovne odločitve in še kaj kar je zaupnega v konkretni organizaciji. Vendar je treba vedeti, da so poslovne informacije uporabne, koristne in učinkovite za konkretni gospodarski subjekt (korporacijo, koncern poslovni sistem, idr.) in za druge le, če so organizirane v nek sistem in prepoznavne kot zaupne. Za ta sistem se je že kar močno uveljavil izraz »poslovni informacijski sistem«, ki združuje poslovno dokumentacijo v klasični in elektronski obliki. Eno od glavnih spoznanj je, da so poslovni informacijski sistemi močno podvrženi napadom od znotraj (človeški viri, okvare, izpadi, informacijske nesreče) in od zunaj (naravne nesreče, informacijski vdori, kriminalni napadi, vohunjenje, prestrezanje, prisluškovanje, idr.). Temu spoznanju sledi drugo, ki pove, da je v gospodarskih družbah in v drugih organizacijah premalo znanja, premalo volje, premalo zavedanja, premalo vnašanja dobrih praks, tu pa tam pa tudi premalo financ za učinkovitejše varnostne mehanizme. Tretje glavno spoznanje pa je, da je veliko vrzeli in varnostnih lukenj pri varovanju poslovnih skrivnosti in drugih zaupnih stvari. Naša spoznanja potrjuje tudi globalna raziskava o varovanju poslovnih skrivnosti, v kateri je sodelovalo 305 vodij informacijske varnosti s celega sveta. Raziskavo je po naročilu korporacij RSA in Microsofta izvedla družba Forrester Consulting (www.microsoft.com/DLP). To pomeni, da se lastniki, upravljavci, nadzorniki in varnostni management občutno premalo ukvarjajo z upravljanjem varnostnih groženj, obvladovanjem varnostnih tveganj in z odpravljanjem varnostnih vrzeli v poslovnih informacijskih sistemih. Tu je v bistvu izhodišče problema, ki bi se ga morali zavedati, lastniki, upravljavci in nadzorniki, še posebej pa varnostni management kot glavni nosilec upravljanja korporativne varnosti. Tiste gospodarske družbe, ki se resno lotevajo varovanja poslovnega informacijskega sistema si izdelajo politiko varovanja informacij in v sistem varovanja uvedejo standarde varovanja informacij in standarde neprekinjenega poslovanja. Kajti poslovni informacijski sistem je sistem, ki mora zagotavljati neprekinjeno poslovanje tudi v izrednih (kriznih) okoliščinah.

Struktura poslovnega informacijskega sistema

Nastanek, urejanje, uporabljanje, pošiljanje, spreminjanje, dodajanje in arhiviranje poslovne dokumentacije o produktih, storitvah, postopkih in procedurah poslovanja omogoča in zagotavlja poslovni informacijski sistem. Gre za funkcioniranje vseh poslovnih funkcij in poslovnih procesov, ki jih upravlja poslovodstvo, izvajajo pa zaposleni v ustreznih organizacijskih enotah. Ker pa je poslovanje določene gospodarske druž-

Tiste gospodarske družbe, ki se resno lotevajo varovanja poslovnega informacijskega sistema si izdelajo politiko varovanja informacij in v sistem varovanja uvedejo standarde varovanja informacij in standarde neprekinjenega poslovanja.

*avtor je član Slovenskega združenja korporativne varnosti

be odvisno tudi od dobaviteljev, poslovnih partnerjev in pogodbenih izvajalcev, navsezadnje pa tudi od konkurence, so sestavni del poslovnega informacijskega sistema tudi podatki in poslovna dokumentacija teh zunanjih dejavnikov. Strukturo poslovnega informacijskega sistema sestavljajo naslednji moduli:

- Upravljavsko-managerski modul - lastniška struktura, lastniki, delničarji, vodstvo in nadzorniki ter vodje posameznih organizacijskih enot, ki potrebujejo informacije za potrebe vodenja in nadziranja;
- Kadrovski modul - podatki vseh zaposlenih, plače, izobraževanje, oprema, drugo;
- Modul proizvodnja produktov in storitev z logistiko - priprava, neposredna proizvodnja**,** nabava, prodaja, skladiščenje, transport;
- Računovodsko-finančni modul, ki zajema bilance uspeha, finance, investicije in bančne transakcije;
- Projektni modul - razvojni projekti, socialni projekti, interdisciplinarni in multidisciplinarni (mednarodni) projekti, okoljski projekti in drugi projekti;
- Komunikacijski modul, ki zajema: intranet, extranet, internet, infranet (prenos alarmnih sporočil) in enkripcijo zaupnih besedil, poslanih po elektronskih medijih;
- Modul družbene odgovornosti po SA 8000 - donatorstvo, humanitarne akcije, odnos do okolja, sponzorstvo, idr;
- Zavarovalni modul (zavarovalni portfelj) - zavarovanje premoženja, osebja, odgovornosti;
- Modul poslovnih partnerjev - dobavitelji, družbeniki, solastniki, drugi;
- Modul pogodbenih izvajalcev - ponudbe, naročila, pogodbe, finančne garancije, nadzor, škode;
- Modul zbranih informacij preko poslovnega poizvedovanja (business intelligence in benchmarking) - informacije o konkurenci in o dogajanjih na trgih.

Moduli so lahko relativno samostojni, vendar so informacijsko, komunikacijsko in varnostno integrirani v celoto poslovnega informacijskega sistema.

Globalne grožnje poslovnemu svetu in varnostni mehanizmi

Na zemeljski obli obstajajo številni prisluškovalni sistemi podprti s satelitsko navigacijo (GPS-ZDA, Galileo.-Evropa Glonass-Rusija Beidou 1/Compas-Kitajska, IRNSS-Indija in drugi), ki prestrezajo elektronske in druge komunikacije. Eden od teh sistemov je ECHELON s številnimi prisluškovalnimi postajami in drugo infrastrukturo kot so denimo centri - s super računalniki za obdelovanje podatkov. Echelon je spoznan kot gigantski in najbolj skrivnosten vohunski sistem, ki so ga razvile ZDA, Kanada, Anglija in Avstralija. Prestreza in prisluškuje mednarodnim telefonskim pogovorom in elektronskim komunikacijam predvsem za interese in koristi velikih korporacij in koncernov, ki si z analizo in uporabo zaupnih podatkov in informacij pridobijo prednosti na svetovnih trgih. Drugi znani in prav tako vohunsko naravnan sistem prisluškovanja je Carnivore (Zver), ki ga upravlja FBI. Zato je šifriranje na bazi kriptografskih algoritmov dobrodošel varnostni mehanizem v mednarodnem elektronskem komuniciranju. V nadaljevanju navajamo nekaj varnostnih mehanizmov, ki prispevajo k višji stopnji varnosti poslovnih informacijskih sistemov.

Ti mehanizmi so:

Simetrična in asimetrična enkripcija (zasebni in javni ključi) zagotavlja varen prenos elektronskih komunikacij. Zanesljivi so 128 in 256 bitni kriptografski algoritmi. Primeri algoritmov: Evklidov algoritem, Dijkstrov algoritem, Algoritem MD5, Evolucijski algoritem, Primov algoritem.

Kvantna enkripcija, ki izhaja iz kvantne teorije in iz Heisenbergovega teorema negotovosti, po katerem kvantne informacije ni mogoče izmeriti. Zaradi tega ni mogoče neopazno prestrezati in prisluškovati elektronskim komunikacijam, kajti vsak poskus prestrezanja se takoj zazna in prenos sporočila se takoj samodejno zaustavi (prekine). Je to morda protiorožje Echelonu?

Enkripcija mobilnih komunikacij, denimo z 256 bitnim kriptografskim algoritmom AES Advanced Encryption Standard.

Penetracijski testi (Penetration Testing) so metoda varnostnega testiranja poslovnih informacijskih sistemov, s katerimi se ugotavljajo morebitne varnostne vrzeli in nato predlagajo izboljšave v strojni, programski in varnostni opremi.

Proti prisluškovalni pregledi poslovnih in drugih prostorov, z namenom, da se najdejo morebitne prisluškovalne naprave in da se hkrati v prihodnje zagotovi profesionalna pristopna kontrola, po potrebi pa tudi proti vlomno varovanje in video nadzor.

Računalniška forenzika preiskuje digitalne nosilce podatkov kot so: CD, DVD, trdi diski, spominske kartice, SIM kartice, USB ključi idr.

Z varnostnim modelom nad varnostne grožnje in konkretne napade

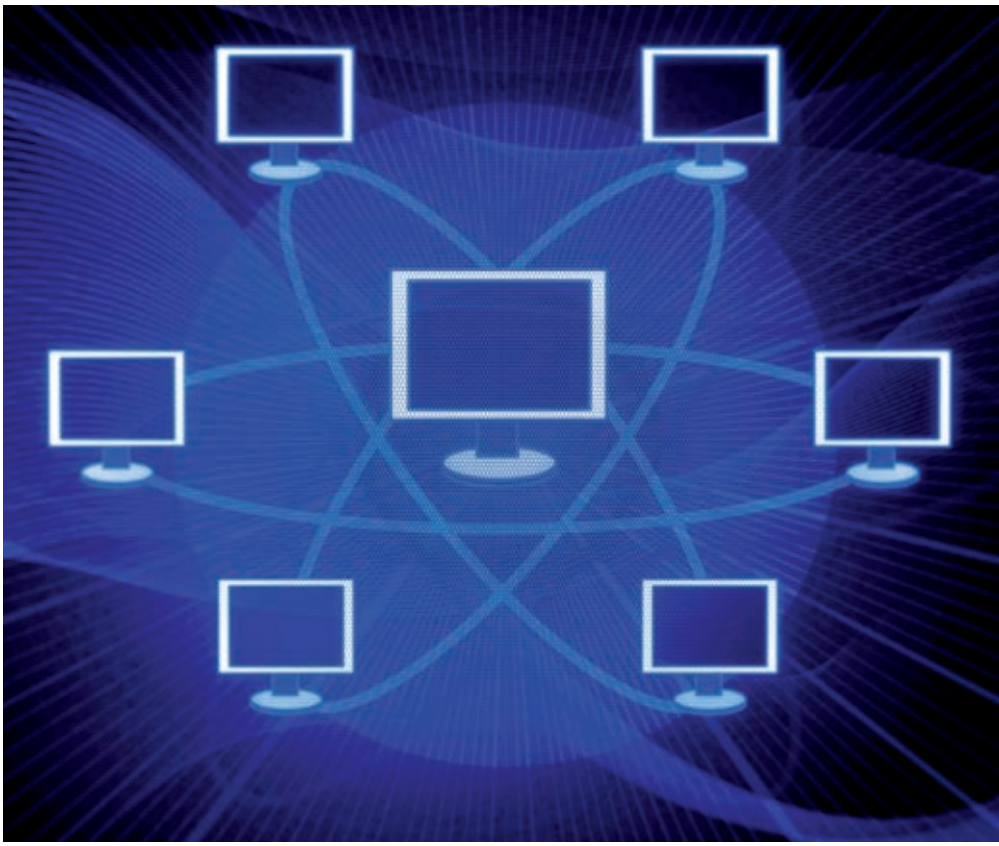
Gospodarske in druge družbe doživljajo vse več raznih napadov na poslovne informacijske sisteme. Na eni strani gre torej za realne varnostne grožnje, na drugi pa za slabosti v informacijski tehnologiji, informacijskih sistemih in upravljavcih in uporabnikih informacij. Vendar pa je treba pomisliti tudi na morebitno multipliciranje slabosti in vrzeli v strojni in programski opremi z napadi od zunaj, kar še poveča ranljivost, ogroženost in tveganja. Na varnostne grožnje in konkretne napade se je treba preventivno odzvati z ustreznim modelom varovanja poslovnega informacijskega sistema (slika v nadaljevanju), ki vključuje identificirane grožnje in napade, krovno in informacijsko varnostno politiko, načrt varovanja strojne in programske opreme na osnovni in rezervni lokaciji ter načrt neprekinjenega poslovanja, vse na bazi varnostnih standardov, standardov neprekinjenega poslovanja in ustreznih poslovnih orodij obvladovanja trgov. Kajti serija standardov varovanja informacij ISO 27000 ponuja široke možnosti celovitega varovanja računalniškega omrežja in celotnega spleta informacij, ki se pretakajo po intranetu, extranetu, internetu in infranetu. Najpomembnejši je sistemski pristop na nivoju celotne organizacije. Sistemski pristop omogočajo standardi varovanja informacij ISO/IEC 27001, 27002 in 27005, ki vključujejo tudi Demingov koncept poslovanja. Za obvladovanje informacijskih tveganj je koristno, da se uporabita še standarda ISO/IEC 31000:2009 – Obvladovanje tveganj – Načela in smernice, ter ISO/IEC 31010:2009 – Obvladovanje tveganj – Ocena tveganja – Tehnike. Standardi omogočajo certificiranje sistema upravljanja varovanja informacij (SUVI), če se gospodarska družba odloči za ta korak.

Model varovanja poslovnega informacijskega sistema

Upravljanje poslovnega informacijskega sistema v celoti je domena službe informatike kot štabne službe, ki upravlja ta sistem na osnovni in rezervni lokaciji. Dostop do profesionalnega upravljanja varovanja poslovnega informacijskega sistema pa ima tudi ustrezna Služba korporativne varnosti, ki mora prav tako imeti status štabne službe.

Poslovni informacijski sistem mora gospodarski družbi omogočati neprekinjeno poslovanje

Načrtovanje neprekinjenega poslovanja (business continuity planning – BCP) je metodologija, ki se uporablja za izdelavo načrta neprekinjenega poslovanja, ki zajema tudi obnovo delovanja ključnih poslovnih in (po potrebi) drugih funkcij podjetja/organizacije/ustanove v primeru kriznih in izrednih razmer. Za uvajanje in upravljanje neprekinjenega poslovanja se uporabljajo tudi različni standardi, ki definirajo načine in postopke uvajanja ter upravljanja neprekinjenega poslovanja. BSI priporočilo PAS 56 predstavlja priporočila za postopke, principe in terminologijo upravljanja neprekinjenega poslovanja, standard BS 25999-1:2006 obravnava minimalne zahteve in dobro prakso pri upravljanju neprekinjenega poslovanja, standard BS 25999-2:2007 pa določa zahteve za vzpostavitev, izvajanje, kontrolo, pregled, vzdrževanje in izboljšave sistema neprekinjenega poslovanja. ISO/IEC 27001 predstavlja standardno specifikacijo za upravljanje učinkovitega sistema nadzora informacijske varnosti (Information Security Management System), z uporabo pristopa stalnih izboljšav. Upravljanje neprekinjenega poslovanja (BCM – Business Continuity Management) poteka po načrtu neprekinjenega poslovanja (BCP-Business Continuity Plan), ki je izdelan po standardu BS 25999 in po standardih varovanja informacij ISO/IEC 27001 in 27002. Zagotavljanje neprekinjenega poslovanja daje gospodarski družbi določene konkurenčne prednosti. V prvi vrsti omogoča načrtno upravljanje s hudimi motnjami, ki jih povzročajo izredni dogodki; hkrati pa zagotavlja proces preprečevanja škod in izgub (Loss Prevention). Za obvladovanje neprekinjenega poslovanja in kriznega vodenja so poleg močnega kriznega štaba potrebni tudi močna služba informatike, močna služba za upravljanje korporativne varnosti in ustrezno organizirana zaščita in reševanje – štab CZ. To so atributi brez katerih se ne moremo pogovarjati o uspešnem organiziranju in poslovanju v kriznih okoliščinah.



Če si gospodarska družba ali pa kakšna druga organizacija želi vzpostaviti ali obdržati sloves zanesljivega partnerja, si mora zgraditi profesionalne varnostne mehanizme, da ne pride do izginotja, kraje, poškodovanja ali uničenja posameznih delov poslovnega informacijskega sistema.

Sklepna beseda

Poslovni informacijski sistem je glavna baza urejenih podatkov za lastnike, upravljavce, management, nadzornike, poslovneže, tržnike, inovatorje, kadrovike, računovodje, vrhunske strokovnjake, varnostni management in vse druge, ki pri svojem delu in poslovanju potrebujejo delček podatkov in informacij tega sistema. Vsi podatki, ki so potrebni za normalno funkcioniranje poslovnih procesov morajo biti na razpolago, zaupne pa je treba pri uporabi maksimalno učinkovito varovati. Na zaupnem segmentu je poslovni informacijski sistem izredno ranljiv in ogrožen zlasti, ko gre za izvirno znanje, bogat intelektualni kapital, kakovostne, drage in priznane blagovne znamke, inovacije, patente, visoko konkurenčno sposobnost in širok splet poslovnih skrivnosti. Če si gospodarska družba ali pa kakšna druga organizacija želi vzpostaviti ali obdržati sloves zanesljivega partnerja, si mora zgraditi profesionalne varnostne mehanizme, da ne pride do izginotja, kraje, poškodovanja ali uničenja posameznih delov poslovnega informacijskega sistema. Zato je nujno, da se poleg fizičnega in tehničnega varovanja v varnostni sistem uvedejo tudi ustrezni standardi in sodobna managerska orodja varovanja poslovnih procesov. To je tudi nujni pogoj za zagotavljanje neprekinjenega poslovanja in obvladovanja kriznega vodenja. ■

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

INTERVJU
Ga. Medeja Lončar, direktorica in
mag. Igor Kulašič, vodja divizije tehnične opreme objektov, Siemens d.o.o.**

NOVA SPOZNANJA IN PREVERJENE REŠITVE NAM OMOGOČAJO VAREN RAZVOJ NAŠIH ORGANIZACIJ

Kompleksno varnostno okolje nas sili v smeri celovitih pristopov k obvladovanju tveganj katerim so izpostavljene naše organizacije. Znanje, dobre prakse in novi produkti so tisti dejavniki, ki jih v naše okolje prinaša podjetje Siemens in s tem širi možnosti integriranih pristopov na področju obvladovanja tveganj.

Ga. Medeja Lončar

1. Vodite Siemens Slovenija, ki je del svetovno priznane in razvejane multinacionalne korporacije Siemens. Kako se strateški management vašega podjetja odziva na dinamične spremembe v svetovnem ekonomskem okolju in seveda s tem povezana tveganja?

Trenutno delujemo v res zahtevnih okoliščinah, smo ena manjših regionalnih družb korporacije Siemens, vendar smo zavezani izpolnjevati iste standarde korporacijskega upravljanja kot če bi delovali na deset ali večmilijonskem trgu. Poleg tega so razmere po Evropi, še zlasti pa v Sloveniji, negotove, finančni viri so težko dostopni in posledica so, med drugim, manjša vlaganja v tehnologije in infrastrukturo. Temu se poskušamo prilagajati z učinkovito in vitko organizacijo, zaradi katere Siemens d.o.o. v korporaciji velja za primer dobre prakse, s fleksibilnostjo pri nastopu na trgu, pa tudi z drugačnimi trženjskimi prijemi, s katerimi poskušamo ključnim kupcem zagotavljati produkte in rešitve za cel spekter njihovih potreb.

2. Skoraj ga ni segmenta moderne družbe, kjer Siemens ne bi bil prisoten s svojimi produkti in tehnološkimi rešitvami. Ta razvejanost pred vas kot managerko postavlja zahtevne dileme kako upravljati s tako kompleksnim sistemom, ki je prisoten na tako raznovrstnem področju? Kakšna je vaša formula za uspešno poslovanje?

Res je, Siemens v svojih štirih sektorjih ponuja med sabo zelo različne tehnologije, zanje praviloma odločitve v podjetjih sprejemajo povsem različne strukture odločevalcev, uporaba tehnologij pa zahteva tudi zelo različne spektre strokovnih znanj. Siemens ima sicer matrično organizacijo, v kateri vertikale (sektorji) igrajo močno vlogo, imajo utečene sisteme vodenja, planiranja in poročanja in zato managerjem regionalnih družb ni potrebno v podrobnosti obvladovati specifik posameznega sektorja ali divizije. Po drugi strani je slovenski trg majhen in ni težko poznati ali pa celo osebno spremljati vseh pomembnejših projektov. Ker v Siemensovem svetu ve-

> Smo ena manjših regionalnih družb korporacije Siemens, vendar smo zavezani izpolnjevati iste standarde korporacijskega upravljanja kot če bi delovali na deset ali večmilijonskem trgu.

*avtor je član Slovenskega združenja korporativne varnosti
**Siemens je korporativni član slovenskega združenja korporativne varnosti

ljamo za eno najmanjših regionalnih družb, nam je morda tudi lažje kot kolegom v večjih državah iskati sinergije med divizijami in pristopati h kupcem celovito in s širšim portfeljem.

3. Raziskave in razvoj imajo verjetno na strateškem nivoju vaše korporacije pomembno mesto za ohranjanje ustreznega tržnega deleža v svetovnem merilu. S tem pa so povezana raznovrstna tveganja varovanja ključnih informacij in patentov pred neposrednimi konkurenti?

Razvoj, raziskave in inovacije so, razen ljudi, najpomembnejše imetje korporacije in osnovni gradnik konkurenčne prednosti. Siemens v raziskave in razvoj vlaga približno 4 milijarde evrov letno, to je okoli 5 odstotkov vseh prihodkov. Rezultat teh vlaganj je tudi več kot 8900 prijavljenih inovacij in 4600 vloženih patentov v letu 2012, kar je novi rekord v Siemensovi zgodovini. Seveda je v interesu korporacije, da to imetje skrbno varuje, in Siemens dejansko veliko vlaga v tehnologije za zagotavljanje varnosti, v procese, ki pomagajo varovati to imetje, predvsem pa v osveščanje svojih zaposlenih. Tudi najboljša tehnologija ne pomaga, če se zaposleni ne zavedajo tveganj ali jih podcenjujejo. To velja za vse sodelavce, ne glede na funkcijo, ki jo opravljajo.

Formula za uspešno poslovanje v mojem oziroma Siemensovem primeru je, da si prilagodljiv, odprt za nove priložnosti, dosleden pri osnovnih načelih in usmeritvah ter da imaš dobro vzpostavljeno mrežo sodelavcev tudi v sektorjih in centralnih funkcijah v drugih regionalnih družbah ter na sedežu korporacije in regije.



4. Korupcija je velik problem vseh družbenih okolij, vključno s Slovenijo. Siemens ima na tem področju od nedavnega ničelno toleranco do teh primerov deviantnosti. Kako uspevate s tem pristopom do preprečevanja korupcije zagotavljati uspešno poslovanje podjetja?

Po uvedbi kompleksnega in strogega programa skladnosti poslovanja je Siemens dosegel zelo dobre poslovne rezultate in visoke stopnje rasti prihodkov. S tem je vodstvo korporacije na globalni in regionalnih ravneh posredovalo vsem zaposlenim zelo pomembno sporočilo, da se skladnost in poslovna uspešnost ne izključujeta, temveč gresta z roko v roki. Tematika je zelo aktualna, zato bo v prihodnosti poštenost, etičnost in skladnost poslovanja lahko postala konkurenčna prednost, denimo v situaciji, ko se na nek razpis prijavi več ponudnikov s podobno tehnologijo in ceno. V nekaterih poslovnih okoljih so v postopke javnega naročanja proaktivno začeli vgrajevati mehanizme, ki zagotavljajo transparentne, racionalne, nadstandardne postopke in s tem bolj pošteno porabo davkoplačevalskega denarja in povečevanje konkurenčnosti nekega okolja.

5. Je pot sodelovanja z raziskovalnimi institucijami po vašem mnenju tista, ki za Siemens tudi v Sloveniji prinaša dodano vrednost in širjenje dobrih praks ter novih produktov?

Siemens intenzivno sodeluje z raziskovalnimi ustanovami, tudi v Sloveniji, čeprav tukaj nimamo kompetenčnih centrov in raziskovalno-razvojnih oddelkov, ki se primarno ukvarjajo z razvojem novih izdelkov. V Sloveniji sicer sodelujemo predvsem pri razvoju inovativnih rešitev na osnovi naših izdelkov. Poleg tega, da podpiramo strokovne prireditve, ki jih organizirajo različne izobraževalne in raziskovalne ustanove in so pomemben način prenosa dobrih praks, bi omenila tudi sodelovanje s Centrom za energetsko učinkovitost Instituta Jožef Stefan pri izdelavi študije Trajnostna mestna infrastruktura - Ljubljana - Pogled v leto 2050. Že zelo dolgo imamo utečeno sodelovanje s tehničnimi fakultetami, kjer uporabljajo našo opremo za laboratorijsko in raziskovalno delo...

6. Na tako zahtevnem položaju so obremenitve zelo velike. Kje uspete najti ustrezno energijo in uskladite službene in družinske obveznosti?

Z nogami stojim trdno na zemlji, novih projektov se lotevam z optimizmom, izzive jemljem športno. Zanima me veliko stvari, družina, literatura, potovanja in druge prostočasne aktivnosti pa mi dajejo veliko energije, ki mi v službi še kako prav pride.

Mag. Igor Kulašič

7. Trenutno vodite divizijo tehnične opreme objektov. Ocenjujete, da je stopnja varnostnega zavedanja strateškega managementa v podjetjih in organizacijah na ustreznem nivoju, da se uspejo zavedati pomena celovitih pristopov do obvladovanja varnostnih tveganj?

Vodstva podjetij se vedno bolj zavedajo pomena varnosti, kar kažejo tudi investicije v tehnološko opremo. Mislim, da je v Sloveniji zelo malo podjetij, ki ne bi imela vsaj osnovnih procesov in tehnologij za zagotavljanje varnosti, k čemur zagotovo prispevajo tudi formalne, regulativne zahteve. Malo manj pa je organizacij, ki so k upravljanju varnostnih tveganj pristopila strateško in celovito, prav tako razmeroma malo organizacij na investicijo v tehnologije za zagotavljanje varnosti gleda preko stroškov celotnega življenjskega cikla, torej nakupa, porabe energetskih virov, upravljanja, vzdrževanja in nadgrajevanja. Razlogov za to je več: slovenski ponudniki so večinoma specializirani na določen segment korporativne varnosti, zato kupci nimajo celovitega pregleda nad tehnološkimi možnostmi.

8. Kakšni koraki bi bili potrebni v smeri povečanja tega zavedanja in kaj lahko Siemens kot svetovna korporacija naredi na tem področju?

Poleg tega tudi poslovna funkcija direktorjev za korporativno varnost v marsikaterem podjetju še nima moči in veljave, ki bi omogočila celovito obravnavo tovrstne tematike.



Bistveno vlogo igra znanje in informiranost, zato so strokovni dogodki, kakršen je Dnevi korporativne varnosti, zelo pomembni za razvoj stroke. V interesu vseh igralcev na trgu tehnologij in storitev korporativne varnosti je, da tovrstne dogodke podpirajo. Več znanja in zavedanja lahko vodi tudi k drugačnim zahtevam in izhodiščem na strani kupcev. Ti se vedno večkrat sprašujejo, kaj želijo doseči z določeno tehnološko rešitvijo. Varnostnega sistema torej ne obravnavajo več zgolj kot nujno zlo. Tudi servisiranje varnostnih sistemov v tujini praviloma poteka v kontekstu celovitega izboljšanja funkcionalnosti, ne zgolj odpravljanja tehničnih napak. V Siemensu skušamo našim kupcem predstaviti kar se da celovit pogled na tehnično opremo v objektu, ker ponujamo celovit portfelj izdelkov, lahko z integracijo različnih sistemov dosežemo veliko sinergij in optimiramo porabo virov.

9. Pomembna dilema, ki se odpira v tem dinamičnem varnostnem okolju je učinkovito varovanje kritične infrastrukture katera je nujna za normalno delovanje širše družbene skupnosti. Kako v Siemensu pristopate do teh novih izzivov v Sloveniji in kako v realno okolje prenašate primere dobrih praks iz mednarodnega okolja?

Gre za izjemno pomembno vprašanje, še zlasti v času ekonomske krize. Nezadovoljstvo širše javnosti prinaša mnogo izzivov pri zagotavljanju varnosti uporabe javne infrastrukture, tukaj gre za tematiko, ki ji v preteklem obdobju ekonomske rasti marsikdo ni posvečal pretiranega pomena. Poleg tega pa ekonomska kriza prinaša tudi veliko izzivov, povezanih z investicijami v varnostne tehnologije. Pri varnostnih vprašanjih smo za nameček vedno soočeni z dilemo med zagotavljanjem zasebnosti in zagotavljanjem varnosti. Vse te okoliščine seveda bistveno prispevajo h kompleksnosti tematike. V Siemensu veliko vlagamo v spremljanje trendov in analitiko, ki nam pomaga pri odločanju o tem, katerim razvojnim projektom in tehnologijam dati prioriteto, predvsem pa nam pomagajo biti celovit sogovornik mestom na področju trajnostne urbane infrastrukture, ki vključuje tudi varnostni aspekt. Primer takšnega celovitega reševanja infrastrukturnih izzivov je nizkoemisijska cona v Londonu, kjer je Siemens dobavil tehnologije za videonadzor registrskih tablic vozil, vendar pa mesto s to tehnologijo, poleg varnosti, rešuje problem trajnosti prometa in čistega zraka v središču mesta. Raziskovalne projekte izvajamo tudi v Sloveniji, v lanskem letu smo zaključili študijo z naslovom Trajnostna urbana infrastruktura – pogled do leta 2050, kjer

smo sodelovali s Centrom za energetsko učinkovitost Instituta Jožef Stefan. Je pa dejstvo, da je Slovenija bistveno manj kompleksno okolje kot velika mesta, ki sicer – tako zaradi finančne moči kot tudi zaradi bistveno višjih tveganj – med prvimi implementirajo sodobne, inovativne tehnologije.

10. Produkti in rešitve vaše divizije se pri večjih projektih povezujejo tudi z vsebinami drugih Siemensovih divizij. Obstaja primer dobre prakse, kjer je vaša divizija pri določenem projektu imela težiščno vlogo pri izvedbi projekta ali se v teh okvirih pojavljate bolj kot podpora ostalim večjim infrastrukturnim projektom?

Dober primer tovrstnega sodelovanja so energetski objekti, tudi objekti industrijskih proizvajalcev, kjer se običajno odločijo za določen segment Siemensovih tehnologij, sčasoma pa preko sodelovanja ta portfelj lahko dopolnimo in ga – seveda v kupčevo korist – optimiramo. Dejstvo pa je, da so v slovenskih podjetjih odločevalci za tehnologije s področja tehnične opreme objektov, ali pa, denimo, avtomatizacije proizvodnje, povsem različni in marsikje še niso prepoznali pomena medsebojnega sodelovanja.

11. Menite, da je okolje strokovnih združenj, kot na primer Slovensko združenje korporativne varnosti, tisto ustrezno za izmenjavo dobrih praks, novih rešitev in spoznanj, ki lahko pomembno vpliva na dvigovanje splošnega zavedanja pri odgovornih strukturah v organizacijah javnega in gospodarskega okolja?

Absolutno. Še zlasti v oteženih gospodarskih razmerah je za vse akterje dobro, da strateško razmislijo o svojem položaju na trgu, mreženje in izobraževanje pa pri tem igra veliko vlogo.

12. Kljub temu, da tehnične rešitve danes doživljajo neverjeten obseg, človek še vedno ostaja najpomembnejši segment v celovitem sistemu zagotavljanja varnosti. Kako zagotavljate procese izobraževanja svojih zaposlenih in nenazadnje tudi končnih uporabnikov vaših storitev?

Osveščanje in informiranje je prvi, morda tudi najpomembnejši korak. V Siemensu intenzivno delamo na zagotavljanju korporativne varnosti preko internih izobraževanj v živo ali preko spleta. Format spletnih izobraževanj vključuje kopico vsakodnevnih situacij in nas opozarja na tveganja, s tem pa močno prispeva k senzibiliziranju zaposlenih. Kot kompleksna organizacija smo izpostavljeni tudi kompleksnim varnostnim tveganjem, torej mnogo izzivov, ki so relevantni tudi za naše kupce, že poznamo iz prve roke. ■

V Siemensu veliko vlagamo v spremljanje trendov in analitiko, ki nam pomaga pri odločanju o tem, katerim razvojnim projektom in tehnologijam dati prioriteto, predvsem pa nam pomagajo biti celovit sogovornik mestom na področju trajnostne urbane infrastrukture, ki vključuje tudi varnostni aspekt.



4. mednarodna konferenca

SIEMENS

Generalni sponzor

Dnevi korporativne varnosti

Upravljanje korporativne varnosti — novi pristopi in izzivi prihodnosti

Ljubljana, 20.—21. marec 2013

Plaza hotel Ljubljana

ICS

Institute for Corporative Security Studies

Kotizacija znaša 250 eur + DDV in vključuje:

vrsto odličnih predavanj z aktualnimi temami,
konferenčno gradivo in CD s predavanji,
knjigo »Management of corporate security - New Approaches and Future Challenges«,
revijo Korporativna varnost (3. številka),
kosilo (sreda in četrtek) v hotelski restavraciji,
slavnostno večerjo z degustacijo vrhunskih vin (v sredo zvečer)...

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

Soorganizator

SECSA
SE Europe Corporate Security Association

Zlati sponzor

Nova panorama
družba za integrirano varovanje

Medijski sponzorji

a&S ADRIA

ZAŠTITA
CROATIAN SECURITY MAGAZINE

SVIJET SIGURNOSTI
Vodeći izvor informacija iz područja sigurnosti
www.svijetsigurnosti.com

Avtor: mag. Miran Vršec / Institut za korporativne varnostne študije-ICS, Ljubljana*



KOLUMNA
miran.vrsec@ics-institut.si

SODOBEN VARNOSTNI SISTEM V PODJETJU – STROŠEK ALI INVESTICIJA

Naj svoja razmišljanja povezana s problematiko dojemanja varovanja kot investicije začnem z naslednjo mislijo:

»Sleherni vložek v varnostni sistem pomeni dodano vrednost pri človeških virih, poslovnih rezultatih, obvladovanju trga in pri družbeni odgovornosti.«

(Vršec Mil. in Vršec Mir., Čaleta D.,
Institut za korporativne varnostne študije, 2011)

Z varovanjem je podobno kot z zdravjem. Ko smo zdravi pretirano ne razmišljamo o tem, kaj vse je potrebno storiti za to, da bi ostali še naprej zdravi. Je že res, da se vedno več ljudi zaveda, da je za to, da si zdrav, potrebno največ vlagati v zdravje ravno takrat, ko si zdrav. Pa vendar se vprašajmo, koliko smo takrat, ko smo zdravi, zares pripravljeni vlagati v naše zdravje (pri tem seveda ne mislim samo na denarne vložke), ko pa smo vendar zdravi. Ko zboliš, postane zavedanje o tem, da smo verjetno storili premalo za svoje zdravje, ko smo bili še zdravi, zato so posledice odprave bolezni vedno - bolj ali manj - boleče, ne samo z vidika bolečine kot take, ampak tudi z drugih vidikov, kot npr.: omejenosti gibanja, izoliranosti od družbe in dogajanja v družbi, z vidika stroškov ipd. Kaj se torej dogaja? Ko izgubljamo zdravje postajamo manj operativni, manj produktivni, bolj občutljivi in ne nazadnje tudi socialno bolj ogroženi, saj nam prihodek praviloma pada, stroški pa naraščajo. Tu poleg stroškov zdravljenja predvsem mislim širše, tudi na ostale stroške, ki niso neposredno povezani z zdravljenjem (logistika, rehabilitacija, morebitna izguba službe ipd.). V Republiki Sloveniji je bil celo ustanovljen Institut za varovanje zdravja, katerega poslanstvo je med drugim usmerjeno v prispevanje k boljšemu zdravju in blaginji prebivalcev Slovenije, kar pomeni, da na nacionalnem nivoju obstaja zavedanje o zdravju kot blaginji in pomenu vlaganja v zdravje.

Verjetno bi se na tam mestu lahko vprašali, kakšno vezo pa ima zdravje z varovanjem?

Kaj hitro lahko ugotovimo, da prav neke neposredne povezave verjetno res nima, lahko pa iz mojih razmišljanj kljub temu potegnemo analogijo in ugotovimo, da je vsebina pojmov v mojem kontekstu razmišljanja dokaj podobna. Tudi z varnostjo je zelo podobno kot z zdravjem. Ko se ne počutimo ogroženi, ko podjetje v nekem okolju posluje sinergično z okoljem, ko procesi potekajo nemoteno, ko je stopnja zadovoljstva zaposlenih, poslovnih partnerjev in drugih akterjev, ki so tako ali drugače povezani s posameznikom ali organizacijo kot tako, pretirano ne razmišljamo o tem, kaj vse je potrebno storiti za to, da bi ta blaginja bivanja, delovanja in/ali poslovanja ostala takšna kot je. Iz lastnih poslovnih izkušenj lahko povem, da takrat veliko ljudi na osebnem in poslovnem nivoju pretirano ne razmišlja o vlaganjih v zmanjševanje tveganj, če pa le teh ni, saj vse teče »kot po maslu«. Pa jih res ni? Pravi guruji menedžmenta in ekonomije znajo povedati, da je potrebno takrat, ko ti gre najbolje, ko organizacija dosega najboljše rezultate, da je takrat pravi trenutek za to, da razmišljaš o obvladovanju

Pravi guruji menedžmenta in ekonomije znajo povedati, da je potrebno takrat, ko ti gre najbolje, ko organizacija dosega najboljše rezultate, da je takrat pravi trenutek za to, da razmišljaš o obvladovanju stroškov in vlaganju v razvoj, tudi v iskanje in razvoj rešitev, ki nam bodo pomagale zagotavljati neprekinjeno delovanje in poslovanje na dolgi rok. Takrat so misli čiste, okolje primerno in sredstva zagotovljena.

*avtor je član Slovenskega združenja korporativne varnosti



stroškov in vlaganju v razvoj, tudi v iskanje in razvoj rešitev, ki nam bodo pomagale zagotavljati neprekinjeno delovanje in poslovanje na dolgi rok. Takrat so misli čiste, okolje primerno in sredstva zagotovljena. Takrat so učinki vlaganj optimalni, poudarjam optimalni in ne maksimalni, kajti maksimalni učinki na dolgi rok vedno niso optimalni. Ko se zgodi škoda, ko poslovni proces zastane, takrat postane zavedanje o tem, da smo verjetno storili premalo za svojo osebno varnost in/ali varnost organizacije. Takrat so posledice odprave napak in ponovnega zagona procesov boleče in predvsem drage (posredni in neposredni stroški odprave posledic škod, izpad proizvodnje ali storitev, izguba ugleda, zmanjševanje konkurenčnih prednosti in dobička ipd.). Osnovni problem, ki ga še vedno, in na žalost vedno bolj zaznavam, je nizka stopnja zavedanja posameznikov in odgovornih ljudi v organizacijah, da je s skrbjo za varnost podobno kot s skrbjo za zdravje, da je za zagotavljanje optimalnega obvladovanja tveganj in optimalne stopnje varnosti v osebnem ali poslovnem okolju potrebno preventivno delovanje. To delovanje temelji na naslednjih izhodiščih: pravočasnem prepoznavanju (identifikaciji) tveganj, ki se pojavljajo v našem osebnem ali poslovnem okolju, določitvi verjetnosti nastanka škodnega dogodka, ki izvira iz prepoznanih tveganj, določitvi realne stopnje ranljivosti in ogroženosti nas samih in/ali organizacije in iskanje ustreznih resursov in rešitev za celovito obvladovanje prepoznane ranljivosti, ogroženosti in tveganj.

Pri iskanju resursov za implementacijo rešitev v prakso je potrebno izhajati iz Cost/Benifit metode. Za vsako rešitev je torej potrebno najti ustrezne resurse (notranje in/ali zunanje) in ugotoviti dodano vrednost angažiranja posameznega resursa v prakso. Naši izvedeni projekti reorganizacije in racionalizacije varnostnih sistemov v različnih organizacijah javnega in zasebnega prava in tudi pri posameznikih so dokazali, da varovanje ni in ne sme biti strošek, ampak investicija. Pri teh projektih smo uspeli posameznike in/ali odgovorne osebe v organizacijah prepričati ravno v to, da nemoteno delovanje in poslovanje organizacije v realnem času še ne pomeni, da bo ta organizacija tako delovala tudi jutri, pojutrišnjem, čez leto in še dlje, če ne bo pravočasno prepoznala čeri in zveri, ki jo čakajo in prežijo nanjo na njeni poti, in pravočasno uvedla v svoje poslovanje ukrepe s katerimi se bo tem čerem in zverem izognila, oziroma če ne gre drugače, vsaj omilila posledice bližnjih srečanj z njimi.

Naj ob zaključevanju svojih razmišljanj dodam še eno ugotovitev:

> *»Prihranek zaradi investicije v varnostni sistem in od povečane stopnje varnosti, ki iz tega izhaja, ter dodatni zaslužki iz zmanjšanja škod in izgub predstavljajo za podjetje čisti dobiček.«*
>
> (Green, G., Purpura, P., 1989: Modern Security and Loss Prevention Management. Boston, London. Butterworth Publishers)

Naj tudi v skrb za varnost vnesemo nekaj pozitivne filozofije razmišljanja in delovanja, kot to vse bolj uspešno počnemo na področju skrbi za zdravje. Verjemite, da se obnese in velikokrat zelo malo stane. Tako bodo samovarovalni in varnostni mehanizmi postali pomembno osebno in/ali poslovno orodje za krepitev osebnosti in/ali blagovne znamke, krepitev dobrega imena, nemoteno delovanje in povečevanje dodane vrednosti, ki se pri posamezniku izkazuje skozi kvaliteto življenja, v organizaciji pa skozi povečevanje konkurenčnih prednosti in dobičkonosnosti poslovanja. ■

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

INTERVJU
G. Gregor Majcen
Direktor Urada Republike Slovenije za varovanje tajnih podatkov**

USTREZEN SISTEM VAROVANJA TAJNOSTI KLJUČ ZA USPEŠNO DELOVANJE ORGANIZACIJE

Menim, da se varnost vse prevečkrat jemlje za samoumevno in se o izboljšavah ter previdnosti začnemo spraševati šele ob odpravljanju posledic nekega neprijetnega dogodka. Dvig varnostne kulture ne pomeni vnašanje nekega nedorečenega strahu ali celo paranoje, ampak zavedanje dejanskih nevarnosti.

1. Na področju upravljanja sistema varovanja tajnih podatkov je ključna institucija v državi Urad Republike Slovenije za varovanje tajnih podatkov. Nam lahko zaupate, katere so tiste ključne naloge, ki jih urad izvaja na podlagi zakonskih predpisov?

Naloge in pristojnosti UVTP so določene v Sklepu o ustanovitvi, nalogah in organizaciji UVTP ter seveda v področni zakonodaji. Na kratko bi naše naloge lahko strnil v spremljanje stanja na področju določanja in varovanja tajnih podatkov, skrb za razvoj tega področja, skrb za izvajanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov, sodelovanje s sorodnimi organi tujih držav in mednarodnimi organizacijami, potrjevanje izpolnjevanja predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa tujim državam in organizacijam. Urad izdaja dovoljenja za dostop do tujih tajnih podatkov, varnostna potrdila za sisteme in naprave za prenos, hrambo in obdelavo tajnih podatkov ter navodila za ravnanje s tajnimi podatki tuje države ali mednarodne organizacije. Poleg tega pripravlja predpise, potrebne za izvajanje ZTP, daje mnenja o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov z ZTP, usklajuje delovanje državnih organov, pristojnih za varnostno preverjanje, in predlaga ukrepe za izboljšanje varovanja tajnih podatkov. Vodimo tudi evidence, predpisane z zakonom, ter organiziramo in izvajamo usposabljanja s področja varovanja tajnih podatkov in še bi lahko našteval.

2. Urad ste prevzeli od svojega predhodnika mag. Milana Tarmana v zelo dobrem stanju. Je bila podlaga za nadaljevanje vašega dela ter izvedbo vaše strategije in vizije razvoja ustrezna?

Res je, ob mojem nastopu je bil Urad v dobrem stanju in upam si trditi, da je še vedno. Morda mi je bilo ob nastopu lažje, ker izhajam z varnostnega področja, poleg tega sem že prej delal v Uradu. Urad je dobro organiziran in uveljavljen v domačem ter mednarodnem okolju. Veliko pomembnih nalog je bilo pod prejšnjim vodstvom že opravljenih, tu so tekoče naloge, seveda pa nam dela, projektov in idej tudi za naprej ne manjka. Moja želja in namen sta ohranitev dobrega položaja Urada, nadaljevati z mednarodnim povezovanjem ter predvsem omogočati gospodarskim subjektom podporo in informacije, ki jih potrebujejo, da bodo lahko lažje sodelovali pri poslih, povezanimi s tajnimi podatki na domačem in tujih trgih. Želim si, da je Urad prepoznaven, da aktivno sodeluje z gospodarsko diplomacijo, gospodarsko zbornico, GOIS-om oziroma da deluje povsod tam, kjer smo lahko koristni. Dogaja se namreč, da predstavniki posameznih gospodarskih subjektov glede tajnih podatkov niso prepričani, na koga se obrniti za informacije, zato lahko enostavno rešljiv problem postane ovira. Poleg tega imamo tudi razvejano mrežo stikov s sorodnimi tujimi varnostnimi organi, kar je prav tako lahko v

*avtor je član Slovenskega združenja korporativne varnosti
**UVTP je korporativni član slovenskega združenja korporativne varnosti



veliko pomoč. Seveda smo vedno pripravljeni nuditi podporo znotraj javne uprave in gospodarstvu.

3. Kateri so po vaši oceni tisti ključni izzivi, s katerimi se boste morali na UVTP v prihodnje še posebej ukvarjati?

Kakor sem že omenil, je to prav gotovo intenzivna povezava z gospodarstvom in pomoč gospodarstvu, velik izziv prinaša razvoj različnih novih tehnologij, nadaljevati moramo z usklajevanjem standardov varovanja tajnih podatkov s standardi EU in NATO, pa tudi sprememba oziroma posodobitev domače zakonodaje na področju varovanja tajnih podatkov je prav gotovo eden izmed ključnih izzivov. Poleg naštetega bi omenil tudi, da smo zelo aktivni pri sklepanju sporazumov o izmenjavi in medsebojnem varovanju tajnih podatkov z državami, s katerimi sporazum še ni sklenjen, pa bi bilo to potrebno. Gre za sporazume, s katerimi se izenačujejo pogoji varovanja tajnih podatkov oziroma so ti sporazumi ustrezna pravna podlaga, da do izmenjave sploh lahko pride. Trenutno imamo sklenjenih in ratificiranih dvajset sporazumov, približno deset pa jih je v različnih fazah postopka. Treba je dodati, da pri pobudah za sklenitev tovrstnih sporazumov izhajamo iz potreb oziroma pobud drugih državnih organov in gospodarstva. Pri tem seveda ne gre pozabiti glavnega poslanstva in ključnega izziva urada, to je dvig varnostne kulture. Menim, da se varnost vse prevečkrat jemlje za samoumevno in se o izboljšavah ter previdnosti začnemo spraševati šele ob odpravljanju posledic nekega neprijetnega dogodka. Dvig varnostne kulture ne pomeni vnašanje nekega nedorečenega strahu ali celo paranoje, ampak zavedanje dejanskih nevarnosti.

4. Moderno dinamično varnostno okolje prinaša nove grožnje, med katerimi so še posebej izpostavljene kibernetske grožnje. Nam lahko zaupate prihodnje aktivnosti Urada za obvladovanja teh tveganj?

Pri tem je treba izhajati iz vloge Urada, kakor je zakonsko opredeljena. Ne želim napovedovati prihodnjih odločitev, ki se bodo sprejemale v RS. Kot skrbniki področja tajnih podatkov se moramo zavedati, in seveda se tudi zavedamo groženj, ki izhajajo iz kibernetskega okolja. Področje našega dela že zdaj glede akreditacij komunikacijsko informacijskih sistemov vključuje skrb za varovanje tudi pred tovrstnimi grožnjami. Pri tem mislim predvsem na prenos podatkov s šifrirno zaščito, zaščito TEMPEST in zelo omejen pristop glede priključevanja omrežij na internet. Ta del našega dela usklajujemo v tesni povezavi z vsemi pristojnimi ministrstvi in s CERT-om. Na to področje smo pozorni pri rednem delu in tudi pri pripravi strateških dokumentov. Poleg naštetega se z omenjenim področjem srečujemo tudi prek stikov s tujimi sorodnimi službami, saj imajo nekatere med njimi širši nabor nalog in je pod njihovo pristojnostjo tudi kibernetska varnost, tako da dobivamo koristne informacije s tega področja. Poudaril bi, da na tem segmentu nismo primerljivi s sorodnimi tujimi službami, saj so zakonske pristojnosti, organizacijski pristopi in rešitve za obvladovanje teh tveganj pač različne.

5. V pripravi je osnutek novega zakona o tajnih podatkih. Kateri dejavniki so se od sprejetja veljavnega zakona tako spremenili, da je bila sprejeta odločitev za izdelavo popolnoma novega zakona o tajnih podatkih?

Potreba po spreminjanju predpisov našega področja dela se zaznava že kar nekaj časa, pa čeprav je od zadnjih večjih sprememb minilo šele šest let. Prvotna želja ni bila, da bi bil zakon popolnoma nov, pač pa naj bi pripravili novelo, vendar se je, ko so strokovnjaki začeli z delom v medresorskih delovnih skupinah, izkazalo, da je treba zakonodajo za to področje v veliki meri prenoviti oziroma posodobiti. K temu so seveda svoje prispevale tudi že prej omenjene spremembe zakonodaje EU in NATO, s katerimi je treba uskladiti naše predpise, če je tako določeno. Spremembe predpisov bodo zajele vsa področja, ki jih ureja ZTP, seveda pa je ključni cilj, zakon spremeniti v skladu z Resolucijo o normativni dejavnosti in zakon narediti jasen, pregleden in predvsem življenjski. Naše področje dela je povezano z varnostjo, zato je zelo dinamično, spremenljivo in zanimivo — hkrati pa seveda predstavlja tudi velik izziv.

6. UVTP predstavlja nacionalni varnostni organ (National Security Authority — NSA) v razmerju delovanja do mednarodnega okolja. To je za urad, ki je po številu kadrovsko precej omejen, verjetno zelo zahtevna naloga.

Po številu uslužbencev smo najmanjši nacionalni varnostni organ v Evropi, vendar je naš delokrog nalog nehvaležno primerjati z nalogami sorodnih organov. Določene naloge so pri sorodnih nacionalnih varnostnih organih v njihovi pristojnosti, pri nas pa te naloge opravljajo

Menim, da se varnost vse prevečkrat jemlje za samoumevno in se o izboljšavah ter previdnosti začnemo spraševati šele ob odpravljanju posledic nekega neprijetnega dogodka. Dvig varnostne kulture ne pomeni vnašanje nekega nedorečenega strahu ali celo paranoje, ampak zavedanje dejanskih nevarnosti.

določena ministrstva ali službe. Vendar pa je ne glede na to naša vloga v mednarodnem okolju enakovredna drugim. Smo dejavni in zastopamo RS v varnostnih odborih in drugih mednarodnih forumih v EU in NATO ter prenašamo dobro prakso in znanje v naše domače okolje. Sodelujemo tudi na področju JV Evrope v Svetu za regionalno sodelovanje (Regional Cooperation Council — RCC), v okviru katerega deluje Zveza nacionalnih varnostnih organov Jugovzhodne Evrope (South East European National Security Authority — SEENSA). Seveda pa ne glede na to, da nas je v Uradu malo, imam kot predstojnik srečo, da lahko rečem, da v Uradu deluje nekaj izjemnih posameznikov, izobrazbena struktura je visoka, večina uslužbencev je na vrhunski ravni na posameznih področjih, v glavnem namreč izhajajo z varnostnega področja, so zelo motivirani, zavzeti in delovni. Vse to pa se kaže tudi pri naših rezultatih.

7. Izobraževanje in usposabljanje sta ključna za zagotavljanje in dvigovanje ustrezne stopnje varnostne kulture in zavedanja med upravljavci tajnih podatkov ter preko tega tudi širšega družbenega okolja. Kako ta segment glede na omejene kadrovske vire v vašem uradu še okrepiti?

Strinjam se, da je usposabljanje in izobraževanje izrednega pomena. Uslužbenci urada izvajajo osnovno usposabljanje s področja obravnavanja in varovanja tajnih podatkov, kjer se letno usposobi okoli 1000 ljudi, organiziramo pa tudi usposabljanje vodij usposabljanja. Vsako leto pripravimo tudi program za dodatno usposabljanje. V letu 2012 smo na željo uslužbencev nacionalnega varnostnega organa BiH, ki so se na nas obrnili za pomoč, izvedli usposabljanje v okviru instrumenta TAIEX. To je instrument Evropske komisije, ki je namenjen državam prejemnicam pomoči na področju približevanja in izvajanja zakonodaje EU. V letošnjem letu načrtujemo še dve tovrstni usposabljanji za predstavnike BiH. Poleg naštetega smo prek organizacije OVSE na študijskem obisku gostili predstavnike srbskega nacionalnega varnostnega organa. Končni cilj izobraževanja vidim v že večkrat omenjenemu dvigu varnostne kulture, ki jo vidim tudi kot neke vrste vzgojo. Začeli smo tudi projekt e-usposabljanje, ki je dobra ideja. Vendar se zavedam omejitev in dejstva, da tovrstno usposabljanje ne more nadomestiti predavatelja v živo, kjer svoje doda interakcija s predavateljem. Razmišljamo tudi o bolj podrobnem strokovnem usposabljanju za posamezno področje, vendar nas pri tem omejujejo kadrovski viri. Glede na težnje po poenotenju standardov varovanja tajnih podatkov v mednarodnem okolju smo se vključili tudi v projekt v okviru Sveta za regionalno sodelovanje (RCC) in v idejo o mednarodnih usposabljanjih, ki bi jih lahko gostili tudi pri nas ali pa pošiljali naše ljudi na usposabljanje v tujino. Ideja se razvija in je še v začetni fazi, vendar menim, da ima projekt velike možnosti, še posebej zaradi možnosti vključitve strokovnjakov z različnih področji in iz različnih držav, z izkušnjami iz različnih okolij in z različnimi pristopi. Zavedati se moramo, da na področju varnosti nismo sami, varnost je nekaj, kjer sodeluje ogromno ljudi iz različnih dejavnosti, ki se med seboj prepletajo in dopolnjujejo. Verjamem v uspeh in dopolnjevanje učinkov, če bi se na primeren način v izobraževanje vključilo strokovnjake z različnih področij.

8. Menite, da so lahko ustrezne referenčne institucije, kakor na primer Institut za korporativne varnostne študije, tisti dejavnik, ki bi v procesu izobraževanja in usposabljanja s področja tajnih podatkov zagotavljal dodatno kakovost in zmogljivost, predvsem na področju gospodarskega in korporativnega okolja?

Kakor sem že omenil, na tem področju nismo sami, področje varnosti je izredno široko in mnogi segmenti se med seboj prepletajo. Varovanje tajnih podatkov je sicer specifično glede določenih pravil ravnanja, ne glede na to pa vključuje vse varnostne elemente širšega vidika varovanja. V tem smislu so teoretične in praktične izkušnje izredno pomembne. Nekdo pa mora vse to povezati in imeti vlogo stične točke med različnimi akterji. Tu vidim delo inštitucije, sploh pa tako povezovalne in delovne kakor je Institut za korporativne varnostne študije, kot nujno potrebno in nepogrešljivo. Iz »bazena« članov ICS bi bilo smiselno črpati vire, da bi naše usposabljanje pridobilo širino in dodatno kakovost. Po drugi strani je pomembna tudi angažiranost posameznikov za obiskovanje seminarjev in poglabljanje znanja s področja gospodarskega in korporativnega okolja, kjer je treba poleg poznavanja varnostnih elementov poznati tudi zakonitosti tega okolja. Tovrstna interakcija državnih organov in gospodarstva v okviru instituta, kakršen je ICS, se potrjuje kot pozitivna tudi v drugih državah.

9. Kako bi lahko po vaši oceni pri slovenskih podjetjih okrepili željo po pridobitvi ustreznih dovoljenj za varovanje tajnih podatkov in jih tako na trgu naredili še bolj konkurenčne?

Predvsem je treba razbliniti strah pred našim področjem in prepričati predstavnike gospodarstva, da so tudi na tem področju poslovne priložnosti. Priložnosti niso le v visoko tehnoloških izdelkih s področja obrambe in varovanja, ampak tudi, na primer, na infrastrukturnem področju. Zadnji primer je prav gotovo gradnja novega sedeža NATO v Bruslju. Vem, da odločitev za pridobitev ustreznih dovoljenj ni enostavna, še zlasti, ker pomeni tudi določene stroške, zato odločitev temelji predvsem na vprašanju, ali se splača, vendar ne smemo pozabiti, da varčevanje pri varnosti morda učinkuje le kratkoročno. Država mora omogočiti čim bolj pregleden in enostaven postopek za pridobitev dovoljenj, mora na nek način tlakovati pot in opozarjati na priložnosti, kar menim, da v veliki meri že počne, odločitev in prepoznavanje priložnosti pa ostaja povsem na strani podjetij. UVTP si bo še naprej prizadeval za promocijo navedenih priložnosti.

10. UVTP je eden izmed najbolj aktivnih korporativnih članov slovenskega združenja korporativne varnosti. Kaj so po vaši oceni dodane vrednosti tovrstnega sodelovanja glede javno-zasebnega sodelovanja?

Dodane vrednosti so prav gotovo v večkrat omenjenem dvigu varnostne kulture, izmenjavi dobrih praks in drugih informacij, možnosti izobraževanja in sodelovanja pri programih izobraževanja, sodelovanju pri projektih, in še bi lahko našteval. Razmišljanje o idejah javno-zasebnega partnerstva na nekaterih področjih varovanja tajnih podatkov je še kako zaželeno. Eno od možnosti vidim npr. v povezavi institutov, podjetij in univerz pri razvoju šifrirnih rešitev. Nacionalno razvite šifrirne rešitve bi bile zelo dobrodošle. Produkti bi bili lahko uporabni in bi postali standard ne samo za državne organe, ampak tudi za gospodarske subjekte. Poleg tega so v ICS tudi predstavniki prej naštetih subjektov. Prepričan sem, da je sodelovanje s slovenskim združenjem korporativne varnosti zelo koristno in veseli smo, da smo del njihovega delovanja. ■

Zavedati se moramo, da na področju varnosti nismo sami, varnost je nekaj, kjer sodeluje ogromno ljudi iz različnih dejavnosti, ki se med seboj prepletajo in dopolnjujejo.

Novi magistrski program 2. stopnje

MANAGEMENT KORPORATIVNE VARNOSTI

Program akreditiran - vpis že poteka

geacollege
Fakulteta za podjetništvo

ICS
Institut za korporativne varnostne študije

Vzemi usodo v svoje roke in ustrezno obvladuj tveganja v svoji poslovni karieri!

Predavanja bodo skrbno izvajali največji strokovnjaki na področju korporativne varnosti.

*

Veliko število gostujočih predavateljev, ter s tem zagotavljanje implementacije praktičnih spoznanj v izobraževalni proces.

*

Sodelovanja v aktivnostih Slovenskega združenja korporativne varnosti (konference, posveti in neposredni obiski različnih organizacijskih okolij).

*

Visoko zaposljivost naših študentov v nacionalnem in mednarodnem okolju.

*

Neposredna podpora pri zagotavljanju službe najboljšim študentom.

*

Za najbolj uspešne študente zagotovitev izvajanja neposredne prakse v okolju mednarodnih korporacij.

*

Širok nabor znanja tudi za delo na različnih nivojih korporativnega upravljanja.

PRIHODNOST PRIPADA PODJETNIM!

Avtorja: Karmen Čaleta, / Institut za korporativne varnostne študije*
Dr. Denis Čaleta / Institut za korporativne varnostne študije*





KADROVSKI MANAGEMENT IN KREPITEV VARNOSTNE KULTURE V KORPORACIJSKEM OKOLJU

Varnost ni pomembna dobrina samo za razvoj posameznika in družbe temveč je ustrezno varnostno okolje nujno potrebno tudi za nemoteno delovanje multinacionalnih korporacij. Predvsem načini in oblike organiziranega zagotavljanja varnosti so se skozi zgodovino s pomembnim vplivom vedno novih tehnologij in znanstvenih spoznanj, drastično spreminjali (Čaleta, 2011). Globalizacija sveta in s tem posredno globalizacija varnosti, moderno družbo postavlja pred zahtevne dileme in sicer kako še naprej svoj razvoj temeljiti na osnovnih postulatih prostega pretoka blaga, storitev in ljudi ter na drugi strani grožnje obvladovati na sprejemljivem nivoju tveganja.

Varnostno okolje 21. stoletja postaja vse bolj kompleksno in dinamično (Borodzicz, 2005). Tveganja in grožnje so zaradi svoje asimetričnosti pojavljanja postale vse bolj obremenjujoče za nemoteno delovanje moderne družbe. Če v tem kontekstu upoštevamo tudi vedno močnejšo odvisnost družbe od delovanja tehnoloških dosežkov moderne dobe, kot so informacijsko-komunikacijska tehnologija, električna energija in drugi energenti, lahko z gotovostjo trdimo, da je ta družba ravno zaradi te odvisnosti še bolj izpostavljena določenim tveganjem, oziroma je v stanju popolne varnosti iluzorno razmišljati. V tem celovitem sistemu nikakor ne smemo in ne moremo zanemariti človeški dejavnik, kot osnovni potencial vsake moderne organizacije. Kakor na eni strani človeški potencial predstavlja temelj vsakega družbenega in v tem okviru tudi organizacijskega okolja, na drugi strani ravno človeški dejavnik predstavlja najšibkejši člen tega sistema, ki ga je nemogoče popolnoma nadomestiti s posameznimi tehnološkimi sistemi. Bertoncelj (2012) ugotavlja, da je posameznik pomemben referent pojma varnosti. Posameznik in družba sta stalno izpostavljena številnim virom ogrožanja. Posamezniki so vsakodnevno izpostavljeni različnim vplivom, ki jih bolj ali manj ogrožajo in predstavljajo stalno tveganje za njihovo fizično, psihično, duhovno in materialno varnost. Zaradi navedenega se je v organizacijskem okolju potrebno zavedati, da trenutno temu dejavniku posvečamo vse premalo sistemske pozornosti. Posameznik se je kot socialni agre-

V tem celovitem sistemu nikakor ne smemo in ne moremo zanemariti človeški dejavnik, kot osnovni potencial vsake moderne organizacije. Kakor na eni strani človeški potencial predstavlja temelj vsakega družbenega in v tem okviru tudi organizacijskega okolja, na drugi strani ravno človeški dejavnik predstavlja najšibkejši člen tega sistema, ki ga je nemogoče popolnoma nadomestiti s posameznimi tehnološkimi sistemi.

*avtor je član Slovenskega združenja korporativne varnosti



gat v marsičem spremenil in s stališča zaposlenega v posamezni organizaciji postal izredno zahteven in zazrt skoraj izključno v zadovoljevanje svojih lastnih potreb, ki jih postavlja daleč pred potrebe organizacije v širšem in ožjem smislu. To med drugim pomeni, da smo zaradi dinamičnega in prožnega trga delovne sile prišli v situacijo hitrega menjavanja zaposlitev in s tem delovnih okolij, kjer je v tako kratkem času nemogoče pri posameznikih vzpostaviti ustrezno pripadnost ožjemu kolektivu in organizaciji v širšem pomenu besede. To pred vodilni management organizacij in še posebej pred korporativno varnostne strokovnjake postavlja zahtevne izzive, kako v globalnem ekonomskem okolju, ki temelji na hudi konkurenčni tekmovalnosti, zagotoviti ustrezno varovanje ključnih poslovnih informacij, do katerih dostopajo zaposleni v posameznih organizacijah. Seveda je prvi logični odgovor v smeri krepitve varnostne kulture, ki pa ima to »pomanjkljivost«, da predstavlja dolgotrajnejši proces, kot bi si v teh dinamičnih časih želeli. Drugo dejstvo pa vsekakor je, da bo potrebno sistemske pristope v korporacijskem okolju prilagoditi v smeri teh dinamičnih sprememb modernega okolja. V tem okviru si je danes težko predstavljati, da vodilni management organizacij v celoti ne uporablja vseh sistemskih vzvodov za obvladovanje tveganj za delovanje njihove organizacije. To pomeni, da kadrovski management in korporativni varnostni management prepleteno izvajata in se vključujeta v proces, ki ga v našem obravnavanem primeru lahko umestimo v zagotavljanje ustrezne stopnje varnostne kulture zaposlenih v tej organizaciji. Ustrezna izbira kadrovskega potenciala, stalno preverjanje okoliščin in indicev, ki bi lahko pri ključnih kadrih organizacije pomenili določena tveganja za odtekanje pomembnih informacij so postali pomembni sistemski predpogoji pri izbiri zaposlenih.

Rezultati izvedene raziskave

Za doseganje razumevanja realne dinamike v organizacijskih okoljih in preverjanje teoretičnih spoznanj so bili izvedeni intervji s strokovnjaki iz šestih organizacijskih okolij. Trije namreč prihajajo iz delovnega področja kadrovskega managementa, trije pa iz okolja korporativno varnostnega managementa. Organizacije iz katerih prihajajo omenjeni strokovnjaki so bile izbrane načrtno tako, da zajemajo vse tri kategorije gospodarske organiziranosti v Republiki Sloveniji in sicer mikro podjetniško okolje, kategorijo majhnih in srednjih organizacij, dve veliki mednarodni korporaciji s sedežem v Republiki Sloveniji, mednarodno korporacijo s sedežem v tujini in večjo organizacijsko obliko (ministrstvo) s področja državne uprave.

Strukturirani intervju je bil sestavljen iz vprašalnika, ki je vseboval vprašanja odprtega tipa. Za vprašanja odprtega

tipa smo se predvsem odločili z razlogom, da gre pri organizacijah za dokaj velike specifike vezane na dejavnost, okolje delovanja in seveda na organizacijsko strukturo (velikost), zato so bili tipi vprašanj te vrste nujni, da so lahko intervjuvanci podrobneje pojasnili okoliščine, ki so pomembne za razumevanje dejavnikov in ukrepov za doseganje ustrezne stopnje varnostne kulture.

Iz tega izhaja tudi, da so bile pri obdelavi zbranih podatkov uporabljene metode kvalitativne (vsebinske) razlage ugotovitev, spoznanj in dognanj. Ker gre za večplastno problematiko, ki je nikakor ni mogoče obravnavati samo iz enega zornega kota je bilo treba uporabiti interdisciplinarni pristop.

Iz analize pridobljenih odgovorov je razvidno, da različne organizacije v svojih okoljih pomen celovitega obvladovanja varnostnih tveganj in s tem še posebej pomen varnostne kulture različno dojemajo in se zaradi svojih specifik tega problema lotevajo tudi na zelo različne načine. Pri manjši organizaciji je zaznati problem kadrovskih in finančnih virov, predvsem s stališča bolj organiziranega pristopa k vzpostavitvi mehanizmov, ki bi se v strukturi organizacije bolj sistematično ukvarjali s problemom dvigovanja varnostne kulture med zaposlenimi. V velikih organizacijah, posebej izstopajo tiste organizacije, ki delujejo v kompleksnem mednarodnem okolju, organizacijsko posvečajo pomembno pozornost varnosti (poudarek na varovanju poslovnih skrivnosti, patentov in ključnih konkurenčnih prednosti) in s tem tudi potrebi po ustrezni stopnji varnostne kulture zaposlenih. V mednarodni organizaciji, kakor tudi v obeh slovenskih organizacijah, ki delujeta v mednarodnem okolju, je varnostna kultura in varnostno zavedanje prepoznano in vzpodbujeno kot pomembna vrednota v organizaciji. V vseh velikih organizacijah obstajajo strateški dokumenti povezani z vsebino krovne varnostne politike in služijo tudi kot podlaga za izdelavo pravilnikov in navodil na nižjih ravneh delovanja. Posebej v organizacijski obliki državne uprave je temu normativnemu delu namenjeno relativno veliko pozornosti. Večji problem je v tem okolju zaznati v fazi implementacije vseh teh predpisov v praksi. Varnostna kultura tudi ni prepoznana kot ena izmed pomembnih vrednot med zaposlenimi. V manjših organizacijskih strukturah delujejo s smeri racionalnega podjetniškega pristopa s čim manjšim predpisovanjem določenih normativov vedenja. Okolje je zelo kompetativno in usmerjeno v doseganje zastavljenih ciljev. Zaradi manjših kolektivov medsebojni odnosi temeljijo na določeni relativno visoki meri zaupanja, ki ne daje toliko pomena formalnim nadzornim mehanizmom, temveč bolj temelji na medosebni interakciji. Varnostno kulturo zaposlenih ne poznajo pod osnovnim pojmom, vendar pa je bilo skozi razgovor jasno dojeti, da zaposleni v teh manjših organizacijah prepoznajo potrebnost varnega delovnega okolja in s tem njihove vloge pri zagotavljanju tega cilja. Mogoče je nekoliko problematičen del povezan z varovanjem ključnih informacij, patentov in ostalih pomembnih podatkov, ki bi lahko z odtekanjem konkurenci pomenil zmanjševanje konkurenčnih prednosti na tržišču.

Kadrovskim procesom in izboru ustreznega kadra z varnostnega stališča v mikro, majhnih in srednjih okoljih ne posvečajo dovolj velike pozornosti in kadrovski postopek temelji predvsem na dokazilih o referencah in izvedenem osebnem intervjuju. V organizacijski obliki javne uprave in v slovenskih korporacijah temu pomenu namenjajo določeno pozornost preko dokazil o nekaznovanosti, v mednarodni korporaciji pa temu področju namenjajo pomembno pozornost tudi preko drugih dokazil, ki dokazujejo, da je oseba vredna zaupanja, še posebej pri delovnih mestih strateškega managementa, razvojnih inženirjih in drugih pomembnih kadrih. O analizi odgovorov, kdo je v organizaciji zadolžen za stanje varnostne kulture v organizaciji so bili odgovori zelo različni od direktorjev na mikro in srednjem nivoju, do varnostnih struktur v organizacijskih oblikah državne uprave, pri slovenskih korporacijah pa je bilo poleg dodana še odgovornost strateškega vodstva. Samo v mednarodnih organizacijah je bilo poudarjeno, da gre tukaj za več nivojsko odgovornost med katerimi je imelo svoje mesto tudi področje kadrovskega managementa. Predvsem v organizaciji državne uprave je bilo prepoznati odsotnost potrebe po sodelovanju med različnimi segmenti znotraj strukture organizacije v smeri zagotavljanja boljše stopnje varnostne kulture zaposlenih. Organizacije, ki so pretežno usmerjene v mednarodno okolje pa so bile prisiljene svojo organizacijsko strukturo urediti v smeri večje prožnosti in nujnega medsebojnega sodelovanja. Dodatno pa to zagotavljajo preko uveljavljanja različnih orodij s področja standardizacije procesov, ki imajo v svoji vsebini tudi pomembne dele vezane z medsektorskim sodelovanjem znotraj organizacije. To dejstvo je bilo razbrati tudi iz vprašanj povezanih z oceno stopnje varnostne kulture v organizaciji. V organizacijah z urejeno lastniško strukturo in z managementom, ki vodi organizacijo usmerjeno pretežno v mednarodno okolje je bilo razbrati, da gre za ustrezno visoko stopnjo varnostne kulture pri zaposlenih. Slabše so to stanje ocenjevali intervjuvanci vezani na organizacijske oblike državnega okolja in organizacij, ki so usmerjene bolj v delovanje v nacionalnem okolju. Vodstvo in njegovo vodenje z zgledom je bilo pri vseh anketirancih prepoznano kot izredno pomemben dejavnik za uveljavljanje zavedanja o pomenu varnostne kulture, kot pomembne vrednote znotraj organizacij. Seveda so bili odgovori različni o vlogi vodstva, vsem pa je bilo skupno, da bi moralo biti vodstvo v tem okviru še bolj aktivno. Strateški management v organizacijah, ki nima predhodnih izkušenj s tega področja ali nima ustreznih znanj je v večini primerov tisti prvi signal, da v organizaciji temu področju ne namenjajo ustrezne pozornosti. To je bilo razbrati tako na mikro, kakor tudi na makro organizacijski ravni intervjuvanih predstavnikov. To je tudi eden izmed pomembnih dejavnikov katerega so prepoznali praktično vsi sogovorniki. Naslednji pa je vsekakor proces usposabljanja in izobraževanja. Le ta je največkrat zelo otežen predvsem zaradi vedno večje dinamike dela, novih organizacijskih oblik, ki predvsem poudarjajo tekmovalnost in cilje, na drugi strani pa vedno manj pozornosti namenjajo kolektivnemu duhu organizacij. Poleg tega so bile izpostavljene tudi kadrovske težave povezane z ustreznimi strokovnjaki znotraj organizacijskih struktur, kateri bi morali imeti ustrezno znanje in izkušnje iz te organizacije, da bi lahko v celoti izvajali take oblike izobraževanja in usposabljanja. V tem okviru so bile izpostavljene tudi finančne težave, ki vedno bolj omejujejo pošiljanje zaposlenih na oblike izobraževanj in usposabljanj, ki jih izvajajo zunanji izvajalci in ponudniki. V mednarodni organizaciji je bilo s strani intervjuvanega

Strateški management v organizacijah, ki nima predhodnih izkušenj s tega področja ali nima ustreznih znanj je v večini primerov tisti prvi signal, da v organizaciji temu področju ne namenjajo ustrezne pozornosti.



sogovornika izpostavljeno, da je v tem primeru pomembno tudi selektivno iskanje ustreznega kadra za določena mesta, kjer je stopnja varnostne kulture prepoznana, kot ena izmed pomembnih karakteristik. S tega stališča imajo kadri, ki prihajajo iz organizacij z urejenim sistemom obvladovanja varnostnih tveganj s poudarkom na ustrezni ravni varnostne kulture, lahko določeno konkurenčno prednost pred ostalimi. Taka oseba je namreč že ustrezno varnostno formirana in jo je potrebno skozi proces uvajanja samo še adaptirati na konkretne specifike organizacije, kjer trenutno deluje. Tudi ostali v organizacijah, kjer skozi kadrovski proces tej vsebini ne dajejo dovolj poudarka pri izbiri kadra, so se strinjali, da je skozi ustrezen način kadrovanja možno rešiti veliko težav, ki se na področju povečevanja varnostne kulture kasneje pojavljajo v organizacijah. V vseh treh organizacijah, ki so pretežno usmerjene v mednarodno okolje so sogovorniki poudarjali vedno večji pomen interaktivnega izobraževanja zaposlenih na daljavo in sicer na delovnem mestu ali na drugih oddaljenih lokacijah. Kot dejavnik, ki ima pomemben vpliv, so bile izražene tudi predhodne izkušnje zaposlenih v organizaciji s posameznimi varnostnimi katastrofičnimi dogodki, ki so se v organizaciji zgodili v preteklosti. V to so vključene naravne nesreče, industrijske nesreče, teroristični napadi, ugrabitve in izsiljevanja ter druga kriminalna dejanja. Slovenija je trenutno še vedno dovolj varno okolje, da predstavniki slovenskih organizacij temu pomenu v svojih odgovorih niso namenjali dovolj velike pozornosti. Predstavnik mednarodne korporacije pa je temu dal posebno pozornost in poudaril, da so ravno taka dejanja in travmatične izkušnje, ki so jim bili priča določeni zaposleni in seveda preko njih tudi ostali, v njihovih okoljih proces zagotavljanja obvladovanja tveganj potisnili v ospredje potreb in vrednot.

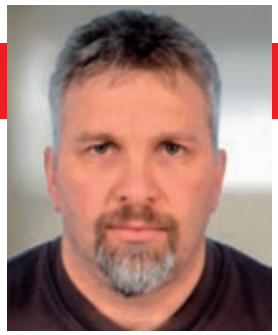
Organizacijsko klimo so vsi prepoznali kot pomembno dejstvo, ki ima ravno tako pomemben učinek na zadovoljstvo zaposlenih z delovnim okoljem in posredno tudi z njihovo pripravljenostjo k močnejšemu sprejemanju vrednot organizacije. V odgovorih posameznih strokovnjakov, ki so v svojih okoljih ocenjevali, da je varnostna kultura na nižjem nivoju, je bila organizacijska klima v organizaciji tudi eden izmed pomembnih dejavnikov, ki so ga povezovali z nižjo stopnjo varnostne kulture zaposlenih. V teh organizacijah jo zaposleni enostavno niso vzeli za tisto okolje, za katero bi bilo vredno storiti kakšen dodaten napor od tistega nujno potrebnega in predpisanega.

Viri

- Bertoncelj, B., 2012. The individual and security. V Čaleta, D. (ur.), Corporate security in global dinamic environment – chalenges and risks. Ljubljana: ICS.
- Borodzicz, E., 2005. Risk, Crisis and Security Management. New York: John Wiley&Sons.
- Čaleta, D., 2011. Varnost mojega podjetja. Podjetnik 11(10), 40-41.
- Čaleta, K., 2012. Vpliv kadrovskega managementa na krepitev varnostne kulture v korporacijskem varnostnem okolju. Diplomsko delo. Ljubljana: Fakulteta za varnostne vede. ■

S tega stališča imajo kadri, ki prihajajo iz organizacij z urejenim sistemom obvladovanja varnostnih tveganj s poudarkom na ustrezni ravni varnostne kulture, lahko določeno konkurenčno prednost pred ostalimi. Taka oseba je namreč že ustrezno varnostno formirana in jo je potrebno skozi proces uvajanja samo še adaptirati na konkretne specifike organizacije, kjer trenutno deluje.

Avtor: Zoran Ulaga, Airport Supervisor, TNT Express Slovenija



VARNOST NA LETALIŠČU

Varnost na letališčih je eden od štirih poglavitnih dejavnikov varnosti zračnega prometa. Poleg izvajanja ter nadzora varnosti na letališčih so potrebne enako zahtevne varnostne aktivnosti pri proizvodnji letal in opreme, pri prevoznikih v zračnem prometu in njihovem osebju ter tudi pri službah kontrole letenja.

Ravno varnost na letališčih je med temi dejavniki najbolj kompleksna in po svoje zanimiva. Zakaj? Letališče je namreč kraj, kjer se odvijajo ključni procesi priprave letenja, je mesto soočenja strogih varnostnih standardov na eni strani in pravic uporabnikov zračnega prometa na drugi strani, je kraj, kjer je izvedba samih varnostnih ukrepov najbolj občutljiva in zato tudi težje izvedljiva.

Pa ni bilo vedno tako. Zračni promet v svoji polpretekli zgodovini, v času svojega največjega razcveta pomni tako liberalne dostope potnikov do letala in letenja z njim, da si jih dandanes pravzaprav niti ne moremo predstavljati. Pojem »varnost letalskega prometa« se je takrat nanašal predvsem na tehnično-tehnološke procese in vidike varnega letenja (dandanes takoimenovano »safety« področje), medtem ko je bilo področje, zajeto pod pojmom »security« praktično nepopisan list. Tako je bilo vse do prvih spoznanj nekaterih konfliktnih družbenih skupin ali posameznikov, da je takšna vrsta prevoza zaradi medijske odmevnosti pravzaprav idealna za preusmeritev pozornosti nase in za izsiljevanje po njihovem mnenju nepriznanih pravic ali privilegijev. Prva, dokaj nedolžna ugrabitev letala za trosenje letakov proti vladajočemu režimu se je sicer zgodila že davnega leta 1930 v Peruju, pravi razmah ugrabitev pa se pojavi v 60-tih letih 20.stoletja, predvsem v ZDA. S pojavom takšnih incidentov, se je pojavila tudi potreba po varnosti in nadzoru nad uporabniki letalskih prevozov. Tako so



V Sloveniji je za varnost letalskega prometa in izvedbo nadzora nad njim zadolžena Javna agencija za civilno letalstvo Republike Slovenije. Agencija deluje na letalskih področjih usposabljanja, licenciranja, certificiranja, varovanja in inšpekcijskega nadzora ter zakonodaje (Zakon o letalstvu, Zbornik letalskih predpisov).



l.1970 v New Orleansu uvedli prvo rentgensko napravo za pregled potnikov in od tega prvega mejnika so se razvijale varnostne naprave, vse do prve od najbolj »zloveščih« naprav (Rapiscan Secure 1000, predstavljena oktobra 2009 v Manchestru), ki potnika ali njegovo prtljago praktično »razgali« pred očmi nadzornega osebja, kar pa že (pre)močno posega v človekovo zasebnost in je danes predmet hudih polemik med varnostno stroko in zagovorniki človekovih pravic. Potniki so že sami v določeni dilemi, saj bi želeli od odgovornih trdna zagotovila za varno letenje, sami pa se takim pregledom težko podredijo in jim vzbuja odpor. Dandanes je v praksi po letališčih sklenjen nekakšen kompromis, da potnik takšno skeniranje lahko zavrne in je pregledan s starimi metodami in dodatnimi pregledi, zanimivo pa bo videti kako se bo v svetu vse bolj poostrenih zahtev varnostnih institucij ta polemika oz. konflikt interesov razvijal v bodočnosti.

Prav tako kot naprave so se razvijali in uvajali tudi novi varnostni procesi, pregledom so se dodajale tudi prepovedi vnosa različnih predmetov, naprav in snovi in v sklopu teh prepovedi je bil verjetno med bolj odmevnimi ukrep proti vnosu tekočih eksplozivov na letalo. Uredba EU o prepovedi vnosa tekočin je zaradi raznovrstnih možnosti priprave eksploziva iz tekočih ali pol-tekočih snovi pojem tekočine zajela zelo na široko in praktično prepovedala vnos poleg vseh tekočin še veliko povsem vsakdanjih snovi kot npr. geli, kreme, paste, ipd. Razlog za tako širok zajem prepovedi je bil tudi v (ne)zmožnosti rentgenskih naprav pri prepoznavanju različnih vrst tekočin.

Seveda se je med tem časom zaradi vse večjih potreb po zagotovitvi varnosti spreminjala tudi zakonodaja in predpisi tako posameznih držav kot tudi za to pristojnih letalskih organizacij. Še dandanes je osnova za vse varnostne standarde dokument ANNEX 17 (Security), sprejet leta 1974 kot dopolnilo Čikaški konvenciji iz leta 1944. Na omenjeni konvenciji v Chicagu je bila ustanovljena Mednarodna organizacija civilnega letenja (ICAO) z namenom, da se poenoti pravila v civilnem zračnem letenju, uvede enotne standarde in tako zagotovi varnost in rednost zračnega prometa. ICAO je še danes najbolj pomembna organizacija za omenjene standarde, Čikaška konvencija pa njen najpomembnejši pravni akt. Slovenija je članica ICAO od leta 1992, v letih od 2010 do 2013 pa je tudi članica Sveta ICAO, poleg Skupščine najpomembnejšega organa ICAO.

Dokument Annex 17 se je uveljavil kot ICAO standard in se je vse do danes dopolnjeval z aktualnimi priporočili in z zahtevanimi minimalnimi standardi. Države na podlagi teh priporočil uzakonijo standarde, zavezujoči pa so prav tako v mednarodnih združenjih kot so IATA, ACI, IFALPI, ICPO- Interpol, ECAC, JAA, EuroControl,ipd. V času po 11.SEP se je na tem področju uveljavilo (in se deloma tudi že opustilo) kar nekaj dodatnih varnostnih procedur in prepovedi, predvsem na zahtevo ameriške varnostne agencije Transportation Security Administration (TSA), v Evropi pa je najbolj aktualen in uveljavljen predpis Uredba EU št. 185 Evropske komisije iz leta 2010.

V Sloveniji je za varnost letalskega prometa in izvedbo nadzora nad njim zadolžena Javna agencija za civilno letalstvo Republike Slovenije. Agencija deluje na letalskih področjih usposabljanja, licenciranja, certificiranja, varovanja in inšpekcijskega nadzora ter zakonodaje (Zakon o letalstvu, Zbornik letalskih predpisov).

Družba Aerodrom Ljubljana ima področje varnosti organizirano v sklopu Strokovne službe za varnost in zaščito ter Varnostno-operativnega centra, izvajanje varnostnih procesov in dejavnosti pa je urejeno pogodbeno z zunanjim izvajalcem varnostnih storitev. Zunanji izvajalec varnostnih storitev je od leta 2006 tudi pooblaščena služba za pregled potnikov in njihove prtljage. Zakonska podlaga za delovanje te službe na letališču je Zakon o letalstvu ter vse zavezujoče mednarodne uredbe o varnosti v zračnem prometu. Poleg potniškega dela ter nadzora nad letališko infrastrukturo pa zunanji izvajalec varnostnih storitev skrbi tudi za varnost in pregled komercialnega tovora, za kar imajo ustrezno kvalificiran kader in standardizirano sodobno opremo.

Tovorni promet z letalskim blagom se je namreč z vidika teroristov že večkrat izkazal za »hvaležen in priljubljen« način, kako je mogoče ogroziti varnost letala. Takih zelo očitnih primerov je bilo v zadnjem času kar nekaj, lep primer sta dve delujoči bombi v paketih na ameriških tovornih letalih iz Jemna v ZDA (oktober 2010). Obe sta bili uspešno odkriti, ena v Londonu, druga v Dubaju. Eksplozivni telesi sta bili pripravljeni iz izredno eksplozivne kombinacije industrijskega kemičnega eksploziva PETN, skriti v tiskalniku, aktivirali pa naj bi se s pomočjo mobilnega telefona, najverjetneje med samim poletom. Zelo podoben primer odkrite bombe beležimo tudi v decembru 2009, namen je bil razstrelitev letala nad Detroitom.

Področja »safety« in »security« imata največ skupnih imenovalcev ravno pri pregledih tovora in potniške prtljage, zato mora biti osebje na teh pregledih resnično dobro usposobljeno za odkrivanje vseh vrst nevarnosti, od tako očitnih terorističnih groženj pa vse do tistega skritega nevarnega blaga, kateri se je v prtljagi ali tovoru znašel povsem iz nevednosti pošiljatelja ali celo brez zavedanja, da predstavlja taka vsebina kakršnokoli nevarnost za letalo. Tudi pri koriščenju storitve prevoza blaga, lahko uporabniki prav tako kot potniki, zaradi zagotavljanja varnosti naletijo na morebitne težave z dodatnimi zahtevami glede opisa blaga, dodatne dokumentacije oziroma dodatnih metod



pregleda in posledično lahko pošiljke v takih primerih tudi zamujajo predvideno dostavo. Da bi se ob enaki ali boljši zagotovljeni varnosti takim situacijam izognili je prav, da se stranke same tudi pri koriščenju tovornega servisa dobro pozanimajo o zahtevah prevoznikov in zakonodajalcev, da poznajo dobro lastnosti svojega tovora in da je ta predvsem zelo dobro in pravilno opremljen z vsemi potrebnimi informacijami in dokumenti. Koristniki kargo prevozov v zračnem prometu imajo na letališčih tudi vso strokovno podporo, na voljo so jim usluge letalskih agentov, primerno usposobljenih in licenciranih za opravljanje te storitve.

Še bolj pomembno je, da se teh groženj in nevarnosti iz obeh področij varnosti dobro zavedamo tudi ponudniki kargo prevozov. Še posebej gre poudariti vlogo letalskih prevoznikov hitre pošte, ekspresnih pošiljk, kateri vršimo celotno dostavo od pošiljatelja do prejemnika in smo prav zaradi tovrstne storitve lahko tarča poskusa ogrožanja varnosti. ■

Avtorja: Zdenko Hriberšek, Direktor Gorenje, d.d. - Varovanje*,
Alma Ribič, mag.var., Gorenje, d.d. - Varovanje





KORPORATIVNA VARNOST KOT KONKURENČNA PREDNOST PODJETJA

Obvladovanje ogroženosti, poslovnega in varnostnega tveganja daje možnost, da se v podjetju čim bolj približajo teoretično zasnovanemu finančnemu ravnovesju (ravnotežju) med finančno ovrednotenimi škodami/izgubami ter stroški zaščite in finančnimi ter drugimi koristmi varnostnega sistema.

Gorenje d.d. je dobitnik nagrade »Slovenian Grand Security Award 2012« v kategoriji »Najbolj varno podjetje«.

V podjetjih ljudski pregovor, »tam kjer ni, še vojska ne vzame«, zagotovo ne velja povsem; prej nasprotno: bolj velja rek »priložnost dela tatu!« V kolikor podjetje pojmujemo kot sistem (in uspešna podjetja predstavljajo zelo kompleksne, včasih tudi težko obvladljive in upravljane sisteme) ugotovimo, da zaradi splošnih značilnosti sistema (entropije, homeostaze, diferenciacije, centralizacije, variabilnosti, sistemske interakcije), nanj delujejo številne silnice in vplivi iz zunanjega okolja, na katere mora ustrezno odgovoriti. Med vsemi ostalimi vplivi so tudi raznovrstna tveganja in grožnje, ki zadevajo predvsem ekonomsko-poslovno, informacijsko, tehnično-tehnološko in ne nazadnje (fizično) varnostno raven. Ker absolutne varnosti ni, potrebuje podjetje lastno varnostno politiko, s katero ne le predvidi potencialne izzive, tveganja in grožnje, ampak določi tudi mehanizme in instrumente, s katerimi se bo tem tveganjem zoperstavilo. Celo več – podjetje bo poizkušalo s tveganji upravljati in na ta način zagotavljati svojo dolgoročno uspešnost (Lobnikar, Sotlar, 2008). Z lastno varnostno politiko so tako opredeljeni cilji varovanja, s katerimi so seznanjeni tako zaposleni v podjetju kot tudi njeni lastniki. Gorenje d.d. je dobitnik nagrade »Slovenian Grand Security Award 2012« v kategoriji »Najbolj varno podjetje«. Ključno vprašanje varnosti podjetja je, kako vzpostaviti zaščitno in hkrati ekonomsko, poslovno in moralno učinkovito varnostno delovanje v podjetju. Poslovodstvo zanima predvsem varnostno delovanje, ki bo finančno znosno in na daljši rok donosno, ter ki bo opravilo svojo preventivno in (če je treba) represivno nalogo. Finančna znosnost se na eni strani nanaša na finančno ovrednotenje škod in izgub, na drugi pa na finančni vložek (stroške) varnostnega sistema. Obvladovanje ogroženosti, poslovnega in varnostnega tveganja daje možnost, da se v podjetju čim bolj približajo teoretično zasnovanemu finančnemu ravnovesju (ravnotežju) med finančno ovrednotenimi škodami/izgubami ter stroški zaščite in finančnimi ter drugimi koristmi varnostnega sistema. Novi varnostni koncepti podjetij temeljijo torej na prvinah ekonomike in poslovnosti podjetja, zatem pa še na pozitivnih prvinah vedenja lastnikov, menedžmenta in zaposlenih, kar sestavlja kulturo posameznega podjetja (Vršec, 1993). Ker absolutne varnosti ni, potrebuje podjetje lastno varnostno politiko. Varnost je samostojna poslovna funkcija v podjetju. Varnost podjetja je samostojna poslovna funkcija podjetja, ki preprečuje nezaželene pojave v podjetju in nezaželene pojave ter vplive iz okolice podjetja na podjetje samo oziroma na ostale poslovne funkcije podjetja (Lobnikar, 2011). Ko govorimo o varnosti, mislimo predvsem na varnost v širšem smislu, od varovanja ljudi in premoženja s fizičnim in tehničnim

Ker absolutne varnosti ni, potrebuje podjetje lastno varnostno politiko. Varnost je samostojna poslovna funkcija v podjetju.

*Gorenje d.d. - varovanje je član Slovenskega združenja korporativne varnosti



varovanjem, varnosti in zdravja pri delu, ekološke varnosti, informacijske varnosti, varnosti znanja oziroma varnosti intelektualne in industrijske lastnine, proizvodne varnosti, požarne varnosti, civilne zaščite, varnosti osebnih podatkov, zavarovanje ljudi in premoženja, izredno pomembnega notranjega sistema nadzora, vzpostavitev internih aktov, idr. Za vse naštete oblike varnosti se izvajajo določene aktivnosti in v skladu s tem so tudi znotraj podjetja organizirana področja dela oziroma službe. Govorimo o določeni stopnji integralnega varnostnega sistema. Korporativna varnost predstavlja izvedbo vseh potrebnih ukrepov za obvladovanje varnostnih tveganj. Korporativno varnost lahko opredelimo kot dejavnost, s katero identificiramo in izvajamo vse potrebne ukrepe za obvladovanje varnostnih tveganj v podjetju. Z njo poskušamo zagotavljati varnost do stopnje, ki zadostuje za ohranjanje vseh poslovnih funkcij v podjetju. Cilj te dejavnosti je zagotavljanje delovanja celotnega integralnega varnostnega sistema. Pomemben segment uspešnega poslovanja podjetja je uporaba poslovno varnostnih standardov v vseh procesih v podjetju, kot so standardi skupine ISO 9000:2000, ISO/IEC 27001 – sistemi vodenja varovanja informacij, BS 25999 – Business Continuity, OHSAS18001 - varnost in zdravje pri delu ter sistem za upravljanje varnosti, ISO 14001 – obvladovanje okoljskih vidikov proizvodne ali storitvene dejavnosti, standardi zasebnega varovanja, idr. ter nekatera poslovno menedžerska orodja: benchmarking, model 20 ključev, sistem uravnoteženih kazalnikov BSC, koncept Kaizen, itd.

Kot pojavno obliko konkurenčne prednosti podjetja je potrebno izpostaviti korporativno varnost.

Kot pojavno obliko konkurenčne prednosti podjetja je potrebno izpostaviti korporativno varnost. Konkurenčno prednost razumemo kot prednostni položaj podjetja v očeh kupcev gledano relativno v primerjavi s konkurenti. Kot glavne pojavne oblike konkurenčne prednosti je treba izpostaviti predvsem nižje cene in diferenciacijo glede na konkurente, pri čemer lahko slednjo še naprej razdelimo na prednost v obliki odličnega proizvoda (storitve), celovitosti ponudbe, hitrega zadovoljevanja potreb kupcev, prilagodljivosti pri zadovoljevanju kupcev in pozitivne podobe podjetja v očeh kupcev. Seveda ima lahko podjetje konkurenčno prednost tudi v večpojavnih oblikah hkrati (Čater, 2007). Kot pojavno obliko konkurenčne prednosti je potrebno izpostaviti tudi korporativno varnost, ki ponuja podjetju edinstveno konkurenčno prednost, kar pomeni, da se je ne da preslikati oziroma kopirati. Govorimo o identificiranju in izvajanju vseh potrebnih ukrepov za obvladovanje varnostnih tveganj. Če želimo opredeliti varnostna tveganja, je potrebno po korakih ugotavljati, kakšno je naše trenutno varnostno stanje, kakšna ogrožanja, od kje in od koga nam pretijo, kakšne so morebitne posledice, itd.

Korporativna varnost predstavlja izvedbo vseh potrebnih ukrepov za obvladovanje varnostnih tveganj.

Korporativna varnost je ena od pomembnih funkcij za delovanje podjetja in se v bistvu prepleta z drugimi funkcijami, kot so kadrovska funkcija, proizvo-



dna, razvojna, nabavna, tržna, logistična, finančna, informacijska funkcija. Prepletanje varnostne funkcije z ostalimi pomeni predvsem, da ustvarja pogoje za stabilnost procesov na vhodu, izvedbi in izhodu. Ustrezno motiviran varnostnik in njegova pripadnost podjetju je velika prednost pri organizaciji lastnega varovanja ljudi in premoženja. Sestavni del korporativne varnosti v podjetju je tudi varovanje ljudi in premoženja z obliko zasebnega varovanja. Izvaja se na podlagi Zakona o zasebnem varovanju, Ur.l. RS, št. 17/2011 in veljavnimi podzakonskimi akti. Podjetje se lahko odloča med organizacijo varovanja z lastno varnostno službo ali s pogodbo prenese odgovornost za varovanje na zasebno varnostno družbo, ki svoje storitve trži na trgu. Pri odločanju se vedno izpostavljajo vprašanja, kaj je za podjetje optimalno, kaj je ugodno iz vidika stroškov in v smislu zagotavljanja najbolj učinkovitega varovanja. Zagotovo obstajajo prednosti in slabosti ene ali druge organizacije varovanja, vendar se mora vrhnji menedžment v podjetju na podlagi svoje varnostne politike, vedenja in zmožnosti odločiti.

Prednosti organizacije varovanja ljudi in premoženja z lastnim varnostnim osebjem:

- ureditev s skupnimi internimi akti znotraj podjetja,
- skrb za dobro ime podjetja – blagovna znamka,
- dobri delovni pogoji,
- skupne oz. enotne varnostne strokovne podlage,
- zagotavljanje stalnega potrebnega varnostnega osebja in poudarek na zavedanju o notranji varnosti podjetja,
- dobro poznavanje lokacije, objektov, zaposlenih – osebja, ranljivih točk, tveganj in ogroženosti,
- ustrezno usposabljanje varnostnega osebja in uporaba tega znanja pri delu,
- primeren osebni dohodek zaposlenih in zadovoljstvo le-teh,
- velika pripadnost zaposlenih– zvestoba lastnemu podjetju,
- omejene možnosti škodljivih povezav med zaposlenimi,
- lažje kreiranje varnostne politike ter planiranje ukrepov,
- prepletanje varnostne funkcije z drugimi poslovnimi funkcijami v podjetju,
- realizacija celovitega varovanja v podjetju,
- racionalno in učinkovito varovanje ljudi in premoženja,
- hitro razreševanje nastalih problemov,
- planiranje preventivnih ukrepov, skupaj z drugimi varnostnimi oddelki oz. službami v podjetju,
- razvoj varnostnih postopkov,
- neposredna odgovornost lastnemu menedžmentu,
- učinkovitejši in neposredni nadzor,
- presojanje kakovosti v sklopu enega sistema,
- višja raven izvedbe varnostnih storitev za lastne potrebe,
- nizko gibanje kadrov,
- razvoj storitev varovanja,
- sodelovanje – ustvarjanje pogojev za možnost sklenitve najbolj ugodnega zavarovanja ljudi in premoženja v podjetju,
- dvig varnostne kulture, idr.

Ustrezno motiviran varnostnik in njegova pripadnost podjetju je velika prednost pri organizaciji lastnega varovanja ljudi in premoženja.



Poleg veliko prednosti lastnega varovanja ljudi in premoženja pa ima le-to tudi nekaj slabosti, kot so nekoliko višji stroški varovanja v primerjavi s pogodbenim in pa morebitna nevarnost »familiarnosti« zaposlenih. Potrebno se je zavedati, da je zaposleni, ki izvaja varnostne naloge in obvladuje tveganja, ključnega pomena v procesu zagotavljanja varnosti. Zagotovo se s pristopom omogočanja vseh prej naštetih prednosti lastnega varovanja izognemo nezadovoljstvu zaposlenih, odtekanju poslovnih informacij in skrivnosti, nizki varnostni kulturi, visokem gibanju kadrov (prihodi in odhodi zaposlenih), pojavu korupcije med zaposlenimi, škodljivimi povezavami z notranjimi kot tudi zunanjimi osebami in drugimi nezaželenimi pojavi, ki lahko ključno vplivajo na varnost v podjetju in povzročijo ogromno finančno ter moralno škodo podjetju. Pomembno je, da se podjetje s prenosom različnih varnostnih funkcij na zunanjega izvajalca zaveda, da se s tem pojavlja še dodatno tveganje in da je v tem primeru izjemno pomembno izvajanje nadzora.

Zato je ključnega pomena, da se podjetje pri odločitvi o vzpostavljanju varnostnega sistema ne oprijema samo znižanja stroškov varnosti in prenosa odgovornosti za to področje na drugega. Upoštevati je potrebno tudi vse druge nefinančne koristi/neotipljive prednosti, ki niso venomer merljive s številkami, so pa zelo pomembne pri organizaciji lastne varnosti na vseh področjih – korporativne varnosti. Korporativna varnost, ki bo z ustreznimi ukrepi zagotavljala varnost vseh poslovnih procesov v podjetju, zagotovo na daljši rok ustvarja finančne in druge efekte ter predstavlja konkurenčno prednost podjetja.

Z zavedanjem odgovornosti vodstva podjetja, ki jo prinaša korporativni pristop k varnosti vseh poslovnih procesov in funkcij v podjetju, je Gorenje v tako resnih časih in razmerah za gospodarjenje ohranilo vire in pogoje za doseganje konkurenčne prednosti. Korporativna varnost in vzpostavljanje oziroma ohranjanje realnih pogojev za varnost vseh poslovnih procesov in virov znotraj podjetja, predstavlja eno temeljnih nalog za doseganje ciljev podjetja, med katerimi je tudi zadovoljen kupec. Prav tako je visoka stopnja varnosti in v povezavi s tem ustrezna motiviranost zaposlenih eden od ključnih pogojev za uspešnost podjetja.

Zaposleni na področju Varovanje, kot tudi vsi ostali zaposleni v poslovnih procesih Gorenja se zavedamo korporativne družbene odgovornosti, kamor sodi tudi odgovornost do korporativne varnosti.

Viri

- Čater, T. Oblike konkurenčne prednosti in njihov vpliv na uspešnost podjetja. Pridobljeno 18.02.2013 na http://www.dmslo.si/media/abstract.t.cater.pdf
- Lobnikar, B., Sotlar A. Celovito upravljanje z varnostnimi tveganji kot dejavnik dolgoročne uspešnosti. Pridobljeno 12.12.2010 na
- http://webcache.googleusercontent.com/search?q=cache:62KRgoEDfwYJ:www.fvv.unimb.si/mojFaks/Files/%C4%8Clanek%25206_20081027_51.doc+varnostni+mened%C5%BEment&cd=11&hl=sl&ct=clnk&gl=si
- Lobnikar, B.,(2011). Informacijska podpora korporativni varnosti.Fakulteta za varnostne vede.
- Vršec, M. (1993). Varnost podjetja – tokrat drugače. Ljubljana. Viharnik ■

V okviru otvoritve mednarodne konference
Dnevi korporativne varnosti bo svečana podelitev nagrad

Slovenian Grand Security Award 2012

ICS

Institut za korporativne varnostne študije

Plaza hotel Ljubljana, 20. marec 2013

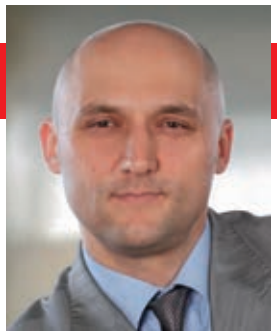
Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikov za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne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

Nagrade bodo podeljene 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: Andrej Kovačič / Institut za korporativne varnostne študije*



INTERNI NADZOR IN NADZOR NAROČNIKOV ZASEBNEGA VAROVANJA NAD DELOM VARNOSTNIH SLUŽB

Zasebno varovanje ima v slovenskem prostoru poseben pomen, zato mora biti nadzor nad njegovim izvajanjem profesionalen, zakonit in dosleden (Kovačič, 2007). Poseben pomen gre pripisovati zato, ker s svojim delovanjem prispeva k zagotavljanju notranje varnosti države. Eden izmed ciljev države je spodbuditi in vzpostaviti različne oblike strokovnega nadzora, s čimer je mogoče prispevati k višji stopnji legitimnosti in kredibilnosti zasebnega varovanja v Republiki Sloveniji.

Gospodarske družbe in ostale organizacije zasebnega in javnega prava, se v več kot polovici primerov[1] odločajo za pogodbeni prenos in skrb za interno varnost na zunanjega izvajalca varovanja - outsorcing. Na ta način glavni management prenese operativno odgovornost in skrb za interno varnost na izvajalca medtem, ko sam še vedno nosi najvišjo odgovornost. Na prvi pogled s t.i. kombinacijo "win win", obe strani pridobita, naročnik zmanjša stroške in se osredotoči na osnovno dejavnost medtem, ko izvajalec proda varnostne storitve. Naročniki pa se morajo pri tem zavedati, da uvajanje outsorcinga pomeni tudi določeno tveganje, saj ne vedo, kdo bo pri njih dejansko izvajal varovanje, kako/če sploh je varnostno osebje preverjeno, iz kakšnega socialnega in kulturnega okolja prihaja, kakšne so njegove delovne izkušnje, ali ima izvajalec profesionalno organiziran interni nadzor itd (Čaleta, 2013). Pri tem nikakor ne smemo pozabiti, da ima varnostnik dostop do večine varovanih prostorov in s tem do premoženja, dokumentacije, informacij, skratka do vitalnih točk poslovanja naročnika. Glede na omenjena dejstva se mora v procesih zagotavljanja korporativne varnosti, naročnik zavedati, da brez lastnega ali najetega zunanjega nadzora, ni mogoče obvladovati vsa tveganja, ki jih v tem pogledu prinaša outsorcing. V okoljih, kjer se management zaveda tovrstnih tveganj in ki je naklonjen k odkrivanju in odpravljanju ugotovljenih nepravilnosti, ima vzpostavljen ustrezen sistem nadzora. Pri tem se je potrebno zavedati, da nadzor prinaša tudi določene ugotovitve, kar posledično ustvarja dodatno delo in skrbi za management, saj je napake in nepravilnosti potrebno odpravljati oziroma se z njimi ukvarjati, kar pa marsikomu ni ravno všeč.

Medsebojna pogodba med izvajalcem in naročnikom mora vsebovati določene nadzorne mehanizme, katerih se naročnik lahko poslužuje, saj so zanj pomembni. Tako lahko ugotavlja ali ima kakovostne storitve ali plačuje zgolj ''papirnato varnost''. Poleg izvajalcev, ki z nizkimi cenami in vprašljivo kvaliteto ''uničujejo'' zasebno varovanje, so tudi naročniki soodgovorni za stanje na tem področju. Naročniki imajo prvič premalo znanja in drugič, se v glavnem odločajo za najnižjo ceno, pri čemer se ne zavedajo, da je lahko na koncu cena, ki jo

Vprašljiva kakovost varovanja in pomanjkanje sistemskega nadzora za obvladovanje tveganj, vpliva na (ne)uspešnost poslovanja naročnika. Tovrstno zavedanje se pogosto pojavi takrat, ko nastopijo težave, ki so zanj lahko usodne.

*avtor je član Slovenskega združenja korporativne varnosti



plačajo veliko večja. Glede na raziskavo je mogoče ugotoviti, da je nadzor naročnikov šibak ali ga sploh ni (Vršec, 2010). Vprašljiva kakovost varovanja in pomanjkanje sistemskega nadzora za obvladovanje tveganj, vpliva na (ne)uspešnost poslovanja naročnika. Tovrstno zavedanje se pogosto pojavi takrat, ko nastopijo težave, ki so zanj lahko usodne. Tveganja, ki jih prinaša vprašljivo varovanje, katerega rezultati so lahko usodni škodni dogodki, v vseh primerih ni mogoče nadomestiti z denarjem. Tukaj imam v mislih predvsem konec poslovanja, izguba ugleda, iznos zaupnih podatkov, informacij in dokumentov, da ne govorimo o izgubi človeških življenj. V nekaterih panogah je (ne)uspešnost poslovanja naročnika lahko tudi v soodvisnosti z izvajanjem varovanja in s tega vidika pri izboru usodno pomembna strateška odločitev managementa.

Interni nadzor v zasebno varnostni službi

Zasebno varnostne službe bi morale imeti vzpostavljen sistematičen in učinkovit sistem internega nadzora, ki bi s svojim delom skrbel predvsem za: opozarjanje zunanjega izgleda in urejenosti varnostnega osebja; izvajanje nadzora nad zakonitostjo in strokovnostjo dela; vzdrževanje profesionalnega in humanega odnosa do zaposlenih; spodbujanje zaposlenih k odličnosti; vzdrževanje kontaktov z naročniki in ostalimi udeleženci ter s svojim pristopom, komunikacijo in zunanjim videzom prispevati k ugledu varnostne službe in poklica nasploh (Kovačič, 2007). Interni nadzor pomaga izvajalcu varovanja pri spremljanju dela in ugotavljanju ali varovanje poteka zakonito, v skladu z zasebno varnostno stroko, poklicno etiko in z navodili naročnika. Pri tem gre za izvajanje notranjega nadzora nad opravljanjem nalog varnostnega osebja pri naročniku varovanja. Nadzor je oziroma bi moral biti podaljšana roka glavnega managementa z integriteto, ki z zaposlenimi vodi ustrezen socialni dialog. Za naročnike in za njihovo varnost bi morala biti pomembna tudi organizacijska klima pri izvajalcu varovanja, kajti ta vpliva na (ne)profesionalno izvajanja varovanja. Še tako dober interni nadzor ne bo mogel vplivati na profesionalnost oziroma kakovost varovanja, če ne bodo urejeni temeljni pogoji in odnosi na relaciji management-varnostno osebje. Za primer, kjer ima glavni management v zasebno varnostni družbi 10-krat višjo plačo od varnostnega osebja, ki je na minimalni plači, ne moremo govoriti o urejenih temeljnih pogojih. V teh primerih je tudi iz strani naročnika iluzorno pričakovati, da bo varnostno osebje profesionalno izvajalo naloge varovanja. Z neurejenimi odnosi in pogoji tudi ni mogoče doseči ustrezne pripadnosti podjetju, ki je v varnostni službi še kako pomembna.

Pogostost in obseg izvajanja nadzora je odvisen od ocenjene stopnje tveganja varovanja oziroma zahtevnosti varovanega objekta. Možnost in način izvajanja nadzora mora biti obvezna sestavina pogodbe med naročnikom in izvajalcem, z natančno določenimi pravicami naročnika in obveznostmi izvajalca. Izvajalec varovanja mora naročniku zagotoviti ažurno in transparentno obveščanje in poročanje ugotovitev internega nadzora ter izdelavo mesečnih in letnih poročil o izvedenih nadzorih na vseh nivojih. Poročilo mora vsebovati tudi ukrepe, ki jih je izvajalec izvedel v primeru ugotovljenih nepravilnosti. Obstaja sicer dilema, ali je mogoče nadzirati samega sebe in nato naročnika obveščati o ugotovitvah, ki bi za izvajalca lahko predstavljalo prekinitev pogodbe o varovanju. Izvajalec mora zagotoviti lasten ali pogodbeni nadzor, ki se izvaja z varnostniki nadzorniki in varnostnimi menedžerji. Gre za osebe, ki morajo biti strokovno usposobljene za opravljanje nadzora in sicer po programu, ki ga do-



loči pristojni minister. ''Med naročnikom in izvajalcem varovanja bi moral biti profesionalen odnos, ki bi zagotavljal obojestransko odgovornost za nedoslednosti in kršitve pogodbe'' (Vršec, 2010).

Nadzor naročnikov nad izvajalcem varovanja – outsorcingom

Gospodarske družbe in ostale organizacije zasebnega in javnega prava imajo različne možnosti izvajanja strokovnega nadzora nad izvajalcem. Učinkovit nadzor je eden izmed osnovnih pogojev za ugotavljanje (ne)izpolnjevanja pogodbenih obveznosti izvajalca ter njegovo (ne)etično delovanje. Nadzor je mogoče izvajati interno in sicer z lastnim strokovnjakom za varnost, ki je usposobljen za izvajanje nadzora nad izvajalcem. Kljub temu ima naročnik možnost, da najame zunanje strokovnjake, ki opravijo nepristranski nadzor nad delom izvajalca. Takšne možnosti ima seveda naročnik tudi v primeru, ko nima zaposlenega strokovnjaka za varnost ali druge osebe, ki bi bila usposobljena za izvajanje nadzora. V obeh primerih je smiselno prepustiti nadzor zunanjim strokovnjakom, ki objektivno analizirajo varnostno situacijo in izdajo strokovno mnenje. Skrb in nadzor nad zagotavljanjem varnosti, kot odgovornosti glavnega managementa vpliva na izboljšanje kakovosti varovanja, kar pomeni možnosti zmanjševanja škode v poslovanju. Pogostost in obseg izvajanja nadzora je odvisen od ocenjene stopnje tveganja varovanja in zahtevnosti varovanega objekta. Nadzor se lahko izvaja kot sprotno nadziranje, kot posamezno presojo ali kot kombinacijo obeh. Prednost sprotnega nadzora je predvsem v hitrejšem odkrivanju pomanjkljivosti oziroma nepravilnosti. Pri tem gre lahko za enkraten nadzor ali za njegovo permanentno izvajanje. V primeru, da naročnik izbere zunanji strokovni nadzor, bo po ugotovljenih in odpravljenih nepravilnostih pridobil certifikat inštitucije, ki je nadzor izvajala. Nadzor je tako namenjen ugotavljanju uresničevanja obstoječih pogodbenih obveznosti, ki jih je potrebno ustrezno prilagajati spremembam in razmeram v poslovnem okolju. Glavni management naročnika s tem pokaže svojo veliko odgovornost in skrb za varnost ljudi in premoženja v svojem poslovnem okolju. Način izvajanja nadzora mora biti sestavni del ustrezno strukturirane pogodbe. To pomeni, da mora biti pogodba zelo natančno definirana. Osnovni namen nadzora nad izvajalcem je, ali se varovanje izvaja zakonito, strokovno in kakovostno ter ali je v skladu s pogodbenimi obveznostmi. Naročniki, ki nimajo internega nadzora oziroma se ne poslužujejo zunanjih strokovnjakov za izvajanje nadzora, so bolj podvrženi varnostnim tveganjem. ''Glede na dejansko stanje v Republiki Sloveniji je nadzor s strani naročnikov varnostnih storitev najšibkejši člen v sistemu nadzora nad zasebnim varovanjem. Nadzor se skorajda ne izvaja, tam kjer se je nesistematičen, površen in ne daje nobenih rezultatov z vidika odgovornosti izvajalca za kršitve (Vršec, 2010).'' Za naročnike zasebnega varovanja, bi moral biti sistematičen nadzor nad delom izvajalcev tako pomemben, kot sama kvaliteta izvajanja varovanja. Zunanji nadzor je eden izmed možnosti, ki naročniku daje informacijo o tem ali je njegovo premoženje in interna varnost ''v pravih rokah''. Nadzor lahko pokaže na mnoge pomanjkljivosti, ki bi se sicer pokazale pri dogodkih, ko jih ne bi bilo več mogoče preprečiti. V nasprotnem primeru lahko nadzor ovrže vse sume o vprašljivem izvajanju varovanja, kar naročniku daje strokovno potrditev medtem, ko izvajalcu referenčno vrednost. Za glavni management gospodarskih družb in ostalih organizacij bi moral biti nadzor nad izvajalcem varovanja – outsorcingom, osnovni standard v poslovanju.

Za naročnike zasebnega varovanja, bi moral biti sistematičen nadzor nad delom izvajalcev tako pomemben, kot sama kvaliteta izvajanja varovanja.

Zaključek

Glede na bolj ali manj znana dejstva menim, da je prišel čas, da naročniki zasebnega varovanja spremenijo svojo miselnost. Pogosto je namreč slišati, da jih ne zanima s kom in kako bo izvajalec izvajal varovanje, koliko je plačano varnostno osebje, ki skrbi za varnost njegovega premoženja, temveč le pričakuje, da bo to opravljeno v skladu s sklenjeno pogodbo. Glede na to, da je varnost ena izmed komponent obstoja in uspešnosti poslovanja poslovnih subjektov, je to vsekakor premalo. Zaradi omenjenega potrebujejo naročniki nad izvajalci, ki skrbijo za varnost, kot vitalne točke poslovanja tudi ustrezen nadzor. Pri tem je zanimivo dejstvo, da gospodarske družbe in ostale organizacije zasebnega in javnega prava, redko zaposlujejo strokovnjake za varnost, ki bi bili med drugim usposobljeni tudi za izvajanje nadzora nad izvajalcem varovanja. Prav tako se naročniki premalo poslužujejo zunanjih strokovnjakov za izvajanje strokovnega nadzora. Seveda se ne smemo izogniti povezanosti nizke cene in vprašljive kakovosti varovanja, pri čemer je nadzor še toliko bolj potreben. Zanimiv je tudi podatek ene izmed raziskav Šretl in Vršec iz leta 2010 o merjenju zadovoljstva naročnikov z varnostnimi storitvami, ki pravi, da so naročniki v glavnem zadovoljni z izvajalcem varovanja. Nadzor nad osebami, ki skrbijo za varnost je tako pomembna dejavnost, ki je ni dobro prepuščati naključjem. To velja še predvsem zaradi dejstva, da kar 61,5 % varnostnikom delo predstavlja le nek izhod v sili, s čimer rešujejo svoj trenutni ekonomski položaj in da je njihova fluktuacija velika (Makše in Čas, 2009).

Menim, da se lahko s skupnim izvajanjem nadzora s strani naročnikov oziroma najetih strokovnjakov in internega nadzora izvajalca, pozitivno pripomore k dvigu kakovosti varovanja. Dobrodošle in pozitivne so tudi možnosti sodelovanja na več nivojih in sicer, kot skupni nadzor inšpektorata RS za notranje zadeve, Zbornice RS za razvoj zasebnega varovanja in naročnika z lastnimi ali zunanjimi strokovnjaki za varnost. Tovrstni nadzori bi zagotovo pokazali ali so naročniki dejansko lahko zadovoljni z izvajalcem varovanja. Torej obstajajo veliki izzivi za prihodnost, pri čemer bi omenjene možnosti sodelovanja sigurno prispevale k višji stopnji legitimnosti in kredibilnosti zasebnega varovanja v Republiki Sloveniji. Za naročnike pa bi moral biti vsekakor pomemben celovit nadzor, ki bi zajemal tudi področje tehničnega varovanja. To področje bi moralo biti pomembno tudi za zavarovalnice[2], kjer bi se izvajal nadzor, ali so izvajalci tudi dejansko montirali ustrezno certificirane komponente[3] v protivlomne in ostale sisteme.

Zaradi izmenjave mnenj in dobre prakse ter pridobivanja strokovnih informacij bi se naročniki zasebnega varovanja morali medsebojno združevati. V slovenskem prostoru že obstaja takšno združevanje in sicer v okviru Slovenskega združenja za korporativno varnost, ki je del Instituta za korporativne varnostne študije, ICS-Ljubljana. V omenjenem institutu smo pripravili rešitve, ki vam bodo na področju izvajanja internega nadzora omogočale dvig kvalitete varnostnih storitev.

Viri

- Čaleta, D. (2013). Procesi outsorcinga in dejavniki izbora zunanjih izvajalcev – dileme in izzivi. Institut za korporativne varnostne študije. ICS Ljubljana.
- Vršec, Mir. (2010), Nadzor nad zasebnim varovanjem – dileme in izzivi. Dnevi zasebnega varovanja, Bled.
- Strategija na področju zasebnega varstva (2010). Ministrstvo za notranje zadeve RS.
- Makše K. in Čas T. (2009). Varnostnik – poklic ali zgolj izhod v sili. Univerza v Mariboru. Fakulteta za varnostne vede, Ljubljana.
- Kovačič, A., (2007). Zunanji in notranji nadzor v zasebno varnostni družbi. Diplomsko delo. Ljubljana. Fakulteta za varnostne vede.
- http://www.ics-institut.com/
- http://www.zrszv.si/
- http://zakonodaja.gov.si/rpsi/r00/predpis_ZAKO5760.html
- http://search.babylon.com/kombinacija+win+win. Pridobljeno dne 22.1.2013. ■

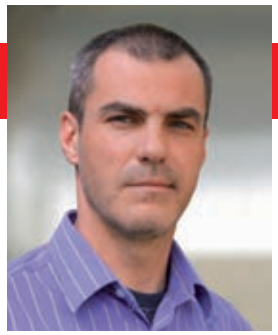
1 Analiza slovenskih podjetij je pokazala, da se v 55 % odločajo za outsorcing varovanja (Kavčič, K., 2007 v Čaleta. D., 2013).

2 Zavarovalnice zavarujejo premoženje in ostale odgovornosti uporabnika oziroma izvajalca varovanja.

3 Senzorji in ostale komponente pri izvajanju tehničnega varovanja se lahko zelo razlikujejo glede na kvaliteto in ceno ter s tem posledično na njihovo zanesljivost v delovanju.

Zaradi izmenjave mnenj in dobre prakse ter pridobivanja strokovnih informacij bi se naročniki zasebnega varovanja morali medsebojno združevati. V slovenskem prostoru že obstaja takšno združevanje in sicer v okviru Slovenskega združenja za korporativno varnost, ki je del Instituta za korporativne varnostne študije, ICS-Ljubljana. V omenjenem institutu smo pripravili rešitve, ki vam bodo na področju izvajanja internega nadzora omogočale dvig kvalitete varnostnih storitev.

Avtor: Domen Pirkmajer / korporativno varnostni manager, TE-TOL*



MODEL ZA IZBOR IZVAJALCA FIZIČNIH STORITEV ZASEBNEGA VAROVANJA

Do dviga kvalitete varnostnih storitev lahko pridemo tudi na podlagi ustreznih razpisnih meril za izbor najugodnejšega ponudnika. Naročniki varnostnih storitev smo sami v celoti odgovorni za izbor kvalitetne storitve, ki je še vedno cenovno sprejemljiva in nam na dolgi rok zagotavlja ustrezno obvladovanje varnostnih tveganj v naših organizacijah.

Razvoj družbe in razmah zasebne lastnine, v novo nastali slovenski državi, sta narekovala tudi razvoj zasebnega varovanja. Tako so se, kot vsaka storitev, tudi storitve zasebnega varovanja znašle na trgu. Slovenski trg varnostnih storitev je preživel že marsikaj, od dumpinških prevzemov, stečajev varnostnih podjetij, pa vse do medosebnih »obračunavanj« zasebno varnostnih podjetij, ko je šlo za zadržanje posla ali pridobitev novega, seveda v teh primerih ni šlo za zdravo konkurenco.

Tisti, ki se z varnostjo profesionalno ukvarjamo, se »krvne slike« zasebnega varovanja, ki kaže na slab ugled panoge v javnosti, na nezakonito izvajanje nosilcev licenc in na nizko tržno vrednost poklica, še kako zavedamo. Vzroke, ki so do takšnega stanja pripeljali, lahko najdemo predvsem v slabem nadzoru, ki nosilcem licenc omogoča nezakonito izvajanje varnostnih storitev, interesu posameznikov/skupin, zaradi česar trpijo razvoj in koristi panoge, nestrokovnem vodenju in usmerjanju varnostnega osebja, ki se kaže v slabem in nestrokovnem izvajanju storitev zasebnega varovanja, zaposlovanju neustreznega kadra, ki krni ugled panoge v javnosti, nestimulativnem osebnemu dohodku in pogojih dela varnostnega osebja, kar posledično pripelje do nemotiviranosti varnostnega osebja za delo.

Tisti, ki se z varnostjo profesionalno ukvarjamo, se »krvne slike« zasebnega varovanja, ki kaže na slab ugled panoge v javnosti, na nezakonito izvajanje nosilcev licenc in na nizko tržno vrednost poklica, še kako zavedamo.

Slabo, če sploh, plačano varnostno osebje predstavlja resno grožnjo varnostnemu sistemu podjetja, ki ga varuje. Tega dejstva bi se moral zavedati vsak naročnik!

Vendar, če velja, da se ponudba izoblikuje na podlagi povpraševanja, moramo naročniki varnostnih storitev velik del krivde za takšno stanje v panogi pripisati sebi. Slabo, če sploh, plačano varnostno osebje predstavlja resno grožnjo varnostnemu sistemu podjetja, ki ga varuje. Tega dejstva bi se moral zavedati vsak naročnik! Torej, če je grožnja identificirana, jo je potrebno obravnavati in se nanj ustrezno odzvati. Ena izmed rešitev, ki zagotavlja socialno varnost in ustrezne delovne pogoje najetemu varnostnemu osebju je v postavitvi modela, ki plače varnostnega osebja vključuje v vrednotenje ponudb.

Model postavlja ceno, kot vrednoteni pogoj, v razmerje. Glede na obseg in zahtevnost pogodbenih del smo v TE-TOL-u to razmerje postavili 60 : 40. Od stotih možnih točk prinese najnižja ponudbena vrednost 60 točk, najvišja plača varnostnika pa 40 točk. V našem primeru so bile štiri različne plače za štiri različno zahtevna delovna mesta, ki so vsaka prinesle največ 10 točk. Model se lahko prilagaja glede na specifiko potreb naročnika varnostnih storitev. Bistveno je, da določimo minimalno osnovno plačo in jasno navedemo, kaj je v tej plači za-

*avtor je član Slovenskega združenja korporativne varnosti

jeto. Tako se izognemo raznim akrobacijam in sprenevedanjem, ko je treba izbranemu ponudniku plače nakazati varnostnemu osebju. Seveda pa je potrebno v samem razpisu enako skrb posvetiti ostalim zahtevam, ki jih dosežemo s postavitvijo obveznih in prednostnih pogojev.

Model nam omogoča, da nadzorujemo komponento, na katero do sedaj nismo imeli vpliva, je pa bistvena za kakovostno izvajanje varnostnih nalog. To so plače najetega varnostnega osebja. S tem najetemu varnostnemu osebju pokažemo, da nam ni vseeno za njihov socialni položaj, da cenimo njihovo delo in da so pomemben del v verigi varnostnega sistema, kateremu pripadajo. Vse to se nam obrestuje v motiviranosti in samoiniciativnosti varnostnega osebja pri delu, predvsem pa s tem pridobimo pripadnost varnostnega osebja do podjetja, ki ga varuje. Zgodi se, da ima varnostnik višjo pripadnost podjetju ki ga varuje, kot svojemu delodajalcu. Cena? Manj dobička za delodajalca, socialna varnost varnostnega osebja in dvig kvalitete varnostnih storitev za naročnika.



Primer izbire ponudnika

Pogoje, ki jih mora izpolnjevati varnostno osebje določimo v razpisni dokumentaciji (obvezni pogoji, prednostni pogoji...): izobrazba, posebna znanja, delovne izkušnje, računalniška pismenost, znanje tujih jezikov itd.

Merila za ocenitev in izbiro ponudbe so naslednja:

Ponudbena vrednost	do 60 točk
Plača delavca za vodenje varnostnih storitev	do 10 točk
Plača delavca za izvajanje varnostnih storitev	do 10 točk
Plača delavca za vodenje požarno-preventivnih storitev	do 10 točk
Plača delavca za izvajanje požarno-preventivnih storitev	do 10 točk
SKUPAJ	**Max. 100 točk**

Opomba: *Obvezno določiti minimalne osnovne bruto ali neto plače varnostnega osebja z jasno definicijo, kaj je zajeto v plači.*

Ponudbena vrednost ☒ Max. št. točk 60:
Število točk za ponudbo se določi po enačbi:
ŠTt = (PVn / PVp) x 60

ŠTt = število točk, ki jih dobi ponudba
PVn = najnižja ponudbena vrednost
PVp = ponudbena vrednost primerjane ponudbe

Plača delavca za vodenje varnostnih storitev ☒ max. št. točk 10:
Število točk za ponudbo se določi po enačbi:
ŠTt = (BPp / BPn) x 10

Plača delavca za izvajanje varnostnih storitev ☒ max. št. točk 10:
Število točk za ponudbo se določi po enačbi:
ŠTt = (BPp / BPn) x 10

Plača delavca za vodenje požarno-preventivnih storitev ☒ max. št. točk 10:
Število točk za ponudbo se določi po enačbi:
ŠTt = (BPp / BPn) x 10

Plača delavca za izvajanje požarno-preventivnih storitev ☒ max. št. točk 10:
Število točk za ponudbo se določi po enačbi:
ŠTt = (BPp / BPn) x 10
ŠTt = število točk, ki jih dobi ponudba
BPp = ponujena osnovna bruto plača primerjane ponudbe
BPn = najvišja ponujena osnovna bruto plača

Delovna mesta	Št.ur	PONUDBA A	PONUDBA B	PONUDBA C	PONUDBA D
Vodja varnostnikov	2500	8,70 €/uro	9,20 €/uro	9,00 €/uro	9,80 €/uro
Varnostnik	7500	7,90 €/uro	8,10 €/uro	8,20 €/uro	8,50 €/uro
Vodja gasilcev	2500	9,50 €/uro	9,80 €/uro	10,00 €/uro	11,30 €/uro
Gasilec	7500	8,50 €/uro	8,60 €/uro	8,40 €/uro	9,20 €/uro
Ponudbena vrednost		**168.500,00 €**	**172.750,00 €**	**172.000,00 €**	**185.500,00 €**
Vrednotenje		**60,00 točk**	**58,52 točk**	**58,78 točk**	**54,50 točk**

Tabela 1: *Simulacija izračuna – PONUDBENA VREDNOST*

$ŠT_A=(PV_A/PV_A)x60;\quad ŠT_B=(PV_A/PV_B)x60;\quad ŠT_C=(PV_A/PV_C)x60;\quad ŠT_D=(PV_A/PV_D)x60$

Delovna mesta	Min. osnovna bruto plača	A Osnovni bruto OD	B Osnovni bruto OD	C Osnovni bruto OD	D Osnovni bruto OD
DM1 Vodja varnostnikov	850,00 €	850,00 €	880,00€	870,00 €	860,00€
DM2 Varnostnik	750,00 €	750,00 €	780,00 €	760,00 €	750,00€
DM3 Vodja gasilcev	870,00 €	870,00 €	900,00€	880,00€	870,00€
DM4 Gasilec	820,00 €	820,00 €	880,00€	830,00 €	820,00€

Tabela 2: *Simulacija izračuna – PLAČE ZAPOSLENIH*

$ŠT_{DM1}=(BPp/BPn)x10;\quad ŠT_{DM2}=(BPp/BPn)x10;\quad ŠT_{DM3}=(BPp/BPn)x10;\quad ŠT_{DM4}=(BPp/BPn)x10$

Delovna mesta	Min. osnovna bruto plača	A Osnovni bruto OD	B Osnovni bruto OD	C Osnovni bruto OD	D Osnovni bruto OD
DM1 Vodja varnostnikov	850,00 €	9,66	10,00	9,89	9,77
DM2 Varnostnik	750,00 €	9,62	10,00	9,74	9,62
DM3 Vodja gasilcev	870,00 €	9,67	10,00	9,78	9,67
DM4 Gasilec	820,00 €	9,32	10,00	9,43	9,32
Vrednotenje		**38,27 točk**	**40,00 točk**	**38,84 točk**	**38,38 točk**

Tabela 3: *Plače varnostnega osebja – VREDNOTENJE*

	Ponudbena vrednost	Plače varnostnega osebja	∑	Izbor
Ponudnik A	60	38,27	**98,27**	**2**
Ponudnik B	58,52	40	**98,52**	**1**
Ponudnik C	58,78	38,84	**97,62**	**3**
Ponudnik D	54,50	38,38	**92,88**	**4**

Tabela 4: *Končni rezultati* ■



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 ali www.ics-institut.com.

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

SKUPAJ SMO MOČNEJŠI!

MARIBORSKI VODOVOD

LUKA KOPER Port of Koper

REISSWOLF secret. service.

TelekomSlovenije

SIEMENS

20 let MIŠKA FMC Group

Zanesljivo vsepovsod POŠTA SLOVENIJE

DARS

Nova KBM PRIPRAVLJENI NA JUTRI

univerzitetni klinični center ljubljana

gorenje Gorenje, d.d.

TE-TOL

INFORMACIJSKI POOBLAŠČENEC

Avtor: Mag. Marko Potokar / Urad Informacijskega pooblaščenca



SMO (ŽE) POSTALI DRUŽBA NADZORA? I. DEL

Današnji svet je prežet s tehniko in brez nje si ga kar ne moremo več predstavljati.

Že dolgo tega je novodobni način življenja spremenil status avtomobila iz razkošja v potrebo. Potrebo, ki je razkošno opremljena z informacijskimi pripomočki: od tistih, ki rešujejo življenje, omogočajo lagodnejšo vožnjo ter optimalno pot do izbranega cilja, do tistih, ki vozniku odvračajo pozornost in oči z (ob)cestnega dogajanja. Večino komunikacije opravimo s pomočjo prenosnega telefona, na delovnem mestu je elektronska pošta postala osnovni medij za izmenjavo sporočil, z njeno pomočjo sklicujemo sestanke med katere smo razpeti, v osebnem življenju nas na (ne)pomembne stvari opozarja urnik v prenosnem telefonu. Če kaj ne postorimo na delovnem mestu, lahko to opravimo od doma, saj nam to omogoča naš priljubljeni prenosni računalnik. Družabne stike mnogi nadomeščajo z uporabo spletnih klepetalnic in drugih socialnih omrežij, mnogi tudi z brezštevilnim pošiljanjem kratkih sporočil. Svet je postal hiter, informacij je vse več, dostopne so v trenutku, vsiljujejo se nam z oglasnih panojev ob cestah, da o televiziji in radiu ne govorimo. Živimo v digitalnem svetu v katerem štejejo natančnost, dejstva in podrobnosti, številke in čas. In temu primerne so tudi tehnologije, ki se uporabljajo za nadzor posameznikov in množice. Nevarno postaja dejstvo, da smo se nekaterih oblik nadzora že tako navadili, da se jih več niti ne zavedamo.

Družba nadzora

Kratka zgodovina nadzora

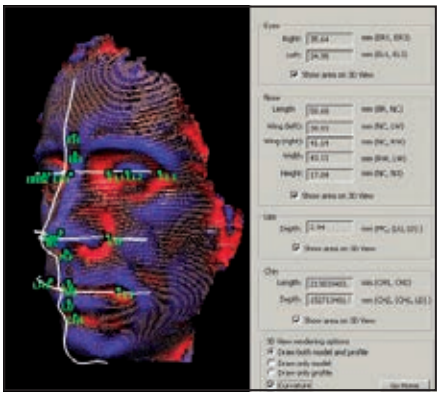
Določene oblike nadzora so obstajale že v prazgodovini, ko so ljudje 'nadzorovali' drug drugega zaradi medsebojne pomoči, kar jim je omogočalo uspešnejše preživetje v divjem prvinskem svetu. Torej se je potreba po nadzoru prvotno pojavila zaradi zagotavljanja varnosti, ki je po hierarhični teoriji potreb Abrahama Maslowa uvrščena na drugo najvišje mesto - takoj za fiziološkimi potrebami. Ko so le-te zadovoljene, se pojavi človekova potreba po zavarovanju pred fizično in psihično škodo. Šele, ko je potreba po varnosti zadovoljena, pridejo do izraza potrebe po pripadnosti, spoštovanju in samoizpolnjevanju. Tako nam postane jasno, zakaj smo ljudje, ko se počutimo ogrožene, za varnost pripravljeni žrtvovati marsikaj.

Z razvojem družbe in organizacijskih oblik so neformalne zamenjale formalne oblike nadzora, torej nadzor, ki ga vrši vladajoči razred oziroma država. Osnovni model, ki opisuje kako nadzor deluje je hipotetični zapor imenovan Panoptikon, ki ga je leta 1791 razvil filozof in pravnik Jeremmy Bentham. Model opisuje okroglo stavbo na obodu katere so zaporniške celice, ločene tako, da med zaporniki ni možna komunikacija. V centru stavbe je prostor v katerem se nahajajo pazniki in iz katerega je kadarkoli moč videti (in slišati) v katerokoli zaporniško celico, brez da bi zaporniki za to vedeli. Hkrati pa je zapor odprt tudi za obiskovalce, ki nadzorujejo tako zapornike kot paznike. Osebe, ki so nadzorovane se tako vedno čutijo pod nadzorom. Nadzor torej temelji na medsebojnem nezaupanju, od zapornika pa se pričakuje, da se bo obnašal tako kot se od njega zahteva in da ne bo niti pomislil, da bi storil kaj narobe. Model Panoptikona je razširil Michael Foucault z modelom družbe disciplíniranja, ki temelji s prehajanjem posameznikov med posameznimi zaprtimi sistemi (Panoptikoni), v katerih je možen popoln nadzor nad posameznikom: od doma (družine) v šolo, službo, vojsko ipd. Posameznik tako nikoli ne ve, kdaj ga oblast 'gleda'.

Moderna družba nadzora

Ko govorimo o moderni družbi nadzora (angl. Surveillance Society) pri tem mislimo na družbo v kateri so naše vsakodnevne aktivnosti avtomatsko zabeležene s pomočjo tehničnih naprav. Točka preskoka se je pojavila po drugi svetovni vojni z razvojem novih komunikacijskih sistemov, danes poznanih pod skupnim imenom informacijske tehnologije (IT). Pravzaprav danes že živimo v družbi nadzora: video nadzorne kamere nas že dolgo časa opazujejo na

Nevarno postaja dejstvo, da smo se nekaterih oblik nadzora že tako navadili, da se jih več niti ne zavedamo.



bencinskih servisih, v nakupovalnih središčih, na parkiriščih in (avto)cestah ter križiščih in tunelih, v podjetjih, šolah in na igriščih, ob prehodu preko državne meje, v zobozdravstvenih in drugih čakalnicah. Ob prihodu v službo se večina izmed nas registrira s svojo elektronsko kartico, pri čemer se v elektronsko podatkovno bazo zabeležijo naši identifikacijski podatki in mesto ter čas prihoda, za nameček nas posname še video nadzorna kamera (ali več njih), podobno velja pri plačevanju s plačilnimi ali kreditnimi karticami, pri čemer se podatki o nas in naših nakupih shranjujejo v informacijskih sistemih ponudnikov storitev, enako velja za kartico zaupanja (res posrečen izraz), ki nam jo na videz brezplačno ponujajo trgovci, v zameno za osebne podatke in kasnejše določanje naših kupnih navad in še česa. V zdravstvu smo že pozabili na papirne zdravstvene knjižice in skoraj že tudi na prehod iz decentraliziranega sistema zdravkomatov na centralni podatkovni sistem. Ko komuniciramo s pomočjo mobilnega telefona naš operater beleži in hrani podatke o tem, katero številko smo klicali, koliko časa je trajala zveza, na kateri lokaciji smo se nahajali, z ustreznim 'zahtevkom' uradnih organov pa tudi vsebino našega pogovora. Ko se na videz svobodno sprehajamo po spletu, nas po njem zares usmerjajo posebni algoritmi in nam predlagajo izbrane spletne strani na podlagi predhodno pridobljenih informacij o tem, kje se ponavadi sprehajamo, kaj iščemo in sklepajo kaj si želimo. Ko si z globalnim sistemom navigacije (GPS) razvajeno pomagamo do želene lokacije praviloma ne pomislimo, da nas tako spremlja globalni Veliki brat, ki je sistem razvil predvsem v vojaške namene in natančnost lokacije prilagaja glede na trenutne varnostno-politične razmere določenega prostora. Če smo bolj ekološko usmerjeni in uporabljamo javna prevozna sredstva naš vstop v avtobus LPP zabeleži sistem Urbane, znotraj njega pa nas za vsak slučaj snema video-nadzorna kamera, ko gremo v knjižnico za hitrejšo storitev poskrbi taista 'enotna mestna kartica', ki

Z razvojem tehnologije pa je družbeni nadzor dobil neslutene razsežnosti.

»...je brezkontaktna pametna kartica, ki omogoča hitro in udobno brezgotovinsko plačilo vožnje z ljubljanskimi mestnimi avtobusi, z vzpenjačo na Ljubljanski grad, parkirnino na belih conah in parkiriščih v upravljanju Javnega podjetja Ljubljanska parkirišča in tržnice ter storitve Mestne knjižnice Ljubljana. Kasneje pa boste Urbano lahko uporabili tudi ob obisku muzejev, športnih zavodov in kulturnih prireditev.«, kot nam obljublja spletna stran Urbane.

Napisano velja za slovenski prostor. Seveda pa nadzor ni omejen z državnimi mejami in če uporabljate socialna omrežja, kot je recimo Facebook, bo za vas morda zanimiva še vedno sveža informacija, da je *»ameriško podjetje Raytheon, specializirano za razvoj in proizvodnjo vojaške in obveščevalne opreme, izdelalo informacijsko rešitev Riot (Rapid Information Overlay Technology), ki omogoča sledenje posamezniku in celo napovedovanje njegovih prihodnjih ravnanj - vse to le na podlagi podatkov, ki jih oseba objavi na družbenih omrežjih in drugje na spletu.«*, kot na svoji spletni strani navaja DNA. Ta informacija nam jasno kaže, kako velike razsežnosti lahko dobi združevanje podatkov o posamezniku na enem mestu. Omenjena tehnologija lahko tako zgradi skoraj popoln profil posameznika z vsemi njegovimi navadami in ga tako spremlja ter napoveduje, kje se bo nahajal in kaj bo počel. Seveda predstavniki podjetja zatrjujejo, da omenjene tehnologije še niso prodali nikomur – ha!

Nadzorne tehnologije

Pravzaprav je nadzor star toliko kot človeštvo. Prvotni nadzor je bil nadzor ljudi nad ljudmi z metodami prisluškovanja, opazovanja, vohunjenja, zasliševanja, sledenja, brskanja po smeteh, socialnega inženiringa, detektivskega dela, ovaduštva, dela pod krinko itd. Ti sistemi so bili dodelani do potankosti, kar je nazorno prikazano v filmu *Življenja drugih (Das Leben der Anderen)*, ki nam pokaže kakšen vrhunski sistem nadzora se da narediti s papirjem in svinčnikom, preprostimi mikrofoni ter z ustrezno motiviranimi operativci. Človeške tovrstne tehnike obstajajo še danes, nadzor se vrši tudi v civilni in zasebni sferi v obliki intervjujev za pridobitev socialne in medicinske pomoči, kredita, zaposlitve, zavarovanja, popisa prebivalstva, izpolnjevanja obrazcev za pridobitev ugodnosti pri nakupovanju in izpolnjevanja raznovrstnih anket. Pozabljamo pa, da obstajata še dve obliki nadzora ljudi nad ljudmi: preverjanje alkoholiziranosti in pregled posameznikov, osumljenih kriminalnega dejanja. Obe obliki nadzora sicer lahko vključujeta uporabo tehničnih naprav (merilniki alkohola v izdihanem zraku, naprave za odkrivanje kovin ipd.), vendar gre v osnovi za subjektivno presojo in človekovo odločitev nad kom izpeljati postopek (eno izmed poročil o družbenem nadzoru navaja, da so v Veliki Britaniji temnopolti posamezniki kar šestkrat pogosteje kontrolirani kot belopolti prebivalci). Z razvojem tehnologije pa je družbeni nadzor dobil neslutene razsežnosti.

Računalniške podatkovne zbirke

Temelj vseh novih nadzornih tehnologij so računalniške podatkovne zbirke. V njih so zbrane nepredstavljive količine podatkov, urejenih po različnih kriterijih, kar omogoča avtomatsko in hitro pregledovanje in pridobivanje novih informacij o posameznikih. Podatkovne baze se med seboj povezujejo, množice podatkov med seboj primerjajo, kar omogoča identifikacijo posameznikov in odkrivanje sumljivih vzorcev vedenja. Centralizacija podatkov omogoča večjo učinkovitost in hitrost obdelovanja podatkov. Vsaka transakcija, ki jo opravi posameznik je zabeležena pa naj bo to uporaba plačilnih in kreditnih kartic, mobilnih telefonov, interneta, plačevanje storitve s kartico zaupanja

Tako oblikovane podatkovne baze se lahko povezujejo z drugimi sistemi nadzora, kot so recimo video nadzorni sistemi in z uporabo ustreznih algoritmov lahko taki sistemi pravzaprav popolnoma razgalijo posameznika in ga oropajo zasebnosti.



ali uporaba storitev javnega sektorja. Tako oblikovane podatkovne baze se lahko povezujejo z drugimi sistemi nadzora, kot so recimo video nadzorni sistemi in z uporabo ustreznih algoritmov lahko taki sistemi pravzaprav popolnoma razgalijo posameznika in ga oropajo zasebnosti. Znan je primer, ko je ena izmed trgovskih verig pričela neki najstnici pošiljati reklamne letake, kjer so se med čokoladami in šminkami pričele pojavljati tudi plenice, otroški vozički in podobni artikli. V podjetju so namreč na podlagi analiz dekletovih prejšnjih nakupov ugotovili, da je dekle zanosilo (več o tem v knjigi The Power of Habit avtorja Charlesa Duhigga).

Telekomunikacije

Pod telekomunikacije poleg klasičnega (stacionarnega) telefonskega omrežja uvrščamo tudi mobilno in računalniško komunikacijsko omrežje z vsemi oblikami komunikacije (glas, tekst, zvok, slika, lokacijski podatki itd.). Z razvojem na področju komunikacijske tehnologije so se spremenile tri stvari: uporabljati so se pričeli mobilni telefoni, optična vlakna in brezžično povezovanje, prišlo je do povezovanja telekomunikacij in računalniškega obdelovanja podatkov, telekomunikacijska podjetja so pričela prehajati v zasebno lastništvo. Vse skupaj je pripeljalo do združevanja tehnologij in medsebojne operabilnosti, kar po domače pomeni, da so različne tehnologije med seboj pričele delovati povezano, tesnejša povezava pa pomeni več informacij in s tem možnost večjega nadzora.

Video nadzorni sistemi

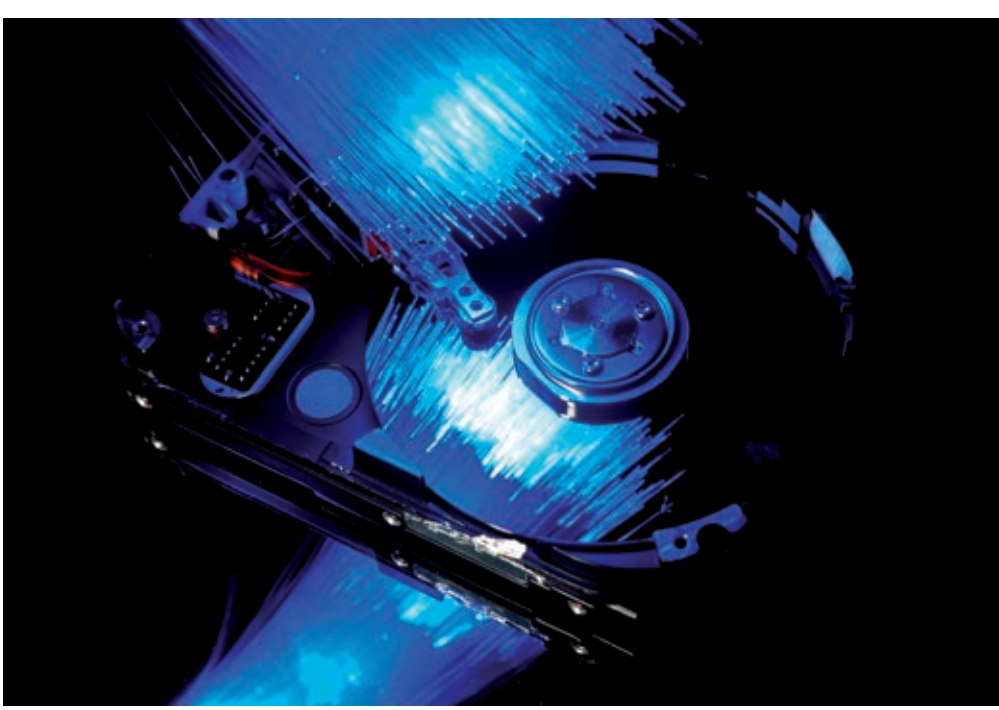
Fotografski nadzor je v uporabi mnogo dalj časa kot si večina izmed nas predstavlja. Praktično od izuma kamere, se je fotoaparat uporabljal za beleženje obrazov in drugih fizičnih značilnosti kriminalcev. Video nadzor na ulicah Velike Britanije se je npr. uporabil pri kronanju angleške kraljice Elizabete II leta 1953, trajno pa se je začel po ulicah nameščati leta 1960. S pojavom digitalnih video nadzornih sistemov je prišlo tudi do razvoja t.i. inteligentnih video nadzornih sistemov (ki so že v uporabi tudi v Sloveniji), najprej kot sistemov za prepoznavo registrskih tablic. Seveda se uporaba teh sistemov ni ustavila na področju varovanja ljudi in premoženja, ampak sega tudi v marketinške vode od sistemov za štetje kupcev in njihovega gibanja v prodajalnah, do sistemov za prepoznavo starosti in spola kupcev.

Biometrija

Skoraj vsi moderni sistemi za identifikacijo uporabljajo (tudi) biometrične značilnosti posameznikov: prstni odtis, odtis dlani, značilnosti roženice, glasovno prepoznavo, obrazno topografijo itd. Biometrične značilnosti so zabeležene na potnih listinah, osebnih računalnikih ali identifikacijskih vstopnih karticah. Največja nevarnost masovne uporabe te tehnologije se skriva v zlorabi le-te. Predstavljajmo si, da policija na prizorišču kaznivega dejanja odkrije posameznikovo DNK, ki jo je tja namestil pravi storilec. Verjamem, da bo nedolžni posameznik moral dokazovati svojo nedolžnost, kar bo veliko večji izziv, kot če bi na prizorišču našli 'samo' njegovo denarnico, ki so mu jo pred časom ukradli.

Zaključek

Seveda pa nadzor sam po sebi ni nekaj negativnega, tako kot orodje še ni orožje. Lahko pa to hitro postane. Enako velja za (informacijsko) tehnologijo, ki nam je prinesla veliko dobrega in polno koristi: od avtomatizacije in s tem razbremenitve človeka, do učinkovitejšega obvladovanja procesov, povečanja kvalitete življenja, časovnih prihrankov, lagodnejšega bivanja, zabave in počitka. Prav tako nobena tehnologija ni posebej nevarna, če se uporablja sama zase, se pa nevarnost zlorabe lahko poveča, če pride do njihovih združevanj. Tehnologija (tudi informacijska) je samo podaljšek roke. V kakšne namene se uporablja pa je odvisno od uporabnika le-te. ■



Avtor: Ivo Mak Mekinc / Vodja Oddelka Fire Safety & Security Solutions – Siemens d.o.o.*



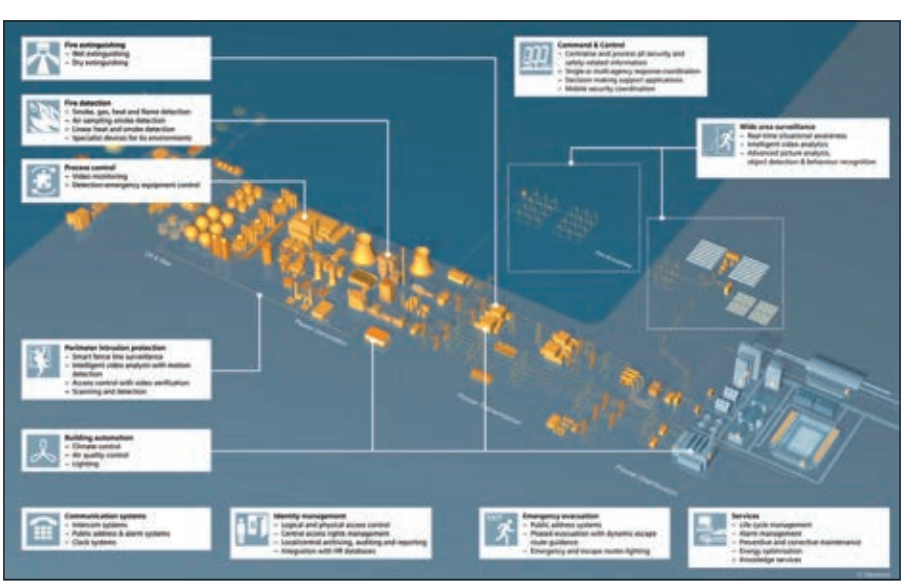
BITI VAREN TUDI JUTRI

Moderna mesta in urbana območja postajajo vedno bolj občutljiva na naravne katastrofe, napade in infrastrukturne prelome oziroma ločitve. Varna območja so tam, kjer so sistemi med sabo integrirani in vodeni s strani organizacije, ki najbolj učinkovito obdeluje trenutno prejete podatke in informacije. Pod določenimi pogoji lahko tehnologija bistveno prispeva k preprečevanju razvoja tveganih in nevarnih situacij.

Mesta si skupaj s pokrajinami prizadevajo za izboljševanje kakovosti življenja svojih prebivalcev, s čimer je povezana tudi njihova uvrstitev na različnih indeksih in lestvicah. Odgovorne administracije želijo za dosego postavljenih ciljev zagotavljati varnostne postopke in storitve, ki so prijazne do okolja in v skladu s postavljeno nacionalno varnostno politiko in veljavno zakonodajo.

Nihče ni dovolj bogat, da bi kupoval poceni

Mesta in urbana območja morajo seveda zagotavljati varnost, saj potem postanejo privlačna za prebivalce in investitorje. Žal pa ni vedno dolgoročno najbolje, da se po opravljeni analizi ugotavljanja ranljivosti, ogroženosti, ocene tveganj in poslovnih uspešnosti upošteva najcenejšo možno izbiro tehnologije in storitev, potrebnih za delovanje določene infrastrukture. Kritična infrastruktura žal ne dopušča slabih izbir, kot so nizka cena, nekvalificirano osebje, nekompetentnost pri ponudbi in izbiri rešitev. Svoboda gibanja, visoka stopnja zasebnosti in varovanja osebnih podatkov so danes vrednote, zaradi katerih ljudje nismo naklonjeni popolnemu nadzoru javnih površin kjerkoli in kadarkoli. Prav to pa pomeni, da morajo podjetja oziroma organizacije same poskrbeti za načrtovanje in izvedbo varovanja svojih površin in objektov.



***Slika 1:** Primer območja pridobivanja in distribucije električne energije, možnih in potrebnih vgrajenih varnostnih sistemov in nujnih medsebojnih povezav z organiziranimi interakcijami.*

Samo prenos informacij v nadzorni center ni dovolj

Sama vgradnja vrhunske opreme za nadzor in varovanje perimetrije, prostorov, prometa v povezavi z dobro usposobljenimi oddelki intervencijskih skupin, reševalcev oziroma varnostnih družb ne zadostuje, če obenem ne posvetimo pozornosti tudi koordiniranemu izvajanju in predhodno načrtovanemu reševanju dobrin ter evakuaciji oseb. Vse pogosteje se dogajajo zastoji pri umikih in nesporazumi pri posredovanjih ali reševanjih zaradi nestrokovnih oziroma nedodelanih reakcij, različnih informacij, nasprotujočih in neusklajenih napotkov ter neznanja in neusposobljenosti udeležencev.

Samo prenos informacij na dežurno intervencijsko mesto torej ni več zagotovilo za uspešno reševanje. Sodobne tehnologije omogočajo prenos podatkov in trenutnih informacij odgovornemu osebju po pripravljenih scenarijih istočasno na različne mobilne sisteme (pametne telefone, dlančnike,...), dopolnjene s potrebnimi, predhodno pripravljenimi navodili oziroma scenariji. Medsebojno sodelovanje in usklajevanje intervencijskega, re-

*Siemens d.o.o. je član Slovenskega združenja korporativne varnosti

Samo prenos informacij na dežurno intervencijsko mesto torej ni več zagotovilo za uspešno reševanje.

ševalnega in odgovornega osebja glede na informacije, pridobljene v realnem času, je za zmanjševanje rizika nujno. Ukrepanje na različnih mestih zahteva vsakič prilagojene scenarije, ki so odvisni tako od vzroka nevarnosti kot tudi od same lokacije. Grožnja s terorističnim napadom se razlikuje od grožnje ropa ali napada, način ukrepanja pa je odvisen tudi od tega, ali se dogodek, povezan s tveganjem, pojavi na letališču, železniški postaji, v nakupovalnem centru, poslovni stavbi ali proizvodnem objektu.

Celovit pristop prinaša boljše učinke

V Siemensu se zavedamo potrebe po upoštevanju vseh znanih standardov, trendov ter naravnega toka usmerjenosti v varnost. Ker ponujamo cel spekter tehnologij za tehnično opremo objektov in smo prisotni v vseh državah sveta, lahko našim kupcem ponujamo lokalno podporo, predvsem pa jih lahko podpiramo glede na njihove branžne specifike in na vseh ravneh intervencijskih struktur. Za različne vrste izzivov na nadzornih in upravljalnih segmentih lahko izvedemo ustrezen varnostni odziv ter zagotovimo hitro in učinkovito načrtovanje, pravilno odločanje za dnevne reševanje problematike in kritičnih dogodkov. Vse to so parametri, ki jih običajno zajamemo že v ponudbah. Delujemo po načelu, da mora biti dežurni osebi na voljo kaj več kot samo prikaz statusa (alarma, kraja in časa dogodka). Naravna smer varovanja zahteva pripravo modelov za pomoč reševanja in izpolnitve želja ter potreb uporabnikov.

Poleg samih tehnologij (ustrezne opreme in elementov za zagotavljanje varnosti) želimo v Siemensu našim kupcem ponuditi tudi varnostno nadzorni sistem, ki je zanesljiv, nadgradljiv, uporabniku prijazen in osredotočen na preprečevanje tveganih dogodkov. Pri razvoju nadzornih sistemov upoštevamo spremenjene zahteve lokalnih varnostnih konceptov. Če je do leta 2001 koncept intervencije temeljil na hitrem odzivu intervencijske enote, se je v zadnjih 10 letih princip varovanja usmeril na ukrepe preprečevanja incidentov (zagotavljanja pogojev, da do incidentov sploh ne bi prišlo) ter na upravljanje odziva na nesreče in izvajanje ukrepov za zmanjšanje njenih posledic.

Siveillance – inteligentni nadzor

V Siemensu so inovacije ob dolgoročnem zagotavljanju trajne vrednosti za naše kupce temeljna vrednota, na kateri temelji tudi naš razvoj tehnologij za zagotavljanje varnostnega koncepta, ki zajema upravljanje in nadzor širših površin in lokacij ter nudi varnostne rešitve na osnovi analitskih odzivov. Siveillance je ime za skupino produktov z inovativnim pristopom združevanja in povezovanja sodobnih, tehnično naprednih sistemov, z rešitvami, ki upoštevajo tržne trende, odprte standarde in zbliževanje fizičnih produktov z IT varnostjo. Siemens kot član OVIF Industry foruma v svoje rešitve vključuje izdelke in opremo na osnovi upoštevanja standardov za povezave. To zagotavlja interoperabilnost med priključenimi sistemi, kot so video produkti različnih proizvajalcev ter naprave za detekcijo in nadzor. Glede varnosti, ukrepov in varovanja se ne odločajo naprave samostojno, ampak jih pri tem vodi sistem, omrežne povezave in programska oprema za njimi. Kamere, opremljene s to tehnologijo, razpoznajo razne situacije, obraze, spremembe, manjkajoče objekte in predmete ter znajo filtrirati neželeno osebje. Prejeta informacija, opozorilo oziroma razna predalarmna stanja se tako pojavijo na zaslonih monitorjev operaterja, kar pa žal ni več dovolj. Nujne so dodatne informacije, navodila za ukrepanje, načrt intervencije, shema objekta, opozorila na nevarnosti, napotki, ... Istočasno se informacije posredujejo imetnikom dlančnikov, pametnih telefonov po predhodno pripravljenem scenariju.

Siemensova tehnologija nudi že izdelane različne module programske opreme za simulacijo reševanja, evakuacij z več tipov lokacij (stadionov, zgradb, območij s prireditvami) z upoštevanjem različnih možnih vplivov stresnih situacij ter možnega obnašanja množic in posameznikov, kjer je poudarek na osnovnih predpostavkah odnosa množic v sorazmerju s časom in nuji po predvideni evakuaciji. Upošteva vse možne spremenljivke, poti umika in se prilagaja pod vplivom različnih faktorjev (zamaški, lijaki ali ozka grla, napačne usmeritve ipd). Model programske opreme se lahko uporabi v urbanih območjih, namenjenih prireditvam, na stadionih, v nakupovalnih središčih, kot tudi v podjetjih glede na branžne specifike njihovega delovanja.

Pametni odziv na tvegane situacije, je bilo vodilo pri zasnovi tehnologije »Intelligent response«, kjer gre za postavitev sistema z modularnimi rešitvami, posebno za kritične infrastrukturne objekte, kjer se zadržuje veliko ljudi. Za take namenske rešitve so na voljo že izdelani paketi pristopa in identifikacije, ki upoštevajo varnostne zahteve za zaščito dostopa in pristopa, uporabljajo video za verifikacijo in biometrijo za identifikacijo, za evakuacijo pa ponujajo inteligentne mehanizme, saj statična signalizacija evakuacijskih poti po izkušnjah in priporočilih na zadošča več. Celoten sistem je robustno zasnovan ter odporen proti negativnim vplivom, naj bodo to sabotaže ali naravne katastrofe. Ima izdelan model uspešnega simuliranja raznih scenarijev za evakuacije, s poudarkom na dveh glavnih dejstvih, in sicer kako obvestiti in opozoriti ljudi, ki so ogroženi, ter kako jih usmeriti in varno voditi iz nevarne lokacije.

Trenutno je vgrajenih veliko sistemov tehničnega varovanja, ki vsak zase predstavlja pozitiven prispevek k izboljšanju varnosti, vendar gledano v celoti ti nepovezani sistemi izgubijo svoj pozitivni pomen, kar pa se žal pokaže zlasti šele v kritičnih situacijah, kot rezultat neprave reakcije in napačnih odločitev osebja.

Pametni odziv na tvegane situacije, je bilo vodilo pri zasnovi tehnologije »Intelligent response«, kjer gre za postavitev sistema z modularnimi rešitvami, posebno za kritične infrastrukturne objekte, kjer se zadržuje veliko ljudi.



Intrunet siveillance - prednosti:

- Medsebojna povezljivost sistemov tehničnega varovanja in nadzora različnih proizvajalcev – končni sistem je prilagodljiv in zmogljiv ter enostaven za uporabo.
- Večja varnost za osebje, varna evakuacija in zaščita (upravljanje in usmerjanje).
- Organizacijski ukrepi v kombinaciji z varovanjem (šolanje in usposabljanje, skrb za kvaliteto), nadzor in poročanje.
- Redni nadzor, servisiranje, nadgradnje ter komunikacija do »najmanjših lokacij«, kjer sporočilo o dogodku (npr. poskus napačne registracije ali tihi alarm nepooblaščenega odpiranja dostopa) sproži takojšnje interakcije (arhiviranje sporočil, prikaz predhodno definirane kamere za video verifikacijo, ustrezna navodila za ukrepanje, dodatna opozorila, obvestila odgovornemu osebju, ...).
- Programski paket Netwach (na voljo kot del Siveillance) je sistem za varnostni nadzor programske in strojne opreme in priključenih komponent ter drugih mrežnih naprav, stikal, strežnikov in zagotavlja zadovoljitev IT varnostnih instrumentov (požarni zidovi, antivirusna oprema, VPN, ...), zlasti pri daljinskih dostopih in nadziranjih.
- Z uporabo interoperabilnega nadzornega sistema (vsi varnostni sistemi so medsebojno povezani in medsebojno vplivajoči) lahko znižamo dolgoročne skupne stroške upravljanja, saj z daljinskimi dostopi (remote access) lahko znižamo stroške vzdrževanja in servisiranja, hitreje odpravljamo manjše napake in sistem redno nadgrajujemo.

Vzorec žil v dlaneh je edinstven za vsakega posameznika in se ne spreminja s staranjem. Princip delovanja tega čitalnika dlani Sipalm je unikaten in temelji na uporabi infrardeče kamere. Elektronski zapis se vnese v interni uporabniški sistem. Uporabnik pridrži dlan v bližini čitalnika, kjer vgrajeni senzor zazna prisotnost ter s pomočjo infrardečega žarka osvetli dlan z infrardečo svetlobo (LED). Kri v žilah z nizko vsebnostjo kisika to svetlobo različno absorbira ter tako ustvari sliko za IR kamero. V primerjavi z identifikacijo prstnih odtisov ali preverjanjem očesne zenice je ustreznejši, brezkontaktni ter identificira 10x več točk ter izpolnjuje vse higienske in varnostne zahteve. Trenutno je v uporabi za približno 8 milijonov oseb. ■



Sipalm – detektor dlani

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 naš̌o ponudbo na naš̌i 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



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).**

Avtor: mag. Marjan Miklavčič / Ministrstvo za pravosodje in javno upravo



VARNOST PRAVOSODNIH ORGANOV V REPUBLIKI SLOVENIJI

Slovenija zagotavlja dokaj visoko stopnjo varnosti v pravosodju, a potrebno se je zavedati, da je sodobno varnostno okolje zelo kompleksno ter nepredvidljivo in temu primerno je potrebna ažurnost ter celovit in usklajen pristop.

Uvod

Sestavni del varnostnega okolja v Sloveniji so tudi pravosodni organi, ki s svojo aktivnostjo le-tega kreirajo v sklopu sistemsko-organizacijskih rešitev celovitega delovanja pravne države. Pravosodni organi s svojo temeljno funkcijo izvajanja sodne oblasti zagotavljajo spoštovanje človekovih pravic in temeljnih svoboščin ter demokracije in načel pravne države (Ustava RS, 1991). Z novo Resolucijo o strategiji nacionalne varnosti Republike Slovenije (2010) pa so pravosodni organi dobili posebno vlogo in pomen zlasti pri zagotavljanju notranje varnosti. V varnostnem okolju predstavljajo tudi kategorijo, ki zaradi potrebe svojega nemotenega delovanja potrebuje zadostno stopnjo varnosti in s tem določeno obliko in obseg varovanja.

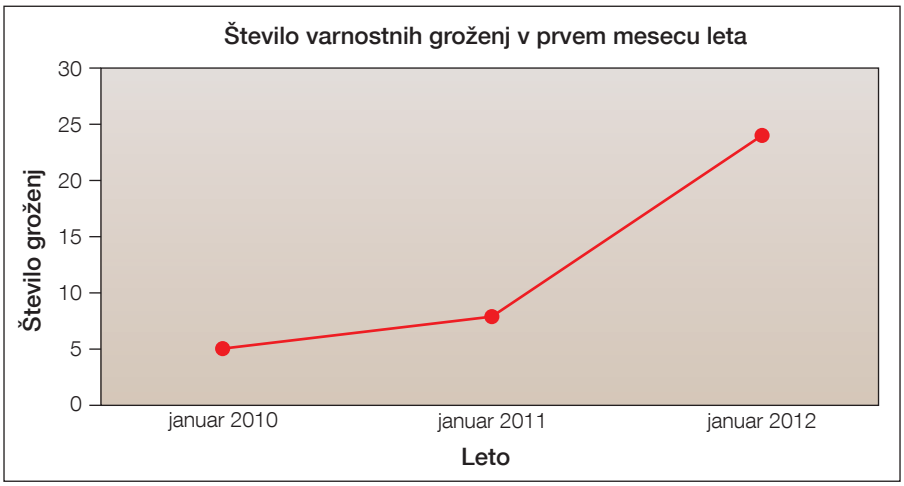
Varnost pravosodnih organov v Sloveniji si predstavljamo kot stanje, za katerega je potrebno, da se ohranja njihova funkcija in namen. Prav tako pa je potrebno zagotoviti varnost oseb, premoženja in podatkov, ki se nahajajo na sodiščih, tožilstvih in pravobranilstvu pred viri ogrožanja (Pravilnik o določitvi varnostnih standardov poslovanja sodišč, 2007). Pri vprašanju varnosti pravosodnih organov in njihovega varnostnega tveganja v slovenskem prostoru se moramo uzreti širše, saj lahko le tako dojamemo širši pomen sorazmerne varnostne zagotovitve pravosodnih organov, vzpostavitve njihove varnostne arhitekture, ki pa je v končnem varnostnem produktu sposobna zagotavljati varnost posamezniku in se odzivati na konkretne varnostne grožnje pravosodnim funkcionarjem, ostalim zaposlenim in strank v postopkih (Miklavčič, 2008). Zagotavljanje varnosti pravosodnih organov prav zato spada med dejavnosti, ki jih država zaradi velikega javnega interesa ureja na normativnopravni in organizacijski ravni in z nadzorovanjem izvajanja dejavnosti.

Na vseh ravneh delovanja države je namreč zaznati, da je ugled državnih institucij močno načet. Med drugim se (ne) spoštovanje državnih institucij kaže tudi v izjemnem naraščanju števila varnostnih dogodkov, usmerjenih zoper delo sodišč, tožilstev in pravosodnih funkcionarjev na splošno. Posebno skrb vzbujajoče je, da so se s področja organiziranega kriminala in kazenskih postopkov, kjer je ogrožanje varnosti pravosodnih funkcionarjev pričakovano in obvladljivo, grožnje in napadi na pravosodne funkcionarje preselili na področje »slehernika«. To pomeni, da so se varnostni dogodki iz velikih, dobro varovanih sodišč, kjer jih je bilo do zdaj največ, preselili na vsa sodišča in jih je trenutno skoraj nemogoče v celoti predvideti, obvladovati in se nanje pripraviti. Storilci niso več le kriminalci in znane problematične osebe, temveč vsakdanji ljudje, ki jim zaradi splošne družbene krize in prakse, da se v zadnjih desetletjih za vse težave v družbi krivda zavrača na sodstvo, tožilstvo in policijo, tedaj, ko se znajdejo v stiski, popustijo vsi zadržki. Najbolj skrb vzbujajoče je, da se je v zadnjem času veliko varnostnih dogodkov zgodilo na področju prekrškov in izvršbe, kjer se država neposredno dotakne ljudi, saj jih »*udari po žepu*«. To kaže, da je pojav neposredno povezan s sedanjo finančno krizo, ki ji kmalu še ni videti konca. Pravosodni funkcionarji, zlasti na manjših, varnostno slabše opremljenih sodiščih,

Pravosodni sistem Republike Slovenije deluje v relativno stabilnem varnostnem okolju, ki se dinamično spreminja glede na vpliv različnih internih ter eksternih varnostnih dejavnikov.

se zato počutijo ogrožene. Mreža sodišč v Republiki Sloveniji je izjemno razvejana, sodišča s tremi ali štirimi sodniki imajo tudi zelo majhni kraji. Na posameznih območjih so okrajna sodišča drugo od drugega oddaljena samo 10 kilometrov (Strategija Pravosodje 2020). Pravosodni sistem Republike Slovenije deluje v relativno stabilnem varnostnem okolju, ki se dinamično spreminja glede na vpliv različnih internih ter eksternih varnostnih dejavnikov. Nepredvidljivi varnostni pojavi, kot so anonimne najave podstavitve eksplozivnih teles, grožnje pravosodnim funkcionarjem in sodnemu osebju ter drugi varnostni dogodki v pravosodnih organih, lahko hitro spremenijo varnostno okolje v pravosodnih institucijah in s tem povzročijo nepredvidljivo človeško, materialno in pravosodno škodo (Ministrstvo za pravosodje, 2008). V Sloveniji je prisotno zavedanje, da se varnost pravosodnih organov kreira na lokalnem, torej bivalnem varnostnem okolju, kjer se posamezni varnostni dogodki tudi pojavljajo. Temu primerno se intenzivira koordinacija varnostnih nalog z drugimi nosilci notranje varnosti, s ciljem zagotoviti hiter zunanji odziv na varnostne potrebe pravosodnih organov in na izredne dogodke povezane s pravosodnimi funkcionarji in ostalimi zaposlenimi v pravosodju. Od leta 2005 dalje, se v okviru izvajanja varnostne politike v pravosodnih organih Republike Slovenije intenzivno vzpostavlja varnostna arhitektura na sodiščih, ki danes sloni na uvedenih različnih oblikah prevencij, oblikah fizičnega in tehničnega varovanja ter partnerskega sodelovanja nosilcev varnostnih nalog[1] v širšem notranjem varnostnem prostoru (Pravilnik o določitvi varnostnih standardov poslovanja sodišč, 2007). Poleg tega, pa se Ministrstvo za pravosodje in javno upravo dobro zaveda, da varnost zaposlenih v pravosodju ni omejena zgolj na delovno mesto v pravosodju, saj kompleksnost varnostnega problema zahteva, da se nivo osebne varnosti pravosodnih funkcionarjev ter osebja dvigne tudi izven delovnega mesta. V ta namen ministrstvo in pravosodni organi sledijo cilju boljšega poznavanja osebnih varnostnih ukrepov. Razvoj varnostnega upravljanja - varnostnega managementa v Sloveniji je sledil kreiranju varnostne politike v pravosodnih organih na treh nivojih in sicer sistemskem, s katerim se ukvarja predvsem država, organizacijskem, ki je v pristojnosti vodij pravosodnih organov (zlasti direktorjev sodišč), in individualnim, katerega kreirajo posamezniki, zlasti sodniki, državni tožilci in državni pravobranilci (Miklavčič, 2008).

Slovenija strmi k vzpostavitvi varnostne arhitekture pravosodnih organov tako, da bi se izražalo dostojanstvo pravosodnih organov, njihova odprtost, istočasno pa bi se zagotavljali varnostni postopki in ukrepi, ki bi zaposlenim in strankam v postopku zagotavljali zadostno varnost in funkcijo organov (Pravilnik o določitvi varnostnih standardov poslovanja sodišč, 2007). Največji uspeh pri kreiranju varnostne arhitekture slovenskih pravosodnih organov je bil dosežen z vzpostavitvijo zaupanja in dobrega sodelovanja med pravosodnimi organi in ministrstvom na eni strani ter nosilci notranje varnosti na drugi strani. Izmenjava informacij med institucijami je dosegla očiten napredek, zato se je moč tudi s preventivno dejavnostjo odzivati na varnostne izzive, kar v preteklih letih v Sloveniji ni bila praksa.



Zunanje varnostno okolje, zlasti na lokalni ravni, je imelo intenziven varnostni vpliv na nemoteno poslovanje sodišč, saj so se novi varnostni izzivi prenašali v notranje varnostno okolje pravosodnih organov.

Varnost in spremenjeno varnostno okolje

Problematika varnosti pravosodnih organov, zaposlenih in strank v sodnih postopkih je glede na število varnostnih dogodkov v letu 2012 ostalo pereče področje dela, na katero se je ministrstvo, pristojno za pravosodje, skupaj s pravosodnimi organi in drugimi institucionalnimi nosilci varnostnih nalog, ustrezno odzivalo z uvedbo sorazmernih varnostnih ukrepov. Z izvedenimi ukrepi se je dosegala zadostna stopnja varnosti, ki je pogoj za varno in nemoteno poslovanje sodišč in drugih pravosodnih organov. Zunanje varnostno okolje, zlasti na lokalni ravni, je imelo intenziven varnostni vpliv na nemoteno poslovanje sodišč, saj so se novi varnostni izzivi prenašali v notranje varnostno okolje pravosodnih organov.

V letu 2012 je bilo zaznati izredno nihanje števila varnostnih dogodkov na sodiščih tako, da smo beležili v prvih treh mesecih skoraj tristo procentov povečanje števila dogodkov, zatem je sledila izrazita umiritev – padec varnostne problematike vse do konca sodnih počitnic. V jesenskem obdobju je število varnostnih dogodkov ostajalo na ravni iz leta 2011. Tako kot v širšem prostoru konec leta 2012 so posamezni varnostni incidenti, povezani s protesti, tudi na sodiščih zahtevali uvedbo dodatnih, sorazmernih varnostnih ukrepov s ciljem ohranjanja varnosti ljudi in nemotenega poslovanja pravosodnih organov.

Varnost ima svojo ceno

Država, njene institucije in v končni fazi državljani občutimo prisotnost ekonomsko-finančne krize na vseh področjih. Ta s seboj prinaša številne, že večkrat omenjene, stranske produkte, ki negativno vplivajo na ozračje v družbi. Ob negativnemu vplivu finančne krize pa se, zlasti zaradi socialne nepravičnosti, intenzivira občutek neučinkovite politike ter pravosodja.

Kriza se odraža tudi pri varnostnih investicijah v pravosodne organe, kjer je moč pričakovati investicijski zastoj. Pravosodni organi so pri izvajanju varnostne po-

litike postavljeni pred konflikt koliko denarja za kakšno ambicijo, kar državo sili v iskanje učinkovite organizacijsko-finančne formule, s katero bi lahko zagotavljala pravosodnim organom pogoje za nemoteno delo, pravosodnim funkcionarjem, ostalim zaposlenim v pravosodju in strankam pa izvajanje varnostnih ukrepov s katerimi bo zagotovljena optimalna stopnja varnosti. Torej jemanje denarja in zategovanje pasu na področju notranje varnosti, se matematično največkrat ne izide, saj so posledice prevečkrat prehude in nepopravljive, prav tako pa se zniževanje proračuna lahko dolgoročno negativno odraža tudi na sposobnosti odzivanja na varnostne grožnje. Vsekakor je potrebna stopnja sorazmernosti, racionalnosti in razumnosti pri uvajanju varnostnih ukrepov, ki zahtevajo finančna sredstva, kar velja tudi za pravosodne organe. Pri kreiranju varnostne politike v pravosodnih organih je tako potrebno razumeti, da varnost ima svojo ceno, tudi ekonomsko, in država bo tukaj morala odigrati svojo vlogo znatno bolj razumsko.

Zaključek

Skozi prispevek lahko ugotovimo, da se je na področju varnosti pravosodnih organov po letu 2006 zgodil velik premik, kar je posledica dinamičnih dogodkov v spreminjajočem se varnostnem okolju sodne veje oblasti. Pristojno ministrstvo za pravosodje se je skupaj s pravosodnimi organi soočilo z varnostnimi izzivi in ob kreiranju varnostne politike ter varnostne sinergije so bili preoblikovani miselni in organizacijski vzorci dojemanja varnosti. To pa je posledično spreminjalo varnostno arhitekturo pravosodnih organov in s tem zagotavljanje optimalne stopnje varnosti, ne glede na varnostne incidente. Lahko trdimo, da je Republika Slovenija še ujela čas, ko je lahko gradila varnostno arhitekturo pravosodnih organov, imela pa je tudi nekaj sreče, da ni beležila varnostnih incidentov s hudimi posledicami. Vsekakor pa se na srečo ne more naslanjati in morala bo intenzivirati razvoj in nadgradnjo »soft security«, kot so oblike samovarovanja, varnostnega managementa, varnostnega izobraževanja itd. Varnost pravosodnih organov mora namreč postati primarna skrb ključnih akterjev, zlasti direktorjev in



predsednikov sodišč, saj je navsezadnje izvajanje varnostnega upravljanja v razpravnih dvoranah pogoj za uspešno ter varno izvajanje sojenja.

Slovenija zagotavlja dokaj visoko stopnjo varnosti v pravosodju, a potrebno se je zavedati, da je sodobno varnostno okolje zelo kompleksno ter nepredvidljivo in temu primerno je potrebna ažurnost ter celovit in usklajen pristop. Vsekakor bo potrebno v prihodnosti še naprej analizirati varnostno okolje, ter iskati ukrepe s katerimi se bo učinkovito zoperstavljalo varnostnim grožnjam. Pri izvajanju varnostne politike pravosodnih organov pa se ne bo smelo zanemariti stopnje sorazmernosti, racionalnosti in razumnosti, saj so Ministrstvo za pravosodje in javno upravo ter pravosodni organi postavljeni pred problem finančne omejenosti. Omejevanje proračuna na področju varnosti lahko prinese hude in nepopravljive posledice, prav tako pa dolgoročno neučinkovitost odzivanja na varnostne grožnje. Temu primerno se bo morala Slovenija zavedati, da ima varnost svojo ceno, pri tem pa odigrati svojo vlogo bolj razumsko. Pravosodni organi in pristojno ministrstvo pa bodo morali v prihodnosti varnost zagotavljati z učinkovitejšimi organizacijskimi rešitvami, bolj utečenim redom, samovarovanjem, z visoko varnostno kulturo ter spoštovanjem pravil.

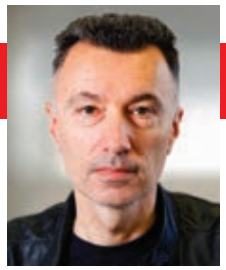
Pri kreiranju varnostne politike v pravosodnih organih je tako potrebno razumeti, da varnost ima svojo ceno, tudi ekonomsko, in država bo tukaj morala odigrati svojo vlogo znatno bolj razumsko.

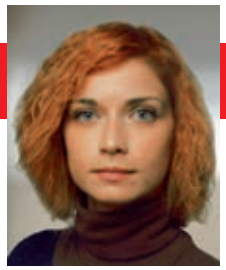
Viri

- Kovačič, M. (2010). Varnostni teater ima svojo ceno. Dnevnik, objava September 1, 2010, http://www.dnevnik.si/tiskane_izdaje/objektiv/1042377549.
- Miklavčič, M. (2008). Management v sodstvu. Ljubljana, Planet GV.
- Miklavčič, M. (2009). Varnost v pravosodju: Varnost na sodiščih. Ljubljana, Ministrstvo za pravosodje, Center za izobraževanje v pravosodju. Ni javno objavljeno gradivo.
- Ministrstvo za pravosodje (2005). Odprava sodnih zaostankov: Projekt Lukenda. Objavljeno September 1, 2010, http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/2005/PDF/projektLukenda.pdf.
- Ministrstvo za pravosodje (2008). Doseženi cilji na področju pravosodja v mandatu 2005-2008. Ljubljana, Ministrstvo za pravosodje.
- Ministrstvo za pravosodje (2010). Informacija Ministrstva za pravosodje o izvrševanju in nadgradnji Projekta Lukenda – realizirane zaposlitve sodnega osebja po Projektu Lukenda. Ljubljana, št. 007-85/2006, datum 19. 9. 2010.
- Pravilnik o določitvi varnostnih standardov poslovanja sodišč, Ur.l.RS, št.41/2007, datum 11.5.2007.
- Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV), Ur.l. RS, št. 27/2010, datum 4.4. 2010.
- Ustava Republike Slovenije, Ur.l. RS, št. 33/91, datum 28.12. 1991.
- Vlada Republike Slovenije (2012). Strategija »Pravosodje 2020«, julij 2012, Ministrstvo za pravosodje in javno upravo. ■

[1] Ministrstvo za notranje zadeve - Policija, Uprava za izvrševanje kazenskih sankcij Republike Slovenije, varnostne agencije, občinsko redarstvo, itd.

Avtor: mag. Kaja Prislan, prof. dr. Bojan Dobovšek / Fakulteta za varnostne vede





FINANČNA KRIMINALITETA V KONTEKSTU FINANČNE KRIZE IN SODOBNIH ASPEKTOV VARNOSTI

V kontekstu trenutne finančne krize, se skušamo skozi kritičen kriminološki diskurz in analizo primerov, ukvarjati z dilemo zagotavljanja finančne varnosti in vidiki njenega ogrožanja. Gre za aktualni prispevek k osvetlitvi vzrokov, groženj in akterjev, ki so privedli do nestabilnosti globalne ekonomije.

Rdeča nit, ki povezuje trenutno krizo je ideja o stalno spreminjajočih se varnostnih konceptih in sodobni varnostni kulturi, ki je privedla do odklonskega upravljanja finančnih in državnih organizacij. Če želimo pojasniti, zakaj je do tega prišlo in izpolniti varnostne potrebe globalnih in individualnih entitet je potrebno koncept varnosti razumeti v kontekstu sodobnih trendov. Kot navaja Kratcoski (2012) je finančna stabilnost eden izmed najpomembnejših varnostnih aspektov osebne in mednarodne varnosti, saj je povezana z različnimi vidiki eksistence posameznika in držav. Spremembe v varnostnih potrebah in kulturi ljudi ter držav so privedle do različnih paradoksalnih varnostnih situacij. Na eni strani ljudje v razvitih družbah težijo k visoki stopnji fizične in socialne varnosti na drugi strani pa jih žene želja po finančni varnosti, predvsem bogastvu. Zaradi visokih finančno-varnostnih potreb pa nekateri uporabljajo metode s katerimi ogrožajo varnost drugih ljudi (Edelbacher, et al., 2012). To je še posebej problematično, kadar se nelegalnih in moralno spornih tehnik poslužujejo tisti, ki so odgovorni za upravljanje in vodenje državnih ali korporacijskih struktur, od katerih je odvisna stabilnost nacionalnega in globalnega gospodarstva (Kratcoski, 2012).

Gre za medsebojno povezane pojave, ki so prisotni v skoraj vsaki razviti državi. Destabilizacija nacionalnih ekonomij in globalne varnosti je splošna posledica kombinacije dveh vrst groženj; tveganega in malomarnega upravljanja finančnih institucij in (beloovratniške) organizirane kriminalitete. Pohlepno vodenje, politična korupcija in vzporedna integracija kriminalnih združb v državne strukture so postale sodobna (hibridna) grožnja finančni varnosti. Paradoksalno tovrstna tveganja izvirajo iz poizkusov spodbujanja gospodarskega razvoja. Prost pretok denarja, ljudi, storitev in blaga, združevanje v mednarodne organizacije, brisanje nacionalnih meja, razvoj sodobne tehnologije in njena integracija v vsakodnevno življenje ter poslovanje so koncepti, ki so pripomogli k razvoju držav. Hkrati pa so ustvarili nove priložnosti za širjenje in razvoj kriminalitete, saj so varnostne pomanjkljivosti, ki jih nismo predvideli, izkoristili nemoralni bankirji, politične skupine in organizirane kriminalne združbe (Edelbacher, et al., 2012). To je skupno privedlo do razvoja t.i. belovratniške mafije, ki se je infiltrirala v legalne državne strukture in skozi vpliv na poslovanje, politiko in ekonomijo sprejema zakone in pravila v lastno in ne javno oz. splošno dobro (Dobovšek, 2012). Pri tem analize ugotavljajo, da največje posledice takšne kriminalitete nastajajo v finančnem sektorju (Tomasic, 2012). V kontekstu sodobnih trendov je finančna varnost trenutno najbolj ogrožen aspekt varnosti, saj jo ogrožajo tisti, ki naj bi zanjo skrbeli.

Da bi razumeli, zakaj je odpovedal nadzor, je potrebno razumeti, da v času go-

V kontekstu sodobnih trendov je finančna varnost trenutno najbolj ogrožen aspekt varnosti, saj jo ogrožajo tisti, ki naj bi zanjo skrbeli.

spodarske in poslovne stabilnosti ni veliko zanimanja za to, kako organizacije dosegajo pozitivne rezultate. Tomasic (2012) v svojem prispevku ugotavlja, da naj bi v takšnih časih obstajala velika toleranca do korupcije in nepravilnosti v poslovanju. Po njegovem mnenju je takšna situacija nastala zaradi različnih vzrokov. Nedotakljivost vodilnih in tvegane korporativne odločitve pogosto podpirajo politične sile, ki ovirajo postopke organov pregona, omejujejo resurse za nadzor in spodbujajo ideologijo, da se država ne sme vmešavati v finančne trge, ki naj bodo samoregulativni. Politični pritiski se izvajajo tudi na regulatorje, ki izvajajo revizije in nadzor. Nadzorni sistemi so pogosto brez ustrezne podpore, velikokrat pa se jim očita, da se naj ne vmešavajo v poslovne modele in načrte finančnih institucij. V nekaterih državah velja tudi prepričanje, da so določene organizacije ali podjetja prevelika in prepomembna za nacionalno gospodarstvo in državo, zaradi česar so zaščitene pred doslednim nadzorom in podvržene nesorazmernim oblikam pomoči. Na drugi strani pa v času gospodarskih in finančnih kriz takšna podpora upade, kar pogosto razkrije finančne prevare in nepravilnosti v delovanju finančnega sistema. Krizne situacije torej odpravljajo varovalne mehanizme koruptivnih in nemoralnih vodij oz. managerjev, vendar to še ne pomeni, da za svoja dejanja tudi odgovarjajo. Kazenska zakonodaja je z vidika ugotavljanja odgovornosti finančnih institucij neučinkovita in velikokrat kontraproduktivna. Po mnenju Tomasica (2012) je neveljavnost zakonodaje za finančne institucije že splošno znana praksa, saj vodstveni kader, ki ne upošteva zakonskih in moralnih pravil, zelo redko občuti posledice s kazenskim pregonom. Problem, ki onemogoča izvrševanje zakonodaje je v tem, da organi pregona že v sami osnovi nimajo ustreznih resursov ali znanja, da bi uspešno preganjali organizirano finančno kriminaliteto, na drugi strani pa jih ovirajo še finančne institucije, ki ne želijo sodelovati ali pomagati v postopkih preiskovanja in odkrivanja odgovornih (Edelbacher, et al., 2012). Kazenske sankcije so v finančnem sektorju nedorečene in redko uporabljene, čeprav so posledice v finančni škodi ogromne in vplivajo na celotno družbo. To predstavlja velik paradoks v primerjavi z izrečenimi kazenskimi sankcijami za manj hude oblike finančne kriminalitete kot so npr. tatvine in ropi. Da bi lahko odpravili takšne dileme in neenakopravno obravnavo ljudi so potrebne dolgotrajne spremembe, v praksi pa se reforme in ukrepi, kot odziv na afere, navadno kažejo v obliki drastičnih sprememb, ki so posledica nepremišljenih in pretiranih reakcij. V sodobnem času je stanje takšno, da si v primeru katastrof vsi želimo hitrih in učinkovitih ukrepov, ko je najhujše mimo pa si nihče več ne prizadeva za trajne in stabilne spremembe (Tomasic, 2012). Hitro sprejemanje novih zakonov in politik (socialnih, gospodarskih in finančnih) z namenom zagotavljanja večje varnosti lahko sicer poveča varnostne prioritete in resurse, vendar lahko vodi tudi v neželene ali pretirane posledice. Na eni strani vse ukrepe pogojujemo z varnostjo (to se dogaja v vseh sodobnih, predvsem zahodnih državah, zaradi globalizacije tveganj in strahu povezanih s finančno krizo), kar lahko vodi v varnostno paranojo (Stumvoll, 2012), poslabšanje splošnega družbenega vzdušja in erozijo zaupanja v sistem ter zmanjšanje zasebnosti ljudi. Na drugi strani pa se z nepremišljenim reševanjem institucij in nesorazmerno državno pomočjo povečujejo tudi priložnosti storilcev, kar lahko vodi v nove prevare in ustvarja nova tveganja (Tomasic, 2012). Finančni sektor je potrebno razumeti kot kritično infrastrukturo, ki vpliva na globalno varnost in varnost vsakega posameznika, zato mora biti zaščitena s posebnimi mehanizmi (kot transportni, energetski, komunikacijski sektor). Tovrstno poslovno okolje mora postati odporno na notranje in zunanje grožnje in biti sposobno hitro okrevati po morebitnih krizah ali varnostnih incidentih (Edelbacher, et al., 2012). Če želimo preprečiti ponovno krizo, se morajo spremeniti obstoječi varnostni ukrepi, predvsem zaradi tega ker veliko organizacij sploh nima določenih protikorupcijskih ukrepov ali mehanizmov nadzora nad poslovanjem (Tomasic, 2012).

Vse pogosteje se razvite države, zaradi transformacije varnostnih konceptov, preprečevanja različnih oblik kriminalitete lotevajo skozi okoljske obrambne mehanizme v okviru situacijske prevencije, kjer gre za urejanje okolja in zmanjševanje priložnosti storilcev. Dejanje naj bi se po teh teorijah zgodilo v določenem prostoru in času, ko so izpolnjeni trije pogoji: motiviran storilec, primerna žrtev in odsotnost varnostnih ukrepov. Za storilca pa mora obstajati majhno tveganje in velika korist (Stumvoll, 2012). V finančnem okolju mora biti glavni namen preventivnih ukrepov trenutno odvračanje storilcev in dolgotrajno spreminjanje kulture vodilnih. Oblikovati je potrebno takšno poslovno in delovno okolje, ki odvrača nemoralna dejanja in spodbuja poštenost in pripadnost zaposlenih. Pri analiziranju in sprejemanju tveganj bi morali postaviti visoke standarde in se izogibati tveganim poslom, zato je priporočljivo sodelovanje neizkušenega vodstvenega kadra s strokovnjaki (t.i »business angels«), ki razumejo poslovne sisteme in lahko pripomorejo k učinkovitemu in racionalnemu obvladanju poslovnih tveganj (Fath, 2012). Nenazadnje bi vsak posel moral imeti implementirane tudi instrumente osebne odgovornosti (Edelbacher, et al., 2012).

Finančni sektor je potrebno razumeti kot kritično infrastrukturo, ki vpliva na globalno varnost in varnost vsakega posameznika, zato mora biti zaščitena s posebnimi mehanizmi (kot transportni, energetski, komunikacijski sektor).

Kazenska zakonodaja je z vidika ugotavljanja odgovornosti finančnih institucij neučinkovita in velikokrat kontraproduktivna.

Zaključek

Stalne spremembe v družbenem življenju in težnje po njegovi poenostavitvi so privedle do različnih pozitivnih in negativnih posledic, ki se kažejo v spreminjajočih varnostnih trendih. Demokratični sistemi, blaginje in kapitalistično usmerjen način poslovanja so močno vplivali na varnostne potrebe in prioritete ljudi, na drugi strani pa se krčijo pravice ljudi. Organizirana, beloovratniška in kibernetska kriminaliteta so v zadnjih letih postale še bolj sofisticirane in prikrite, zaradi česar jih je zelo težko odkrivati in preganjati. Posebej velik problem se kaže v njihovi medsebojni združitvi v hibridno transnacionalno grožnjo, ki je pogosto integrirana v večje, za nacionalna gospodarstva, pomembne korporacije in institucije. In ker so te kriminalne organizacijske strukture povezane s političnimi sistemi od katerih je odvisno stanje pravne in demokratične države, za takšne organizirane storilce ustvarjajo močno zaledje, ki ga je z obstoječimi nadzornimi mehanizmi skoraj nemogoče odpraviti.



Organizirana, beloovratniška in kibernetska kriminaliteta so v zadnjih letih postale še bolj sofisticirane in prikrite, zaradi česar jih je zelo težko odkrivati in preganjati.

Ko so države v poizkusih prilagajanja spremembam prevzele odgovornost za zagotavljanje različnih aspektov varnosti, so pri tem povzročile tudi velike varnostne probleme. Namen takšnega prevzema odgovornosti je bilo povečanje učinkovitega upravljanja groženj na nacionalni in globalni ravni, ki bi se moral zagotavljati z doslednim nadzorom in enakopravno obravnavo ljudi. Nasprotno pa so države ustvarile situacijo v kateri so ljudje postali prepuščeni sami sebi, varnost pa je zagotovljena zgolj peščici vplivnih posameznikov. Razvoj varnostnih konceptov lahko zato na drugi strani razumemo tudi kot nazadovanje. Takšno situacijo smo sicer ustvarili ljudje sami, ko smo težili k večji stabilnosti, razvoju in racionalnejšemu življenju. Postopno in neopazno pa se je s tem razvijala kultura samo-učinkovitosti, individualizma, egocentrizma in pohlepa, ki je pripeljala do neuresničenega namena državnega nadzora in zmanjševanja človekovih pravic. To je ustvarilo situacijo s katero so se znova začele spreminjati varnostne potrebe ljudi, ki se postopno, zaradi vse večjih nestabilnosti, razlik in nevarnosti, vračajo na primarno raven. Kot kaže trenutna situacija, pa se bo ogroženost v prihodnosti stopnjevala, saj države ne razumejo (ali nočejo razumeti) trenutnih trendov, zaradi česar odpovedujejo pri izpolnjevanju svojih obveznosti. Njihovi sistemi družbenega nadzorstva bi morali biti fleksibilni, saj vsaka krizna situacija ustvarja drugačne varnostne potrebe in ranljivosti. V praksi pa so ti sistemi rigidni, neprilagodljivi, za splošno prebivalstvo pa neenakopravni. Očitno primanjkuje politične volje, ki je pod vplivom različnih neformalnih mrež, da bi naslovila potrebe ljudi. Trenutne varnostne zahteve ljudi pravzaprav niso radikalne ali neracionalne, temveč se nanašajo zgolj na področja, ki so jim zakonsko in teoretično že zagotovljena. Spremembe morajo biti torej v vedenju in kulturi vseh ljudi in ne zakonodaji. Če bi resnično želeli popraviti nastalo škodo, ki je ogrozila eksistenco večjega dela svetovnega prebivalstva bi morali upoštevati zgolj nekatera osnovna moralna načela in uvesti nekaj dodatnih nadzornih ukrepov, ki so teoretično dobri, v praksi pa neuporabljeni. Glede na analize trenutnega stanja v finančnih in večjih korporacijah bi bil potreben povečan in dosleden nadzor nad vplivnimi organizacijami v finančnem sektorju. Pri tem je treba povečati tveganje z vsemi vrstami odgovornosti in zmanjševati negativne spodbude (kot so npr. tudi neustrezne politike odškodnin oz. odpravnin). V splošnem poslovnem okolju pa je problem še v tem, da se tiste organizacije, ki so stabilne in poslujejo legitimno, na krizne situacije odzivajo reaktivno. Premalo pozornosti se namenja postopkom okrevanja oz. zagotavljanja neprekinjenega poslovanja in ukrepom preprečevanja groženj. Za to so potrebne natančne analize tveganj in njihove ocene, pri izbiri najprimernejših ukrepov pa bi se morala upoštevati tudi pravila kriznega managementa. Splošno bi bilo torej potrebno izboljšati mednarodni nadzor in doslednost pri izvrševanju zakonodaje, medtem ko bi morala biti glavna naloga korporacij in finančnih institucij zagotavljanje ustrezne ravni poslovne kulture, transparentnega poslovanja in obvladovanja tveganj. Pri tem je, če želimo celovito nasloviti nastalo problematiko, sodelovanje različnih organizacij in organov neizogibno. Organizacije in vodilni se morajo zavezati k odkrivanju nepravilnosti in nevestnemu poslovanju ter pri tem sodelovati z revizorji, regulatorji, organi pregona in mediji. Glede uspešnosti in integritete podjetij, je ključno podrobno spoznati stranko in preučiti njeno zgodovino, ker le takšna preventiva pomeni večjo varnost. Velja pregovor: Ni vse zlato kar se sveti!

V finančnem okolju mora biti glavni namen preventivnih ukrepov trenutno odvračanje storilcev in dolgotrajno spreminjanje kulture vodilnih.

Viri

- Dobovšek, B. (2012). Rule of law versus financial crime. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 161-176. Florida: CRC Press.
- Edelbacher, M., Theil, M. in Kratcoski, P. C. (2012). Financial crime: Past, resent, and future. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 391-408. Florida: CRC Press.
- Fath, C. (2012). Business angels: Can they help to prevent another financial crisis? V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 357-372. Florida: CRC Press.
- Kratcoski, P. C. (2012). New security concepts. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 1-6. Florida: CRC Press.
- Stummvoll, G. (2012). Changing concepts of security: The preventive turn in defensive design. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 7-22. Florida: CRC Press.
- Tomasic, R. (2012). The financial crisis and the haphazard pursuit of financial crime. V M. Edelbacher, P. Kratcoski in M. Theil (ur.), Financial crimes: A threat to global security, str. 177-204. Florida: CRC Press. ■

Avtor: doc. dr. Janez Mekinc / Fakulteta za turistične študije Turistica, Univerza na Primorskem



KOMPLEKSNOST VARNOSTI V TURIZMU

Turizem v svetu je bolj kot od česar koli drugega odvisen od varnosti. Pri odločanju za turistično storitev in turistično destinacijo, kamor bomo potovali, postavimo varnost kot prioriteto, ki je mnogokrat bolj pomembna od samih stroškov.

Prav varnost je tista, ki lahko potovanje spremeni iz nekaj lepega in prijetnega, v popolno nočno moro. Zanimivo strokovno vprašanje, ki se nam postavlja samo od sebe, je vloga in umeščenost korporativne varnosti v upravljanje varnosti turističnih destinacij. Če je korporativna varnost uveljavljen pojem v funkcioniranju hotelske industrije in ostalih nastanitvenih ali storitvenih obratov, kot so zdravilišča, večji zabaviščni parki, marine za turistična plovila, ect., je na področju destinacijskega managementa pojem korporativne varnosti v fazi odkrivanja. Vzroke lahko iščemo v dejstvu, da se šele v zadnjem obdobju varnost destinacije dojema kot celovit sistem upravljanja varnosti, v katerega so vpleteni vsi relevantni subjekti turizma, ki na konkretni destinaciji delujejo. Torej gre za celovito upravljanje varnosti, kjer sodelujejo gospodarski subjekti, ki neposredno izvajajo turistične storitve, kot so hoteli, turistične agencije, gostinski lokali; državne inštitucije, kot so policija, ministrstva ali direktorati za turizem, javni zavodi, ki delujejo na področju turizma; lokalne inštitucije, kot so regionalna in lokalna turistična organizacija, občinsko redarstvo, različne reševalne službe (gasilci, gorski reševalci, jamarski reševalci, ect.) ter turistična društva. Če povzamemo Vršca (2012) lahko opredelimo, da lahko le vsi ti turistični subjekti skupaj učinkovito obvladujejo s fenomenom varnosti v destinacijskem managementu, kjer se ustvarja nova vrednost na bazi upravljanja poslovnih procesov, sredstev, kapitala, informacij, komunikacij in človeških virov. Elementi korporativne varnosti se v destinacijskem managementu izražajo predvsem pri upravljanju in obvladovanju izrednih varnostnih dogodkov. Destinacijski management mora z ustreznimi analizami tveganj predvideti možnost pojava izrednih dogodkov večjega ali velikega obsega ter imeti pripravljene preventivne in kurativne ukrepe. Prav predstavitev kompleksnosti upravljanja z varnostjo na turistični destinaciji, pa je namen tega prispevka.

Valuta s katero lahko zagotavljamo varnost pa so realne in koristne informacije. Vse sodobne države pripravljajo za svoje državljane koristne in aktualne informacije za potovanje v posamezne države. Pri turizmu premalokrat izhajamo iz dejstva, da je največja gospodarska panoga na svetu po prihodku. Gotovo lahko iščemo vzroke za omenjeno dejstvo v množičnosti posameznikov in organizacij/podjetij, ki se ukvarjajo s turistično dejavnostjo, saj je slednja v takšni ali drugačni obliki prisotna v vseh delih našega planeta. Zaradi navedene odvisnosti turizma od varnosti, je pomembno razumeti korelacijo med varnostjo, vzroki kriz in njun vpliv na turizem. Mednarodni turizem, ki v zadnjih dvajsetih letih dosega izjemen vzpon, zgolj s splošnimi ekonomskimi teorijami kriznega managementa ne more reševati svojih specifičnih problemov. Turizem je namreč multidisciplinarna dejavnost in prav zato je ključnega pomena, korporativno upravljanje varnosti na turistični destinaciji. Že sama struktura mednarodnega turizma (Gee *et al*, 1997) kaže, da so v turistični proces vključene tako gospodarske družbe (organizatorji potovanj in turistične agencije, hoteli, hotelske verige, letalske, avtobusne družbe, tematski parki ...), kot tudi lokalne, regionalne in nacionalne turistične organizacije, številna strokovna združenja, pa tudi podjetja, katerih uspeh ali preživetje je samo posredno odvisno od turizma (taksisti, cvetličarji, živilsko-predelovalna industrija). Če so vsi ti deležniki vključeni v turistični proces, so torej vključeni tudi v krizo, ki prizadene turizem. Ne glede na dejstvo, da je bil slogan »turizem je sredstvo za doseganje miru« zelo popularen med turističnimi subjekti, pa naj je šlo za turistično industrijo, svetovalce za turizem ali posameznike iz akademske sfere, je dejstvo, da ima turizem na makro ravni, zelo majhen vpliv na mir in varnost. Turizem je mnogo bolj odvisen od miru in varnosti, kot pa obratno (Hall et al., 2003). To trditev je potrebno dopolniti z dejstvom, da je varnost, kot element kakovosti, ključnega pomena vseh turističnih destinacij, vendar pa lahko specifičnosti posameznih varnostnih kriz različno vplivajo na razvoj turizma posamezne destinacije. S specifičnostjo varnostnih kriz mislimo na njen obseg, posledice, ki jih prinaša ter medijsko pozornost, ki jo sproža. V sodobnem globaliziranem svetu imajo posamezni viri ogrožanja varnosti in posledično tudi krizne razmere vse bolj transnacionalne razsežnosti, torej se širijo neodvisno od državnih meja. Podobno ugotavlja tudi Dobovšek (2009: 66–68), ko trdi, »Globalna razsežnost turizma je povzročila, da varnostni problemi ne vplivajo samo na turizem določene destinacije, regije oziroma države, ampak da vplivajo na globalne turistične tokove in povzročajo

V sodobnem globaliziranem svetu imajo posamezni viri ogrožanja varnosti in posledično tudi krizne razmere vse bolj transnacionalne razsežnosti, torej se širijo neodvisno od državnih meja.

neravnovesja ter nihanja v svetovnem gospodarstvu.« S prvim terorističnim napadom usmerjenim neposredno na turiste v Luksorju, leta 1997, ko je pod streli islamskih skrajnežev umrlo 62 ljudi, se je v mednarodnem turizmu naselila negotovost. V panogi, ki je slovela kot človeku prijazna storitvena dejavnost, nekakšna »brezdimna industrija«, ki povezuje ljudi različnih kultur, je še zlasti po napadih v ZDA 11. septembra 2001 postalo jasno, da krize (v turizmu) niso več samo stvar cikličnih gibanj mednarodnega gospodarstva, temveč postajajo del tako imenovane »nove normalnosti« (TOURCOM, 2004). Turistična dejavnost posamezne destinacije ni neposredno odvisna samo od varnostne situacije v njenem okolju, temveč tudi od širšega varnostnega okolja, lahko rečemo od globalne varnosti, če se le spomnimo posledic terorističnega napada 11.9. v New Yorku na logistiko potovanj po celem svetu. Varnost v vseh svojih elementih je zato postala ključni dejavnik kakovosti in razvoja turizma in jo je potrebno resno obravnavati na vseh ravneh turistične ponudbe, pa naj gre za varnost turista ali varnost turistične destinacije.

Varnost v vseh svojih elementih, je zato postala ključni dejavnik kakovosti in razvoja turizma in jo je potrebno resno obravnavati na vseh ravneh turistične ponudbe, pa naj gre za varnost turista ali varnost turistične destinacije.

Ko pogledamo zgodovino kriz v turistični dejavnosti ugotovimo, da je kriz najmanj toliko kolikor je različnih destinacij in okoliščin, v katerih deluje turistična industrija. Avtorji (Wilks, 2006 in Wilks in Page, 2003) se v glavnem strinjajo, da so napadi na Združene države Amerike 11. septembra 2001 za vedno spremenili naše razumevanje varnosti v mednarodnem turizmu. Do drugačnega razumevanja pomena celovite varnosti v turizmu je prišlo zlasti po terorističnih napadih v drugih krajih in državah (Bali, Casablanca, Riyadh, Jakarta, Madrid, Londonu, teroristični napad Andersa Breivika na Norveškem), nadalje ob pojavu novih zdravstvenih nevarnosti (SARS, ptičja gripa, BSE, A1 H1N1), očitnem povečanju naravnih nesreč (cunami, potresi, vulkanski izbruhi[1]) ob očitnih znakih klimatskih sprememb ter zadnje globalne ekonomske krize, katerih posledica so množični nemiri v Grčiji in Španiji. Ne moremo niti mimo množičnih oboroženih konfliktov in nemirov na območju severne Afrike zaradi tako imenovane arabske revolucije, ki so popolnoma ohromile turizem v teh državah (Egipt, Tunizija, Alžirija, Libija, Sirija).

Krize, ki posredno ali neposredno vplivajo tudi na turistično industrijo lahko v osnovi delimo na čas njenega stopnjevanja. Glede na čas stopnjevanja ločimo med nenadnimi in razvlečenimi krizami. Pri tem je za nekatere tipe kriz (naravne nesreče) značilen zelo hiter prehod v krizno stanje in počasen, večleten povratek v normalno stanje (poplave v New Orleansu; cunami v Indoneziji, potres na Haitiju in Japonskem.). Krize s kompleksnimi dolgoročnimi posledicami praviloma izpostavijo kritične poglede in vprašanja z večjimi razsežnostmi (npr. japonska jedrska nesreča). Primer hitrega/nenadnega prehoda v krizno stanje so tudi teroristični napadi, vendar pa je praviloma njihov povratek v normalno stanje mnogo hitrejši (bombni napad v Sharem el Sheikh). Nekatere druge krize prehajajo v krizno stanje počasneje (epedemije ali pandemije nalezljivih bolezni in okužb), vendar je tudi povratek v normalno stanje hitrejši, kot pri razvlečenih krizah. Poznamo pa tudi krize, katerih prehod v krizno stanje je lahko dolgotrajen (vpliv organiziranega kriminala na določeni destinaciji), vendar pa je tudi reševanje krizne situacije počasno in dolgotrajno. Glede na trajanje je Ritchie (2009, 30) krize razdelil na tri kategorije. V prvo kategorijo spadajo nenadne krize, ki se praviloma pojavijo brez opozorila in se je zato na njih težko ali nemogoče pripraviti. V drugi kategoriji so pojavne krize, ki se pojavljajo in razvijajo počasneje, zaradi česar jih lahko preprečimo ali pa občutno omejimo njihove posledice. V tretjo kategorijo pa spadajo trajnostne krize, ki lahko trajajo teden, mesec dni ali pa celo več let. Proces nastanka in trajanja krize, lahko razdelimo tudi na potencialno fazo, v kateri je možnost za nastanek krize majhna, vendar pa lahko na podlagi analize podatkov in informacij predvidimo, da lahko pride do težav. V latentni fazi, v kateri so že jasno vidni konkretni znaki krize, vendar jih je mogoče s preventivnimi ukrepi preprečiti, ali pa se lahko pripravijo učinkoviti kurativni ukrepi za odpravljanje posledic. Zadnja faza je akutna faza v kateri je kriza že v polnem razmahu, njeni znaki so oči-



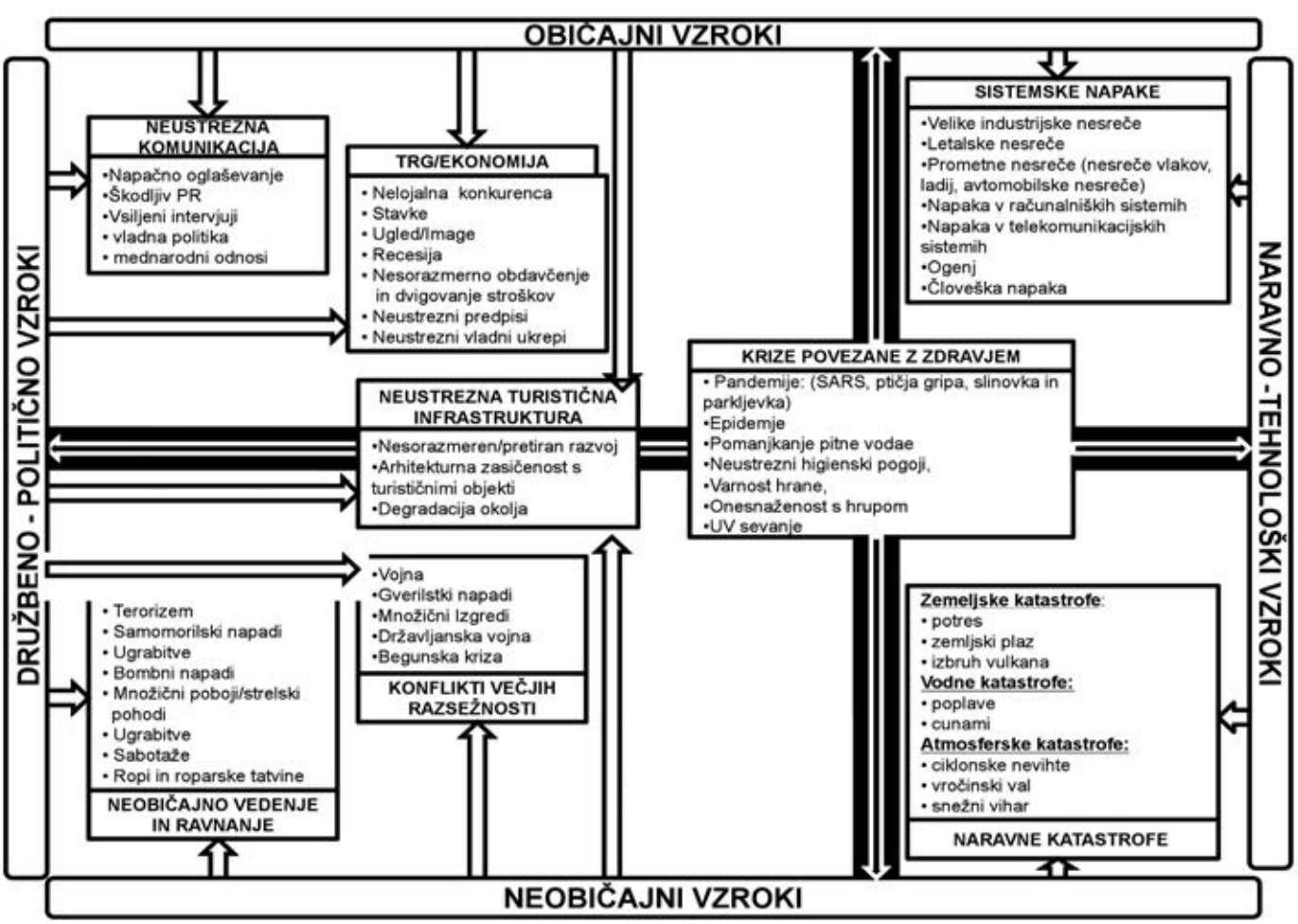
tni, časa za preventivne ukrepe ni več, obvladovanje krize je močno oteženo in usmerjeno le v kurativne ukrepe za odpravo vzrokov in posledic, maneverskega prostora za odločanje je vse manj in pogosto je že viden obseg posledic in škode. Da bi lažje razumeli obseg možnih vzrokov za nastanek kriz v turizmu, ki so geografsko lahko lokalne, regijske, meddržavne, celinske ali pa celo globalne, si bomo ogledali model generičnih vzrokov kriz v turizmu (slika 1). V modelu smo želeli prikazati obseg vzrokov za pojave kriz v turizmu. Krize smo razdelili na običajne oziroma neobičajne na eni osi, ter družbeno-politične oziroma naravno-tehnične na drugi osi.

Če se v določeni državi ali destinaciji pojavi varnostna kriza, to seveda najbolj vpliva prav na turizem. Želja vsakega turističnega gospodarstva je, da se po krizi čim prej povrne zaupanje turistov do varnosti v njihovi državi oziroma destinaciji. Zanimiva je ugotovitev McKercher in Hujeve (2003), da imajo praviloma turisti kratek spomin, kar zadeva varnostno situacijo na neki destinaciji, saj bodo obnovili potovanje na njo takoj, ko bo neposredna nevarnost izginila. Zgodovina nas uči, da varnostne katastrofe, nimajo uničujočega učinka na pretok turistov, je pa dejstvo, da se turistične destinacije različno učinkovito odzivajo na posledice varnostnih kriz. Pomembna razlika pri krizah je v njihovem izvoru/vzroku. Če je vzrok človek (vojne, terorizem, družbeni nemiri) so posledice nezaupanja v določeno destinacijo veliko večje, kot v primeru, ko je vzrok narava (potresi, cunami, vulkani). Pri tem je potrebno poudariti, da imajo naravne nesreče (Haiti) v nestabilnih državah tudi dalnosežne posledice, saj povzročijo kolaps pravne države, kar posledično pomeni manjšo varnost. V stabilnih državah imajo naravne nesreče (orkani in tornadi v ZDA) manjše posledice. Ti primeri kažejo, da je odziv destinacije na generične vzroke kriz, odvisen od njihove razvitosti, stabilnosti in urejenosti. Bolj ko je okolje na destinaciji (država, regija) upravno, administrativno, tehnično, družbeno in politično urejeno in stabilno, lažje se bo soočila z ukrepi za preventivno preprečevanje varnostnih kriz ali z ukrepi za odpravljanje posledic krize in vzpostavljanja prvotnega stanja.

Viri

- Dobovšek, B. (2009). Transnacionalna kriminaliteta. Ljubljana: Fakulteta za varnostne vede.
- Gee, C.Y., Makens, J.C., Choy, D.J.L. (1997). The Travel Industry (3nd ED.) John Wiley&Sons, New York.
- Hall, M., Timothy, D. J., Duval, D.T., (2003). Security and Tourism: Towards a New Understanding?, Safety and Security in Tourism: Relationship, Management and Marketing, The Haworth Hpress, New York.
- McKercher, B., Hui, E.L.L. (2003). Terrorism, Economic Uncertainly and Outbound Travel from Hong Kong. Safety and Security in Tourism: Relationship, Management and Marketing (edited by Hall at al) The Haworth Hpress, New York.
- Ritchie, B. 2009. Crisis and disaster management for tourism. Channel View Publications. Bristol.
- TOURCOM: First world conference on tourism communications (2004). Conference proceedings, ed. Rok Klančnik. Madrid: UNWTO.
- Vršec, M. (2012). Vloga korporativne varnosti. Korporativna varnost 1 (1), 9-11.
- Wilks, J. and Page, S.J. (eds) (2003) Managing Tourist Health and Safety, Elsevier: Oxford. ■

[1] Še posebej izbruh vulkana Eyjafjallajökull na Islandiji, ki je dobesedno ohromil letalski promet nad severno Evropo.



Slika 1: *Model generičnih vzrokov kriz v turistični industriji (Mekinc, Cvikl, 2012)*



IZOSTREN ČUT ZA VAŠE PERILO.

Izjemna zmogljivost delovanja, ergonomija detajlov in logična izbira ustreznih nastavitev potrjujejo odličnost nove generacije pralnih in sušilnih strojev. Inteligentna senzorska tehnologija SensorIQ samodejno uravnava pranje in sušenje ter prispeva k visoki energijski učinkovitosti. Za popolno nego perila poskrbi vrhunska tehnologija SensoCare, saj spoštuje različne potrebe sodobnega uporabnika. Edinstven program za občutljivo belo perilo **UltraWHITE** zagotavlja popolno belino že pri 30° C. Patentirana tehnologija sušenja TwinAir v kombinaciji z IonTech glajenjem vlaken poskrbi za dodatne **UltraSOFT** negovalne učinke.

www.gorenje.si

gorenje

4. mednarodna konferenca

Dnevi korporativne varnosti

Ljubljana, 20.—21. marec 2013

Ujemite zadnja prosta mesta!



ICS

Institut za korporativne varnostne študije

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

www.ics-institut.si