Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha! | Letnik 2014, marec • št. 6



5. jubilejna mednarodna konferenca Dnevi korporativne varnosti

Ljubljana, 18. – 19. marec 2014

Pomen zavedanja o vlogi korporativne varnosti v energetskem sistemu

g. Blaž Košorok, generalni direktor HSE d.o.o.

5. mednarodna konferenca

Dnevi korporativne varnosti

1. mednarodna konferenca

Informacijska varnost - danes in jutri

Ljubljana, 18.—19. marec 2014

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, ki bo izšla ob tej konferenci,
revijo Korporativna varnost (6. številka),
kosilo (sreda) 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

Sponzorji

SHOP

IRONKEY by imation

Medijski pokrovitelji

a&S ADRIA

ZAŠTITA
ČASOPIS ZA ZAŠTITU OSOBA I IMOVINE

SVIJET SIGURNOSTI



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 2014

Izvod revije je brezplačen

Naslovnica:
Dreamstime

ISSN 2232-6170

Obvestilo uredništva:

V reviji št. 5 je bil pri članku z naslovom »Vloga učinkovitega komuniciranja pri obvladovanju poslovnih tveganj« naroben zapis imena avtorice. Pravilno je Mirjam Toporiš Božnik.

Za napako se opravičujemo.

Dinamično okolje v katerem živimo pred nas predstavlja vedno nova tveganja in izzive. Le ti nas opomnijo, kako smo odvisni od neprekinjenega delovanja kritične infrastrukture. Pomanjkanje zavedanja o pomenu procesov zagotavljanja korporativne varnosti ima za organizacije in družbo kot celoto, zelo velike finančne in druge nepopravljive posledice. Korporativna varnost ni omejena samo na procese zagotavljanja fizične in tehnične varnosti v organizacijah, temveč kot pomemben segment obsega tudi zagotavljanje neprekinjenosti poslovanja. Ta proces ima še posebej pomembno vlogo v okviru organizacij, ki obvladujejo kritično infrastrukturo. Kritična infrastruktura je že v svojem bistvu opredeljena kot tiste zmogljivosti, procesi ali objekti, ki so neobhodno potrebni za normalno delovanje širše družbene skupnosti. Upravičeno se nam postavlja vprašanje ali se strateški management v regiji dovolj zaveda pomena teh dejavnikov in njihovega vpliva na uspešnost in učinkovitost delovanja njihovih organizacij, posredno pa tudi vpliva na delovanje družbe. Dogodki v realnem okolju nam na žalost kažejo na dejstvo, da je to zavedanje največkrat potisnjeno v ozadje in ni na tisti pričakovani ravni kot bi moralo biti. Normativno pravno in deklerativno so procesi in pristojnosti še nekako urejeni, ko pa pridemo v situacijo, ko je potrebno zagotoviti učinkovitost odzivanja na neposredne grožnje in tveganja pa hitro spoznamo, da ti sistemi v celoti odpovejo. To nam neposredno kaže tudi zadnji primer naravne nesreče v Republiki Sloveniji, kjer je ledeni dež in s tem posledično žled v nekaj dneh ohromil delovanje skoraj polovico države. V takih trenutkih se zavemo kako ranljiva je moderna družba, ki je v popolnosti odvisna od delovanja določenih infrastrukturnih zmogljivosti brez katerih si težko zamislimo normalno življenje. Zaradi žleda in s tem posledično podrtih dreves, ki so poškodovali velik del elektroenergetskih prenosnih zmogljivosti (daljnovodov in drugih električnih vodnikov) je bilo v določenem trenutku brez električne energije več kot 88.000 uporabnikov. Po grobi oceni je nastalo za 120 milijonov škode od tega več kot 70 milijonov na elektroenergetskem sistemu. Po strokovnih ocenah ELES-a je bilo uničenih 30 kilometrov daljnovodov in 2000 kilometrov distribucijskih elektroenergetskih vodov. Velika škoda je bila povzročena tudi na transportni infrastrukturi. V danem trenutku smo se zavedali, da brez električne energije, moderno življenje kakršnega poznamo danes, ni mogoče. Podsektor električne energije je osrednjega pomena in v soodvisnosti z drugimi podsektorji predstavlja glavni dejavnik za delovanje družbe. Zaradi izpada so bili na velikem delu Slovenije, ki jih je prizadela naravna nesreča onemogočeni procesi delovanja javnih služb, kot so šole, vrtci, državni uradi, velike probleme pa je zaradi izpada proizvodnje utrpelo tudi gospodarstvo. Danes,ko je začel teči proces odpravljanja posledic tega dogodka se lahko vprašamo ali so bili upravljalci kritične infrastrukture ustrezno pripravljeni za izredni dogodek, ki se je tokrat pokazal v obliki žleda. Že hitra analiza nam pokaže, da temu ni bilo tako. Načrti neprekinjenega poslovanja so v veliki večini dobro teoretično opredeljeni, nimajo pa ustrezno razdelanih in predvsem v praksi preverjenih operativnih ukrepov, ki bi zagotovili neprekinjenost delovanja sistema kritične infrastrukture v posameznem podsektorju. Podhranjenost vložkov v vzdrževanje, kadrovski potencial ter njihovo izobraževanje in opremljanje v vsaki večji grožnji rezultira v slabem odzivanju in nezmožnosti zagotavljanja neprekinjenega poslovanja ključnih organizacij. Vso breme je tudi tokrat padlo na gasilsko organizacijo, ki je v večini sestavljena iz prostovoljnih pripadnikov.

Korpopratvna varnost ima kot eden od ključnih procesov v podjetjih zelo pomembno vlogo na področju vzpostavitve sistema neprekinjenega delovanja. Strateško načrtovanje in iz tega izhajajoči operativni ukrepi morajo zagotavljati odgovore na večino groženj in tveganj s katerimi se organizacija sooča pri svojem delu. Temu procesu bo potrebno v prihodnosti nameniti veliko več prostora in zavedanja na nivoju strateškega managementa organizacij..

Doc. dr. Denis Čaleta
Glavni urednik



“ZRNO NA ZRNO POGAČA” – ALI “KITAJSKA LEKCIJA”

Ekonomsko oziroma industrijsko vohunjenje je brez dvoma eden izmed najbolj resnih virov ogrožanja korporativne varnosti, ki se odvija na vseh nivojih.

10



INTERVJU
Dr. Franc Željko Županič
Direktor Kontrole nadzora zračnega prometa d.o.o.

USTREZNA PROCESNA UMESTITEV KORPORATIVNE VARNOSTI POT DO BOLJ UČINKOVITEGA OBVLADOVANJA TVEGANJ

12



STRATEŠKO NAČRTOVANJE PROCESOV KORPORATIVNE VARNOSTI

Naravne, globalne in lokalne grožnje ter iz tega izhajajoča varnostna in druga tveganja nas silijo, da se zamislimo o učinkovitosti obstoječih varnostnih sistemov.

23



KORPORATIVNA VARNOST IN POSLOVNA ETIKA

V najširšem razumevanju etične vloge managerjev lahko trdimo, da je management pravzaprav veda oziroma disciplina, ki temelji na etiki saj praktično vsaka managerska odločitev vpliva na ljudi ali naravno okolje in bi vsaj teoretično morala ta vidik tudi upoštevati.

27

geacollege
Fakulteta za podjetništvo

MANAGEMENT KORPORATIVNE VARNOSTI

Novi magistrski program

55

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

INTERVJU
g. Blaž Košorok
Generalni direktor Holdinga Slovenske elektrarne d. o. o.**

POMEN ZAVEDANJA O VLOGI KORPORATIVNE VARNOSTI V ENERGETSKEM SISTEMU

V energetskem sistemu je potrebno na področju obvladovanja tveganj narediti velike korake v pravo smer. Samo sistemski pristop uvajanja korporativne varnosti v vse procese delovanja naših podjetij, lahko zagotovi ustrezno neprekinjenost delovanja, varnost poslovanja in nenazadnje boljšo konkurenčnost.

HSE je izredno kompleksna organizacija, ki pod svojim okvirom združuje cel spekter različnih gospodarskih subjektov, ki predstavljajo pomemben del sistema proizvodnje električne energije v Sloveniji. Kako je po vaši oceni upravljalsko možno učinkovito upravljati tako razvejan sistem?

Morate vedeti, da glede HSE obstaja zgodovina, ki jo morate poznati, če želite razumeti upravljanje tega kompleksnega sistema. HSE deluje od leta 2002 in je bil seveda ustanovljen z določenim namenom. Pred tem so bile družbe združene pod okriljem Elektrogospodarstva Slovenije oziroma EGS, distribucije ELES in podobno. Po odločitvi lastnika Republike Slovenije je po tem prišlo do razdružitve in sicer do ustanovitve holdinga. Od tega trenutka pa do danes, se v pojmovanju holdinga ni zgodilo veliko. V primeru HSE gre za, če gledamo zakon o gospodarskih družbah, dejanski holding. Ne gre pa za to, kar je po mojem mnenju imel ustanovitelj pred očmi, in sicer neke vrste pogodbeni holding. Se pravi močan holding, ki bi upravljal, financiral in vodil investicije. Nam se namreč dogaja, da imamo holding, neko družbo d.o.o., ki ima pod upravljanjem 5-6 odvisnih družb. Težava se pojavlja v tem, da so omenjene družbe z vključitvijo v holding zadržale svojo popolno pravno samostojnost in subjektiviteto. To je sicer lahko pravno ustrezno, vendar se je potrebno zavedati, da pri pogodbenem holdingu lahko dajete obvezna navodila in drugo, kar je nujno za učinkovito upravljanje. S pričo tega, ker tak holding v pravnem bistvu nikoli ni zaživel, se sedaj srečujemo z vrsto težav. Imamo postavljene hčerinske družbe, ki delujejo v različnih lokalnih okoljih (od Štajerske, Primorske, Zasavja in Posavja) in vsaka živi relativno lagodno življenje brez ustreznih sinergij. In to je slabo. Tukaj nikoli ni bil vzpostavljen dejanski piramidalni sistem upravljanja.

Za uspešno sprejemanje strateških odločitev je zelo pomembna poglobljena ocena tveganj in ogrožanj vaše celotne organizacije. Kako pristopate k obvladovanju tveganj, ki lahko pomembno škodno vplivajo na neprekinjenost delovanja vašega sistema?

No zavedati se moramo, da predstavlja HSE kot skupina z vsemi svojimi odvisnimi družbami, ki so proizvajalke električne energije, več kot polovico proizvedene električne energije v Republiki Sloveniji. V skupini proizvedemo 8 TW ur električne energije, kar je vrh slo-

Prevečkrat se ti procesi obvladovanja tveganj, ki so zelo pomembni za uspešnost in neprekinjenost delovanja organizacije povezujejo z nepotrebnimi stroški.

*avtor je član Slovenskega združenja korporativne varnosti
**korporativni člani Slovenskega združenja korporativne varnosti



venske proizvodnje. Na eni strani imamo termo proizvodnjo, ki je zanesljiv, konvencionalni vir, na drugi strani pa je hidro vir, ki je obnovljivi vir energije. Se pravi takrat, ko je dobra hidrologija, dobra vodnatost rek se aktivno koristi ta vir energije. V zadnjem letu in pol je vodnatost dobra zato s pridom koristimo ta vir energije. Skupaj pa obstaja komplementarnost oziroma povezljivost teh dveh virov. Kar pa se tiče vašega vprašanja glede korporativne varnosti in celovitega obvladovanja tveganj, pa mislim, da je bilo na tem storjenega premalo. V osnovi se pojavlja problem zavedanja o pomenu tega procesa. Po mojem osebnem mnenju živimo v času, ko se daje temu premalo poudarka. Prevečkrat se ti procesi obvladovanja tveganj, ki so zelo pomembni za uspešnost in neprekinjenost delovanja organizacije povezujejo z nepotrebnimi stroški. Zavedati pa se moramo, da skupaj, kot sistem HSE, tvorimo eno elektro-energetsko hrbtenico. Nenazadnje nudimo tudi sistemske storitve operaterju ELES-u. Vse to strateško predstavlja izredno pomemben segment, ki potrebuje varno in celovito upravljanje. Mislim, da smo v preteklih letih namenili temu segmentu premalo pozornosti in počasi prehajamo v zavedanje, da je to pomemben del, ki smo ga do sedaj spuščali.

Del podjetij, ki delujejo v vašem holdingu spadajo v obseg tako imenovane kritične infrastrukture. Kakšni so vaši pristopi, da obvladate tveganja v tem segmentu na obvladljivem nivoju? Ima te v načrtu posebne projekte, ki bodo zagotovili ustrezne podlage za učinkovito izgrajevanje integralnega varnostnega sistema v podjetju?

No predvsem to slednje, kar ste omenili na koncu, ustrezen integralni sistem, se mi zdi v prihodnjosti ključnega pomena. Mislim, da bo potrebno v prihodnje tej temi posvetiti veliko pozornosti. Na to temo smo že govorili z nekaterimi odgovornimi ljudmi saj na žalost v preteklosti nismo temu področju namenjali dovolj pozornosti. Spomnili se boste iz podjetja TE-TOLa, da je bil objekt deklariran kot objekt posebnega pomena za obrambo in neposredno delovanje širše družbene skupnosti. Mislim, da lahko podobno govorimo skoraj za večino objektov, ki delujejo na področju proizvodnje električne energije, kot ključnega vira ze nemoteno delovanje družbe. Pri samem dojemanju te stvari je bilo premalo pozornosti posvečeno tej temi. Tako, da nas na tem področju zagotovo čaka še veliko dela.

Vaše managerske izkušnje so že vrsto let povezane z delovanjem v energetiki. V prejšnjem podjetju TE-TOL ste izvedli nekaj pomembnih projektov zagotavljanja integralne varnosti in neprekinjenosti poslovanja. Ste te izkušnje in dobre prakse prenesli tudi v vaše novo okolje HSE?

Mislim, da ja. Menim, da so se z Institutom za korporativne varnostne študije, ki predstavlja edino institucijo, ki celovito pristopa k obvladovanju tveganj, vzpostavili dobri odnosi, neka pravilna pod-stat, katero jo treba prenesti naprej. Nenazadnje je podsektor proizvodnje električne energije, ponekod tudi malo toplote, izredno pomemben. Vsi ti primeri projektov celovitega obvladovanja tveganj, ki v praksi dajejo ustrezne učinke in rezultate, morajo služiti kot primeri dobre prakse. To pomeni, da na tej poti uvajanja dobrih rešitev ne smemo



zastati, temveč jih je potrebno uveljaviti v celotnem energetskem sektorju.

Kako v vaši organizaciji dojemate pomen procesov javno-zasebnega partnerstva pri zagotavljanju določenih aktivnosti varovanja kritične infrastrukture? Lahko v Sloveniji sploh govorimo, da smo pravilno razumeli izzive in dileme, ki jih prinašajo ti procesi?

Naj vam postavim proti vprašanje »Zakaj bi se zasebni lastnik slabše zavedal pomena korporativne varnosti?« Osebno ne vidim težav na področju javno zasebnega-partnerstva ali če konkretneje govoriva o vstopu strateških partnerjev v delovanje organizacij. Mislim, da je vsakemu v interesu neka integrirana ali pa višja stopnja zavedanja korporativne varnosti. To ni nujno samo praksa za državna podjetja. Pomena varnosti delovanja osnovnega procesa v organizacijah se premalo zavedajo. Mislim, da je v resnih poslovnih okoljih to v velikem interesu zasebnih lastnikov in se s tem veliko ukvarjajo. Poglejmo naše konkurente, ki imajo zelo razvit sistem korporativne varnosti. Vzemimo primer nekega »complains officer-ja«, ki med drugim na koncu dneva lahko predstavlja pomemben subjekt v verigi korporativne varnosti. Osebno težav s tem, da bi me bilo strah kakršnega koli javno-zasebnega partnerstva niti najmanj nimam. Mislim, da je to lahko en korak naprej, da se izboljšajo razmere na tem področju. Mogoče zasebni partner prinese več tega zavedanja in znanja. Če pogledate našo skupino, mi se o korporativni varnosti premalo pogovarjamo, pa naj si bo to pri odtekanju informacij, know-howa ali podobnega. To je problem.

V zadnjem obdobju smo priča pojavu odtekanja ključnih informacij iz slovenskih podjetij in njihovo posredovanje javnim medijem. Menite, da je stanje varnostne kulture v vaši organizaciji na dovolj visokem nivoju, da se taki pojavi lahko preprečujejo in seveda kaj je še možno narediti za izboljšanje stanja?

Mislim, da je stanje varnostne kulture v HSE slabo. Lahko pa bi bilo sicer še slabše, vendar se s tem ne moremo zadovoljiti. Prepričan sem, da obstaja kar nekaj poti, kako bi se to stanje spremenilo. Predvsem z zavedanjem pomena varnostne kulture in seveda zavedanjem pomena poslovnih skrivnosti in ključnih informacij, ki lahko v končni posledici močno vplivajo na uspešnost delovanja podjetja, s tem pa tudi na ohranitev delovnih mest, višini dohodkov in podobno. Vi ste, se spomnim, večkrat imeli predavanja, kako se posamezni dokumenti označujejo in hranijo. Ironija tega fenomena je to, da več kot je rdečih številk in štampiljk strogo zaupno oz. poslovna skrivnost, bolj nekatere ljudi mami, da te informacije od-

Pomena varnosti delovanja osnovnega procesa v organizacijah se premalo zavedajo. Mislim, da je v resnih poslovnih okoljih to v velikem interesu zasebnih lastnikov in se s tem veliko ukvarjajo.

nesejo ali zlorabijo. Težava je v tem, da je proces grajenja ustrezne varnostne kulture izredno dolgotrajen proces, ki zahteva tudi sankcioniranje tistih, ki tega predpisanega sistema ne upoštevajo. Naj omenim samo praktičen primer slabega razumevanja procesa varovanja ključnih informacij. Pred kratkim je v medije prišel stopnjevan dokument z oznako »poslovna skrivnost – strogo zaupno« s katerim je razpolagal ozek krog ljudi, ki so dokument potrebovali za svoje delo. V procesu varovanja so bili izvedeni vsi ukrepi varovanja pa je dokument vendarle nepooblaščeno prišel v javnost. To dokazuje, da je človek še vedno najšibkejši člen varnostnega sistema vsakega podjetja. Ampak zakaj? Pomena varnostne kulture ali zavedanja, da razpolagajo z nekim dokumentom pač ljudje, enostavno v naši skupini ne razumejo. Bolj kot so posamezni dokumenti označeni s različnimi stopnjami tajnosti, lažje jih sporočajo, ker s tem pač želijo škodovati svoji organizaciji. Na žalost ta škodoželjnost ne pozna meja. Verjetno so navdušeni nad tem, da se potem vidijo v časopisu, oz. vidijo članek z dokumentom, ki so ga odtujili. Seveda svoj del odgovornosti nosijo tudi mediji, ki se vse prevečkrat opirajo na anonimne prijave oz. priče, brez, da bi ustrezno kritično preverili realna dejstva. Zelo pogosto smo priča vprašanjem »na podlagi anonimke vas sprašujem to« ali pa »iz dobro obveščenih virov smo izvedeli«, ali pa »na podlagi dokumenta, ki ga imam pred sabo ste pa vi to in to napisali«. Premalo se zavedamo škodljivih posledic, ki zaradi tega nastopajo za Slovensko gospodarstvo. Težko je s polnim imenom in primkom odgovarjati na neke anonimke, ki so lahko popolnoma neosnovane. Zakaj bi morali zgubljati energijo zaradi anonimk, ki so se največkrat pokazale kot neresnične oz. so dobra osnova za manipulacijo? V tem trenutku se namreč preseže meja dobrega okusa in to je seveda stvar preiskovalnih organov in policije, da razišče take primere in sankcionira osebe, ki so odtujile dokumente oz. manipulirajo z neresničnimi podatki. Ti dogodki ne škodujejo samo posamezni osebi, temveč Slovenskemu gospodarstvu, kot celoti. Nenazadnje pa je izdaja poslovne skrivnosti kaznivo dejanje.

Ali v vašem podjetju na strateškem nivoju obstaja funkcija povezana s korporativno varnostjo? Imate na tem področju kakšne načrte, kako ta proces še bolje integrirati v vse poslovne procese vaše organizacije?

Na žalost tega še nimamo urejenega. V tem trenutku te funkcije še nimamo formalno opredeljene v pravilniku sistemizacije delovnih mest. Mislim pa, da je sedaj priložnost, ko bo prišlo do spremembe pravilnika o sistemizaciji.





Temu področju je potrebno dati večji pomen in ga vtkati v vse procese delovanja našega podjetja.

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

Mislim, da temu področju v vseh družbah dajemo premalo pomena. Velike težave se pojavljajo že pri razumevanju obravnavanega področja korporativne varnosti saj ga zamenjujejo oz. napačno povezujejo z varstvom pri delu, osnovnim fizičnim varovanjem in drugim aktivnostmi, ki so sicer samo del tega širokega procesa, ki ga predstavlja korporativna varnost s ciljem celovitega obvladovanja tveganj. Korporativno varnost v očeh strateškega managementa ne razumemo na ustrezen način. Ko z nekom govoriš prevečkrat opaziš, da korporativno-varnostnega managerja velikokrat zmotoma povezujejo ravno z besedo varnostnik. To nerazumevanje ima verjetno za posledico tudi, da je bilo do nedavnega zaposlovanje na tem področju povezano z bivšimi uslužbenci policije ali pa kriminalistične policije, ki so zaradi takšnih ali drugačni zaslug zasedli ta delovna mesta. Osebno menim, da imajo za delovanje v korporativnem okolju premalo ustreznih znanj. V tem delu vidim ključno vlogo ICS-a in Slovenskega združenja korporativne varnosti, da z organiziranjem raznih srečanj, posvetov, izobraževanj in okroglih miz dvigujete zavedanje in prinašate nova znanja v slovenski prostor. Zelo pomembno vlogo v tem okviru predstavlja magistrski program managment korporativne varnosti, ki ste ga razvili skupaj s GEA College. V tem delu bomo poskušali svoj del v mozaiku dodati tudi v HSE saj smo eden izmed korporativnih članov Slovenskega združenja korporativne varnosti. ■

Korporativno varnost v očeh strateškega managementa ne razumemo na ustrezen način. Ko z nekom govoriš prevečkrat opaziš, da korporativno-varnostnega managerja velikokrat zmotoma povezujejo ravno z besedo varnostnik.

Avtor: g. Andrej Podvršič / DuPont de Nemours International SA*



"ZRNO NA ZRNO POGAČA" – ALI "KITAJSKA LEKCIJA"

Ekonomsko oziroma industrijsko vohunjenje je brez dvoma eden izmed najbolj resnih virov ogrožanja korporativne varnosti, ki se odvija na vseh nivojih.

Danes naj bi se večino poslov odvijalo v virtualnem svetu in za ilustracijo si poglejmo nekaj podatkov.

Leta 1995 je bilo cca 16 milijonov internetnih uporabnikov ali 0,4% celotnega svetovnega prebivalstva, konec 2013 pa jih je že preko 2.7 milijarde ali 38.8% celotnega prebivalstva. Pravijo, da se vsako sekundo na novo registrira 8 novih internetnih uporabnikov!

Internet ponuja neomejene poslovne možnosti za vse uporabnike, na žalost pa tudi za tiste, ki ta virtualni svet uspešno zlorabljajo. Vsak dan se pojavi na trgu okoli 250 000 novih virusov, 30.000 internetnih strani je dnevno tako ali drugače okuženo z virusi. Vsi se trudimo na vse pretege zavarovati svoje informacijske sisteme in vlagamo milijone za obrambo, kar je seveda potrebno, vendar pa nas to ne sme zazibati v lažni občutek, da se vse dogaja samo v virtualnem svetu. Resnični dogodek, ki ga opisujem v nadaljevanju, to brez dvoma potrjuje in nam lahko vsem služi kot dober opomnik.

Pisalo se je leto 2011. Medtem, ko so v računalniških centrih 3 multinacionalnih korporacij (med njimi na žalost tudi naše) divjale vojne med cyber nepridipravi, ki so lansirali milijone napadov na omrežja in računalniškimi strokovnjaki, ki so se trudili ohraniti trdnost požarnih zidov in ostalih obrambnih mehanizmov, se je v oddaljeni Iowi sredi polj, istočasno dogajalo nekaj čisto drugega.



*avtor je član Slovenskega združenja korporativne varnosti

V Iowi je pridelovalec koruze, imenujmo ga Joe, začel svoj jutranji obhod svojih polj in občudoval poganjke nedavno posajene koruze ter se veselil potencialno dobre letine. Na kolovozu je opazil parkiran mali kamionet, v katerem je s prižganim motorjem sedel voznik. Joe seveda dobro pozna vse svoje sosede in voznik tudi že po izgledu ni bil domačin. Pristopil je k vozniku, ki je očitno nekoga čakal in takoj zatem sta se vozniku pridružila še dva sopotnika. Joe jih je seveda vprašal kaj počnejo in ali jim lahko kako pomaga. Starejši moški, očitno vodja, mu je odgovoril, da so na gostovanju na bližnji univerzi in da so si ogledovali polja. Pogled v notranjost avta je Joeju razkril številne sveže, s koreninami pobrane poganjke, skrbno zavite v moker papir in vrtno orodje. Joe jih je ravno hotel pobarati, kaj bodo s tem počeli in ali so to vzeli z njegovega polja, ko je zazvonil njegov mobilni telefon. Neznanci so hitro izkoristili trenutek njegove nepozornosti in se nemudoma odpeljali v neznano. Joeju se je celotna zadeva zazdela precej sumljiva in obvestil je vodstvo podjetja, s katerim je imel pogodbo o gojenju testnih vzorcev novih vrst žitaric.

Podjetje je zadevo preučilo in hitro so ugotovili, da na bližnji univerzi ni nobenih gostujočih strokovnjakov ali študentov, ki bi prišli iz Azije. O sumljivem dogodku in akterjih so obvestili FBI, ki je informacijo vzel pod drobnogled in začela se je dolgotrajna preiskava. V zacetku 2014 so agentje FBI aretirali omenjenega starejšega moškega in njegovih pet pomočnikov ob povratku iz Kitajske. Vsi aretirani so Kitajski državljani z veljavno vizo za bivanje in delo v ZDA.

Zgodba se je seveda začela veliko prej in sicer je leta 2010 v ZDA legalno vstopilo omenjenih 6 kitajskih državljanov. Ustanovili so ameriško podružnico kitajskega podjetja, ki se ukvarja z vzgojo, proizvodnjo in trženjem žitaric in drugih poljščin na Kitajskem. Podatek, da ima matično podjetje na Kitajskem kar 67 podružnic je dovolj zgovoren. Kupili so večjo farmo, s pripadajočimi polji in skladišči v osrednjem delu ZDA. Nato so začeli potovati po zveznih državah ter obiskovali velike farme, katere opravljajo testno pridelovanje novih vrst žitaric, kakor tudi komercialno gojenje le-teh.

Očitno je, da so na določen način prišli do lokacij testnih polj treh velikih korporacij, (LG; Monsanto in DuPont Pioneer HI-Breed). V zadnjih dveh letih so kupovali in pa tudi kradli semena v različnih fazah kaljenja in rasti s testnih polj, jih ustrezno klasificirali, skladiščili in pošiljali na Kitajsko. Njihov cilj je bil priti do novih vrst žitaric, katere so omenjena tri podjetja razvijala za bodočo komercializacijo in na Kitajskem, na podlagi ukradenih poslovnih skrivnosti, razviti svojo znamko žitaric. Seveda za prodajo.

FBI je zoper vse aretirane vložil kazensko ovadbo, kateri je sledila obtožnica, ki jih bremeni zarote zoper že omenjene tri multinacionalne korporacije in kraje poslovnih skrivnosti. Trenutno se vsi nahajajo v priporu in grozi jim dolgoletna zaporna kazen in plačilo več milijonske odškodnine.

Ekonomsko oziroma industrijsko vohunjenje je brez dvoma eden izmed najbolj resnih virov ogrožanja korporativne varnosti, ki se odvija na vseh nivojih. Zagotovo ne zapišem nič novega, da številne države podpirajo in omogočajo tovrstno dejavnost, ki se poslužuje identičnih metod kot obveščevalne službe. Veliko univerz, bodisi v zasebni ali državni lasti, štipendirajo študij v tujini za pridobitev akademske izobrazbe na področju uporabnih znanosti. Tuji študentje, ki uspešno pridobijo akademsko izobrazbo se pogosto zaposlijo in zaživijo v tujini. Mnogi med njimi z razlogom, saj imajo posebno nalogo, ki jo morajo opraviti za svojo državo ali podjetje. Nekateri med njimi so pravi »speci agentje«, mnogi med njimi pa so tarča raznih oblik pritiskov, kot so sklicevanja na državljansko dolžnost, raznih oblik izsiljevanj, marsikdo pa tudi podleže čaru šelestečih zelenih bankovcev oziroma drugih obljubljenih bonitet.

Varovanje intelektualne lastnine je poleg varovanja življenja in zdravja zaposlenih, ena izmed prioritetnih nalog vsakega varnostnega managarja, bodisi v zasebnem ali javnem sektorju. Organizicije vlagajo letno milijonske zneske v raziskave in razvoj novih produktov, potrebna so leta in leta testiranj in pridobitev ustreznih dovoljenj, da lahko podjetje končno začne s komercialnim trženjem. Za ilustracijo, DuPont de Nemours International SA investira letno povprečno 2 milijarde US $ v raziskave in razvoj. V to vsoto niso vključeni stroški ostalih številnih administrativnih postopkov, ki so potrebni za končno komercializacijo proizvodov. Pred petimi leti je bil življenski ciklus proizvoda približno leto dni, nato pa se je na trgu pojavil podoben/identičen proizvod, seveda po bistveno nižji in konkurenčni ceni. Danes strokovnjaki ocenjujejo to življensko dobo na 3 mesece ali celo manj, kar pomeni, da je nekdo v času 3 mesecev "opravil potrebno delo", za katero je lastnik originalnega produkta porabil milijone dolarjev in vrsto let. Problem in nastala škoda je bistveno večja, če temu zaradi izgube trga prištejemo tudi izgubo delovnih mest.

Varovanje intelektualne lastnine je poleg varovanja življenja in zdravja zaposlenih, ena izmed prioritetnih nalog vsakega varnostnega managarja, bodisi v zasebnem ali javnem sektorju.

Opisana resnična zgodba, ki čaka epilog v zvezni državi Kalifornija, je dober opomnik vsem nam, da kljub sofisticiranim in tehnično dognanim načinom zaščite informacijskih sistemov, ne smemo pozabiti na osnovne principe uspešnega modela varovanja kritičnih infrastruktur. Seveda bomo nadaljevali z investicijami v tehnično varovanje kritičnih infrastruktur, obenem pa ne smemo zanemariti varnostno osveščanje in usposabljanje vseh zaposlenih, ki je temelj vsakega varnostnega sistema. Samo organizacije bodisi zasebnega ali javnega značaja, v katerih so zaposleni z visoko osveščeno varnostno kulturo, se lahko uspešno soočajo s tovrstnimi viri ogrožanja. V nasprotnem primeru, se bodo s pogačo posladkali nepridipravi. ■



Avtor: Aljoša Kandžič*

INTERVJU
Dr. Franc Željko Županič
Direktor Kontrole nadzora zračnega prometa d.o.o.**

USTREZNA PROCESNA UMESTITEV KORPORATIVNE VARNOSTI POT DO BOLJ UČINKOVITEGA OBVLADOVANJA TVEGANJ

Pomembno je, da so odgovorne osebe za področje varnosti, skupaj s celotnim sistemom procesa korporativne varnosti sposobne nuditi ustrezno in kompetentno podporo za odločanje na prvem nivoju.

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

Nacionalno-varnostni sistem sestavljajo različni organi in službe, ki zagotavljajo varnost s preprečevanjem in odpravljanjem ogrožanja temeljnih vrednot, ki jih določa ustava in zakoni. Menim, da celoten sistem deluje dokaj dobro, vsaj pri tistih oblikah groženj, ki jih poznamo in nanje znamo reagirati, saj so pristojnosti posameznega subjekta določene z zakonom in se aktivnosti utečeno izvajajo. Večjo težavo vidim pri novonastalih oblikah groženj, torej pri tistih, s katerimi nimamo izkušenj in kjer lahko pride do dvoma o pristojnosti posameznega organa ali službe, saj se neka grožnja lahko preliva na več področij. Za uspešno delovanje nacionalno-varnostnega sistema se mi zdi bistveno dobro sodelovanje vseh vpletenih, časovna usklajenost delovanja, vključno s hitrim prenosom podatkov. Pravzaprav gre za stvari, ki vodijo k uspehu tudi na drugih področjih življenja.

Trenutno varnostno okolje je predvsem osredotočeno na t.i. asimetrične grožnje, med katerimi se vedno bolj izpostavlja informacijsko vojskovanje (kibernetsko vojskovanje). Pri tem se zastavlja vprašanje, kako je nacionalno-varnostni sistem pripravljen na kibernetske grožnje oziroma na grožnje naperjene proti informacijsko-komunikacijski infrastrukturi in energetskim sistemom.

Nacionalno-varnostni sistem nudi ustrezne temelje in podporo za zagotavljanje varnosti na omenjenem področju posameznim subjektom kritične infrastrukture in po potrebi širše, naj si bo to v obliki ustreznih usmeritev za preventivno delovanje ali pa s primerno pomočjo v primeru izvedenih kibernetskih napadov.

Vodite izredno kompleksno in razvejano organizacijo, ki je že zaradi svojih osnovnih procesov zelo izpostavljena celemu nizu tveganj. Kako se s stališča strateškega managerja spopadate z uravnoteženjem razmer-

Za uspešno delovanje nacionalno-varnostnega sistema se mi zdi bistveno dobro sodelovanje vseh vpletenih, časovna usklajenost delovanja, vključno s hitrim prenosom podatkov.

*avtor je član Slovenskega združenja korporativne varnosti
**korporativni člani Slovenskega združenja korporativne varnosti



Foto: Dean Dubokovič

ja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov Kontrole zračnega prometa.

V Kontroli zračnega prometa Slovenije, d.o.o. nepretrgoma potekata dva procesa, ki pokrivata oziroma celovito obvladujeta tveganja, gre za proces varnosti v zračnem prometu in proces varovanja.
Vsekakor morajo biti ti procesi obvladovanja tveganj in ukrepi za njihovo obvladovanje ustrezno oblikovani, da na eni strani dovoljujejo nemoteno delovanje glavnih procesov kontrole zračnega prometa ter na drugi strani zagotavljajo varnost, ne dopuščajo vmešavanja v tehnologijo dela oziroma varnost civilnega letalstva, katerega neločljiv del je Kontrola zračnega prometa Slovenije, d.o.o. Najvišja stopnja varnosti in varovanja sta skozi kulturo podjetja vtkana v delovanje vseh ostalih glavnih in pomožnih procesov.

Ste eden izredno redkih primerov slovenske prakse, ki trenutno deluje na strateškem nivoju vodenja poslovne organizacije in ima predhodne izkušnje na najvišjih položajih različnih subjektov nacionalno varnostnega sistema, imate pa neposredne izkušnje tudi iz akademskega področja, kjer ste pridobili doktorat znanosti. Nam lahko zaupate, kako vam te bogate izkušnje pomagajo pri delovanju na trenutnem področju vodenja Kontrole zračnega prometa?

Delo, ki ga opravljam kot direktor Kontrole zračnega prometa Slovenije, d.o.o., zahteva interdisciplinarna znanja na strateški in tudi operativni ravni. Moje izkušnje iz vojaškega in civilnega letalstva, diplomacije ter z akademskega področja mi pri tem nedvomno pomagajo. Kot nekdanji generalni direktor Direk-

Pomembno se mi zdi zavedanje, da je korporativna varnost osnovni pogoj za dobro delovanje. Sredstva investirana v varnost se povrnejo z odsotnostjo škodnih dogodkov, ki bi sicer lahko pomenili občutno višji strošek odprave posledic teh dogodkov za posamezno podjetje ali v določenih primerih družbo kot celoto.



Foto: Dean Dubokovič

torata za civilno letalstvo na pristojnem ministrstvu v Republiki Sloveniji sem bil med drugim odgovoren za ukrepe varovanja civilnega letalstva kakor tudi kritične infrastrukture s področja civilnega letalstva, kar mi sedaj zelo koristi. Izkušnje iz preteklega pedagoškega dela na Fakulteti za varnostne vede, kjer sem pridobil doktorat na področju varnostnih ved, pa so tudi neprecenljive pri vodenju tega zahtevnega in kompleksnega podjetja.

V Sloveniji se osebe, ki so zadolžene za strateško načrtovanje in izvajanje procesa korporativne varnosti zelo redko nahajajo na prvem nivoju odločanja oz. v njegovi bližini. Menite, da bo to počasi postala praksa tudi v slovenskem prostoru?

Pomembno je, da so odgovorne osebe za področje varnosti, skupaj s celotnim sistemom procesa korporativne varnosti sposobne nuditi ustrezno in kompetentno podporo za odločanje na prvem nivoju. Skozi dvig strokovnosti in kompetentnosti oseb, zadolženih za področje varnosti, bo sčasoma prišlo tudi do premika na nivoju odločanja. Primerna umeščenost odgovornih oseb in za njimi v organizacijsko strukturo postavljen proces upravljanja varnosti oziroma korporativne varnosti, lahko bistveno pomagata tako pri strateških kot tudi enostavnih dnevnih poslovnih odločitvah. Pomembno se mi zdi zavedanje, da je korporativna varnost osnovni pogoj za dobro delovanje. Sredstva investirana v varnost se povrnejo z odsotnostjo škodnih dogodkov, ki bi sicer lahko pomenili občutno višji strošek odprave posledic teh dogodkov za posamezno podjetje ali v določenih primerih družbo kot celoto. Vsekakor bo s povečanjem zavedanja varnosti, dvigom varnostne kulture in prenosom določenih dobrih praks iz evropskega prostora, v posameznih organizacijskih sestavah in eventuelno tudi širše v slovenskem prostoru, prišlo do spremembe, prenosa in umestitve procesa korporativne varnosti na primeren nivo odločanja.

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

Kritična infrastruktura je relativno nov oziroma sodoben pojem. Kontrola zračnega prometa Slovenije, d.o.o. je bila že pred pojavom tega termina uvrščena na seznam subjektov kritične infrastrukture oziroma zavezancev za obvezno organiziranje varovanja in s tem dolžna, zaradi narave dela, zagotavljati varnost objektov, sistemov in zaposlenih v družbi.

Za podjetje je predvsem pomembno celovito obvladovanje tveganj, ki ga izvaja, kot že povedano, skozi dva poslovna procesa, in sicer proces varnosti v zračnem prometu in proces varovanja. Kontrola zračnega prometa Slovenije, d.o.o. je pomemben in neločljiv element civilnega letalstva in je kot taka dolžna zagotavljati varovanje civilnega letalstva, tehnologijo dela kontrole zračnega prometa oziroma navigacijskih služb zračnega prometa, ter pri tem izpolnjevati najvišje možne standarde varovanja, skladno z mednarodnimi in nacionalnimi standardi in varnostno prakso.

Vpeljani sistemski ukrepi gredo v smeri zagotavljanja t.i. celovitega varnostnega pristopa, kjer imajo pomembno mesto predvidevanje in ocenjevanje tveganj, zavedanje o pomenu varnosti in varnostne kulture ter nadzor oziroma preverjanje nad delovanjem in primernostjo sprejetih ukrepov oziroma kontrol za obvladovanje prepoznanih tveganj.

Menite, da država s svojimi pristojnimi organi dovolj upošteva realno stanje in potrebe upravljavcev kritične

infrastrukture ali gre zakonska regulativa v smeri predpisovanja nečesa, kar je v praksi nemogoče zagotavljati?

Država na zakonodajni ravni predpiše pravila za subjekte uvrščene v kritično infrastrukturo, posamezna konkretna področja pa naj bi se urejala s podzakonskimi akti, ki se sprejemajo z zamudo ali pa do njih sploh ne pride.

Država na področju varovanja kritične infrastrukture sprejema generične rešitve oziroma prihaja do prenosa rešitev iz ene panoge v drugo, le-teh pa zaradi specifik posamezne dejavnosti oziroma panoge ni moč vedno aplicirati na konkretne upravljavce kritične infrastrukture in njihovo dejavnost.

Subjekti so tako v veliki meri prepuščeni lastni iniciativi in iznajdljivosti pri reševanju konkretnih problemov oziroma zagotavljanju ustreznega nivoja varnosti. (tekst za okvir)

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

Izzivi, ki se pojavljajo gredo predvsem v smeri zagotavljanja ustrezne kakovosti varnostnih storitev v primeru javno-zasebnega partnerstva, kar je lahko še toliko bolj občutljivo v primeru subjektov kritične infrastrukture.

Pri tem se še posebej izpostavlja vprašanje, ali se posveča dovolj pozornosti nadzoru kakovosti izvajanja varnostnih storitev v smislu ponudnikov varnostnih storitev, da bi le-ti bili sposobni nuditi strokovno in kakovostno storitev naročniku. Pri tem izstopajo predvsem naročniki oziroma subjekti, ki jih ne zavezuje samo slovenska področna zakonodaja, ampak so dolžni spoštovati in implementirati mednarodne akte s področja njihove dejavnosti, ki vključujejo tudi zagotavljanje varnosti, kar je lahko še posebej zahtevno, zato je pomembno sodelovanje obeh akterjev, saj le-tako lahko zagotavljamo ustrezno raven varnosti subjektov in njihovih poslovnih procesov.

Velik del nadzora nad kakovostjo storitev je prepuščen izključno naročniku, upravljavcu kritične infrastrukture, pri katerem pa ni nujen pogoj, da poseduje dovolj strokovnih znanj za izvajanje nadzora nad izvajalcem storitve, kar je še posebej občutljivo v primerih, ko so zasebna varnostna podjetja fokusirana le na finančne vidike partnerstva. Pristojnosti in odgovornosti vseh vpletenih morajo biti uravnotežene.



Foto: Dean Dubokovič

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

Stanovsko združevanje je vsekakor pomemben element pri konstantnem izboljševanju oz. dvigovanju ravni varnosti v posameznih organizacijah in slovenskem prostoru, širjenju varnostne kulture in zavedanja o pomenu varnosti. Zanimiva je izmenjava izkušenj, opisi dobrih ter slabih praks itd. Preko svojega članstva in skozi promocijo zavedanja o varnosti lahko združenje vpliva na splošni dvig varnostne kulture in varnostnih standardov. Praksa žal pogosto kaže, da mora za vidnejše premike v družbi preteči veliko vode. ■

Pomembno je, da so odgovorne osebe za področje varnosti, skupaj s celotnim sistemom procesa korporativne varnosti sposobne nuditi ustrezno in kompetentno podporo za odločanje na prvem nivoju. Skozi dvig strokovnosti in kompetentnosti oseb, zadolženih za področje varnosti, bo sčasoma prišlo tudi do premika na nivoju odločanja.

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);

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah. **SKUPAJ SMO MOČNEJŠI!**

www.ics-institut.si

Avtor: mag. Miran Vršec / Inštitut za korporativne varnostne študije, Ljubljana*



KOLUMNA

miran.vrsec@ics-institut.si

ZAŠČITA IN REŠEVANJE TER ZAGOTAVLJANJE NEPREKINJENEGA POSLOVANJA.

Se bolj splača vlagati v preventivo ali hazardirati in prekomerno tvegati?

Zadnja naravna katastrofa, ki je prizadela praktično celotno Slovenijo je ponovno pokazala na ranljivost okolja, države, njenih inštitucij, gospodarskih subjektov in posameznika. Praktično čez noč sta sneg in žled povzročila ogromno škodo na gozdovih in električnem omrežju, ki – kot smo lahko ponovno ugotovili, predstavlja ožilje države. Ko je le to na enem delu poškodovano, v trenutku odmre območje, ki ostane brez napajanja z električno energijo. Ko pa združimo izpad delovanja dela ožilja (električnega omrežja) in poškodbe vitalnih sistemov, kot so npr. cestna in železniška infrastruktura, mobilne komunikacije in drugo pa kaj hitro lahko postanemo ne samo omejeni v delovanju, temveč celo odrezani od sveta in pomoči.

V prejšnji državi je bil vzpostavljen sistem akcij imenovanih NNNP »Nič nas ne sme presenetiti« s katerimi smo preverjali pripravljenost enot civilne zaščite in obrambe ter ljudstva na ukrepanje v primeru nesreč, ki bi lahko prizadele večja območja oziroma večje število prebivalcev. Vzpostavljen je bil sistem družbene samozaščite. Že od malih nog se je krepila zavest posameznika o potrebni preventivni naravnanosti in vključenosti slehernega posameznika v sistem obvladovanja nesreč in zmanjševanja njihovih posledic na okolje, državo inštitucije in nenazadnje slehernega posameznika. Še živo se spominjam, kako smo v šoli izvajali vaje evakuacije v primeru potresa, požara ali kakšnega drugega namišljenega nenadnega pojava oziroma nesreče, ki bi lahko ogrozila delovanje šole in življenja posameznika. To je bilo takrat povsem samoumevno. Zakaj? Ker je bilo to v zavesti posameznika. Nihče se takrat ni »praskal za ušesi in vihal nosu«, ko je bilo potrebno investirati v opremo, prostore, infrastrukturo in usposabljanje za potrebe omenjenih akcij. Država je imela posluh in je vlagala sredstva v to področje. Preventivno delovanje je bil del našega vsakdana, odzivanje na nesreče pa skoraj rutina. Tako je bilo na nivoju države. Kaj pa na nivoju podjetij? Takratne organizacije združenega dela so morale praktično enkrat letno posredovati občinskemu komiteju za splošno ljudsko obrambo in družbeno zaščito poročila oziroma svoje ugotovitve iz varnostno političnih ocen skladno s predhodno danimi vsebinskimi smernicami za izdelavo omenjenega poročila. Enako je veljalo za krajevne skupnosti. Sistem je bil torej naravnan tako, da so se enkrat letno na občinskem nivoju obravnavala in analizirala ta poročila. Povratne informacije v obliki povzetka so se povratno posredovale organizacijam in krajevnim skupnostim in tako omogočale usklajeno in samozaščitno varnostno načrtovanje. Kako je sistem dejansko deloval v praksi ni predmet mojega trenutnega razmišljanja, saj želim zgolj nakazati, kako je bil sistem vzpostavljen takrat. Naj ta pogled v prejšnji sistem zaključim z aforizmom meni dragega vzornika in očeta, ki ga je zapisal davnega leta 1988 v eni izmed svojih knjig »Kdor skrbi za lastno in družbeno varnost, ima življenje na vajetih«.

V novodobni družbi, ko je država Slovenija članica praktično vseh pomembnih evropskih združenj in organizacij, leta pri načrtovanju nacionalne varnosti in zaščite upošteva vse bolj globalni vidik, s tem pa se zmanjšuje vloga države pri urejanju varnosti in zaščite na lokalnem nivoju še bolj pa se to čuti na nivoju posameznih gospodarskih družb, tudi tistih, ki so na nek način posebnega pomena za državo. Svetla točka v tem sistemu je Gasilska zveza Slovenije, ki je uspela

*avtor je član Slovenskega združenja korporativne varnosti

Svetla točka v tem sistemu je Gasilska zveza Slovenije, ki je uspela ves ta čas ohraniti svoj prvinski sistem delovanja, ki zagotavlja učinkovito delovanje predvsem na lokalnem nivoju preko svojih osnovnih organizacijskih enot, to je profesionalnih in prostovoljnih gasilskih društev, ki delujejo skorajda v vsaki vasi.

ves ta čas ohraniti svoj prvinski sistem delovanja, ki zagotavlja učinkovito delovanje predvsem na lokalnem nivoju preko svojih osnovnih organizacijskih enot, to je profesionalnih in prostovoljnih gasilskih društev, ki delujejo skorajda v vsaki vasi. Njeno učinkovitost delovanja je pripisati dejstvu, da se v lokalna gasilska društva združujejo posamezniki iz lokalnega okolja, ki dobro poznajo in tekoče spremljajo varnostno in drugo problematiko v okolju v katerem bivajo. Pa še nekaj je potrebno vedeti. Pomemben vir financiranja predstavljajo lastna sredstva in donacije posameznikov in podjetij predvsem iz lokalnega okolja, kar še dodatno krepi zavest po nujnosti financiranja, organiziranja in delovanja na lokalnem nivoju. Finančni vložki države v sistem zaščite in reševanja in v procese za zagotavljanje neprekinjenega delovanja (zlasti kritične infrastrukture) so ključnega pomena za učinkovito obvladovanje in reševanje posledic tako naravnih kot tudi drugih nesreč in ima širši vpliv na okolje in delovanje države. Nesporno dejstvo pa je, da se država vse bolj umika iz lokalnega okolja, s tem pa se zmanjšujejo tudi finančni vložki države tudi v sistem varnosti, zaščite in reševanja na lokalnem nivoju.

Vloga države je torej vse bolj usmerjena v pripravo sistemskih rešitev, to je priprave zakonodajnih okvirjev in zagotavljanje prepletenosti med državo, njenimi organi, lokalnimi skupnostmi in gospodarskimi subjekti, medtem ko financiranje in operativno izvajanje ukrepov, potrebnih za obvladovanje ogroženosti, prepušča lokalnemu nivoju in gospodarskim subjektom. Če se malce bolj fokusiramo na gospodarske subjekte lahko ugotovimo, da je država uspela definirati, katere panoge predstavljajo zanjo kritično infrastrukturo, ni pa še podrobneje definirala, katere so njene obveznosti pri obvladovanju tveganj v kritični infrastrukturi in katere so obveznosti gospodarskih subjektov, ki so del te kritične infrastrukture. Tu predvsem mislim na določitev deležev financiranja ukrepov in rešitev za obvladovanje ogroženosti, saj zahteve države predstavljajo za te subjekte dodatno finančno breme, ki ga verjetno sami ne bodo zmogli prenesti. Obenem je država v podzakonskih aktih s področja zasebnega varovanja določila zavezance, ki morajo obvezno organizirati službo varovanja. Tem zavezancem država nalaga obvezno organiziranje službe varovanja, kar od zavezancev zahteva vlaganje dodatnih finančnih sredstev v obstoječe sisteme varovanja in obvladovanja ogroženosti.. Tudi na





tem področju država na eni strani nalaga dodatne zahteve zavezancem, po drugi strani pa nima predvidenih rešitev, kako bo sama s finančnimi vložki pomagala tem zavezancem pri nadgrajevanju obstoječih sistemov varovanja in obvladovanja ogroženosti.

Če se sedaj vrnem na izhodiščno vprašanje opredeljeno v naslovu kolumne lahko najprej ugotovim, da so gospodarski subjekti, tudi tisti, ki so del kritične infrastrukture in tisti, ki so zavezani obvezno organizirati službo varovanja, bolj ali manj prepuščeni sami sebi in lastnim zmožnostim financiranja v sisteme varovanja in obvladovanja ogroženosti. Prepuščeni so torej osnovni dilemi, koliko vlagati v preventivne ukrepe, ki zagotavljajo pravočasno prepoznavanje nevarnosti in ogroženosti in zagotavljajo učinkovito ukrepanje in koliko hazardirati, torej koliko prepuščati situacije naključjem. Zadnja naravna katastrofa, ki je prizadela Slovenijo je pokazala, kako ranljiva je država in še kako bolj so ranljivi gospodarski subjekti in posamezniki. Gre za šolski primer iz katerega že lahko nakažemo del odgovora na izpostavljeno dilemo. Če bi pred mesecem dni izvedli anketo v gospodarskih subjektih in med prebivalstvom na temo potrebe po zagotavljanju neodvisne preskrbe z električno energijo s pomočjo agregatov, ki omogočajo neodvisno preskrbo z eklektično energijo in s tem zagotavljajo neprekinjeno delovanje, bi verjetno veliko odgovorov nakazovalo, da je to nepotreben strošek, saj je država tista, ki mora poskrbeti za nemoteno dobavo električne energije. Zaključek bi bil po vsej verjetnosti ta, da je nabava agregata nepotreben strošek. Verjetno bi se večina s tem strinjala, pa vendar nas tovrstne naravne katastrofe opozarjajo na dejstvo, da temu ravno ni tako. Ko primerjamo strošek izpada delovanja dela procesa ali celotnega procesa s stroškom nakupa agregata, lahko kaj hitro ugotovimo, da je strošek nabave agregata zanemarljiv v primerjavi s škodo, ki lahko nastane zaradi izpada delovanja. Ne gre le za nemožnost operativnega delovanja na kratek rok, gre lahko za posledice z dolgoročnimi negativnimi učinki, ki se kažejo v izgubi naročil, izgubi ugleda in dobrega imena, torej tudi v izgubi dela trga, ki je lahko za določene gospodarske subjekte celo pogubno.

V boju z naravo hazardiranje (priseganje na vse ali nič in priseganje na srečo) torej ne pride v poštev. Na podlagi analize ranljivosti in ogroženosti. ■

Ne gre le za nemožnost operativnega delovanja na kratek rok, gre lahko za posledice z dolgoročnimi negativnimi učinki, ki se kažejo v izgubi naročil, izgubi ugleda in dobrega imena, torej tudi v izgubi dela trga, ki je lahko za določene gospodarske subjekte celo pogubno.

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



RAZVOJ INTERNIH INFORMACIJSKOVARNOSTNIH STANDARDOV NA PODLAGI MODELIRANJA NAPADOV

Poenotenje varnostnih kontrol in prepoznavnost sta glavna razloga, da se organizacije odločajo za splošne in mednarodno priznane standarde varovanja informacij. Vendar če želimo ustrezno varovati informacije pred ofenzivnejšimi agenti grožnje, je nujen razvoj internih informacijskovarnostnih standardov.

Uvod

Za interne informacijskovarnostne standarde je značilno, da so osredotočeni na posamezne delovne procese in že v osnovi oblikovani glede na sposobnosti potencialnih agentov grožnje. To je še posebej pomembno, saj razvoj internih informacijskovarnostnih standardov, kakršne za posamezna korporativna okolja razvija Center za informacijsko varnost pri Inštitutu za korporativne varnostne študije, temelji na metodi modeliranja napadov.

Obravnavani standardi so primerni tako za manjše organizacije, kjer je upravljanje z informacijsko varnostjo na ravni splošno znanih praks uporabe varnostnih kontrol, kot tudi za velika korporativna okolja, ki že imajo vzpostavljene konkretne sposobnosti na področju informacijske varnosti. V tem primeru se z vidika agentov grožnje obravnavajo različne skupine, največkrat visoko sposoben organiziran kriminal z dostopom do ustrezne tehnologije in kadrov, nelegalno delovanje določenih tujih državnih subjektov ter notranji sovražniki, t. i. insiderji.

Prednosti internih informacijskovarnostnih standardov

Uporaba posameznemu korporativnemu okolju prilagojenih, internih informacijskovarnostnih standardov ima številne prednosti. Razvoj in uvedba obravnavanih standardov sta stroškovno ugodna, hitrejša in precej bolj pregledna. Uporaba internih informacijskovarnostnih standardov na podlagi modeliranja napadov je primerna za različna korporativna okolja:

- Organizacije, ki že imajo odlično vzpostavljen sistem varovanja informacij in želijo dodatno varovati ključne procese pred dovršenimi izvedbami groženj.
- Manjša korporativna okolja, ki imajo v posesti izrazit know-how ter druge poslovne informacije in so lahko na podlagi tega tarča resnih agentov grožnje.
- Manjša in srednje velika podjetja, ki želijo izboljšati raven upravljanja z informacijsko varnostjo.

Pri internih varnostnih standardih je bistveno, da omogočajo boljše varovanje ključnih procesov v organizaciji pred izvedbami groženj, proti katerim kljub morda že ustreznemu ali celo nagrajenemu sistemu varovanja informacij organizacija ni zadostno varovana. Seveda pa je treba vedeti, da specializirani interni varnostni standardi niso zamenjava za splošne sisteme varovanja informacij. Interni varnostni standardi so osredotočeni na predhodno izbran nabor kritičnih delovnih procesov v kor-

Uporaba posameznemu korporativnemu okolju prilagojenih, internih informacijskovarnostnih standardov ima številne prednosti. Razvoj in uvedba obravnavanih standardov sta stroškovno ugodna, hitrejša in precej bolj pregledna.

*avtor je član Slovenskega združenja korporativne varnosti



porativnem okolju. Nato pa je treba še pred začetkom opredeliti nabor agentov grožnje, saj je od tega odvisna ekspertna aplikacija znanja pri analitičnem procesu ter posledično poglavitna dodana vrednost takšnih standardov.

Ključne lastnosti procesa modeliranja napadov

Modeliranje napadov je eden izmed najpomembnejših načinov, kako najti šibke točke. Pomembno je za dvig zavedanja o realni situaciji, ki se nam lahko zgodi. Modeliranje napadov pripomore k temu, da se pripravimo na možne scenarije, ki jih v praksi ne želimo preizkusiti. Če se nanje pripravimo, lahko ustrezno zaščitimo korporativno okolje, da do dejanskega varnostnega incidenta ne pride.

V procesu modeliranja napadov uporabljamo različne statične in dinamične modele. Izbor modela je odvisen od obsega izpostavljenosti posameznega korporativnega okolja, obstoječih informacijskovarnostnih zmogljivosti in drugih analitičnih zahtev. Za dobro varovana okolja z visoko stopnjo varnostnega zavedanja uporabljamo lasten »izboljšan strukturni model« (Ivanc, Klobučar, 2013). Ta model temelji na modularnem pristopu, ki omogoča ekspertnim analitikom različnih strok istočasno delo na razvoju modela.

Model napadov je orodje za razvoj scenarijev napadov. Pri procesu razvoja internih informacijskovarnostnih standardov je ključnega pomena znanje analitikov, ki modelirajo napade. Zato eksperti konstantno delajo na sledečih, med seboj povezanih točkah:

- obravnava varnostnih vprašanj z vidika agentov grožnje
- spremljanje novih tehnik napadov
- analiza napadalnih metod

Konstantno delo analitikov na omenjenih področjih je predpogoj za zagotavljanje uspešnosti na področju modeliranja napadov in s tem odlične zasnove internih informacijskovarnostnih standardov, prilagojenih posameznemu korporativnemu okolju. Uvedba internih varnostnih standardov z metodo modeliranja napadov je v informacijsko bolje razvitih državah predpogoj tudi za zagotavljanje operacijske varnosti in zasnove varnostnih območij v državnih organizacijah z najvišjo stopnjo varnostnega zavedanja.

Zaključek

Razvoj internih informacijskovarnostnih standardov je primeren tako za mala kot velika korporativna okolja in predstavlja stroškovno učinkovit način izboljšanja varovanja informacij. Z metodo modeliranja napadov je omogočeno boljše razumevanje implementacije napadov, prepoznava varnostnih šibkosti in analiza obstoječe varnostne politike. Interni informacijskovarnostni standardi so nuja v današnjem času. Center za informacijsko varnost pri Inštitutu za korporativne varnostne študije (ICS CIS) zagotavlja različnim korporativnim okoljem podporo pri zahtevnih odločitvah na področju informacijske varnosti ter predstavlja osrednjo organizacijo za razvoj in uvedbo internih informacijskovarnostnih standardov z metodo modeliranja napadov. ■

ICS – Center za informacijsko varnost



ICS

Institute for Corporative Security Studies

Delovno področje ICS—Centra za informacijsko varnost:

razvoj podjetju prilagojenih informacijsko-varnostnih

standardov in kontrolnih seznamov z metodo modeliranja napadov;

tečaji OSINT - obveščevalna dejavnost javnih virov ;

taktični penetracijski testi;

ekspertne analize in pomoč pri odločanju vodstvenim kadrom s področja

informacijske varnosti v korporativnih okoljih;

Več na www.ics-institut.si!

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



STRATEŠKO NAČRTOVANJE PROCESOV KORPORATIVNE VARNOSTI

Naravne, globalne in lokalne grožnje ter iz tega izhajajoča varnostna in druga tveganja nas silijo, da se zamislimo o učinkovitosti obstoječih varnostnih sistemov.

Opredelitev procesov korporativne varnosti

V tem sestavku predstavljamo način pristopa k izboljšanju varnostnih mehanizmov v gospodarskih in drugih družbah. Govorimo torej o upravljanju korporativne varnosti. Pri strateškem načrtovanju procesov korporativne varnosti moramo izhajati vsaj iz treh postavk, ki so:

- Temeljna izhodišča.
- Sprejetje in implementacija varnostne politike.
- Izdelava varnostnega elaborata.

Pri tem moramo vedeti katere procese uvrščamo v sistem upravljanja korporativne varnosti. Izhajamo iz integralnega varnostnega sistema, ki zajema vsa področja varnosti. Sistem upravljanja korporativne varnosti torej zajema naslednje procese:

- Proces upravljanja zaščite in reševanja ter varstva okolja.
- Proces upravljanja varnosti in zdravja pri delu ter varstva pred požari in eksplozijami.
- Proces upravljanja integriranega fizičnega in tehničnega varovanja.
- Proces upravljanja varstva podatkov in poslovnih skrivnosti.
- Proces upravljanja varovanja informacij in elektronskih komunikacij.
- Proces upravljanja zaščite blagovnih znamk, konkurenčnih prednosti in ugleda.
- Proces upravljanja varnostne dokumentacije.
- Proces upravljanja načrta varovanja in vzpostavljenega varnostnega režima.
- Proces upravljanja varnostno nadzornega centra-upravljanje izrednih dogodkov.
- Proces upravljanja, vodenja in usposabljanja varnostnega osebja.

V celoti gre torej za upravljanje procesov korporativne varnosti, pri čemer nas v tem sestavku najbolj zanima varnosti elaborat, ki je edino pravo in realno merilo profesionalnega pristopa k vzpostavljanju integralnega varnostnega sistema, oziroma k vzpostavljanju sistema upravljanja korporativne varnosti.

Temeljna izhodišča

Prvo izhodišče: Korporativno upravljanje je opredeljeno v Načelih korporativnega upravljanja (OECD - Organisation for Economic Co-operation and Development, 2004)), ki se v strnjeni obliki vidijo v naslednjem:

- Praksa korporativnega upravljanja mora biti konsistentna z načeli pravne države.
- Odgovornosti med posameznimi organi morajo biti jasno ločene in v javnem interesu.
- Nadzorni in izvršni organi morajo imeti jasna pooblastila in integriteto.
- Proces korporativnega upravljanja mora zajemati tudi ukrepe za preprečevanje korupcije in drugih kriminalnih ravnanj.

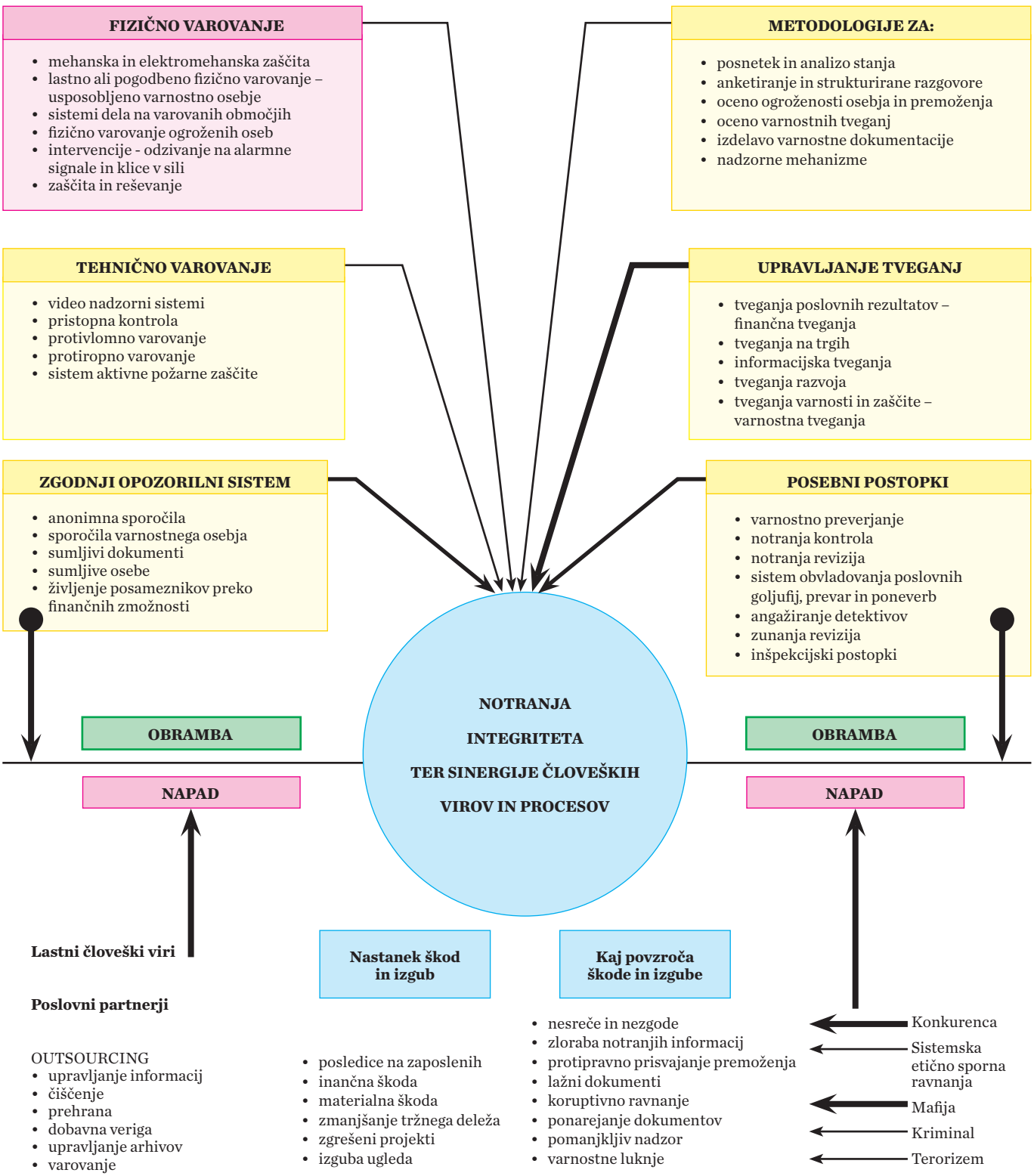
Drugo izhodišče: Zakonodaja, ki ureja področja varovanja in zaščite kot so varstvo pred naravnimi nesrečami, varnost in zdravje pri delu, varstvo pred požari, varstvo okolja, idr.

Tretje izhodišče. Uvajanje in posodabljanje standardov kakovosti in varnostnih standardov kot so denimo ISO 14001, OHSAS 18001, ISO/IEC 27000 idr.

*avtor je član Slovenskega združenja korporativne varnosti

Sprejetje in implementacija krovne varnostne politike

Krovni dokument upravljanja korporativne varnosti je varnostna politika (več o tem Vršec, v: Korporativna varnost, 2012, št. 2). Že pri izdelavi varnostne politike je smiselno, da izhajamo iz metodološke in vsebinske sheme pristopa k upravljanju korporativne varnosti (glej sliko v nadaljevanju), ki nam, daje celovit vpogled v nevarnosti, tveganja, škode in protiukrepe.



Metodološka in vsebinska shema pristopa k upravljanju korporativne varnosti

Priprava krovne varnostne politike je strateška naloga lastnikov, poslovodstva in nadzornikov. Vendar pa je poslovodstvo tisti subjekt, ki je prvi odgovoren za korporativno upravljanje, torej tudi za upravljanje korporativne varnosti na bazi krovne varnostne politike. Glavnemu varnostnemu managerju, ki je član poslovodstva, z močjo odločanja, pa se zaupa in naloži naloga implementacije krovne varnostne politike, to je organizacija izdelave in operativne izvedbe varnostnega elaborata.

Izdelava in izvedba varnostnega elaborata

Varnostni elaborat predstavlja implementacijo sprejete varnostne politike in je hkrati pokazatelj varnostne strategije ter podlaga za izdelavo notranjih aktov in operativne varnostne dokumentacije kot so načrti varovanja, navodila, varnostni režimi itd.
Varnostni elaborat v osnovi zajema naslednje faze izvedbe:

- Posnetek obstoječega stanja.
- Analiza obstoječega stanja.
- Predlogi varnostnih izboljšav (zlasti) na strateškem nivoju.

Posnetek obstoječega stanja zajema naslednje aktivnosti:

- operativni (terenski) pregled območij in zgradb,
- proučitev organiziranosti sistema varovanja na strateškem in operativnem nivoju ,
- ogled sistema fizičnega varovanja,
- ogled sistemov tehničnega varovanja,
- preučitev varnostnih režimov,
- preučitev alarmnega in odzivnega sistema v sklopu upravljanja z varnostno nadzornim centrom,
- pregled varnostno vitalnih točk,

Priprava krovne varnostne politike je strateška naloga lastnikov, poslovodstva in nadzornikov. Vendar pa je poslovodstvo tisti subjekt, ki je prvi odgovoren za korporativno upravljanje, torej tudi za upravljanje korporativne varnosti na bazi krovne varnostne politike.

- pregled obstoječih dokumentov varovanja (načrt varovanja, navodila in drugo),
- razgovori s kompetentnimi osebami odgovornimi za posamezna področja varnosti in zaščite.

Analizo obstoječega stanja opravimo z naslednjimi aktivnostmi:

- analiza in povzetek ugotovitev iz operativnega pregleda območij in zgradb,
- analiza in povzetek ugotovitev v zvezi z organiziranostjo sistema varovanja na strateškem nivoju,
- analiza in povzetek ugotovitev iz ogleda sistema fizičnega varovanja,
- analiza in povzetek ugotovitev iz ogleda sistemov tehničnega varovanja,
- analiza in povzetek ugotovitev v zvezi z vzpostavljenimi varnostnimi režimi,
- analiza in povzetek ugotovitev v zvezi z vzpostavljenimi alarmnimi in odzivnimi sistemi,



- nabor in opis ranljivih - varnostno vitalnih točk na območjih in v zgradbah,
- povzetek in analiza ugotovitev iz pregleda obstoječih dokumentov varovanja,
- predstavitev vsebine razgovorov s kompetentnimi osebami odgovornimi za posamezna področja varnosti in zaščite na strateškem nivoju,
- predstavitev vsebine razgovorov s predstavniki poslovodstva,
- analiza ranljivosti, ogroženosti in varnostnih tveganj v notranjem in zunanjem okolju (matrika ogroženosti) in razvrstitev tveganj v matriko tveganj z uporabo splošnega in Andersenovega modela upravljanja s tveganji.

Predlogi varnostnih izboljšav, morajo temeljiti na posnetku obstoječega stanja in strokovni analizi ranljivosti, ogroženosti in varnostnih tveganj v notranjem in zunanjem okolju. Zajemati morajo vsaj naslednje izboljšave:

- vzpostavitev sistema upravljanja z varnostnimi tveganji na strateškem nivoju,
- vzpostavitev korporativnega varnostnega managementa na strateškem in operativnem nivoju,
- vzpostavitev sistemske notranje pravne ureditve na področju upravljanja z varnostno dokumentacijo,
- optimizacija sinergije fizičnega in tehničnega varovanja,
- vzpostavitev učinkovitega alarmnega in odzivnega sistema v sklopu upravljanja varnostno nadzornega centra,
- vzpostavitev učinkovitega nadzora nad delovanjem sistema varovanja na strateškem in operativnem nivoju (tudi nadzora nad pogodbenim varovanjem),
- vzpostavitev sistema neprekinjenega delovanja in kriznega upravljanja korporativne varnosti v izrednih varnostnih razmerah.

Ko je varnostni elaborat izdelan ga je treba (v obliki povzetka) predstaviti poslovodstvu. Ob predstavitvi notranji in/ali pogodbeni izdelovalci elaborata nakažejo tudi strokovno, organizacijsko, kadrovsko, logistično in finančno plat implementacije elaborata. Poslovodstvo se v določenem času izreče za sprejetje in/ali dopolnitev elaborata in (običajno) za fazno izvedbo elaborata.

Priporočilo

Glede na to, da je Inštitut za korporativne varnostne študije referenčna organizacija za uvajanje in razvoj upravljanja korporativne varnosti v industriji in gospodarstvu, še posebno pa v kritični infrastrukturi (energetika, zdravstvo, transport, bančni sistem, prehrambena industrija, idr.) je logično, da management, strokovnjaki, raziskovalci in pedagogi te institucije razvijajo korporativno varnost kot strateško konkurenčno prednost. Evidentno je namreč, da je treba na področju upravljanja korporativne varnosti stopati s pospešenimi in profesionalnimi koraki, ki vsebujejo tudi potrebne etične vrednote. ■



Avtor: Izr. prof. dr. Jaka Vadnjal, Dekan GEA College-Fakulteta za podjetništvo



KORPORATIVNA VARNOST IN POSLOVNA ETIKA

V najširšem razumevanju etične vloge managerjev lahko trdimo, da je management pravzaprav veda oziroma disciplina, ki temelji na etiki saj praktično vsaka managerska odločitev vpliva na ljudi ali naravno okolje in bi vsaj teoretično morala ta vidik tudi upoštevati.

Ožji konstrukt etične vloge managerjev, ki temelji predvsem na neoklasični ekonomski teoriji po drugi strani pravi, da bi morali managerji predvsem služiti interesom lastnikov. Edina etična obveznost je v tem kontekstu maksimizacija vrednosti podjetja za lastnike, ki jo je potrebno dosegati v okviru veljavne zakonodaje. Ta zgolj ekonomska paradigma je v realnem življenju seveda bistveno bolj kompleksna saj managerske odločitve posegajo v življenja ljudi, zaposlenih v podjetju, njihovih družin in ljudi, ki so del poslovnega okolja podjetja. Prav zato se etičnim vprašanjem in dilemam ne moremo izogniti pri praktično nobeni managerski odločitvi, zato etičnega ravnanja in managerskih vlog in nalog ni mogoče ločiti. Prav zaradi tega korporativno varnost, ki jo razumemo predvsem kot celostno varovanje organizacije (tehnično, fizično, informacijsko, okoljsko, finančno itd.) lahko označimo kot stroko, ki ima za podlago predvsem razmislek o tem, kaj je etično in kaj ne.

Kaj je etično voditeljstvo?

Etična vloga managerjev je pravzaprav tisto, kar strokovnjaki imenujejo etično voditeljstvo (ang. Ethical leadership), kar razumemo kot kombinacijo med moralno osebnostjo (lastnosti managerja kot človeka) in moralnim managerjem (njegovo funkcijo ozioma vlogo). Kaj pomeni, če za nekoga rečemo, da je moralna oseba? Običajno razumemo, da gre za osebo, ki ima integriteto, je poštena in zaupanja vredna. Integriteta ne vsebuje samo pravičnosti in poštenja ali resnicoljubnosti, ampak tudi skrb za zdravje celotne organizacije, ki jo nekdo upravlja. Integriteta tudi pomeni, da se organizacija ravna po etičnih načelih in pravilih in da je moralna osebnost tista, ki ima osebno integriteto in ji lahko zaupamo. Če manager vprašanja korporativne varnosti razume zgolj kot (nepotreben) strošek, bi ga težko označili kot zaupanja vrednega človeka saj je bodoča tveganja pripravljen vrednotiti zgolj ekonomsko, vprašanja moralnega ravnanja pa so bistveno širša.

Poleg naštetega »biti moralna oseba« pomeni tudi ustrezno obnašanje: delati pravične stvari, skrbeti za druge ljudi, biti odprt in imeti razdelane standarde osebne integritete. Ključno pri etiki je delati dobre stvari, še posebej v težavnih okoliščinah in pri managerjih vključuje sposobnost presojanja, kaj je v določenih okoliščinah prava in dobra stvar. Primer take dileme je zelo aktualen: ob nedavnih težavah z žledom so morali nekateri prostovoljni gasilci pri delodajalcih prositi za dopust, da so lahko nesebično pomagali. Kaj si lahko mislimo o človeku (podjetniku, managerju), ki ni pripravljen poslati človeka, ki ga sicer ima na plačilni listi, na pomoč ljudem v stiski? Da bi bil sposoben odločati se v težkih etičnih dilemah, mora biti človek odprt, da se uči iz različnih virov, pri čemer mora predvsem paziti, da ne prizadene ali škodi ljudem in mu je dejansko veliko do tega, da bi z ljudmi dobro ravnal, tako med sprejemanjem odločitev, kot tudi v obdobju, ko je odločitve potrebno uveljaviti. Da bi bil sposoben sprejemati dobre etične odločitve, mora posameznik imeti jasno razvit oseben nabor vrednot in osebni kodeks obnašanja in integritete, ki omogočata posamezniku jasno usmeritev pri sprejemanju odločitev. Manager, ki ne razume pomena korporativne varnosti in v svojih vlogah deluje izrazito kratkoročno, v svojem bistvu ravna sebično saj mu je ključno, da bo na kratek rok maksimiral dobiček, kar je razumljivo saj velika večina managerskega nagrajevanja izhaja iz bilančnih dobičkov, ki se danes ponekod celo kvartalno obračunavajo.

Integriteta ne vsebuje samo pravičnosti in poštenja ali resnicoljubnosti, ampak tudi skrb za zdravje celotne organizacije, ki jo nekdo upravlja.

Ko je potrebno sprejeti težke odločitve je najbolje, da se moralna osebnost drži svojih ključnih vrednot, da poskuša biti objektivna in poštena (fer), da pokaže skrb za družbo in blaginjo vseh njenih deležnikov. Vendar biti moralna osebnost ni dovolj, da bi nekdo postal moralni voditelj. Moralno voditeljstvo pomeni tudi, da je vodja moralni manager, kar se kaže predvsem v dejstvu, da tega managerja podrejeni prepoznavajo kot zgled dobrega ravnanja. To pomeni predvsem vzpostavitev sistema nagrad in discipline za etične in neetične odločitve, ki jih sprejmejo drugi, tako da se navzven pošilja jasno sporočilo, kaj je za organizacijo sprejemljivo in kaj nesprejemljivo obnašanje. Poleg tega moralni management pomeni odkrito komuniciranje, ki mora biti še posebej eksplicitno in pogosto glede etike in vrednot, ki vodijo organizacijo. Anekdotično lahko ugotovimo, da je v Sloveniji takega ravnanja zelo malo. Nekaj več ga je v zelo uspešnih podjetjih, ki so nastala iz nič in svoj uspeh na nek način gradijo na etičnem in moralnem ravnanju. Po drugi strani pa predvsem v divje privatiziranih sistemih opažamo predvsem izrazito neoliberalne vrednote, v katerih se na prvo mesto postavlja pogosto špekulativni kratkoročni donos na kapital. Pogosto se pojavi vprašanje, ali so posamezniki lahko etični managerji, če v zasebnem življenju njihovo obnašanje ni ravno etično ali obratno. Glede na to, da se karakter posameznika odraža v vseh njegovih odločitvah in aktivnostih, bi bila taka nekonsistentnost težko razumljiva.



Okviri etičnega odločanja

Managerji v večjih in manjših podjetjih se vsakodnevno srečujejo s težavnimi etičnimi dilemami. Pomembno je, da se managerji zavedajo, da so etični elementi vključeni v praktično vse dnevne aktivnosti in z njimi povezane odločitve. Pri odločitvah je potrebno enakovredno upoštevati managerski (ekonomski) in etični vidik vsakega problema. Pogosto se pojavijo izzivi, ko je z vidika managerja oziroma njegove organizacije zelo jasno, kaj je dobro in kaj je slabo. Večina managerskih odločitev je zakonitih, nekatere pa sežejo tudi čez meje pravno sprejemljivega ali so na robu. Za take odločitve načelno velja, da so neetične, tako da se z vidika etike ni težko odločiti.

Problemi etičnega odločanja nastopijo takrat, ko odločitve vsebujejo moralni konflikt. Ta nastopi takrat, ko se mora nekdo odločiti med vsaj dvema navidezno slabima izbirama, ali kjer se pojavijo večplastne etične odločitve, ki so pogosto v medsebojnem konfliktu interesov. V takih okoliščinah , ki so v podjetju zelo pogoste, mora biti manager sposoben razmisliti o vseh posledicah in etičnih implikacijah tako, da se sprejme najboljša možna odločitev z vsemi omejitvami in posledicami.

Ko je potrebno sprejeti težke odločitve je najbolje, da se moralna osebnost drži svojih ključnih vrednot, da poskuša biti objektivna in poštena (fer), da pokaže skrb za družbo in blaginjo vseh njenih deležnikov.

Če se odločitev ne da sprejeti, tako da bi bili vsi zainteresirani zmagovalci, je potrebno razmišljati o novem okviru za sprejemanje odločitev. Kot primer naj navedem dilemo managerskega kolega, ki bi moral investirati veliko denarja v čistilno napravo, da bi zadostil bolj strogim okoljski standardom. Prostega denarnega toka v podjetju ni, lastniki si umivajo roke, sam pa je razpet med odločitvijo, ali naj gre v investicijo, izpostavi podjetje tveganju in posledično ogrozi 200 delovnih mest? Razmišlja da bi odstopil, vsekakor pa je v tej zgodbi velik del etičnosti razpleta na strani lastnikov, ki tega dela svoje vloge ne razumejo.

Da bi managerjem olajšali odločitve, je skupina strokovnjakov v tujini pripravila okvir, ki temelji na idejah filozofov in etikov in vključuje štiri vidike etičnega razmišljanja: (1) pravice in dolžnosti, (2) utilitarianizem, (3) pravičnost in (4) pozornost, kot jih prikazuje razpredelnica 1.

Razpredelnica 1: Okvir za etično sprejemanje odločitev

Pravice in dolžnosti
Gre za pravila, ki so na nacionalni ravni v obliki zakonov in drugi predpisov. Tako na primer delovnopravna zakonodaja predpisuje pravice (delno dolžnosti) delavcev in dolžnosti (in deloma pravice) delodajalcev. Na mednarodni ravni tak okvir predstavljajo različne mednarodno predpisane deklaracije kot na primer Deklaracija Združenih narodov o človekovih pravicah.

Utilitarianizem
To je usmeritev, da naj bo odločitev taka, da bo čim bolj ugodna za čim širši krog zainteresiranih ljudi. Gre za analizo stroškov in koristi, ki jo je težko narediti v številkah, zato je v veliki meri odvisna od razvitih sposobnosti tistega, ki mora presojati, saj gre za kompleksno temeljno vprašanje: kdo vse bo prizadet zaradi odločitve in kakšna je škoda ali korist za posameznika ali skupine.

Pravičnost
Pri tem konceptu je potrebno upoštevati, da je potrebno vse, ki jih bo odločitev doletela obravnavati enakopravno in jim dati enake možnosti. Pri tem prihaja do dilem, ali bodo okoliščine po odločitvi še vedno enake ali ne. V filozofiji ta koncept poznamo kot »kategorični imperativ«, ki ga lahko razložimo z vprašanjem, ali lahko neka odločitev kasneje postane univerzalno pravilo v podobnih primerih.

Čuvanje povezav
Gre za vidik, kako odločitve vplivajo na odnose med posameznimi skupinami, oziroma obratno: ali ti odnosi vplivajo na odločitve. Klasičen primer neetičnega ravnanja s tega vidika je nepotizem oziroma dajanje prednosti zaradi sorodstvenih povezav. Podobno v nekaterih podjetjih zaščitijo dolgoletne uslužbence itd.

Vir: Prirejeno po Encyclopedia of Business Ethics and Society



Prva paradigma učinkovitega etičnega obnašanja organizacije je v jasno opredeljenem smislu obstoja in viziji, ki jo mora poznati celotna organizacija, torej vsi njeni zaposleni skupaj z okoljem, v katerem delujejo.

Da bi se managerji lahko učinkovito odločali o etičnih dilemah, je najbrž koristno, da se ne odločajo samo intuitivno, ampak na podlagi upoštevanja vseh kriterijev. Včasih se je potrebno tudi odločati, ali je kakšen dejavnik morda prevladujoč. Če ima manager pred sabo dilemo, ali bo nekdo umrl, ali pa bo nekaj ljudi ostalo brez dela, je verjetno jasno, čemu bo dal prednost. Druga skrb je, če je en kriterij v določeni situaciji pomembnejši od ostalih. Včasih lahko z neetično odločitvijo povzročimo še večjo škodo za vse vpletene. Tako odločitev , ki je v bistvu neetična, lahko štejemo kot etično, če ni bilo namena neetičnega odločanja. Naslednja dilema je, ali manager želi, da bi njegova odločitev postala javna in da se pojavi v časopisih in na televiziji. Nekaterim posameznikom gode, da so v središču pozornosti, drugim je to lahko odveč. Za managerje, ki delujejo v različnih kulturnih okoljih po svetu, velja, da imajo v vsaki kulturi neko pravilo, ki gre približno takole: Ne stori drugim ničesar, kar ne želiš, da bi drugi storili tebi.



Moralni razvoj

Moralni razvoj posameznika se po navadi zgodi v treh fazah. V mlajšem obdobju se človek predvsem zgleduje po vzornikih, najprej doma, kasneje v šoli in potem pri mentorjih sodelavcih in drugih, ki usmerjajo njegovo profesionalno pot. V naslednji fazi, ko je posameznik soočen s tem, da mora sprejemati odločitve tudi skozi prizmo etike in morale začne študirati različna pravila, zakone, etične kodekse, torej dokumentirane zbirke pravil, ki so jih konsenzualno sestavili za določene poklice, panoge itd. V tretji fazi se začne lastni moralni razvoj. Po nekaterih raziskavah to fazo doseže samo 20% vseh ljudi, ki si v moralno zrelem obdobju začnejo postavljati svoj moralno etični okvir v okviru katerega sprejemajo svoje managrske in druge odločitve. V Sloveniji smo priča veliko zgodbam, ki jih uvrščamo v kompleksno polje korupcije. Morda temu botruje tudi dejstvo, da je med odločevalci veliko mladih ljudi, ki niso imeli niti časa, da bi šli skozi potrebne faze moralnega razvoja. Tako se jim nekatera dejanja, ki jih sicer razumemo kot koruptivna, zdijo normalna in skrbeti bi nas moralo, če sprejemljivost koruptivnih dejanj že prihaja v (nepisane) kodekse etičnega obnašanja.

Kodeksi obnašanja

Mnoge velike korporacije imajo lastna pravila obnašanja, ki managerjem pomagajo pri odločitvah v kontekstu etičnih dilem ali moralnih konfliktov. Taki pravilniki morajo imeti podporo drugih notranjih sistemov, ki opredeljujejo na primer nagrajevanje, informiranje, zaposlovanje, napredovanje, komunikacijo in druge aktivnosti. Brez te podpore je težko pričakovati učinkovito etično odločanje, za katerega mora vrhnji zgled dajati vrhnji management korporacije. Zaradi medkulturnih razlik v različnih okoljih je v mednarodnih korporacijah ravnanje po enotnih pravilih oteženo, zato lahko pomagajo nekateri mednarodni strandardi, kot je na primer 10 ključnih principov poslovne etike, ki ga je pripravila OECD.

Managerji in etika v organizacijah

Mnogim managerjem je težko govoriti o etičnih vprašanjih. Raziskave kažejo, da je to posebej v primerih, ko njihov osebni etični kodeks ni dobro umeščen v delovanje organizacije ali drugače: managerji lahko imajo svoje standarde, po katerih se ravnajo, vendar to ni kultura celotne organizacije, kjer se zato ne počutijo dobro. V takih primerih so tudi pričakovanja lastnikov ključnega pomena.

Prva paradigma učinkovitega etičnega obnašanja organizacije je v jasno opredeljenem smislu obstoja in viziji, ki jo mora poznati celotna organizacija, torej vsi njeni zaposleni skupaj z okoljem, v katerem delujejo. Zaposleni se morajo počutiti kot del delovne skupnosti in ne zgolj kot podrejeni. Etično voditeljstvo mora delavcem zagotavljati sistemsko perspektivo, kar pomeni, da organizacija računa na njih, da bodo z organizacijo osebnostno in strokovno rasli zaposleni in organizacija z njimi. Etično voditeljstvo pomeni, da je največji poudarek na delovanju poslovnih procesov in ne na hierarhiji, kar pomeni, da bo bistveno bolj cenjeno delo in prispevek posameznika k organizacijskemu uspehu in ne bo pomembno njegovo ugajanje nadrejenim. Zaposlenim je potrebno dati čim več možnosti odločanja in tako spodbujati individualno odgovornost, ki bo temeljila na resnici, integriteti in poštenosti, ki so značilnosti moralne osebe. Tako obnašanje managerjev na dolgi rok spodbuja konstruktiven dialog med vsemi deležniki organizacije. Etični voditelj bo tako vzpostavil občutek predanosti organizaciji in skupnemu cilju, tako da bo poudarjal vrednote, kot so držanje obljub, smiselno postavljal zaposlenim nujne prioritete in spodbujal kreativno vključevanje zaposlenih v procese, namesto izključevanja podrejenih iz kakršnihkoli možnosti odločanja. ■

NATO Advanced Research Workshop

Managing Terrorism Threats to Critical Infrastructure Challenges for South Eastern Europe

Beograd, 12. - 15. May 2014

ICS

Institute for Corporative Security Studies

EDUCONS UNIVERZITET

The Institute for Corporate Security Studies and the University EDUCONS are organising a NATO Advanced Research Workshop »Managing Terrorism Threats to Critical Infrastructure – Challenges for South Eastern Europe« which will take place on 12 .– 15. May, 2014 in Belgrade, Serbia.

www.ics-institut.com

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Avtor: Dr. Polona Selič, univ. dipl. psih. / Inštitut za psihofiziološke študije PARES[1]



SODOBNO PSIHOFIZIOLOŠKO PREISKOVANJE VERODOSTOJNOSTI IZJAV S POLIGRAFOM: UPORABA POLIGRAFSKE METODE NA PODROČJU KADROVANJA

Sodobna poligrafija razlikuje med testi prepoznavanja in testi za odkrivanje zavajanja. Celotno polje psihofiziološkega preiskovanja verodostojnosti izjav s poligrafom sestavlja več tehnik in pristopov, ki v pomembni meri določajo tudi samo proceduro oziroma izvedbo.

Izhodišča: koncepti v sodobni poligrafiji

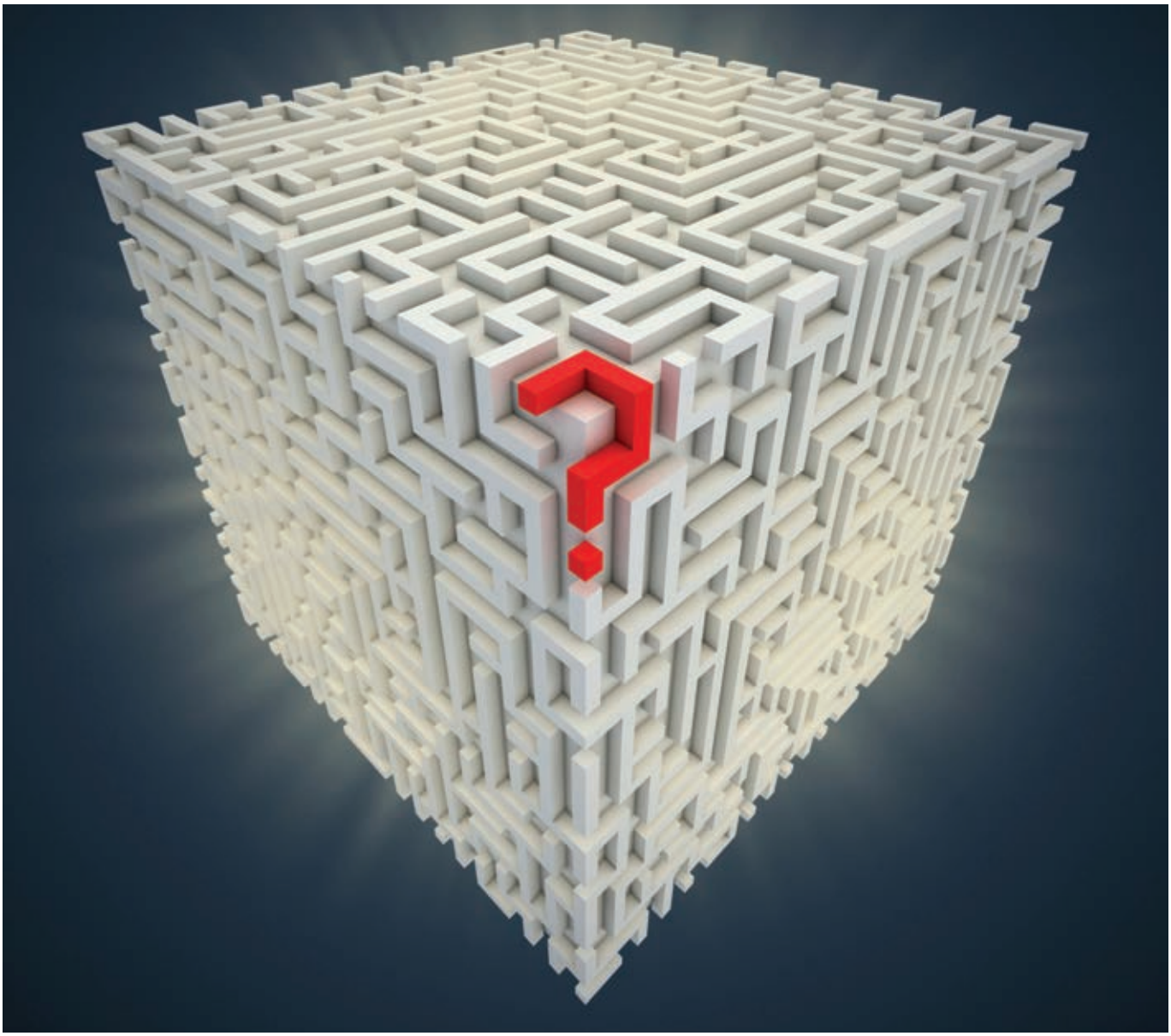
Vse psihofiziološke tehnike preverjanja verodostojnosti izjav s poligrafom so sestavljene iz zaporedja procesov/postopkov: uvodni razgovor, izvajanje (administracija) testa – predstavitev z navodilom in zapisovanje/beleženje odgovorov, vrednotenje – pretvorba surovih podatkov v (standardne ali točkovne) vrednosti ter razlaga (interpretacija) z diagnostičnimi zaključki. Poligrafski testi imajo specifičen namen, zato so vsebinsko zasnovani za testiranca posebej. Pri tem so upoštevane njegove osebne lastnosti in značilnosti (obravnavanega) dejanja (1). To pomeni, da so individualizirani ob uporabi uveljavljenih in preverjenih testnih formatov – vrsta vprašanja na posamezni poziciji je predpisana, vsebina je prilagojena obravnavanemu primeru in testirani osebi (njenemu besedišču, zmožnosti razumevanja ipd.). Kljub temu pa se tudi poligrafski testi oziroma vprašanja, ki jih zastavljamo testirani osebi, podrejajo psihološki, logični in semantični analizi.
Značilnost (posebnost) poligrafskih testov so enopomenski odgovori, prisilna izbira med »da« oziroma »ne«. Tudi vprašanja v poligrafskem testu imajo funkcijo »dražljajev/stimulusov«, ki naj bi (pri testirani osebi) izzvali spremembe v delovanju (fiziološke spremembe). Odzivi se primerjajo z drugimi odzivi posameznika (na vprašanja drugačne vrste – nevtralna, relevantna, irelevantna, primerjalna/kontrolna ipd.) v isti testni situaciji (1).

Poligrafski testi tako omogočajo preverjanje splošnih dejstev in/ali postavljanje posebnih vprašanj, ki se nanašajo izključno na posameznika oziroma na dejanje (2).

Merske značilnosti poligrafskih testov
Poligrafski se od psiholoških testov razlikujejo v merskih značilnostih (1).

1 ***Veljavnost*** testa je natančnost, s katero test meri ravno tisto lastnost, ki naj bi jo meril oziroma jo nameravamo meriti. Razlikujemo vsebinsko, sestavno, sočasno in napovedno veljavnost (3). Pri poligrafskih testih je pomembno odkrivanje zavajanja ali poznavanja okoliščin. Torej je veljaven (natančen) tisti test oziroma testni format, s katerim lahko razlikujemo osebe, ki zavajajo (ali poznajo okoliščine obravnavanega dogodka), od onih, ki govorijo resnico (»naivne« testirane osebe, nevpletene v obravnavani dogodek). Relevantni dražljaj je ustrezno formulirano vprašanje, iz-

[1] izredna profesorica za kriminalistiko in docentka za socialno psihologijo Katedra za družinsko medicino, Medicinska fakulteta v Ljubljani;



rečeno kar se da nevtralno, enakomerno in brez posebnih poudarkov. Če vsa vprašanja v poligrafskem testu niso enako zastavljena, je lahko odziv testirane osebe vezan na način spraševanja in ne na vsebino. V takšnih primerih lahko gre za učinke presenečenja ipd. (4, 5).

2 Objektivnost testa je stopnja neodvisnosti rezultatov in njihove interpretacije od ocenjevalca. Test je docela objektiven, kadar različni ocenjevalci pridejo do povsem enakih rezultatov (t. i. medosebna skladnost ocenjevalcev). Objektivnost zajema in zadeva izvajanje (standardizacija pogojev), vrednotenje in interpretacijo. Slednja je največja pri normiranih testih storilnosti (3). Poligrafski test se objektivnemu približa le, ko se dobljeni rezultati (reakcije) ocenijo na način, ki izključuje subjektivno oceno (presojo) izpraševalca in drugih spremenljivih dejstev. Zato morajo biti vprašanja v poligrafskem testu pravilno strukturirana in postavljena na način, ki izključuje dvoumne reakcije. Pri poligrafskih testih je pomemben način izvedbe (monotoni, enakomerni način spraševanja, upoštevanje predpisanih presledkov) ter način vrednotenja poligrafskih zapisov, ki je predpisan (6).

Merske značilnosti poligrafskih testov so ustrezne in zadovoljujoče, kadar je njihova izvedba kar najbolj standardizirana, poligrafski preiskovalec pa s svojim vedenjem (vključno z govorjenjem) ne izzove dodatnih/neželenih/nekontroliranih odzivov pri testirani osebi.

3 Zanesljivost je stopnja stabilnosti, s katero test meri vedenje ali lastnosti testiranca. Povsem zanesljiv test daje v različnih okoliščinah iste rezultate. Zanesljivost lahko povečamo s podaljševanjem testa (povečamo obseg in število nalog), z zvečanjem občutljivosti in z izboljšanjem objektivnosti (3). Zagotavljanje zanesljivosti s podaljševanjem je pri poligrafskih testih omejeno, saj je dolžina celokupnega testiranja (aplikacije vseh testov s ponovitvami) odvisna od količine razpoložljivih (prikritih) informacij ter drugih psiholoških in fizioloških dejstev (elementi dejanja/dogodka,

adrenalinska izčrpanost ipd.). Nedvomno pa je s kar najbolj standardiziranim načinom izvedbe poligrafskih testov možno doseči, da beležimo odzive na vprašanja o dogodku/dejanju (= predmet merjenja) in ne na delovanje poligrafskega preiskovalca ali kakršnih koli drugih neidentificiranih intervenirajočih dejavnikov (7, 5).

4 ***Občutljivost*** testa se kaže v razpršitvi rezultatov. Večja ko je razpršitev (večje kot so individualne razlike med ocenjevanimi osebami), večja je občutljivost testa (3). Občutljivost poligrafskega testa ni povezana z dolžino vprašalnika oziroma z dolžino vprašanj. Da s poligrafskim testom identificiramo osebe, ki podajajo lažne odgovore na postavljena vprašanja, so pomembna tista relevantna vprašanja, s pomočjo katerih lahko zaznamo specifične reakcije posameznika, ter njihova primerjava s primerjalnimi vprašanji, kadar gre za teste s primerjalnimi vprašanji (8).

Vrednotenje poligrafskih zapisov

V postopku vrednotenja v glavnem opisujemo štiri kategorije reagiranja po posameznih parametrih - brez reakcije (točkovna vrednost 0), šibka reakcija (točkovna vrednost ± 1), srednje intenzivna reakcija (točkovna vrednost ± 2) in zelo močna reakcija, ki jo ovrednotimo s ± 3; takšna ocena je dopustna samo enkrat v testu po posameznih parametrih (dihanje, elektrodermalna odzivnost, kardiovaskularne spremembe). Pri poligrafskih testih nismo zainteresirani za zvezno razporeditev izmerjenih/ocenjenih vrednosti. Prizadevamo si za kar se da nedvoumno razlikovanje med iskrenimi (nevpletenimi) in neiskrenimi (vpletenimi) testiranimi osebami, brez nedoločnih ocen (1).

Merske značilnosti poligrafskih testov so ustrezne in zadovoljujoče, kadar je njihova izvedba kar najbolj standardizirana, poligrafski preiskovalec pa s svojim vedenjem (vključno z govorjenjem) ne izzove dodatnih/neželenih/nekontroliranih odzivov pri testirani osebi. Vsakršna hotena ali nenamerna ali nenadzorovana intervencija poligrafskega preiskovalca lahko povzroči napačno oceno – bodisi lažno pozitivno (poligrafski preiskovalec meni, da testirana oseba zavaja, čeravno ne) bodisi lažno negativno (zavajanje testirane osebe oceni kot iskrenost) (5).

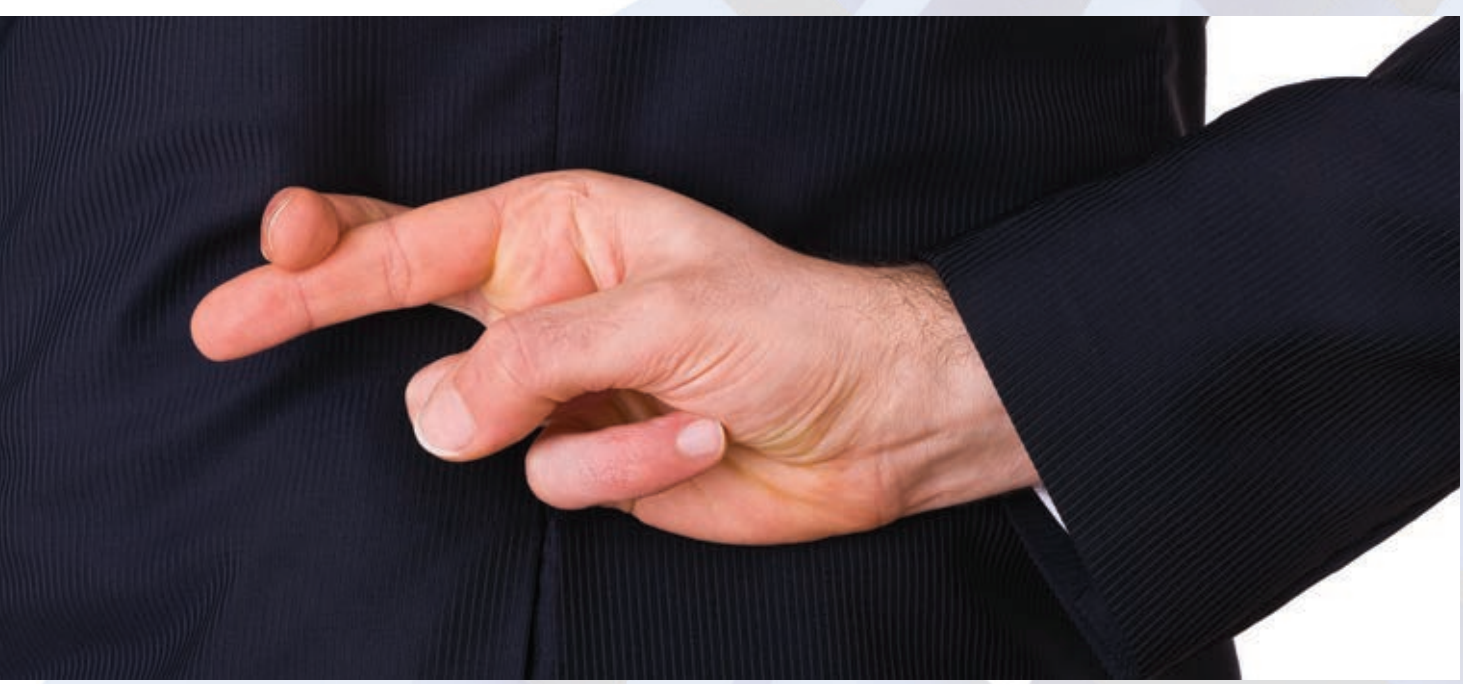
Z merskimi značilnostmi poligrafskih testov so tesno povezana pravila odločanja. Pravilo odločanja narekuje, pri katerih (točkovnih) vrednostih oziroma najmanjših/največjih vrednostih točk pri posameznih primerjavah (odzivov na relevantno in primerjalno vprašanje), gre za zavajanje oziroma iskrene odgovore (1).

Nekatere poligrafske tehnike vključujejo t. i. globalno oceno, vse razpoložljive informacije (o primeru), analizo poligramov pa dopolnijo tudi z opaženimi besednimi in nebesednimi vedenjskimi znaki (klinični pristop). Druge v oceni upoštevajo izključno numerično ovrednotene psihofiziološke odzive ter dosledno izključujejo vse »nepoligrafske« informacije (numerični pristop) (9)

Znanstvene podlage psihofiziološkega preiskovanja verodostojnosti izjav s poligrafom

Primerjava učinkovitosti in uporabnosti rezultatov izvedene poligrafske metode, analize rokopisa, prepoznave očividcev in daktiloskopske analize v eksperimentalnih pogojih je (ob upoštevanju nedoločenih ocen) pokazala delež pravilnih ocen pri poligrafski metodi 90 %, analizi rokopisa 85 %, prepoznavi očividca 35 % in daktiloskopiji 20 %. Primerjalna analiza različnih preiskovalnih metod na realnih primerih je pokazala pozitiven rezultat psihofiziološke preiskave verodostojnosti izjav s poligrafom v 89 %, tradicionalnih forenzičnih preiskav pa v 74 %. Učinkovitost posameznih forenzičnih preiskav v primerjavi s poligrafsko metodo je bila enaka v eksperimentalnih in realnih pogojih, ko je bila zanesljivost poligrafske metode 90 % in grafološke analize 85 %, oziroma 95% in 94 % brez nedoločenih ocen (9).

Leta 2003 je Nacionalni svet za raziskovanje (raziskovalno dejavnost) Združenih držav Amerike (NRC) (10) namenil posebno poročilo pregledu razpoložljivih znanstvenih podlag, prednostim in omejitvam različnih metod odkrivanja zavajanja ter dal poseben poudarek poligrafski metodi. Poročilo upošteva oba temeljna pristopa psihofiziološkega preiskovanja verodo-



Več-tematski testi so uporabni predvsem kot presejalni testi v kadrovanju, v postopkih spremljanja storilcev spolnih deliktov po prestani zaporni kazni in na področju nacionalne varnosti (19).

stojnosti izjav s poligrafom in sicer prepoznavanje in odkrivanje zavajanja. Koncept prepoznavanja izhaja iz predpostavke, da bo izpostavljenost znanemu dražljaju (podatki, slike ipd.), umeščenemu v set smiselno podobnih, vendar ne povezanih dražljajev, izzvala jasen psihofiziološki odziv. Tehnike, s katerimi odkrivamo zavajanje, ne temeljijo na prepoznavi znanih (skritih) posebnosti/podrobnosti, marveč primerjajo odziv na neposredno vprašanje o obravnavanem dogodku z odzivi na druga vprašanja, uvedena po predpisani proceduri (1).

Odkrivanje zavajanja je bolj uporabno, saj ne terja »prikritih« informacij, vendar je izvedba testov poznavanja manj zahtevna. Izvedba tehnik za odkrivanje zavajanja zahteva ustrezno strokovno usposobljenost poligrafskega preiskovalca ter nadzor kakovosti, sicer prihaja do napak, ki pa ne odražajo vrednosti same tehnike (1). Za tehnike/teste odkrivanja zavajanja NRC opisuje veljavnost v intervalu 81 do 91 %, z vrednostjo mediane pri 86 %. Pri tehnikah prepoznavanja je po oceni NCR interval veljavnosti med 85 in 96 %, vrednost mediane pa 88 % (10).

Raziskovalni podatki kažejo, da so poligrafske tehnike (gledano v celoti) nekoliko bolj učinkovite v preverjanju verodostojnosti (izločanju nevpletenih) kot v odkrivanju zavajanja (9). Odkrivanja zavajanja se poveča s številom ponovitev testa, četrta ponovitev zmanjša število nedoločenih ocen (11). Če izključimo nedoločene ocene je zanesljivost vsaj 92 %, kar je znano na polju forenzične psihofiziologije že več kot pol stoletja (12). Raziskovalni podatki tudi potrjujejo visoko veljavnost in zanesljivost poligrafske metode, kadar je izvedena s strani ustrezno usposobljenih poligrafskih preiskovalcev (13). Že v sedemdesetih letih 20. stoletja je bila preverjena zanesljivost ocen poligrafskih preiskovalcev s polletnimi in več kot enoletnimi izkušnjami; ugotovili so 79 % zanesljivost pri prvih in 92 % zanesljivost pri drugih (14, 15).

Raziskovalne pozornosti je bila deležna učinkovitost testov z eno ali več temami (16). Obravnava ene ali več tem je kriterij, po katerem je mogoče razdeliti oziroma opredeliti teste, s katerimi odkrivamo zavajanje. Večina avtorjev se zavzema za eno temo, ker tako sestavljen test ne dopušča dvomov, nesporazumov in delovanja spremenljivk, ki jih ni mogoče vnaprej opredeliti in/ali kontrolirati. Po drugi strani pa so testi, ki sledijo več temam, časovno ekonomični, zato so v ZDA dokaj razširjeni (9). Testov, ki izvorno sledi eni temi, ne smemo poljubno uporabljati kot več-tematske. Pozicije vprašanj določene vrste prav tako ni mogoče spreminjati, saj je na primer pri tehniki primerjave polj konstrukcija prilagojena tako teoretičnim izhodiščem kot tudi kasnejšemu vrednotenju psihofizioloških odzivov (9). Test je izziv za testirano osebo, ne glede na njeno dejansko vpletenost v obravnavano dejanje (17). Pri tem so za nevpleteno osebo ogrožujoča kontrolna vprašanja, za »storilca« pa relevantna. Ta se nedvoumno nanašajo na sporno dejanje in naj bi izzvala v osebi strah pred kaznijo oziroma odkritjem, zato je čustveni naboj pomembno večji kot pri kontrolnih vprašanjih.

Presejalni testi v kadrovanju

Več-tematski testi so uporabni predvsem kot presejalni testi v kadrovanju, v postopkih spremljanja storilcev spolnih deliktov po prestani zaporni kazni in na področju nacionalne varnosti (19). Namenjeni so vrednotenju posameznikovih ravnanj v okoliščinah, ki praviloma ne dopuščajo neodvisnega preverjanja. Pri varnostnem preverjanju so ta vedenja opredeljena kot varnostno tveganje (npr. hazardiranje, dolžniško-upniška razmerja ipd.) (20).

Več-tematski testi so večidel sestavljeni iz relevantnih, irelevantnih in kontrolnih vprašanj. Vrstni red vprašanj do neke mere vpliva na veljavnost celotnega testa. Predvsem je po-



membno, da v celotni strukturi ni več kot treh relevantnih vprašanj (vedenj, opredeljenih kot npr. varnostno tveganje), test pa ne sme presegati predpisane dolžine. Pri več-tematskih presejalnih testih je zanesljivost v obratni zvezi s številom obravnavanih tem (relevantnih vprašanj). Relevantna vprašanja morajo biti zelo jasna in usmerjena na preteklo ravnanje/vedenje (9).

Med testi s kontrolnim vprašanjem so presejalni več-tematski testi v kadrovanju najbolj uporabljeni. Njihovo vrednost je najlaže ponazoriti s primeroma 1 in 2.

PRIMER 1: Velika agencija za zasebno varovanje razpiše 100 prostih delovnih mest. V postopku kadrovske selekcije ne uporabljajo poligrafske metode. Prijavi se 200 kandidatov, od tega 25% takšnih, ki zaradi svojega preteklega vedenja ne ustrezajo standardom in zahtevam razpisa (zloraba opojnih substanc, prevare, nasilno vedenje, hazardiranje in podobno). Če med prijavljenimi izberemo po slučaju, bomo dobili 75% »ustreznih« in 25% »neprimernih« zaposlenih.

PRIMER 2: Druga agencija za zasebno varovanje v razpisu za 100 prostih delovnih mest objavi tudi, da je uporaba poligrafske metode del izbirnega postopka. Če nam slučaj omogoči 50% pravilnih odločitev, vzemimo, da nam prinese izvedba poligrafske metode 70% pravilnih odločitev, kar je pomembno manj od raziskovalnih podatkov - laboratorijskih in študij realnih primerov. Po izvedbi poligrafske metode, izbiramo samo med tistimi, ki so test opravili. Z upoštevanjem nizke arbitrarno določene natančnosti poligrafske metode, smo na 100 delovnih mest razporedili 87 »ustreznih« in 13 »neprimernih« oseb. Tudi izjemno nizka (70%) točnost poligrafske ocene je izboljšala možnosti »ustreznih« kandidatov za 12 na 100 in v enaki meri zmanjšala tveganje za izbor »neustreznih«.

Več-tematski testi na področju kadrovanja so podvrženi natančnemu spremljanju in kritični obravnavi (21, 22). Poligrafska metoda še vedno ostaja najboljši način za odkrivanje zavajanja v posebnih okoliščinah in pogojih nacionalne, javne in zasebne varnosti.

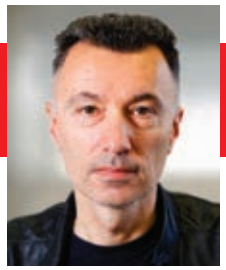
Zaključek

Dosledno upoštevanje veljavnih in znanstveno preverjenih principov lahko odgovori na večino izzivov pri aplikaciji poligrafskih tehnik v kadrovanju. Ustrezen nadzor kakovosti izvedbe psihofiziološke preiskave verodostojnosti izjav s poligrafom pa mora zagotoviti, da se uporabljajo ustrezni testi in pravila odločanja, da je pri vrednotenju upoštevano predpisano število kriterijev, ob nujni izvedbi prilagoditvenega testa, ki poveča točnost odločitev pri »realnih« testih (v zvezi z obravnavanim vedenjem). Odstopanje od teh pravil pomeni nestrokovno rabo poligrafskega instrumenta ter zlorabo koncepta psihofiziološkega preiskovanja verodostojnosti izjav s poligrafom.

Reference

1. Selič, P. (2009). Preverjene poligrafske tehnike - analiza. *Revija za kriminalistiko in kriminologijo*, letn. 60, št. 4, str. 332-343.
2. Abrams, S., Abrams, J. (1993). *Polygraph testing of the pedophile*. Portland: Ryan Gwininner Press, str. 110.
3. Selič, P. (2007). Osnovni psihološki testi - psihološki inštrumenti za merjenje in ocenjevanje osebnosti in sposobnosti. V: Kersnik, J. (ur.), *Diagnostične preiskave za vsakdanjo uporabo*. Ljubljana: Zavod za razvoj družinske medicine, 461-467.
4. Abrams, S. (1989). *The complete polygraph handbook*. Lexington, MA/Toronto: Lexington Books, str. 188-190.
5. Kircher, J.C., Raskin, D.C. (2002). Computer methods for the psychophysiological detection of deception. In: Kleiner, M. (ed.) *Handbook of polygraph testing*. San Diego/ London: Academic Press, 287-326.
6. Abrams, S. (1989). *The complete polygraph handbook*. Lexington, MA/Toronto: Lexington Books, str. 47-8.
7. Abrams, S. (1989). *The complete polygraph handbook*. Lexington, MA/Toronto: Lexington Books, str. 199-201.
8. Selič, P. (2004). Psihofiziološka preiskava verodostojnosti izjav s poligrafom. In: Maver, D. et.al. *Kriminalistika: uvod, taktika, tehnika*. Ljubljana: Uradni list, str. 353-376.
9. SELIČ, P. (2005). Psihofiziološka preiskava verodostojnosti izjav s poligrafom - uporabnost in učinkovitost v realnih in eksperimentalnih pogojih. V: ŠUGMAN, Katja (ur.), et al. *Poligraf v kazenskem postopku*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti, str. 37-51.
10. National Research Council (2003). *The polygraph and lie detection*. National Academic Press: Washington, DC.
11. Raskin, D.C., Hare, R.D. (1978). Psychopathy and Detection of Deception in Prison Polulation. *Psychophysiology*, 15: 126-36
12. Elson, D.G., David, R.G., Saltzman, J.A., Burke, C.J. (1952). *A Report of Research on Detection of Deception*. Office of Naval Research, University of Indiana, Bloominigton.
13. Abrams, S. (1977). *A Polygraph Handbook for Attorneys*. Lexington, Massachusetts: Lexingron Books, str. 99-115.
14. Horvath, F.S., Reid, J.E. (1971). The Reliability of Polygraph Examiner Diagnosis of Truth and Deception. *Journal of Criminal Law, Criminology and Police Scie***nce**, 62: 276-81
15. Abrams, S. (1989). *The complete polygraph handbook*. Lexington, MA/Toronto: Lexington Books, str. 200.
16. Matte, J.A. (1998). *Forensic psychophysiology using the polygraph*.Scientific Truth Verification – Lie Detection (2nd ed.). Williamsville, NY: J.A.M. Publications, str. 264.
17. Backster, C. (1994). *37TH Annual Polygraph Examiner Work Conference*. San Diego: The Backster School of Lie Detection.
18. Selič, P. (2002). Možnosti in omejitve psihofiziološke preiskave verodostojnosti izjav s poligrafom v realnih pogojih slovenske kriminalistične prakse. *Varstvoslovje*, 4, 3, s. 235-243.
19. Krapohl, D.J., Stern, B.A., Ryan, A.H. (2003). Exclusionary or nonexclusionary: A review of the evidence. *Polygraph*, 32 (4): 245-250
20. Selič, P., Juratovec, A. (2001). Možnosti varnostnega preverjanja s pomočjo poligrafske metode. V: BELIČ, Igor (ur.). *Javna predstavitev mnenj o predlogu Zakona o tajnih podatkih*. Ljubljana: Ministrstvo za notranje zadeve RS, str. 205-210.
21. Cumming, A. (2003). CRC Report for Congress: Polygraph Use by the Department of Energy: Issues For Conress. *Polygraph,* 32 (4): 211-9
22. Krapohl, D.J., Cushman, B. (2006). Comparison of Evidentiary and Investigative Decision Rules: A Replication. *Polygraph*, 35 (1), 55-64.■

Avtorji: dr. Bojan Dobovšek, dr. Jure Škrbec, Sašo Pristavec
Fakulteta za varnostne vede





PREVENTIVA KORUPCIJE V ZASEBNEM SEKTORJU

Kriminaliteta, ki po svetovnih (evropskih) in slovenskih podatkih, statističnih kazalcih organov pregona in preventive ter javnomnenjskih raziskavah strmo narašča od približno leta 2000 dalje, lahko zaradi številnih negativnih socialnih, ekonomskih in družbeno-moralnih posledic prizadene pomemben delež prebivalstva, v celoti ogrozi nacionalno varnost ter ogroža družbene in demokratične vrednote.

Poleg klasičnih premoženjskih (nasilnih ter drugih) oblik kriminalitete (tatvine, ropi, prepovedana trgovina z drogo) predstavljajo v sedanjem času grožnjo državi, družbi in navsezadnje posamezniku predvsem korupcija (Resolucija o preprečevanju in zatiranju kriminalitete RS, 2004). Slednja je na svetovni in slovenski ravni čedalje bolj usmerjena v korist nosilcem moči (predvsem v javnem sektorju), ki jo izvršujejo z zlorabo položaja (Van Duyne, 1997), v zasebnem sektorju pa celo počasi postaja normalni del vsakdanjega poslovnega procesa (Škrbec, 2012).

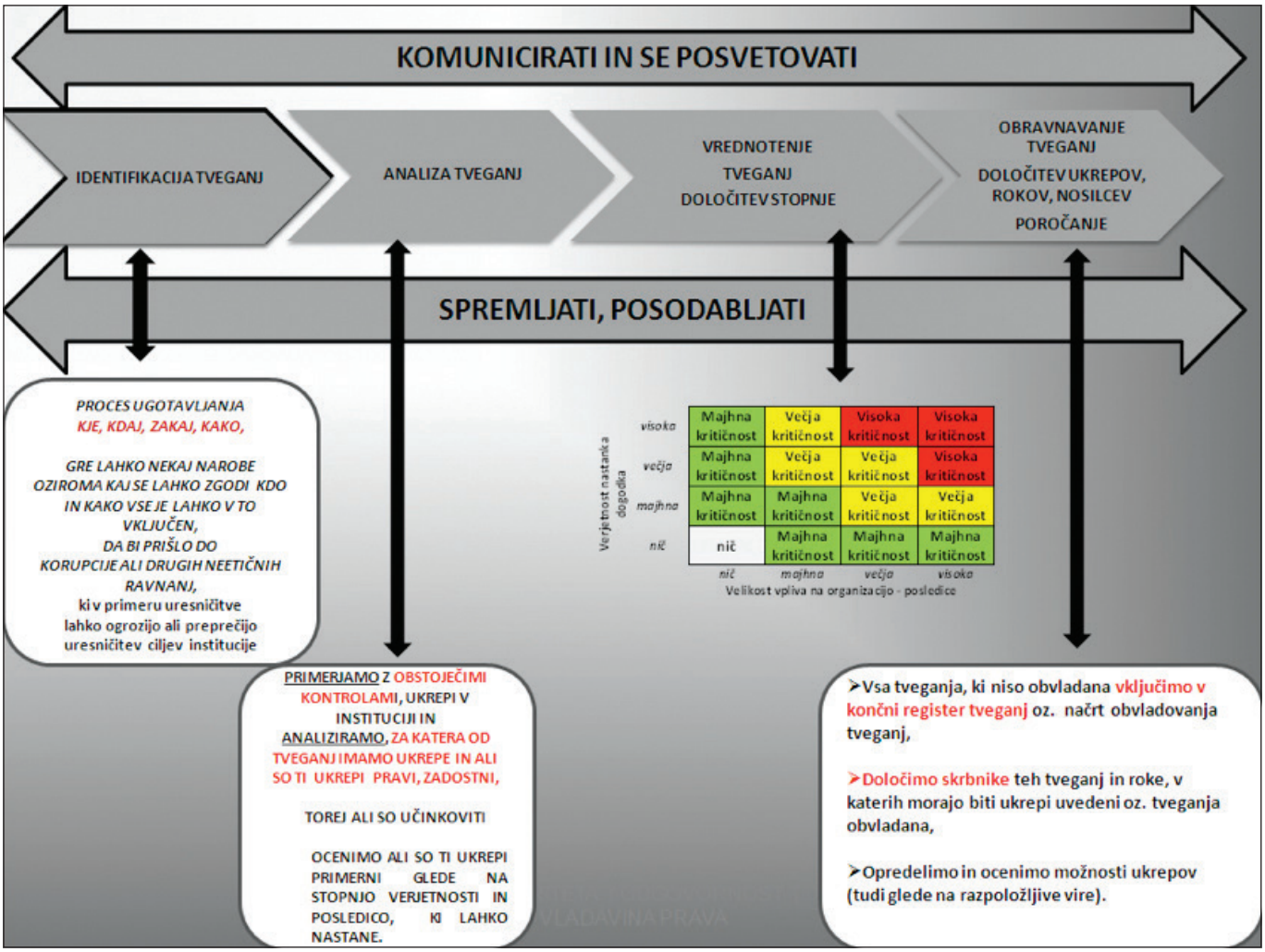
Zaradi preprečevanja tako korupcije, ki jo opredeljujemo kot vsako kršitev dolžnega ravnanja uradnih in odgovornih oseb v javnem ali zasebnem sektorju, kot tudi ravnanje oseb, ki so pobudniki kršitev ali oseb, ki se s kršitvijo lahko okoristijo, zaradi neposredno ali posredno obljubljene, ponujene ali dane oziroma zahtevane, sprejete ali pričakovane koristi zase ali za drugega, kot tudi drugih neetičnih, nemoralnih in drugih nezakonitih ravnanj pa sta tako javni sektor, kot tudi zasebni sektor, vzpostavila določene preventivne ukrepe.

Javni sektor

Javni sektor s tem v zvezi od leta 2004 (sprejetje Zakona o preprečevanju korupcije) dalje pozna t.i. načrt integritete, ki pomeni obligatorno orodje za vse institucije javnega sektorja za identifikacijo tveganj in načrt odprave le-teh. Gre za zakonski ukrep za krepitev integritete in transparentnosti ter preprečevanje in odpravljanje korupcije in nasprotja interesov vsake institucije javnega sektorja. Pri čemer je poudarek na sistematično urejeno zbirko načrtnih in premišljenih meril, podatkov, postopkov, opravil, ravnanj, mišljenj, odločanj in delovanj (glej sliko), s katerimi ocenimo verjetnost nastanka tveganj koruptivnih, protipravnih ali drugih neetičnih ravnanj znotraj institucij in posledic teh ravnanj ter določimo ukrepe in kontrole za njihovo pravočasno odkrivanje, obvladovanje, odpravljanje oziroma preprečevanje nastanka novih. S tem se ohranja oziroma povečuje integriteta zavezanca (Kaj je načrt integritete? Pridobljeno dne 2.7.2012 na http://www.kpk-rs.si/sl/pogosta-vprasanja/integriteta).



Slika št. 1: Potek načrta integritete



Vir: Komisija za preprečevanje korupcije, 2012

Kot izhaja iz slike in spletne strani Komisije za preprečevanje korupcije, upravljanja z načrtom integritete naprej zahteva identificirati vsa tveganja, ki grozijo instituciji. Pri tem lahko analiziramo zakonodajo, delovne procese, organizacijske pogoje, človeške faktorje in druge dejavnike, ki lahko predstavljajo vir ogrožanja. Ko imamo identificirana tveganja sledi analiza le-teh, pri čemer opravimo primerjavo med obstoječimi kontrolnimi (preventivnimi) ukrepi in ocenimo ali so le-ti uspešni in učinkoviti. Vsa tveganja v naslednji fazi ovrednotimo iz vidika verjetnosti nastanka nekega škodnega dogodka in velikost posledice na institucijo, s čimer pridobimo stopnjo tveganja – semafor – kjer rdeča barva pomeni izredno visoko tveganje, ki ni obvladano, zaradi česar se moramo pri slednjem ustaviti, o njem premisliti in ukrepati čim hitreje; rumena pomeni srednje visoko kritičnost, kar pomeni, da je potrebno spremljati ta tveganja, saj niso v celoti odpravljena in moramo skrbeti, da se njihova stopnja ogroženosti (kritičnosti) ne poveča; zelena barva pa pomeni, da je sicer tveganje identificirano, pri čemer pa je že obvladano in ne predstavlja več nevarnosti za institucijo. Zadnja faza v načrtu integritete je določitev ukrepov, ki bi odpravili tveganja, določitev rokov in odgovornih oseb, ki bodo odgovorni za spremljanje stanja. Skozi celotni postopek je potrebno komunicirati in se med zaposlenimi posvetovati o morebitnih novih rešitvah in morebitnih novih tveganjih ter kako jih odpraviti. Cilj načrta integritete je torej vsa tveganja spremeniti v »zeleno bravo«, kjer bo tako verjetnost nastanka škodnega dogodka nizka, velikost posledice morebitnega dogodka pa zelo majhna.

Zasebni sektor ima zgoraj omenjeni proces (slika) zelo podobno opredeljen, razlikuje se zgolj v uporabi različnih (drugih) standardov in njihovi neobvezni identifikaciji tveganj. V nadaljevanju si poglejmo posebnosti oziroma značilnosti zasebnega sektorja glede upravljanja s tveganji.

Zasebni sektor

Zasebni sektor kot rečeno pozna podobna orodja, znana pod imeni standardi upravljanja oziroma upravljanje s tveganji (angl. *Risk management*). V nasprotju z javnim sektorjem je pri podjetjih izrazito pomembnejša in potrebnejša konkurenčna prednost, ki jo lahko opredelimo kot niz faktorjev in sposobnosti, ki podjetju omogočajo trajno in boljše poslovanje glede na konkurenco (Dimovski, Penger in Peterlin, 2009). V bitki za tržni delež se prenekateri managerji in tudi zaposleni poslužujejo poslovnih praks, ki bi po definiciji lahko pomenile korupcijo (Škrbec in Pristavec, 2012). Vodilo podjetja torej ne sme biti le prodaja čim večjega števila produktov v čim krajšem času, temveč bi morale biti prvine dobrega podjetja avtentično vodstvo ter zaposleni, ki si prizadevajo za integriteto tako v podjetju kot v svojem zasebnem času ter s tem

prispevajo k preprečevanju možnosti za nastanek korupcije (Marič, Mešnjak in Pfeifer, 2011).

Na podlagi Raziskave o gospodarskem in poslovnem okolju, poslovni etiki in neuradnih plačilih na slovenskem iz leta 2009 (Valicon, 2010) je bilo ugotovljeno, da je kot najpogostejše koruptivno ravnanje prirejanje razpisnih pogojev določenemu ponudniku. Pogoste prakse takšnega delovanja so moralno in etično sporne ter lahko celo kaznive in lahko na dolgi rok negativno vplivajo na poslovanje organizacije, ki jih v primeru razkritja takšnega delovanja privedejo do več negativnih posledic, npr.: slabo ime v okolju kjer podjetje deluje; izguba poslovnih partnerjev; izguba naročnikov (kupcev) in kazenski pregon oseb, ki so osumljene povzročitve kaznivega dejanja. Valicon (2010) prav tako ugotavlja, da gospodarske družbe v zasebnem sektorju za upravljanje s tveganji zelo redko (6% malih podjetij, 1% srednje in velikih podjetij) izvajajo načrte integritete po ZPKor; da 62% malih podjetij in 39% srednje in velikih podjetij ne uporablja nobene metodologije za odpravljanje tveganj (CAF, ISO standard, PRSPO). Takšne in podobne metode uporablja 15% malih podjetij in 47% srednjih in velikih podjetij; medtem ko četrtina podjetij uporablja ukrepe kot so npr: kontrola poslovanja, notranja nenapovedana revizija posameznika, preverjanje poslovnih partnerjev, konkretno preverjanje posameznega podjetja in kontrola naročil.

Na podlagi Zakona o gospodarskih družbah (Uradni list RS, št. 65/2009 in sprem.; dalje ZGD-1) morajo imeti družbe, če je to pomembno za presojo premoženja in obveznosti družbe, njenega finančnega položaja ter poslovnega izida, v poslovnem poročilu prikazane tudi cilje in ukrepe upravljanja finančnih tveganj družbe, vključno z ukrepi za zavarovanje vseh najpomembnejših vrst načrtovanih transakcij, za katere se posli zavarovanja računovodsko posebej prikazujejo ter izpostavljenost družbe cenovnim, kreditnim, likvidnostnim tveganjem in tveganjem v zvezi z denarnim tokom. Zakon o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju (Uradni list RS, št. 126/07; dalje ZFPPIPP) pa v 2. odstavku 30. člena predpisuje, da mora poslovodstvo zagotoviti, da družba redno izvaja ukrepe upravljanja tveganj, tako likvidnostnih, kot tudi v povezavi s kapitalsko ustreznostjo ter drugimi ukrepi upravljanja tveganj, ki so po pravilih poslovno-finančne stroke potrebni in primerni glede na vrsto in obseg poslov, ki jih družba opravlja.

> Vodilo podjetja torej ne sme biti le prodaja čim večjega števila produktov v čim krajšem času, temveč bi morale biti prvine dobrega podjetja avtentično vodstvo ter zaposleni, ki si prizadevajo za integriteto tako v podjetju kot v svojem zasebnem času ter s tem prispevajo k preprečevanju možnosti za nastanek korupcije (Marič, Mešnjak in Pfeifer, 2011).

Zasebni sektor ima več kot 30 etičnih kodeksov tako profesionalnih kot neprofesionalnih združenj. Poznamo nekaj glavnih etičnih kodeksov, ki jih uporablja zasebni sektor, še posebej, ko gre za podjetje v kateri ima delež država in za podjetja, ki kotirajo na borzi. Vsak od teh kodeksov ima velik vpliv na zagotavljanje integritete v privatnem sektorju. Združujejo pa vrednote kot so poštenost, odgovornost, integriteta in lojalnost ter načela kot so enakost, preglednost ter poročanja, poštenega dela, revizije in sistema notranjih kontrol. (Pristavec, 2012).



Zaključna razprava – kako izboljšati preventivni boj v zasebnem sektorju

Upravljanje s tveganji je v zadnjem času zelo uporabljen proces v organizacijah, tako javnega kot zasebnega sektorja. V javnem sektorju še posebej izraziteje, saj je bil rok za oddajo načrtov integritete v mesecu juniju 2012 - do takrat so bile vse institucije javnega sektorja dolžne opraviti celotni proces načrta integritete oziroma upravljanja s tveganji. Obveznost uporabe tovrstnih orodij za upravljanje s tveganji pa hkrati predstavlja tudi prvo razliko med javnim in zasebnim sektorjem. **Zasebni sektor namreč v Sloveniji ne pozna zakonskih obveznosti upravljanja in identifikacije tveganj**. Druga izstopajoča razlika je v sami uporabnosti in širini ocene tveganj. Javni sektor se v primerjavi z zasebnim, ne osredotoča zgolj na finančno področje (torej finančna tveganja) pač pa v vse elemente, ki sestavljajo institucijo kot takšno – delovne procese, finančno poslovanje, človeške vire, organizacijske pogoje in druge. Podjetja ocenjujejo v večini zgolj finančne kazalce tveganj, glede ostalih tveganj v smislu zagotavljanja integritete, poštenosti in odgovornosti pa se lahko ravnajo po neobveznih etičnih kodeksih. Tretja pomembnejša razlika med javnim in zasebnim sektorjem pa je **v nadzoru nad spremljanjem procesa upravljanja s tveganji.** Pri javnem sektorju prevzema to vlogo nadzornika Komisija za preprečevanje korupcije. Zasebni sektor takšnega »skupnega in enotnega« organa nima.

Glede na navedeno bi radi izpostavili v razmislek vprašanja ali bi bilo smiselno znotraj zasebnih podjetij sprejeti podoben in prilagojen "načrt integritete" – kot interni akt v podjetju, ki bi moral biti obvezen, vsaj za srednja (50 – 250 zaposlenih) oziroma velika podjetja (nad 250 zaposlenih). Za večjo transparentnost porabljenih javnih sredstev, kot pogoj za kandidiranje na javnih razpisih in večjo konkurenčnost zasebnih podjetij bi bilo smiselno zahtevati, da ima organizacija vpeljan sistem upravljanja s tveganji ali pa sprejet interni akt – načrt integritete. Pozitivni odgovori na takšna vprašanja bi poleg višje stopnje integritetnega delovanja podjetij posledično pomenilo tudi večji ugled organizacij in zagotovilo, da gre za varno in zanesljivo poslovanje. Takšen sistem sta vpeljali že Japonska ter Malezija (UNODC, 2012) - državi sta zasebnim podjetjem ponudili sklenitev integritetnih paktov (angl. *Integrity pack*), s čimer sta dosegli, sicer na prostovoljni bazi, da so se zasebna podjetja zavezala spoštovati nacionalne in mednarodne proti-korupcijske akte, s čimer so postale tudi predmet samega nadzora implementacije s strani državnih organov. V kolikor se organizacija ni držala teh načel in v kolikor je bila dokazana kršitev s strani podjetja, je takšno podjetje pristalo na črni listi, zaradi česar ni smelo poslovati z državo v nadaljnjih 5-ih letih.

Podjetja ocenjujejo v večini zgolj finančne kazalce tveganj, glede ostalih tveganj v smislu zagotavljanja integritete, poštenosti in odgovornosti pa se lahko ravnajo po neobveznih etičnih kodeksih.

Viri

- Dimovski, V., Penger, S., Peterlin, J., (2009). *Avtentično vodenje v učeči se organizaciji*, Ljubljana: GV Založba.
- Komisija za preprečevanje korupcije (2012). *Kaj je načrt integritete?* Pridobljeno dne 12.2.2013 na http://www.kpk-rs.si/sl/pogosta-vprasanja/integriteta.
- Marič, M., Mešnjak, M. in Pfeifer, N. (2011). Integriteta kot eden od ključnih dejavnikov za uspešnost podjetij na trgu. 30. Mednarodna konferenca o razvoju organizacijskih znanosti – Organizacija prihodnosti, 23. – 25. marec 2011, Portorož.
- Pristavec, S. (2012). *Risk management standards – ensuring integrity in public and private organisations.* Criminal Justice and Security in Central and Eastern Europe. Contemporary Criminal Justice Practice and Research. September 19-21, 2012, Ljubljana: Univerza v Mariboru, Fakulteta za varnostne vede.
- Škrbec, J. (2012). *The impact of Corruption on the Rule of Law in the Republic of Slovenia – Facts versus public Fiction.* Criminal Justice and Security in Central and Eastern Europe. Contemporary Criminal Justice Practice and Research. September 19-21, 2012, Ljubljana: Univerza v Mariboru, Fakulteta za varnostne vede.
- Škrbec, J. in Pristavec, S. (2012). *Načrt integritete oziroma upravljanje s tveganji v javnem in zasebnem sektorju*. 13. dnevi varstvoslovja, 7. in 8. junij 2012, Portorož: Univerza v Mariboru, Fakulteta za varnostne vede.
- United Nations Office on Drugs and Crime (2012). Open-ended Intergovernmental Working Group on Prevention, 27. – 29. Avgust 2012, Dunaj. Pridobljeno 2.9.2012 s http://www.unodc.org/unodc/en/treaties/CAC/working-group4.html.
- Valicon (2010). *Raziskava o gospodarskem in poslovnem okolju, poslovni etiki in neuradnih plačilih na Slovenskem za leto 2009.* Pridobljeno dne 4.4.2012 na: https://www.kpk-rs.si/sl/korupcija-integriteta-in-etika/analize-raziskave-in-statistika/raziskave-in-statistika.
- Van Duyne, P. C. (1997). Organized crime, corruption and power. *Crime Law and Social Change, 26*(3), 201–238. ■



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

Slovenian Grand Security Award 2013

ICS

Institut za korporativne varnostne študije

Plaza hotel Ljubljana, 18. marec 2014

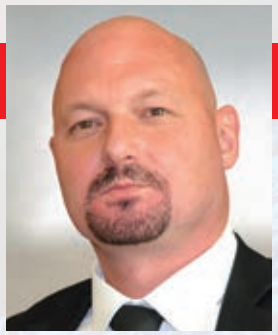
Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikov za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne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



VARNA RABA INTERNETA IN SPLETNO NADLEGOVANJE

Nasilje zaznamuje človeštvo že od vsega začetka. Najtipičnejša in najpogostejša, čeprav ne tudi najučinkovitejša reakcija na frustracijo, je agresija.

Agresija in nasilje

Pojav agresije in nasilja raziskujejo različne vede. Psihologija izhaja iz frustracije t.j. položaja, v katerem posameznik ne more zadovoljiti nekaterih svojih potreb in želja, ki iz njih izhajajo. Pri psihološki agresiji je bistveno sovražno stališče subjekta do objekta agresije. Spremlja ga občutek sovraštva in jeze, pogosto pa pride tudi do transferja agresije: namesto, da bi frustrirani posameznik napadel pravi vir frustracije, svojo agresijo prenese na osebo ali predmet, ki nima nobene zveze s prvotno frustracijo. Primer takega transferja bi bila situacija, ko se nezadovoljena ženska znaša nad sodelavci v službi. Agresija je pogosto kompenzacija pomanjkanja moči in gotovosti. Tako deček, ki pretepa šibkejše od sebe, pravzaprav kompenzira svojo nesposobnost, da bi obvladal močnejše. Ne glede na razloge za nasilno delovanje se z nasiljem ne soočamo le v družbi, ampak tudi kot posamezniki. In to že precej kmalu. Nasilje med mladostniki danes ni osamljen pojav, nasprotno, z njim se srečujejo tako rekoč v vseh vzgojno-izobraževalnih ustanovah, kjer ugotavljajo, da dobiva vedno nove oblike in razsežnosti. Tudi naše okolje pri tem ni izvzeto. Pred kratkim smo v medijih lahko zasledili primer, ko je učenec ene od ljubljanskih šol tako ustrahoval sošolce, da nekateri niso hoteli več v šolo. Ta primer pa ni osamljen, o čemer govorijo tudi rezultati mednarodne raziskave HBSC, ki Slovenijo po deležu 13- letnikov, ki se pretepajo, uvrščajo na deseto mesto med 36 državami. Ena izmed razlag nasilnega vedenja pravi, da nasilje med otroki izhaja iz nasilnih vedenjskih vzorcev odraslih, ki jih mladi prevzemajo, ko pa se pojavi, se v konflikt prej ali slej vključijo tudi odrasli in od njih je odvisno, ali se bo nasilnost razvila ali umirila. Če otrok izhaja iz okolja, kjer se konflikti rešujejo z nasiljem, potem je malo verjetno, da bi jih sam znal reševati drugače. Katerakoli razlaga že je pravilna, je dejstvo, da imamo človeška bitja nasilje v sebi. Kdaj in na kakšen način nasilje izbruhne je odvisno od vzgoje, situacije in samokontrole, zato bi se v družbi moralo poudariti širjenje znanja in zavedanja o varnostni kulturi ter vzgoji za nenasilje, ki je eden od mehanizmov, s katerim bi lahko povečali varnost.

Nasilje na internetu

Z razvojem informacijsko-komunikacijske tehnologije se je nasilje preselilo tudi v navidezni svet interneta. Poleg neomejene možnosti informiranja, izobraževanja in komuniciranja, ki jo s svojimi storitvami omogoča internet, v njegovem svetu obstajajo tudi manj prijetne in celo nevarne stvari. Poleg poneverb, zlorab, otroške pornografije in sovražnega govora, je ena izmed njih tudi spletno nadlegovanje (angl.: Cyber Bullying). Spletno nadlegovanje je nadlegovanje, ki ga posameznik ali skupina nad žrtvijo izvaja s pomočjo infomacijsko-komunikacijske tehnologije: na internetu preko elektronske pošte, forumov, klepetalnic in drugih družabnih omrežij, lahko pa tudi s pomočjo mobilnih telefonov in drugih komunikacijskih naprav. Razlika med spletnim in klasičnim nadlegovanjem na šolskem dvorišču je ta, da je spletno nadlegovanje lahko časovno in krajevno neomejeno. Žrtev se tako nima več kam umakniti oziroma se zateče v komunikacijsko osamo.

Pred dobrim letom je odmeval tragični primer kanadske osnovnošolke, ki je nekega dne skupaj s prijateljicami uporabila spletno kamero in prek nje neznancu za hec pokazala svoje prsi. Moški, ki jo je pripravil do tega, je te fotografije javno objavil. Sošolci so se zaradi fotografij obrnili proti njej, se iz nje norčevali, jo zaničevali ter jo izločili iz družbe. Dekle je zato zamenjala šolo, zapadla v droge in alkohol. Svojo življenjsko zgodbo je zaupala tudi na portalu YouTube, kjer je o dolgotrajnem spletnem nadlegovanju objavila tudi posnetek. Malo več kot mesec dni kasneje je svojo situacijo videla

Nasilje med mladostniki danes ni osamljen pojav, nasprotno, z njim se srečujejo tako rekoč v vseh vzgojno-izobraževalnih ustanovah, kjer ugotavljajo, da dobiva vedno nove oblike in razsežnosti.

*avtor je član Slovenskega združenja korporativne varnosti

tako brezizhodno, da je storila samomor. Skupina Anonymous je obljubila pomoč pri iskanju identitete spletnega nadlegovalca in obljubo tudi izpolnila. Oktobra 2012 so sporočili, kdo naj bi bil domnevni morilec - šlo naj bi za 30-letnika iz Britanske Kolumbije, ki je bil trenutno že v sodnem postopku zaradi spolnega nadlegovanja neke druge mladoletne osebe.

Za spletno nadlegovanje pa ni značilno, da se pojavlja le med mladostniki. Obstaja tudi med odraslimi, uporabljajo pa ga tudi učenci proti učiteljem. Pred kratkim se je na eni izmed slovenskih osnovnih šol zgodil primer, ko sta učenki snemali učitelja brez njegove vednosti (kaj šele privolitve) in posnetke skupaj z ustreznimi komentarji objavljali kot smešnice na internetu. Podoben primer se je zgodil učiteljici, kateri so učenci ukradli identiteto in v njenem imenu na Facebooku zbirali nove prijatelje. Znan je tudi primer učitelja matematike, v katerega imenu so nezadovoljni učenci na spletu objavljali neprimerne vsebine, zaradi česar je bil klican na zagovor k ravnatelju. Na srečo pri nas do sedaj še ni znanega tako tragičnega primera, kot je bil kanadski.

V nadaljevanju si bomo ogledali vrsto storitev s pomočjo katerih poteka komunikacija na spletu in (ne)varnosti uporabe le-teh.

Internet (INTERconnected NETwork)

Ko govorimo o internetu (splet, medmrežje), pod tem pojmom razumemo globalno omrežje, ki ga sestavljajo različna računalniška omrežja. Razvit je bil v akademskem okolju, da bi z njim omogočili hitrejši pretok informacij. Glede na prvotne uporabnike je internet temeljil na načelu poznavanja in medsebojnega zaupanja. Ker je bila njegova uporaba sprva omejena in nekomercialna (uporabljale so ga akademske in vladne organizacije), za njegovo uporabo pa je bilo potrebno kar precej tehničnega znanja, tudi ni bilo potrebe po posebnih pravilih obnašanja in zaščiti izmenjave informacij.

Devetdeseta leta prejšnjega stoletja pa so prinesla preobrat: razvili so se spletni brskalniki t.j. uporabnikom prijazni programski vmesniki za delo na spletu, hkrati pa je bila odstranjena omejitev glede komercialne rabe interneta. Tako je internet postal nov medij za komuniciranje. Zavedati pa se moramo, da pri uporabi interneta za seboj z vsakim korakom puščamo (elektronske) sledi. Na spletu obstajajo različni programi, ki pregledujejo spletne strani in komunikacijske poti, lovijo informacije s kom, kdaj, kje pa tudi kaj smo komunicirali, posebni programi imenovani *e-mail extractorji* omogočajo pridobivanje e-naslovov iz poljubnih virov in so le ena vrsta *spletnih žanjcev*, programov-pajkov, ki pregledujejo in zbirajo informacije s spletnih strani, forumov, družabnih omrežij ipd. Vedeti moramo, da je odločitev kaj in komu bomo zaupali v našem virtualnem življenju na spletu, popolnoma naša. Zavedati se moramo, da smo za svojo varnost (in zasebnost) na prvem mestu odgovorni sami!

Razlika med spletnim in klasičnim nadlegovanjem na šolskem dvorišču je ta, da je spletno nadlegovanje lahko časovno in krajevno neomejeno. Žrtev se tako nima več kam umakniti oziroma se zateče v komunikacijsko osamo.

Osebni podatki in zasebnost

Pri uporabi spletnih storitev se moramo zavedati, da je splet odprto okolje, kar pomeni, da je zagotavljanje zasebnosti s strani ponudnika omejeno (če sploh obstaja). Popolnoma naša odločitev je, katere podatke o sebi bomo razkrili in komu oziroma kje. Seveda našo zasebnost in zasebnost drugih ščitijo zakoni, a so le-ti v različnih državah sveta različni – splet je pa svetovno omrežje. Ko je podatek enkrat na spletu, ponavadi ostane tam za vedno. *Osebni podatek* je vsak podatek, ki enolično določa ali je z njim možno enolično določiti posameznika. Vsak posameznik odloča če in komu bo zaupal osebne podatke in kaj ta oseba lahko z njimi počne (razen v primeru, ko zakon določa drugače).

Ko so pred desetletji pravniki v okviru OZN poskušali najti definicijo pojma *zasebnost* so se po nekaj letih odločili, da je *zasebnost znano nedoločljiva fraza*; to pomeni, da si zasebnost vsak predstavlja



Zavedati pa se moramo, da pri uporabi interneta za seboj z vsakim korakom puščamo (elektronske) sledi.

po svoje. Za manekenko objava njenih slik na internetu ni vdor v zasebnost, saj je to del njenega posla, popolnoma drugače pa objavo svojih fotografij lahko vzame kdo drug... Bolje določljiva je *informacijska zasebnost*, ki zajema zbiranje in upravljanje z osebnimi podatki in jo poznamo tudi kot varovanje osebnih podatkov. Varovanje osebnih podatkov je sistemsko urejeno z Zakonom o varstvu osebnih podatkov (ZVOP-1).

Spletne komunikacijske tehnologije

Elektronska pošta (*e-mail*) je še vedno eno izmed najpomembnejših sredstev komuniciranja v virtualnem svetu. Za omogočanje storitve e-pošte so 'odgovorni' t.i. poštni strežniki (npr. *Yahoo, GMail, Hotmail*), ki posameznim uporabnikom nudijo uporabo e-poštnih nabiralnikov, do katerih lahko dostopajo s pomočjo spletnega brskljalnika ali pa z uporabo poštnih odjemalcev – računalniške aplikacije, postavljene na uporabnikovem računalniku (*Microsoft Office Outlook, Microsoft Outlook Express*). Pot e-pisma zna biti precej zamotana, saj ta ponavadi od pošiljatelja do prejemnika potuje preko več različnih strežnikov; tako se lahko primeri, da do naslovnika pride 'obogatena' z računalniškim virusom, črvom ali kakšno drugo obliko zlonamerne kode. Posebno primerne za nečiste namene so priponke, saj se v njih prav lahko skriva zlonamerna koda.

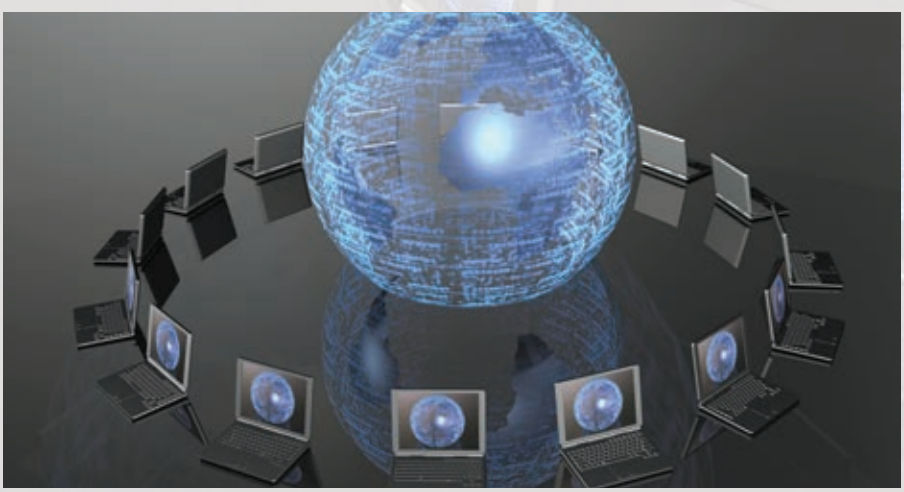
Pod pojmom ***socialna omrežja*** razumemo skupnost ljudi in tehnologijo, ki tej skupnosti omogoča medsebojno komunikacijo. Komunikacija je omogočena s pomočjo računalniškega omrežja (spleta), načini izvedbe (aplikacija) pa so različne (forumi, spletne klepetalnice ipd.). Širši pojem je *virtualna skupnost* (angl. *Virtual community*), *socialna skupnost*, *e-skupnost* ali *online* skupnost. Interakcija članov tovrstnih skupnosti poteka preko komunikacijskih medijev kot so pisma, telefon, elektronska pošta ipd. Namen druženja je lahko družabne, profesionalne ali izobraževalne narave.

Forum (tudi *web forum*) je spletno mesto za izmenjavo mnenj o določeni temi.

Spletne klepetalnice so storitev interneta, ki uporabnikom omogoča medsebojno komunikacijo na spletu. Vabljive so predvsem zato, ker omogočajo relativno anonimnost udeleženca in navidezno reševanje problema osamljenosti posameznikov, ki frustracijo poskušajo zmanjšati s komuniciranjem preko spleta. Značilnost vsebine pogovorov na spletnih klepetalnicah je, da so le kopije tistih iz realnega življenja: sogovornike predvsem zanima kdo smo, kaj počnemo, kako 'v resnici' izgledamo ipd. Seveda nam anonimnost omogoča, da svobodneje izražamo svoja mnenja, saj nas ne omejuje strah pred (prevelikimi) sankcijami; po drugi strani pa tudi omogoča, da se anonimnež predstavi 'boljšega' kot je v resnici – in tu se skrivajo pasti nepremišljene uporabe te storitve.

Takojšnje sporočanje (tudi *instant messaging*) je tehnologija, ki uporabniku omogoča takojšnjo dostavo sporočila uporabniku (npr. *Windows Messenger, ICQ*).

Internet Relay Chat *(IRC)*: nevarnost uporabe tovrstne tehnologije je v tem, da so ponavadi seje med odjemalcem in strežnikom nešifrirane (le malo IRC strežnikov uporablja *Secure Socket Layer* protokol), kar pomeni, da lahko prisluškovalni programi (imenovani *sniffer-ji*) pridobijo uporabnikovo geslo. Obstaja tudi t.i. *IRC takeover* – zlonamerni prevzem seje (kanala).



Priporočila za varno rabo spleta

Namesto zaključka podajmo nekaj nasvetov za varno rabo interneta:

1. Splet uporabljajmo 's pametjo' (sami lahko najbolj poskrbimo za svojo varnost).
2. Pri brskanju po spletu uporabljajmo antivirusni program in požarni zid.
3. V spletni klepetalnici vedno uporabljajmo vzdevek.
4. Uporabljajmo varna gesla, ki naj ostanejo naša skrivnost.
5. Spreminjajmo gesla dovolj pogosto.
6. Ne odpirajmo pošte in priponk od neznancev.
7. Ne presnemavajmo datotek iz nezanesljivih virov.
8. Ne izdajajmo svojih osebnih podatkov (niti podatkov svojih prijateljev, domačih itd.).
9. Ne objavljajmo osebnih fotografij, niti fotografij svojih prijateljev.
10. Ne verjemimo vsega kar piše na spletu.
11. Ne srečujmo se z neznanci iz spletne klepetalnice (tudi če se ti zdijo v virtualnem svetu naši prijatelji).
12. Ne zaupajmo slepo ‚prijateljem', ki jih spoznamo v klepetalnicah.
13 Spoštujmo spletni bonton (netiquette).
14 Nadlegovanje preko interneta je nedopustno! Če nas kdo nadleguje preko spleta ali če naletimo na neprimerno vsebino to povejmo drugim (prijateljem, staršem, uradnim organom).
11. In nenazadnje: ne pretiravajmo z uporabo spleta.

Viri

- De Becker, G. (1999). *Protecting the Gift: Keeping Children and Teenagers Safe (and Parents Sane)* . The Dial Press, New York.
- *Nasilje in varnost v šolah*. Inštitut za varnostno kulturo. Pridobljeno na http://www.institut-ivk.si/
- *Nasilni učenci ustrahujejo tudi učitelje*. Nedeljski dnevnik, 28.01.2014.
- Potokar, M. (2009). *(Ne)varna raba spletnih storitev*. Merkurjeve novice, Merkur d.d.
- *Spletno nadlegovanje vodilo najstnico v samomor*. Pridobljeno na http://www.varniinternet.si/novice/485-spletno-nadlegovanje-vodilo-najstnico-v-samomor
- Zvonarević, M. (1977). *Psihologija za tretji razred gimnazije*. Državna založba Slovenije, Ljubljana. ■

Avtor: Sanja Androić, magistrica managementa / Mariborski vodovod*



POVEZANOST MANAGEMENTA ZNANJA, UPRAVLJANJA S POSLOVNO DOKUMENTACIJO IN KORPORATIVNE VARNOSTI

Področja management znanja, upravljanje s poslovno dokumentacijo in korporativna varnost so medsebojno prepletena in so izredno pomembna za uspešnost podjetja.

Najprej se na kratko dotaknimo osnovnih definicij omenjenih področjih. Management znanja je pomemben del managementa vsakega podjetja in ga Scarborough in dr. (v Omerzel Gomezelj, 2009, str. 19) definirajo kot ''katerikoli proces ali postopek ustvarjanja, pridobivanja, širjenja in rabe znanja, kjerkoli se znanje pojavlja, z namenom stopnjevanja znanja zaposlenih in predvsem uspešnosti organizacije''. Upravljanje s poslovno dokumentacijo je nepogrešljiv del poslovanja vseh podjetij ne glede na dejavnost, ki jo opravljajo, saj je to področje povezano s vsemi poslovnimi procesi v podjetju. Upravljanje s poslovno dokumentacijo lahko poimenujemo kar pisarniško poslovanje, ki ga Žumer (2008, str. 26) opredeljuje kot izvajanje postopkov odpiranja, evidentiranja, klasificiranja in razvrščanja po zadevah, signiranja, dodeljevanja v reševanje, določanja zaporednih številk dokumentov ali zadev papirne ali elektronske pošte podjetja. Seveda se področje upravljanja s poslovno dokumentacijo ukvarja tudi z evidenco in odpremo izhodne pošte podjetja, hrambo papirne in elektronske poslovne dokumentacije in tudi z upravljanjem interne poslovne dokumentacije, ki nastaja pri poslovanju podjetja ne glede na dejavnost. Korporativna varnost je vključena v dnevno poslovanje managementa podjetij v obliki zagotavljanja normalnega pretoka poslovnih procesov, odpravljanja morebitnih težav z varnostjo, ustvarjanja varnih delovnih pogojev itd. (Trivan, 2013, str. 61–62). Avtor Čaleta (2011, str. 40–41) meni, da je ''korporativna varnost'' v najširšem pomenu ''dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Zato je ena od osnovnih funkcij za delovanje podjetja in se nujno izvaja v tesnem sodelovanju z vsemi drugimi ključnimi funkcijami v podjetju. Celostno področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj nujno vključuje področje varnosti, procesa neprekinjenega poslovanja in varnosti pri delu.''

Področja management znanja, upravljanje s poslovno dokumentacijo in korporativna varnost po našem mnenju povezuje znanje in načine upravljanja z njim, saj se znanje pojavlja pri upravljanju vseh raziskovanih področij in jih tudi medsebojno povezuje.

Področja management znanja, upravljanje s poslovno dokumentacijo in korporativna varnost po našem mnenju povezuje znanje in načine upravljanja z njim, saj se znanje pojavlja pri upravljanju vseh raziskovanih področij in jih tudi medsebojno povezuje. Za uspešno poslovanje vsakega podjetja je potrebno znanje v vseh oblikah, ki ga je potreb-

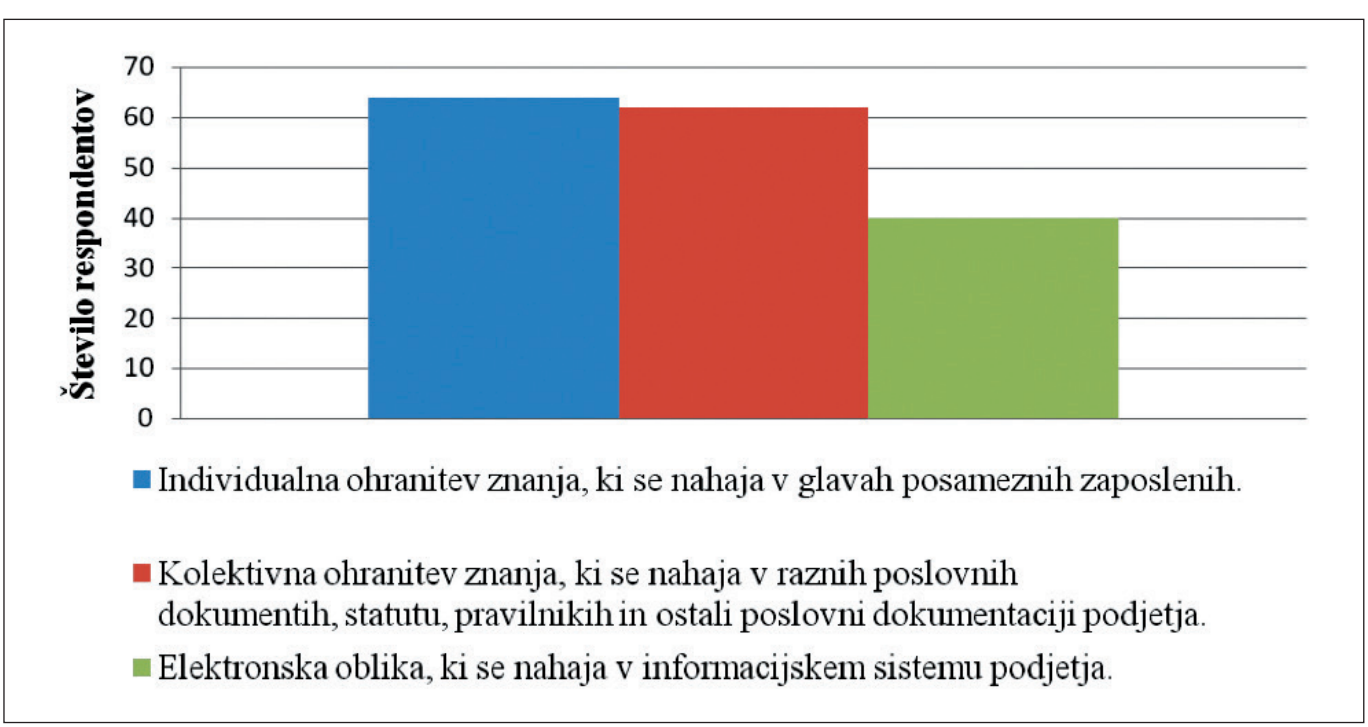
*avtorica je članica Slovenskega združenja korporativne varnosti

Področje korporativne varnosti za svoje delovanje med drugim potrebuje tudi poslovno dokumentacijo in znanje, ki pa ju tudi hkrati varuje, saj zraven premoženja in zaposlenih varuje tudi procese, podatke, informacije in dokumentacijo.

no tudi ustrezno upravljati. Potrebno ga je prepoznati, zapisati, nadgrajevati in seveda tudi ustrezno hraniti. Najpogosteje se pri poslovanju v podjetjih uporablja eksplicitno ali kodirno znanje, ki ga najdemo zapisanega predvsem v obliki navodil, pravilnikov, zbirk podatkov, itd. Vedno bolj pridobiva na pomembnosti tiho znanje posameznih zaposlenih oziroma implicitno znanje, ki temelji na izkušnjah in intuiciji posameznika in se težko izrazi ter zapiše. Urejeno področje upravljanja z znanjem se na nek način prenaša v upravljanje s poslovno dokumentacijo in korporativno varnost. Pri upravljanju s poslovno dokumentacijo se namreč dela s podatki, informacijami in dokumenti, ki so posredno povezani z znanjem podjetja in zaposlenih posameznikov. Področje korporativne varnosti za svoje delovanje med drugim potrebuje tudi poslovno dokumentacijo in znanje, ki pa ju tudi hkrati varuje, saj zraven premoženja in zaposlenih varuje tudi procese, podatke, informacije in dokumentacijo. Zaključimo lahko, da so si raziskovana področja medsebojno potrebna za nemoteno lastno delovanje in tudi za uspešno poslovanje podjetja.

Delna predstavitev rezultatov raziskave iz leta 2013

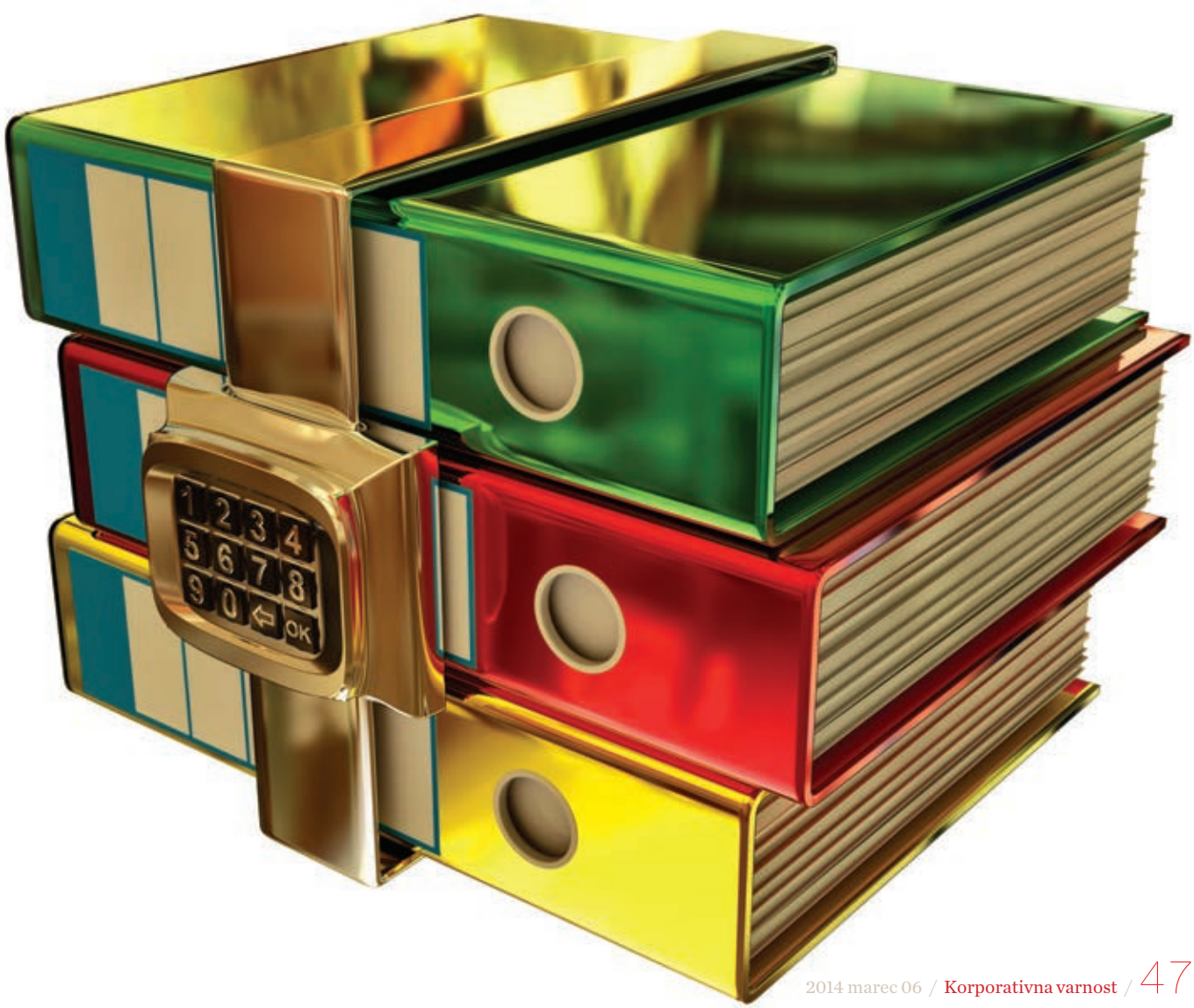
Raziskava izvedena v letu 2013 v slovenskih podjetjih je potrdila povezanost področij managementa znanja, upravljanje s poslovno dokumentacijo in korporativna varnost. Reprezentativni vzorec 166 respondentov je pokazal, da 2 % respondentov ocenjuje povezanost raziskovanih področij kot zelo močno, 22 % kot močno, 51 % ocenjuje povezanost področij kot delno, 16 % respondentov kot šibko, 10 % jih pa meni, da je povezanost zelo šibka (Androić, 2013, str. 61). Zanimive so ocene respondentov zaposlenih v slovenskih podjetjih glede pomembnosti raziskovanih področij. Prav vsi respondenti menijo, da lahko znanje zaposlenih prinese podjetju konkurenčno prednost. Ocene respondentov o najpogostejši obliki ohranjanja so lepo razvidne iz spodnje slike 1. 39 % respondentov ocenjuje kot najpogostejšo obliko ohranjanja znanja v slovenskih podjetjih individualno ohranitev znanja, ki se nahaja v glavah posameznih zaposlenih. Po mnenju 37 % respondentov sledi kolektivna ohranitev znanja, ki se nahaja v raznih poslovnih dokumentih, statutu, pravilnikih in ostali poslovni dokumentaciji podjetja. Kot najmanj pogosto obliko ohranjanja znanja v podjetju so respondenti izbrali elektronsko obliko, ki se nahaja v informacijskem sistemu podjetja, kar nas je glede na moderno tehnološko družbo v kateri živimo rahlo presenetilo. (Androić, 2013, str. 38-62)



Slika 1: Pogostost oblik ohranjanja znanja (Androić, 2013, str. 42)

Večini respondentov zaposlenih v slovenskih podjetjih se zdi področje upravljanja z poslovno dokumentacijo podjetja pomembno, saj je 55 % respondentov ocenilo to področje kot zelo pomembno, 40 % kot pomembno, 4 % pa jih je bilo neodločenih. Pri ocenitvi pomembnosti področja korporativne varnosti v podjetju je bila slika malce drugačna, čeprav je večina ocenila področje kot pomembno. 45 % respondentov je ocenilo področje kot zelo pomembno, 40 % kot pomembno, 1 % kot skoraj nepomembno, 15 % pa jih je bilo glede ocene neodločenih. Rezultat bi lahko verjetno pripisali manjšemu poznavanju področja in obsega korporativne varnosti, saj najverjetneje več zaposlenih in vodstev v slovenskih podjetjih vsaj delno pozna področje upravljanja s poslovno dokumentacijo in management znanja. Za korporativno varnost pa slišijo prvič ali pa njeno definicijo ali obseg razumejo drugače. Zanimivo je tudi, da so respondenti v omenjeni raziskavi ocenili, da večina slovenskih podjetij nima zaposlene osebe, katere delovna zadolžitev bi bila zgolj skrb za procese managementa znanja, saj se je samo 21 % opredelilo, da imajo v podjetju zaposleno takšno osebo. Kar 52 % respondentov je ocenilo, da imajo v podjetju zaposleno osebo, ki skrbi zgolj za upravljanje in hranjenje poslovne dokumentacije. Samo 19 % respondentov pa je ocenilo, da imajo v podjetju zaposleno osebo, ki skrbi zgolj za korporativno varnost. (Androić, 2013, str. 38-62)

V spodnji preglednici 1 vidimo odgovore respondentov na vprašanje ''Kaj po vašem mnenju obsega korporativna varnost?'' pri katerem je bilo možno izbrati več odgovorov. Reprezentativni vzorec 166 respondentov zaposlenih v slovenskih podjetjih je pokazal, da večina zaposlenih v slovenskih podjetjih žal resnično ne ve kaj obsega korporativna varnost, saj je definicija korporativne varnosti, ki obsega celotno dejavnost korporativne varnosti, zasedla zgolj 18 % delež vseh odgovorov med podanimi možnostmi. 25 % delež vseh odgovor zaseda odgovor, da je korporativna varnost dejavnost, ki obvladuje varovanje procesov, podatkov, informacij in dokumentacije. 18 % delež zaseda odgovor, da je korporativna varnost dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v podjetju. Ta odgovor je tudi definicija korporativne varnosti, ki seveda obsega celotno dejavnost korporativne varnosti. Sledijo odgovori, ki pokrivajo samo posamezna področja ali posamezne dejavnosti korporativne varnosti. 13 % delež vseh odgovorov zaseda odgovor, da je korporativna varnost dejavnost, ki obvladuje varnost podjetij. 12 % delež zaseda odgovor, da je to dejavnost, ki obvladuje varnostna tveganja. 10 % delež zaseda odgovor, da je korporativna varnost dejavnost, ki obvladuje varnost korporacij. Po 6 % delež vseh odgovorov zasedata odgovor, da je to dejavnost, ki obvladuje neprekinjeno poslovanje in odgovor, da je to dejavnost, ki obvladuje varovanje zaposlenih. 5 % delež zaseda odgovor, da je korporativna varnost dejavnost, ki obvladuje tehnično in fizično varovanje premoženja. Najmanj oziroma 4 % delež vseh odgovorov pa zaseda odgovor, da je korporativna varnost dejavnost, ki obvladuje varnost pri delu. (Androić, 2013, str. 52)



Preglednica 1: Ocena obsega korporativne varnosti

Odgovori na vprašanje ''Kaj po vašem mnenju obsega korporativna varnost?'' (Možna je bila izbira več odgovorov)	**Delež vseh odgovorov med podanimi možnostmi v %**
Je dejavnost, ki obvladuje varovanje procesov, podatkov, informacij in dokumentacije.	25%
Je dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v podjetju.	18%
Je dejavnost, ki obvladuje varnost podjetij.	13%
Je dejavnost, ki obvladuje varnostna tveganja.	12%
Je dejavnost, ki obvladuje varnost korporacij.	10%
Je dejavnost, ki obvladuje neprekinjeno poslovanje.	6%
Je dejavnost, ki obvladuje varovanje zaposlenih.	6%
Je dejavnost, ki obvladuje tehnično in fizično varovanje premoženja.	5%
Je dejavnost, ki obvladuje varnost pri delu.	4%

Analiza raziskave nam kaže premajhno poznavanje obsega korporativne varnosti v slovenskih podjetjih. Lahko bi rekli, da v slovenskih podjetjih tudi premalo poznajo pomen korporativne varnosti, saj če zaposleni v tako majhni meri poznajo obseg korporativne varnosti se njegovega pomena ne morejo zavedati v dovolj veliki meri. Očitno bo potrebno na nek način seznaniti in podučiti vodstva in zaposlene v slovenskih podjetjih v prvi fazi kaj je korporativna varnost, kaj obsega in kaj lahko pripomore ustrezno upravljanje tega področja k uspešnosti in ustreznemu poslovanju podjetja. Seveda so izvzeta redka slovenska podjetja, ki se izredno zavedajo pomembnosti področja korporativne varnosti in imajo nekatera celo zaposlene strokovnjake korporativne varnosti ali imajo celo oddelek v podjetju, ki skrbi za to področje.

Menimo, da je urejeno področje korporativne varnosti izrednega in ključnega pomena za uspešno in dolgoročno poslovanje posameznega podjetja ne glede na urejenost posameznih področij in procesov, saj če le ti niso ustrezno varovani enostavno ne morejo biti ustrezno urejeni ter varni pred raznovrstnimi zlorabami in izgubami.

Zaključek

Za zaključek bi povzeli ocene izvedene raziskave, da bi morala podjetja za optimalnejšo skrb za področje managementa znanja, upravljanja s poslovno dokumentacijo in korporativno varnost ter njihovo močnejšo medsebojno povezanost narediti predvsem naslednje:

- Izboljšati skrb za področje managementa znanja, upravljanje s poslovno dokumentacijo in korporativno varnost ter organizirati ta področja kot samostojna poslovna področja podjetja, kjer bi se skrb za le ta prepustila posameznim strokovnjakom.
- Motivirati svoje zaposlene in vodstva, da bi zapisovali svoje tiho znanje in poskrbeti tudi za ustrezen zapis, organiziranje, prenos in varovanje le tega.
- Pogosteje bi bilo potrebno obveščati zaposlene o novostih in zakonodaji z omenjenih področij ter postopkih za upravljanje s temi področji.
- Poskrbeti bi bilo potrebno za močnejšo medsebojno povezanost področij management znanja, upravljanje s poslovno dokumentacijo in korporativna varnost. (Androić, 2013, str. 71-72)

Menimo, da je urejeno področje korporativne varnosti izrednega in ključnega pomena za uspešno in dolgoročno poslovanje posameznega podjetja ne glede na urejenost posameznih področij in procesov, saj če le ti niso ustrezno varovani enostavno ne morejo biti ustrezno urejeni ter varni pred raznovrstnimi zlorabami in izgubami. Največje tveganje pa je vsekakor človek ne tehnologija, a več o tem mogoče v katerem od prihodnjih člankov.

Viri

- Androić. S. (2013). *Upravljanje s poslovno dokumentacijo in korporativna varnost* (magistrsko delo). Mednarodna fakulteta za družbene in poslovne študije, Celje.
- Čaleta, D. (2011). Varnost mojega podjetja. *Podjetnik, 11*(10), 40–41.
- Omerzel Gomezelj, D. (2009). *Management znanja v majhnih in srednjih podjetjih.* Koper: Univerza na Primorskem, Fakulteta za management Koper.
- Trivan, D. (2013). Corporate security in the Southeast European countries under conditions of global economic crisis. V D.Čaleta in M. Vršec (ed.), *Management of Corporate Security – New Approaches and Future Challenges* (str. 51–62). Ljubljana: Institute for Corporative Security Studies.
- Žumer, V. (2008). *Poslovanje z zapisi. Upravljanje in hramba dokumentarnega gradiva, klasifikacijski načrti za razvrščanje gradiva z roki hrambe in elektronska hramba gradiva v digitalni obliki.* Ljubljana: Planet GV. ■

Avtorja: Mag. Marko Potokar / Inštitut za varnostno kulturo*
Andrej Kovačič / Inštitut za korporativne varnostne študije*





VARNOSTNA TVEGANJA ZAPOSLENIH NA DELOVNEM MESTU Z VIDIKA OSEBNE VARNOSTI

Zagotavljanje varnosti zaposlenih in nasilje na delovnem mestu je že nekaj časa resen in vedno večji problem. Obvladovanje tovrstnih tveganj s celovitim pristopom ter z usposabljanjem zaposlenih, bi morala biti v okviru zagotavljanja varnosti in zdravja pri delu, prioriteta organizacije.

Uvod

Pri zavedanju in dojemanju varnostnih tveganj na delovnem mestu imata znanje in motivacija pomembno vlogo. Usposobljenost, znanje in motivacija zaposlenih na področju osebne varnosti na delovnem mestu so povezani z varnostno kulturo v organizaciji. Koncept ohranjanja dobre varnostne klime je zelo pomemben za samo varnostno učinkovitost v organizacijah.

Varnostna tveganja nad zaposlenimi prihajajo iz mnogih virov. To so lahko nezadovoljne in nasilne stranke ali roparji. Posebej so izpostavljena delovna mesta kjer delo poteka neposredno z ljudmi, saj so ta z vidika fizične varnosti bolj izpostavljena. Vrsta varnostnih tveganj na delovnem mestu in zavedanje le-teh, pomembno vpliva na počutje in zdravstveno stanje zaposlenih. Že določena vrsta groženj lahko vpliva na poklicno identiteto zaposlenih. Napadi in nasilna dejanja nad zaposlenimi imajo lahko tudi za organizacijo dolgoročne posledice. Dejavniki tveganja so lahko zelo različni in sicer od pomanjkanja varnostne politike glavnega vodstva organizacije, do splošnega gospodarskega stanja v družbi. V prispevku bo obravnavana problematika varnostnih tveganj na delovnem mestu z vidika zagotavljanja osebne varnosti in vloga usposabljanja zaposlenih za njeno izboljšanje.

Zakon o varnosti in zdravju pri delu

Krovni predpis na področju varnosti in zdravja pri delu je Zakon o varnosti in zdravju pri delu (v nadaljevanju ZVZD-1). Prenovljen je bil 3. junija 2011, veljati pa je pričel po šestmesečnem prehodnem obdobju, 3. decembra 2011. Delodajalcem je prenovljeni zakon naložil veliko novih nalog in odgovornosti, katere večino so jih bili ti dolžni opraviti takoj. Med njimi sta tudi dve, ki pomenita, glede na dosedanjo zakonsko ureditev novosti. Prva določa, da mora delodajalec zagotoviti potrebno ureditev in opremo na delovnih mestih, kjer obstaja nevarnost za nasilje tretjih oseb (23. člen ZVZD-1), druga pa pravi, da je potrebno sprejeti ukrepe za preprečevanje, odpravljanje in obvladovanje primerov nasilja, trpinčenja, nadlegovanja in drugih oblik psihosocialnega tveganja na delovnih mestih, ki lahko ogrozijo zdravje delavcev (24. Člen ZVZD-1).

ZVZD-1 kot krovni predpis na področju varnosti in zdravja pri delu določa pravice in dolžnosti delodajalcev in delavcev v zvezi z varnim in zdravim delom ter ukrepi za zagotavljanje varnosti in zdravja pri delu. Določbe tega zakona se uporabljajo v vseh dejavnostih za vse osebe, ki so navzoče v delovnem procesu. Z vidika zagotavljanja osebne varnosti zaposlenih sta, kot omenjeno pomembni dve novosti. Prva je ta, da mora delodajalec načrtovati postopke za zmanjšanje nevarnosti za nasilje tretjih oseb. V prvem odstavku 23. člena ZVZD-1 je namreč opredeljeno, da mora delo-

Glavno vodstvo je odgovorno za varnost svojih zaposlenih ter mora slediti politiki ničelne tolerance do nevarnih vedenj na delovnem mestu, ki ogrožajo osebno varnost zaposlenih.

*avtorja sta člana Slovenskega združenja korporativne varnosti

dajalec na delovnih mestih, kjer obstaja večja nevarnost za nasilje tretjih oseb, poskrbeti za tako ureditev delovnega mesta in opremo, ki tveganje za nasilje zmanjšata in ki omogočata dostop pomoči na ogroženo delovno mesto. Nadalje je v tem členu določeno tudi, da mora delodajalec načrtovati postopke za primere nasilja iz prvega odstavka tega člena in seznaniti z njimi delavce, ki na takih delovnih mestih delajo.

Druga novost zadeva nasilje, trpinčenje, nadlegovanje in psihosocialno tveganje. Tako je v 24. členu ZVZD-1 določeno, da mora delodajalec sprejeti ukrepe za preprečevanje, odpravljanje in obvladovanje primerov nasilja, trpinčenja, nadlegovanja in drugih oblik psihosocialnega tveganja na delovnih mestih, ki lahko ogrozijo zdravje delavcev.

Poleg določil o zagotavljanju osebne varnosti zaposlenih s strani delodajalca, je novost tudi promocija zdravja na delovnem mestu. Tako je v 6. členu ZVZD-1 določeno, da mora delodajalec načrtovati in izvajati promocijo zdravja na delovnem mestu. Delodajalec mora za promocijo zdravja zagotoviti tudi potrebna sredstva in način spremljanja njenega izvajanja.

Lahko rečemo, da prenovljeni ZVZD-1 daje delodajalcem dovolj pravne podlage za ureditev področja varovanja tudi z vidika osebne varnosti zaposlenih.

Naloga vodstva pri zagotavljanju osebne varnosti zaposlenih

Varnostna politika je v organizaciji krovni dokument za načrtovanje in zagotavljanje osebne varnosti zaposlenih. Glavno vodstvo je odgovorno za varnost svojih zaposlenih ter mora slediti politiki ničelne tolerance do nevarnih vedenj na delovnem mestu, ki ogrožajo osebno varnost zaposlenih.Obe strani se morata zavezati, da se bo varnost na delovnem mestu krepila z ničelno toleranco. Pri tem ima pomembno vlogo varnostni priročnik za zaposlene, kjer so določeni vsi postopki, ki jih je potrebno izvesti ob zaznani nevarnosti. Pri tem so konkretno določene tudi naloge in odgovornosti tako organizacije, kot zaposlenih. Varnostna tveganja morajo temeljiti na analizi konkretnih nevarnosti delovnega mesta, z vidika ogrožanja od zunaj.

Potrebno je sprejeti celovit načrt za ohranjanje varnosti vseh zaposlenih na delovnem mestu. To vključuje vzpostavitev sodelovanja vseh internih strokovnjakov, policije in drugih, ki lahko pomagajo identificirati načine za preprečevanje in zmanjšanje varnostnih tveganj na delovnem mestu. Vodstvo mora s predstavniki zaposlenih aktivno sodelovati, da skupaj razvijejo ustrezne strategije za zagotavljanje varnega delovnega okolja. Pri zagotavljanju osebne varnosti zaposlenih je naloga vodstva, da redno spremlja varnostne dogodke in da izvaja oceno ukrepov ter prilagaja način varovanja in izboljšanja fizične varnosti. Pri tem je potrebno redno ocenjevati stanje in vsako grožnjo ter vsake incidente resno obravnavati. Menedžerji morajo prepoznati situacije visokega varnostnega tveganja, da se zaposlenim lahko zagotovi varno delovno okolje. Vodstveni delavci bi morali biti usposobljeni za zmanjševanje nevarnosti in zagotavljanje ustrezne varnosti zaposlenih. Po usposabljanju bi morali menedžerji biti sposobni prepoznavati potencialno nevarne situacije in vpeljati potrebne spremembe in postopke za zmanjšanje ali odpravo nevarnosti. Pri tem je potrebno opraviti podrobno analizo dogodkov in sprejeti ukrepe za preprečitev ponovitve nevarnosti za zaposlene. Vodstvo mora z zaposlenimi deliti poročila o varnostnem stanju in o sprejetih ukrepih za preprečevanje nasilja in ogrožanja njihove osebne varnosti. Poročila o incidentih, evidence analiz nevarnosti in korektivnih ukrepov ter spremembe v programih za zaščito zaposlenih je potrebno obravnavati na rednih sestankih varnostnega kolegija, katerega član je predstavnik zaposlenih. Pri obravnavi varnostnih dogodkov in informacij v zvezi z njimi mora biti zagotovljena zaupnost občutljivih poslovnih in osebnih podatkov zaposlenih.



Osebna varnost in varnostna tveganja zaposlenih

Ena ključnih potreb je, da se zaposlene ustrezno usposobi za zaznavanje in prepoznavanje zgodnjih opozorilnih znakov pred izbruhom nasilja. Prepoznava opozorilnih znakov je izredno pomembna in ob pravilnem ravnanju lahko odločilna za preprečitev nevarnosti.

Osebna varnost med drugim zagotavlja tudi ukrepe za zaščito zaposlenih pred nasilnimi dejanji. Pri tem gre prav tako za pravilno postavitev in oblikovanje varnega delovnega mesta in sprejetje postopkov za ravnanje v nevarnih dogodkih. Postopki zajemajo ključna področja ukrepanja v različnih situacijah na delovnem mestu in sicer:

- oceno tveganja;
- opredelitev nevarnosti;
- preprečevanje in nadzor;
- usposabljanje zaposlenih z igro vlog;
- upravljanje in ublažitev posledic;
- skrb in podpora prizadetih zaposlenih;
- spremljanje vrednotenja.

Cilj je, da bi odpravili ali zmanjšali izpostavljenost zaposlenih pogojem, ki vodijo k poškodbam in drugim nevarnim situacijam.

Zaposleni morajo imeti zaupanje v vodstvo, da je skrb za njihovo varnost zelo pomembna. V primeru pomanjkanja in nerazumevanja zaposlenih, bo varnostna kultura in klima na nizki stopnji. V takih razmerah tudi spodbujanje zaposlenih, da nemudoma poročajo o vseh incidentih in predlagajo načine za zmanjševanje ali odpravo tveganj, ne bo prineslo pozitivnih rezultatov.

Usposabljanje zaposlenih za samozaščitna ravnanja

Zaposleni, ki delo opravljajo neposredno s strankami in na izpostavljenih delovnih mestih, potrebujejo ciljno usposabljanje. Program vključuje psihološke komponente ravnanja nasilnih in nevarnih strank, vrste motenj in načine za fizično obvladovanje in preprečevanje nasilja. Program je prilagojen varnostnim tveganjem na različnih delovnih mestih in ponuja pridobivanje znanja zaposlenim, da ti takoj prepoznajo potencialno nevarne stranke in situacije. Pomembno je sodelovanje zaposlenih, da poročajo o vseh dogodkih v skladu z ničelno toleranco. Vsaj enkrat letno mora odgovoren za program pregledati njegovo vsebino, metode in pogostost usposabljanja. Vrednotenje programa lahko vključuje intervjuje z zaposlenimi in analize vseh zaznanih ter obravnavanih incidentov.

Usposabljanje mora zajemati teme, kot so:

- politika preprečevanja varnostnih tveganj na delovnem mestu;
- prepoznavanje dejavnikov tveganja, ki povzročijo ali pripomorejo k incidentom;
- pravočasno prepoznavanje vedenja ali opozorilnih znakov, ki lahko privedejo do napadov;
- načini za preprečitev oziroma pomiritev konfliktne situacije;
- akcijski načrt za odziv v nasilnih razmerah, vključno z razpoložljivostjo pomoči, odziv na alarmne sisteme in komunikacijski postopki;
- delovanje varnostnih naprav, kot so alarmni in video nadzorni sistemi;
- usmeritve in postopki poročanja in vodenja evidenc;
- usmeritve in postopki za pridobitev zdravstvene oskrbe oziroma prve pomoči.

Ena ključnih potreb je, da se zaposlene ustrezno usposobi za zaznavanje in prepoznavanje zgodnjih opozorilnih znakov pred izbruhom nasilja. Prepoznava opozorilnih znakov je izredno pomembna in ob pravilnem ravnanju lahko odločilna za preprečitev nevarnosti.

Zaveza vodstva o zagotavljanju organizacijske skrbi za varnost zaposlenih daje motivacijo in vire za učinkovito spopadanje z ogrožanjem varnosti na delovnem mestu. Zaposleni, kot dejanski partnerji vodstva organizacije pri izboljševanju varnostnih razmer, se bodo na delovnem mestu počutili bolj varne.

Zaključek

Zagotavljanje varnega in zdravega delovnega okolja bi moral biti eden izmed glavnih ciljev vsake organizacije. Zavedati se moramo, da samo določbe v zakonih in sprejeti notranji organizacijski pravilniki, še niso dovolj. Spremeniti je potrebno organizacijsko kulturo in sistem vrednot zaposlenih, kar lahko dosežemo le z iskreno podporo in zgledi najvišjega vodstva. Ključno za zvišanje nivoja varnosti je ustrezno usposabljanje zaposlenih za samozaščitno ravnanje. Posebno pomembna pri tem je dobra psihofizična pripravljenost, kar lahko organizacija doseže s programi za promocijo zdravja in telesne aktivnosti zaposlenih. Poleg ustrezno prilagojene vadbe, je izredno pomembna tudi pravilna psihološka priprava posameznikov na reagiranje v konfliktnih situacijah. Bistveno je, da se tako zaposleni kot delodajalci zavedajo, da je le z ustrezno usposobljenostjo mogoče zagotavljati ustrezno obvladovanje varnostnih tveganj in s tem varno delovno okolje.

Viri

- Potokar, M. in Kovačič, A. (2013). *Fit zaposleni – dodana vrednost korporativni varnosti v organizacijah*. Revija korporativna varnost, ICS.
- Zakon o varnosti in zdravju pri delu (ZVZD-1). (2011). Uradni list RS, št. 43/2011. ■



Avtor: Jelenko Vidic, Slovensko združenje korporativne varnosti



RAVNANJE S TVEGANJI – IV. DEL

Po mnenju strokovnjakov je ocena ranljivosti eden najbolj kritičnih vidikov vrednotenja ogroženosti.

V nadaljevanju obravnave ravnanja s tveganji si poglejmo še nekaj zapisanih dejstev in tolmačenj o ranljivosti (vulnerabilnost; vulnelrability)[1], ki je pomembna (in najbolj kritična) sestavina analize tveganj. Z zgoščenim prikazom želimo le na kratko predstaviti kompleksnost koncepta ranljivosti.

Na splošno velja da, če hočemo nadzorovati, kontrolirati in preprečiti neželene škodne dogodke (nesreče, škodljiva ravnanja, dejanja, ipd.), ali zmanjšati njihov vpliv, moramo določiti ranljivost. Preprosto jo opredelimo kot slabost, ki je lahko izkoriščena, da bi se uresničila neka grožnja. Razumevanje in zmanjševanje ranljivosti je nedvomno naloga interdisciplinarnih skupin, saj je potrebno razumevanje tako naravnih procesov kot tudi človeka (človeškega sistema). Pojem ranljivost se večinoma uporablja za analize različnih dejavnikov in procesov, ki imajo vpliv na družbo.

Ker ne obstaja splošna definicija ranljivosti, se navadno uporablja pojem v takšnem smislu, ki nam najbolje služi. Ljudje razumejo pojme vezane z ogroženostjo glede na svoje izkušnje, zato je tudi ranljivost močno odvisna od dojemanja ljudi. Stopnja sprejemljive ogroženosti pa je med ljudmi različna in je odvisna od stopnje izobrazbe, spola, lokacije in drugih ekonomskih, socialnih in političnih razmer (CRP, 2004). Tudi v raznih raziskavah ima uporaba pojma ranljivosti različne pomene, odvisno od raziskovalne usmeritve in ciljev. In, kot pravi Sterlacchinijeva (2011), v znanstveni literaturi ni soglasja o natančnem pomenu besede ranljivost, ter se zdi, da je odprt za razlago.

Dojemanje ranljivosti

Ranljivost je močno odvisna od dojemanja ljudi. Ločimo notranje dimenzije (nesposobnost oz. sposobnost odzivanja ljudi) ter zunanje dimenzije (izpostavljenost tveganju, šokom, stresu). Je torej socialni izraz. Socialna ranljivost je povezana z dostopnostjo sredstev, stopnjo ekonomskega razvoja, sposobnostjo napovedovanja pojavljanja nevarnosti, s prilagajanjem in sprejemanjem razmer, ki jih nevarnosti sprožijo ter planiranjem ukrepov. Nevarnosti imajo različen vpliv na različne skupine ljudi v skupnosti in je odvisen od njihove sposobnosti spoprijemanja z nevarnostjo.

Ljudje razumejo pojme vezane z ogroženostjo glede na svoje izkušnje, zato je tudi ranljivost močno odvisna od dojemanja ljudi.

Po Heijmansu (2001, v CRP, 2004:51) ločimo, glede na vzrok, tri načine dojemanja ranljivosti: **narava** kot vzrok (tehnične, znanstvene rešitve): ta pogled krivi naravo in naravno nevarnost kot vzrok ranljivosti ljudi, ki je odvisna od intenzitete, magnitude in trajanja zunanjih šokov. Ranljivost je rezultat nevarnosti (vključuje intenziteto) in tveganja (izpostavljenost dogodkom); **cene** kot vzrok (ekonomske in finančne rešitve): kljub naraščanju tehnoloških in znanstvenih kapacitet, ljudje še vedno trpijo, ker so napovedovanja in tehnologije predrage. Ranljivost se lahko zmanjša s sprejemanjem varnostnih ukrepov, vključevanjem zavarovalništva in zagotavljanjem finančne podpore; **socialne strukture** kot vzrok (politične rešitve): ta pogled kaže, da imajo nesreče različen vpliv na ljudi, ki živijo na ogroženih območjih. Ni samo izpostavljenost nevarnosti tista, zaradi česar so ljudje izpostavljeni tveganju, temveč tudi socio-ekonomski in politični procesi v družbi, ki generirajo ranljivost.

Obstajajo štiri glavne vrste ranljivosti: socialna, ekonomska, politična in kulturna. Po Alcantara-Ayala (2002, prav tam) pa jih lahko delimo na: materialno ali ekonomsko ranljivost (pomanjkanje sredstev), socialno ranljivost (prekinitev socialnih vzorcev), organizacijsko ranljivost (pomanjkanje močnih nacionalnih ali lokalnih institucionalnih struktur), izobraževalna ranljivost (pomanjkanje dostopa do informacij ali znanja), motivacijsko ranljivost (pomanjkanje javnega zavedanja), politično ranljivost (omejen dostop do politične moči), kulturno ranljivost (prepričanje in navade), fizično ranljivost (slabe zgradbe šibkih posameznikov). Takšna razdelitev nakazuje, da ima vsaka socialna skupnost različne vrste ranljivosti, ki ni samo rezultat dejanj, odločitev in izbire, ampak je rezultat interakcije narave, ekonomije, kulture in politike prostora, kjer živijo ljudje. Ranljivost določuje tako naravni kot človeški sistem.

Definiranje ranljivosti

Kakor pri drugih terminih in pojmih vezanih na ravnanje s tveganji, se tudi tu srečamo z množico razlag in definicij. Definiranje ranljivosti se je okoli leta 1975 močno razpršilo po posameznih raziskovalnih področjih. Geologi, hidrologi in gradbeniki so preučevali znanstvene rešitve v zvezi z naravnimi nevarnostmi, medtem ko so sociologi, antropologi in družbene vede poudarjale človeško obnašanje, odzive in pripravljenost na nesreče (Đurović, 2006).

Množico pristopov, pogledov in tolmačenj danes pokaže tudi selektivni pregled literature mnogih znanstvenih disciplin, ki z različnih zornih kotov obravnavajo ranljivost (Alwang, Siegel, Jorgensen, 2001). Pri bežnem pregledu tako lahko najdemo na enem mestu kar triinštirideset definicij ranljivosti (www.weADAPT.org, 2011; Musser, 2002). Nekateri primeri definicij:

- Ranljivost je značilnost človeškega obnašanja, socialnih in fizikalnih okolij, ki opisuje stopnjo dovzetnosti (ali odpornosti) učinkom npr. naravnih nevarnosti. Ranljivost je določena s kombiniranjem zavedanja o nevarnosti, stanja človeških naselbin in infrastrukture, javne politike in administracije in organizacijske moči pri obvladovanju nesreč. Revščina je v mnogih krajih sveta eden glavnih vzrokov ranljivosti. (CENAT, 2004).
- Ranljivost kot termin označuje stopnjo ali stanje v katerem bi lahko človek, skupina ali družbeno-ekonomska struktura bila prizadeta z nesrečo (upoštevajoč njihove sposobnosti, da predvidijo nevarnost, da se jo obranijo in si opomorejo od posledic). Lahko jo opazujemo skozi tri velika, medsebojno povezana področja: fizično-materialnega, družbeno-organizacijskega in motivacijsko-miselnega. (Jakovljević, 2006).
- Ranljivost je pričakovana stopnja izgub (ali poškodb) danega ogroženca ali skupine ogrožencev ob morebitni nesreči. Govorimo o potresni, poplavni, požarni in drugi ranljivosti. Ocenjujemo jo navadno z vrednostmi med 0 in 1 (Lapajne, 1987).
- Ranljivost ogroženca (človeška življenja, materialne dobrine in okolje) lahko obravnavamo kot verjetno stopnjo poškodb v odvisnosti od magnitude pojava in kakovosti strukture oz. karakteristik ogroženca (Đurović, 2005).
- Ranljivost je stopnja možne posledice pri delovanju določenega pojava z določeno jakostjo. Ranljivost podamo med vrednostmi 0 (ni vpliva) in 1 (najhujše posledice). Obraten pojem od ranljivosti je *odpornost*, ki pove koliko so določena tla odporna na določen pojav (CRP, 2004).
- Ranljivost lahko opredelimo kot "karakteristike osebe ali skupine v smislu njihove sposobnosti predvidevanja, ravnanja, upiranja in okrevanja od učinkov naravne nevarnosti", kar predpostavlja da so nekatere skupine znotraj družbe bolj nagnjene k temu, da utrpijo škodo in izgubo zaradi dane naravne nevarnosti (Blaikie in drugi,1994,v: webADAPT, 2011).
- Ranljivost je »kakršnakoli slabost oz. napaka v fizičnem stanju (položaju) organizacije, postopkov, menedžmenta, administracije, »hardwara in softwara«, ki se lahko izrabi za povzročitev škode tako instituciji, poslovnosti ali dejavnosti«. (Pečar, 2000).

Ocenjevanje ranljivosti

Z vidika korporativne varnosti je zanimiv zapis profesorja Pečarja (2000), ki pravi, da v gospodarstvu večine sodobnih držav v strukturi lastništva prevladujejo zasebni lastniki, imetniki bogastva, ki so ranljivi in ogroženi itd. in so »tisti, ki morajo sami upravljati svoja tveganja, upoštevati grožnje (ne samo tiste s kriminalom, ampak tudi z nezgodami in drugimi nevšečnostmi) ter so na ta način »prisiljeni gospodarno ravnati predvsem s svojo ranljivostjo. Odgovornost analiziranja in ocenjevanja je torej na strani lastnikov, uprav, managerjev, saj se država na notranje varnostnem področju nikoli ne srečuje s »tveganjem«, za katerega bi bila odgovorna drugače kot morda politično (prav tam: 108). Ali lahko v korporativnih okoljih kakovostno to sami opravijo, pa je drugo vprašanje.

Po mnenju strokovnjakov je ocena ranljivosti eden najbolj kritičnih vidikov vrednotenja ogroženosti. V literaturi prevladujejo empirični pristopi, kjer se razlikuje ranljivost človeškega življenja in ranljivost ekonomskih dobrin. Prednost teh pristopov je v enostavnosti, slabost pa velika subjektivnost ocene in visoka stopnja negotovosti. Poenostavljeno lahko rečemo, da sta analiziranje in ocenjevanje ranljivosti procesa identificiranja, vrednotenja, izbora ter ocenjevanja varnostnih ranljivosti različnih sistemov. V procesu se ugotavljajo občutljiva mesta, šibke točke, slabosti, dovzetnost, nagnjenost k ranljivosti, ipd. različnih vplivnih dejavnikov. Ko se v procesu ocenjevanja prepozna, določi, izmeri, ovrednoti vse zahtevane dejavnike ter njihov vpliv, se nadaljuje z ugotavljanjem sprejemljive stopnje ranljivosti oziroma potrebne odpornosti, glede na odnose med ostalimi parametri celotne analize tveganja.

Tveganje = Ranljivost x Grožnja x Vpliv (posledice) Protiukrepi

kjer je **Ranljivost = (Izpostavljenost) + (Odpornost) + Prožnost**
(I= izpostavljenost ljudi in premoženja; O= ukrepi za preprečevanje, izogibanje, zmanjšanje škode; P= sposobnost, zmožnost, prilagodljivost za obnovo, okrevanje in vzpostavitev prvotnega stanja).





Dumke (2012) dejavnike, ki vodijo k ranljivosti, v poslovno orientiranem pristopu k analizi ranljivosti, opisuje kot notranje (osebje, vzdrževanje, drugi ljudje, vodstvo in organizacija, tehnične napake/nevarnosti, lastnosti/značilnosti sistema) in zunanje (finančne, tržne, zakonske, infrastrukturne, socialne, okoljske). Pri ocenjevanju pa je treba raziskati in upoštevati še druge različne vplivne komponente oziroma dimenzije, kot so npr.: fizično-funkcionalna, socialno-ekonomska, socialno-kulturna, ekološko-okoljska, politično-institucionalna, itd. (Sterlacchini, 2011).

Da bi zagotovili večjo objektivnost ocenjevanja, se uporabljajo različni deduktivni in induktivni pristopi, študije primerov, analize scenarijev, matematična modeliranja, linearna programiranja, ekspertne presoje, inženirske analize, analitične in statistične tehnike, itd. Raziskovalcem in sodelujočim strokovnjakom so za to na razpolago različna ocenjevalna orodja, tehnike in metode. Nekatere so bile predstavljene že v prejšnjih člankih, v tem omenjamo le nekatere (za različna področja uporabe), kot npr.**: BRAVA (**Baseline Rapid Assessment of Vulnerability for Adaptation), **CRiSTAL** (Community- based Risk Screening Tool– Adaptation and Livelihoods), **CEDRA** (Climate change and Environmental Degradation Risk and Adaptation assessment), **MBVA** (Model-based Vulnerability Analysis), **HRVA** (Hazard, Risk and Vulnerability Analysis), **I-VAM** (Infrastructure Vulnerability Assessment Model), **IRAM** (Infrastructure Risk Analysis Model), **MAA** (Multidimensional activity analysis), **ROSA** (Risk and vulnerability analysis), **IBERO** (Instrument for preparedness evaluation of area responsibility), **VAM** (Vulnerability Assessment Methodology – Electric Power Infrastructure), in druga, ki pa jih tu zaradi množice ne moremo predstaviti.

Sklepno

Zgoščeni prikaz je le izziv za razmišljane o večrazsežnosti in kompleksnosti pojma ranljivosti. Zavedajoč se pomanljivosti zapisanega, je bil glavni namen opozoriti na težavnost obravnave tega elementa v okviru analize, ocene, presoje, vrednotenja in obvladovanja tveganj, ki so bili predstavljeni v prejšnjih člankih. Težavnost pristopa k obravnavi je pogojena z mnogimi definicijami in različnimi vidiki obravnave posameznih znanstvenih disciplin. Vsekakor pa ne smemo zanemariti našega subjektivnega zaznavanja in dojemanja, ter objektivnih dejstev obravnavanega, pri našem bodočem ukvarjanju s to problematiko v okviru korporativne varnosti.

Viri

- Alwang,J., Siegel, P.B., Jorgensen, S.L.(2001). Vulnerability: a view from different disciplines. Pridobljeno 13.2.2014 na: http://siteresources.worldbank.org/SOCIALPROTECTION/Resources/SP-Discussion-papers/Social-Risk-Management-DP/0115.pdf.
- CENAT (2004). Coping with risks due to natural hazards in the 21st century. Monte Veritŕ Workshop 2004, 28. 11.–3. 12. 2004. http://www.cenat.ch (2.2.2006).
- CRP (2004): »Metodologija za določanje ogroženih območij in način razvrščanja zemljišč v razrede ogroženosti zaradi zemeljskih plazov - končno poročilo«, UL FGG, Poročilo KSH d-78, Ljubljana, maj 2004.
- Dumke, D. (2012). Assessment of Supply Chain Vulnerabilities. Pridobljeno 31.2.2014 na: http://scrmblog.com/review/assessment-of-supply-chain-vulnerabilities.
- Đurović, B., Ribičič, M., Mikoš, M. (2005). RHDM postopek analize potencialne ogroženosti zaradi odlomne nevarnosti. Geologija, 48/1, str. 33-51, Ljubljana, 2005.
- Đurović, B. in Mikoš, M. (2006). Pojmi in izrazje teorije tveganj zaradi naravnih, geološko in geografsko pogojenih nevarnosti. Geologija 49/1. Pridobljeno 2008 na:http://www.geozs.si/publikacije_arhiv/Clanki/Geologija_49_1/Durovic%20&%20Mikos.pdf.
- Jakovljević, V.(Ur.) (2006). *Etiologija ugrožavanja ljudi, materijalnih dobara i životne sredine.* V Kekovič, Z., Kešetović, Ž. Krizni menadžment I, Prevencija krize. Univerzitet u Beogradu, Fakultet bezbednosti.
- Lapajne, J. 1987: Strokovna beseda. – Ujma *1*, 94, Ljubljana.
- Musser, L. (2002). Vulnerability Bibliography. Pridobljeno 14.2.2014 na: http://weadapt.org/knowledge-base/vulnerability/vulnerability-definitions.
- Pečar, J. (2000). Nadzorovanje – temelj in vsebina varovanja in varnosti (Kaj z »varstvoslovjem?«). *Revija za kriminalistiko in kriminologijo, 51/2000/1, str. 105-114.*
- Sterlacchini, S. (2011). Vulnerability Assessment: concepts, definitions amd methods. Pridobljeno 13.2.2014 na: http://changes-itn.eu/Portals/0/Content/2011/Poland/Sterla_CHANGES_final_2011.pdf.
- WEADAPT (2011). Vulnerability definitions. Pridobljeno 14.2.2014 na: http://weadapt.org/knowledge-base/vulnerability/vulnerability-definitions.

[1] Angl.: vulnerability: ranljivost. Vulnerabilnost –ranljivost, (dovzetnost) občutljivost za poškodbe; vulnerabilen (n.lat.: vulnerabilis – iz lat. vulnus, vulneris: rana, ranljiv) 1. dovzeten za poškodbe ali okužbe (med) 2. občutljiv za napade kritike ■

geacollege
Fakulteta za podjetništvo



MANAGEMENT KORPORATIVNE VARNOSTI

Magistrski program

Magistrski program **Management korporativne varnosti**

Magistrski program Management korporativne varnosti je namenjen izobraževanju ter usposabljanju podjetnikov in managerjev za obvladovanje poslovno varnostnih mehanizmov in upravljanje varnostnih tveganj v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Z magistrskim študijem Management korporativne varnosti omogočamo študentom poglobljeno podiplomsko izobraževanje, v katerem pridobijo teoretična in aplikativna znanja s področja poslovno varnostnega managementa, s kompetencami za upravljanje korporativne varnosti. Poudarek je na: geostrateških in političnih vidikih varnostnih tveganj, varnostnih standardih v poslovnih procesih, prepoznavanju in analiziranju ranljivosti, ogroženosti in varnostnih tveganj, upravljanju varnostnih tveganj, informacijski in komunikacijski varnosti, načrtovanju in razvoju korporativne varnosti, procesih nadzora, zavarovalništvu, financah, gospodarskem poizvedovanju, ekoloških vidikih in varnemu delovnemu ter poslovnemu okolju.

RAZPISANE SMERI

- Korporativni varnostni manager
- Korporativni varnostni manager – podjetnik

TRAJANJE ŠTUDIJA IN STROKOVNI NASLOV

- 2 leti
- magister/magistrica managementa korporativne varnosti

Kaj omogoča študij Managementa korporativne varnosti



Pridobiti ustrezna multidisciplinarna znanja, ki temeljijo na znanstveno raziskovalnem delu in praktičnih izkušnjah ter dobrih praksah v nacionalnem in mednarodnem korporativnem okolju. Študentje bodo pridobili znanja za upravljanje z varnostnimi tveganji in vodenje organizacijskih struktur na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah. Poseben poudarek je na varnostnih mehanizmih v organizacijah, ki upravljajo s kritično infrastrukturo (energetika, telekomunikacije, informatika, transport, finančne institucije, prehrambena industrija idr.). Bodoči magistri bodo v času študija pridobili vsa potrebna znanja in kompetence, ki so potrebne za delovanje v podjetniškem okolju tudi kot samostojni podjetniki, ki bodo drugim organizacijam nudili (tržili) tovrstne strokovne storitve s področja načrtovanja, izvajanja in upravljanja korporativne varnosti.

PARTNERJI PROGRAMA

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

ICS
Institut za korporativne varnostne študije

SECSA
SE Europe Corporate Security Association

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



mag. Boris Novak, generalni direktor Pošte Slovenije

Vpisni pogoji

V 1. LETNIK SE LAHKO VPIŠE:

• kdor je končal študijski program prve stopnje z ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...) z najmanj 180 kreditnimi točkam po ECTS,
• kdor je končal študijski program za pridobitev visoke strokovne izobrazbe z ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), sprejet od 1. 1. 1994 do 11. 6. 2004,
• kdor je končal študijski program prve stopnje ali za pridobitev visoke izobrazbe, sprejetim od 1. 1. 1994 do 11. 6. 2004 drugih strokovnih področij, vendar pa morajo pred vpisom opraviti diferencialne izpite do 24 kreditnih točk, ki jih glede na strokovno področje predhodnega študija določi pristojna komisija GEA College - Fakultete za podjetništvo na podlagi individualne vloge kandidata.

PO MERILIH ZA PREHODE SE V 2. LETNIK LAHKO VPIŠEJO:

• diplomanti študijskega programa za pridobitev univerzitetne izobrazbe, sprejetega pred 11. 6. 2004, iz sorodnih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki se jim praviloma priznajo študijske obveznosti v obsegu do 40 KT,
• diplomanti študijskega programa za pridobitev univerzitetne izobrazbe, sprejetega pred 11. 6. 2004, drugih strokovnih področij, ki se jim praviloma priznajo študijske obveznosti v obsegu do 30 KT,
• diplomanti specialističnega študija podjetništva GEA College - Fakultete za podjetništvo, ki se jim prizna 60 KT,
• diplomanti specialističnega študija sorodnih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki se jim praviloma priznajo študijske obveznosti v obsegu do 40 KT,
• diplomanti specialističnega študija drugih strokovnih področij, ki se jim praviloma priznajo študijske obveznosti v obsegu do 30 KT,
• študent drugostopenjskega študijskega programa ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki izpolnjuje pogoje za vpis v višji letnik (40 KT ali več).

Predmetnik

Obvezni skupni predmeti
PREDMET
Management korporativne varnosti – obvezni predmet
Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju – obvezni predmet
Pravni vidiki korporativne varnosti – obvezni predmet
Ekonomika obvladovanja tveganj v poslovnem okolju

Obvezni usmeritveni predmeti
SMER - Korporativni varnostni manager
Varnostni standardi v poslovnih procesih
Upravljanje varnostnih tveganj
Načrtovanje in razvoj korporativne varnosti

Obvezni usmeritveni predmeti
SMER - Korporativni varnostni manager - podjetnik
Varnostni standardi v poslovnih procesih
Upravljanje varnostnih tveganj
Načrtovanje in razvoj korporativne varnosti

Izbirni predmeti (študent izbere dva)
PREDMET
Management človeških virov
Okoljski vidiki korporativne varnosti
Metode raziskovanja varnostnih pojavov
Zavarovalništvo v procesih zagotavljanja gospodarske varnosti
Gospodarsko poizvedovanje in varovanje poslovnih informacij
Informacijska varnost

Študijski praktikum v 1. in 2. letniku

Magistrsko delo

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

Andrej Podvršič, EMEA Director of Security
DuPont de Nemours International Sŕrl



CILJI ŠTUDIJA

Ključni cilj programa je izobraziti in usposobiti strokovnjake, ki imajo poslovna, pravna, tehnična in druga znanja ter dobro poznavanje in razumevanje globalnega ter nacionalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja, za celovito upravljanje korporativne varnosti v različnih organizacijah.

V programu bodo diplomanti pridobili naslednje kompetence:

• Znanje s področja globalnih družbenih, ekonomskih, političnih in varnostnih vidikov.
• Razumevanje, oblikovanje in uvajanje varnostnih politik in varnostnih strategij v kontekstu družbenega in gospodarskega razvoja ter poslovne uspešnosti.
• Sposobnost proučevanja varnostnih pojavov, izdelava varnostnih elaboratov ter analiziranje in ocenjevanje ranljivosti, ogroženosti in tveganj.
• Zmožnost uvajanje celovitih (integralnih) varnostnih sistemov, ki obsegajo varovanje ljudi in premoženja, informacij in poslovnih skrivnosti, poslovno poizvedovanje, okoljske vidike, obvladovanje izrednih dogodkov, neprekinjeno delovanje vitalnih poslovnih funkcij in procesov v izrednih okoliščinah.
• Prepoznavanje koristnosti uvajanja varnostnih standardov v sklopu sistemov vodenja kakovosti proizvodnje, logistike in trženja.
• Poznavanje metodologij za upravljanje procesov korporacijske varnosti v smislu poslovnih funkcij, načrtovanja investicij v varnostne izboljšave, zavarovanja tveganj in razumevanja postopkov (javnega) naročanja storitev korporacijske varnosti.

Magistrski program **Management korporativne varnosti**



»Ko smo pred časom skupaj s partnerji – Inštitutom za korporativno varnost začeli pripravljati magistrski program Management korporativne varnosti, smo se zavedali, da orjemo ledino. Sestavili smo kakovosten program, ki je unikaten pri nas in tudi v Evropi. Tudi drugod po svetu je zelo malo študijskih programov ali smeri, ki bi bile vsaj podobne, če že niso popolnoma primerljive. Program izobražuje za nov poklic. Verjamemo, da je to eden od poklicev prihodnosti. Lastna varnost vse bolj postaja odgovornost posameznikov in organizacij. V tehnološko vse bolj zapletenem svetu, v katerem vzporedno potekajo tudi nagle spremembe v družbi in okolju, je celostno obvladovanje varnostnih procesov izziv, ki terja za to posebej usposobljene strokovnjake. Z ustreznim predznanjem in delovnimi izkušnjami z različnih področij širšega obvladovanja varnostnih procesov in tveganj bodo študentje magistrskega programa znali nadgrajena znanja predvsem povezovati v zaključene celote. Študentje bodo kasneje prevzeli najodgovornejša mesta v podjetjih, kjer se bodo ukvarjali z integralnimi varnostnimi procesi. V večjih podjetjih bodo ti strokovnjaki našli zaposlitev (managerji), v manjših pa bodo lahko nudili svoje storitve (podjetniki).«

izr. prof. dr. Jaka Vadnjal, dekan fakultete



»Podiplomski študij managementa korporativne varnosti je pri nas, pa tudi širše v kontinentalni Evropi, popolnoma nova smer izobraževanja, ki je prilagojena stalno spreminjajočemu se okolju in s tem najnovejšim kočljivim situacijam v podjetjih, institucijah ne glede na njihovo lastništvo. Te situacije so precej bolj tvegane in kompleksne, kot so bile pred leti. Opravka imamo s celo paleto različnih tveganj, katerim smo danes izpostavljeni praktično vsi. Ozrite se okrog sebe in opazujte, kaj se dogaja. Varovanje v svojem klasičnem smislu fizičnega varovanja predstavlja danes v podjetjih in institucijah samo majhen del vsega ščitenja, če uporabim kar ta izraz, ki ga posameznik, podjetje, institucija mora imeti oz. si ga organizirati. Magister managementa korporativne varnosti bo ta oseba, ki bo v podjetjih, institucijah organizirala in vodila službo oz. organizacijsko enoto, ki bo pokrivala to integralno in izjemno pomembno področje ščitenja pred različnimi tveganji v najširšem smislu v teh turbulentnih in nevarnih časih. V sodobneje organiziranih in nekoliko večjih pravnih osebah pa bo ta oseba kar član uprave za to integralno področje.«

doc. dr. Draško Veselinovič, direktor in predavatelj



»Živimo v dinamičnem gospodarskem okolju, kjer je varnost postala dobrina, ki ni več samo po sebi umevno dejstvo. Informacijska globalna družba pred nas postavlja veliko priložnosti, odpira pa tudi tveganja, katerih se je potrebno v podjetjih in drugih organizacijskih sredinah zavedati in jih tudi ustrezno obvladovati. V tem okviru posebej izpostavljam organizacije, ki obvladujejo kritično infrastrukturo, katera je nujno potrebna za delovanje širše družbene skupnosti. Ker popolne varnosti ni možno zagotoviti, je znanje korporativno varnostnih managerjev tista dodana in primerjalna vrednost, ki na strateškem nivoju bistveno vpliva na učinkovitost in kakovost obvladovanja tveganj v podjetjih. To so znanja, ki so in bodo v slovenskem in širšem regijskem prostoru v naslednjih letih izredno iskana. S temi znanji in dobrimi praksami ter najnovejšimi spoznanji vas bomo "oborožili", ko boste stopili na trg polno priložnosti za vaše uveljavljanje. Najboljšim študentom pa bo skozi povezave Slovenskega združenja za korporativno varnost in mednarodne asociacije SE European Corporate Security Association (SECSA) tudi omogočena priložnost za pridobivanje izkušenj v neposrednem organizacijskem okolju.«

doc. dr. Denis Čaleta, predsednik Slovenskega združenja za korporativno varnost



»Krizne razmere, vsesplošna ogroženost, varnostna tveganja ter pomanjkljivi varnostni in nadzorni mehanizmi že kar nekaj časa kličejo po dvigu kakovosti tistega dela managementa v gospodarskih in drugih subjektih, ki upravljajo z varnostjo ljudi, procesov in premoženja. Izhajamo tudi iz premise, da le profesionalni in celovit varnostni sistem odločilno prispeva k preprečevanju škod in izgub, k bogatenju poslovnih izidov ter k dvigu kulture, ugleda in konkurenčnih prednosti. Gre za fenomen sinergije poslovnih in varnostnih procesov ter intelektualnega kapitala, da složno in pregledno upravljajo z določeno družbo. To pomeni, da obstoječi in novi management korporativne varnosti potrebuje nova znanja, ki zagotavljajo učinkovito upravljanje varnosti ter dvig statusa in ugleda posameznih managerjev korporativne varnosti zlasti v konici korporativnega upravljanja. Inovativni magistrski program, ki je pred vami, daje lastnikom, upravljavcem in nadzornikom ter zainteresiranim posameznikom možnost in priložnost, da ustvarijo nekaj več za varnost zaposlenih, poslovnih procesov, kapitala in razvoja.«

doc. dr. Milan Vršec

Kontakt

Dodatne informacije so vam na voljo na naši spletni strani **www.gea-college.si**, veseli pa bomo vašega klica na telefonski številki **01 588 13 00** ali e-pošte na **korpo@gea-college.si**.

GEA College – Fakulteta za podjetništvo, Dunajska 156 (stolpnica WTC), 1000 Ljubljana



ICS PUBLIKACIJE

ICS

Institute for Corporative Security Studies

www.ics-institut.si



Holding Slovenske elektrarne d.o.o. Koprska ulica 92, 1000 Ljubljana, Slovenija



POZITIVNA ENERGIJA NARAVE

Skupina HSE je največji slovenski proizvajalec in trgovec z električno energijo. Kot zaupanja vreden partner stremimo k ustvarjanju trajnih in trdnih poslovnih odnosov. Zato tako domačim kot tujim odjemalcem zagotavljamo varno, zanesljivo in kakovostno oskrbo z električno energijo. Ker se zavedamo vloge pri ustvarjanju prijazne prihodnosti, znanje usmerjamo v iskanje optimalnih rešitev iz okolju prijaznih, obnovljivih virov. Za energijo, ki bo poganjala domišljijo naslednjih rodov.

OSNOVNI CERTIFIKAT Družini prijazno podjetje

Modra energija
Obnovljivi viri sedanjosti in prihodnosti
www.modra-energija.si

MODRA GENERACIJA
www.modra-generacija.si

Modri Jan
www.modri-jan.si

hse
Moč energije
www.hse.si