Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

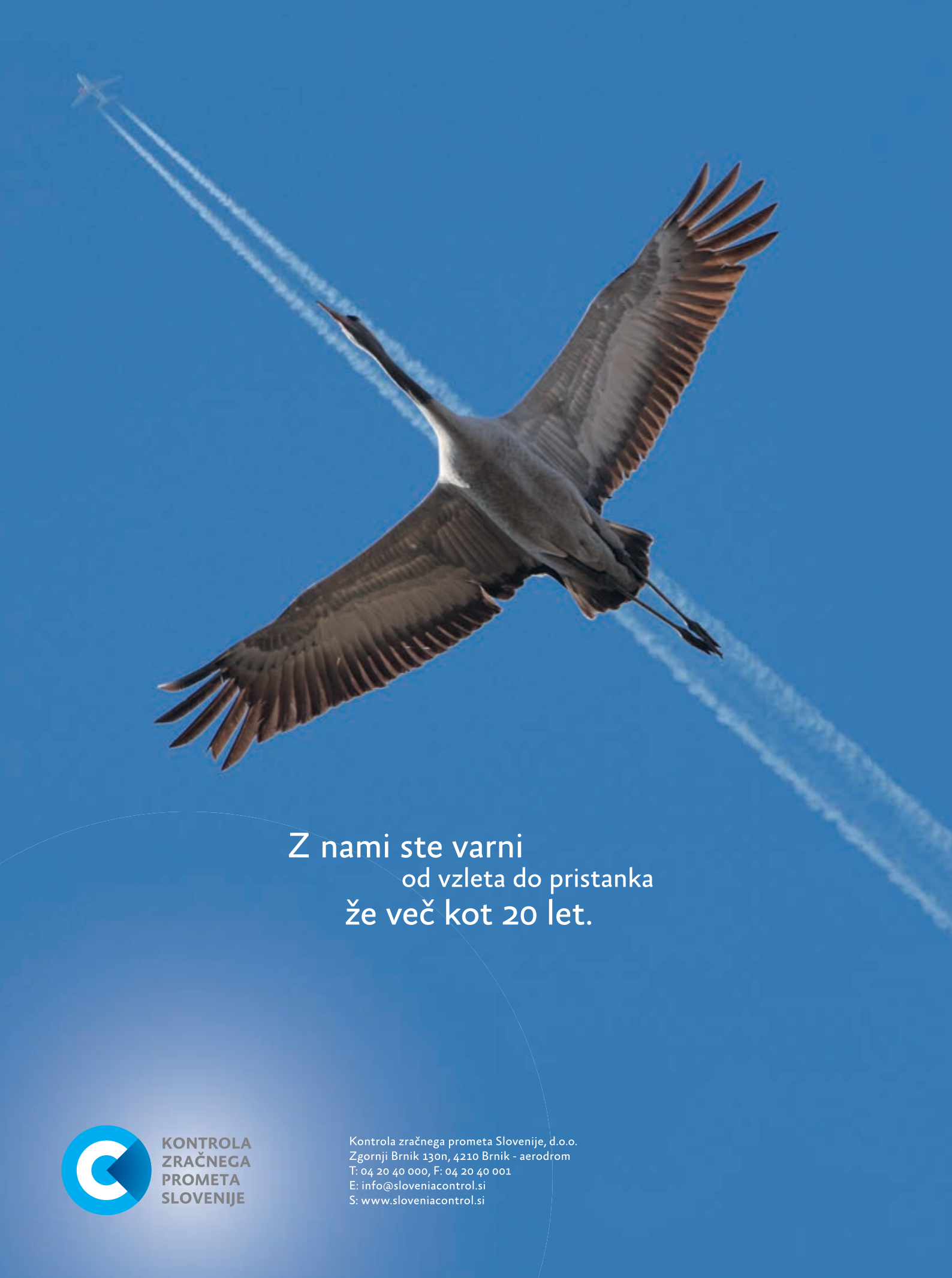
Letnik 2017, junij • št. 14



Magistrski študijski program "Management korporativne varnosti"

Vzpostavitev sistema kibernetske varnosti kot nujni predpogoj za normalno delovanje Republike Slovenije

mag. Dobran Božič, direktor Urada za varovanje tajnih podatkov



KONTROLA ZRAČNEGA PROMETA SLOVENIJE

Kontrola zračnega prometa Slovenije, d.o.o.
Zgornji Brnik 130n, 4210 Brnik - aerodrom
T: 04 20 40 000, F: 04 20 40 001
E: info@sloveniacontrol.si
S: www.sloveniacontrol.si



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:
izr. prof. dr. Denis Čaleta

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
junij 2017

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

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

Revija Korporativna varnost si vztrajno odmerja vedno večji medijski prostor v strokovni javnosti, saj se krog bralcev vedno boj širi. Seveda se je potrebno zavedati, da k temu dejstvu, poleg aktualne in kvalitetne vsebine, pomembno pripomore tudi dinamično varnostno okolje, ki nas vedno znova sili v iskanje novih rešitev in odgovorov na tveganja in grožnje katerim so izpostavljena naša organizacijska okolja. Pomembno mesto, v tem trendu vedno večjega povpraševanja po sami strokovni reviji, pa vsekakor pomeni tudi kontinuiranost izhajanja, saj smo tokrat že pri izidu 14. številke.

V obdobju priprave tokratne številke smo bili priča nizu kompleksnih varnostnih groženj, ki so jih pred nas postavili teroristični napadi, neprestan migracijski pritisk na zunanje meje EU in s tem tudi sprejetje bolj restriktivnih mejnih ukrepov na schengenski meji, kibernetska tveganja in obsežni hekerski napadi, cel niz tveganj, katerim so bile izpostavljene gospodarske organizacije, pa vse do geopolitičnih premikov, ki smo jim priča skoraj vsak dan in nas stalno navdajajo z neprestano dinamiko spreminjanja stabilnega varnostnega okolja, kakršnega smo bili vajeni v preteklosti. Vse to pred strokovnjake s področja korporativne varnosti postavlja dileme, kako biti v takih razmerah, pri vodenju razvejanih organizacij, učinkovito orodje v rokah strateškega managementa. Ravno pri strateškem managementu se varnostno zavedanje o pomenu korporativne varnosti, in varnosti nasploh, počasi dviguje in prihaja v ospredje. Vendar se vse prevečkrat dogaja, da strokovno znanje in sposobnost korporativno varnostnega managementa v organizacijah, ni na ustreznem nivoju, da bi izkoristil ta »zvezdniški trenutek« in se v določenih situacijah izkazal kot učinkovit mehanizem za ustrezno obvladovanje tveganj. Ta lažna zazibanost in samozadovoljnost je v svetu takih dinamičnih sprememb, kakršne se vsakodnevno dogajajo, praktično obsojena na takojšen neuspeh. Zaradi navedenega je potrebno, bolj kot kadarkoli do zdaj, vlagati v stalno izobraževanje in dograjevanje svojih znanj ter veščin. Revija Korporativna varnost predstavlja ustrezno platformo stalnega izmenjevanja dobrih praks in najnovejših spoznanj, kar je za strokovno javnost izredno pomembno.

Tudi tokrat nam vsebina 14. številke prinaša veliko aktualnih vsebin, ki odpirajo najbolj izpostavljene dogodke zadnjega časa. Skozi odmevne intervjuje, reportaže iz vsebinsko odličnih dogodkov, pa vse do strokovnih člankov, ki pred nas postavljajo zadnja spoznanja iz aktualnih področij, se bo našlo dovolj raznovrstne vsebine, ki vam bo omogočila pridobiti dovolj odgovorov in dobrih praks za vaše uspešno poslovanje.

V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji.

izr. prof. dr. Denis Čaleta
Glavni urednik



REVIZIJA VARNOSTNIH SISTEMOV V KRITIČNI INFRASTRUKTURI

Morda je sedaj, ko je Zakon o kritični infrastrukturi v fazi obravnave in sprejemanja in ko so podane že skoraj vse evropske in nacionalne pravne podlage za upravljanje evropske in nacionalne kritične infrastrukture pravi čas, da naredimo korak k implementaciji sprejete regulative.

14



SLOVENIJA NUJNO POTREBUJE USTREZNO UREDITEV ODGOVORNEGA RAZKRIVANJA VARNOSTNIH RANLJIVOSTI

Informacijski pooblaščenec Republike Slovenije, nacionalni center SI-CERT in Institut za korporativne varnostne študije (ICS) so z namenom iskanja odgovorov na izzive, povezane s številnimi primeri razkritij ranljivosti informacijskih sistemov in omogočanja široke javne razprave o pomembnih vprašanjih informacijske varnosti organizirali posvet z okroglo mizo.

25



INTERVJU
g. Franci Petek, poveljnik Gasilske zveze Slovenije

POŽARNA ZAŠČITA KLJUČNI TEMELJ KORPORATIVNE VARNOSTI

36



NADZOR NA DELOVNEM MESTU: VEČ KOT JE OMEJITEV, VEČ JE KRŠITEV

Skladno z zakonodajo se delo opravlja po navodilih in pod nadzorom delodajalca, zato je ta upravičen tudi do nadzora nad zaposlenimi. Nadzor na delovnem mestu je legalna in legitimna pravica delodajalca.

40



MONOPOL DRŽAVE NA PODROČJU ZAGOTAVLJANJA NACIONALNE VARNOSTI – ALI SPLOH ŠE OBSTAJA ?

Danes se sprašujemo, ali ta klasičen državni monopol na področju uporabe sile in ta klasična interna delitev področij zagotavljanja varnosti na omenjena njena državna sektorja še vedno velja.

44

Avtor: izr. prof. dr. Denis Čaleta / Inštitut za korporativne varnostne študije

INTERVJU
mag. Dobran Božič, direktor Urada za varovanje tajnih podatkov

VZPOSTAVITEV SISTEMA KIBERNETSKE VARNOSTI KOT NUJNI PREDPOGOJ ZA NORMALNO DELOVANJE REPUBLIKE SLOVENIJE

Urad za varovanje tajnih podatkov je s prihodom novega direktorja dobil ključno vlogo na področju koordinacije aktivnosti za vzpostavitev sistema kibernetske varnosti v Republiki Sloveniji. Izkoristili smo priložnost in se pogovorili z mag. Božičem, da nam pomaga predstaviti ključne korake na področju delovanja Urada za varovanje tajnih podatkov, ki ga vodi.

Urad Republike Slovenije za varovanje tajnih podatkov je ključna institucija v državi ko govorimo o upravljanju sistema varovanja tajnih podatkov. Nam lahko zaupate katere so tiste ključne naloge, ki jih urad izvaja na podlagi zakonskih predpisov.

Naloge UVTP so opredeljene v Sklepu o ustanovitvi, nalogah in organizaciji UVTP-ja, Zakonu o tajnih podatkih in Aktu o notranji organizaciji in sistemizaciji delovnih mest v UVTP-ju. UVTP skladno z navedenimi predpisi opravlja naslednje poglavitne naloge:
(1) Spremlja stanje na področju določanja in varovanja tajnih podatkov ter skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v državnih organih, organih lokalnih skupnosti, pri nosilcih javnih pooblastil ter v gospodarskih družbah in organizacijah, ki pridobijo tajne podatke ali razpolagajo z njimi; (2) Skrbi za izvajanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij; (3) Nadalje skrbi za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije ter v zvezi s tem opravlja zlasti naslednje naloge: izdaja dovoljenja za dostop do tajnih podatkov, izdaja varnostna potrdila pravnim osebam, varnostna potrdila za sisteme in naprave za prenos, hrani in obdeluje tajne podatke, potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa tujim državam in organizacijam, predlaga varnostno pre-

> Z razvojem in naraščanjem pomena omrežij, informacijskih sistemov in komunikacijskih povezav je postajala suverenost nad nacionalnim kibernetskim prostorom vse pomembnejša. Države, ki se zavedajo suverenosti nad svojim kibernetskim prostorom, le tega varujejo in branijo.



verjanje za izdajo dovoljenja za dostop do tajnih podatkov in potrebujejo dovoljenje za dostop do tajnih podatkov tuje države ali mednarodne organizacije, izdaja navodila za ravnanje s tajnimi podatki tuje države ali mednarodne organizacije, nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki jih morajo organi izvesti takoj, ter izmenjuje podatke z nacionalnimi varnostnimi organi in mednarodnimi organizacijami; (4) Pripravlja predloge predpisov, ki so potrebni za izvajanje ZTP-ja, daje mnenje o skladnosti splošnih aktov organov in organizacij z ZTP-jem, usklajuje delovanje državnih organov, pristojnih za varnostno preverjanje, in predlaga ukrepe za izboljšanje varovanja tajnih podatkov; (5) Vodi evidenco dovoljenj za dostop do tajnih podatkov, evidenco izdanih dovoljenj fizičnim osebam za dostop do tujih tajnih podatkov, evidenco izdanih varnostnih dovoljenj organizacijam, evidenco izdanih varnostnih dovoljenj organizacijam za dostop do tujih tajnih podatkov in evidenco začasnih dostopov do tajnih podatkov ter (6) Organizira in izvaja usposabljanja s področja obravnavanja in varovanja tajnih podatkov in opravlja druge naloge, določene s predpisi, sprejetimi na podlagi ZTP-ja.

Seveda se urad ne ukvarja samo z varovanjem tajnih podatkov. Kje so tiste dodatne pristojnosti, ki jih izvajate v uradu?

Na 129. redni seji, dne 6. 4. 2017, je Vlada Republike Slovenije sprejela Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov. Ministrstva in vladne službe imenujejo osebe za koordinacijo kibernetske varnosti in navedeno sporočijo UVTP-ju. S tem sklepom se dopolni Sklep o ustanovitvi, nalogah in organizaciji UVTP-ja. Posledično se v skladu z navedenim sklepom in zakoni določijo strokovne naloge in organizacija UVTP-ja na področju kibernetske varnosti.

S tem se v skladu s Strategijo kibernetske varnosti vzpostavlja osrednjo koordinacijo nacionalnega sistema kibernetske varnosti in ne nazadnje se začenja vzpostavljati tudi pogoje za njegovo stabilno delovanje. Poleg nalog s področja kibernetske varnosti bo UVTP opravljal tudi vse dosedanje naloge na področju tajnih podatkov.

V okviru varnosti omrežij in informacijskih sistemov ter zagotavljanju obvladovanja incidentov na kibernetske grožnje ima velik pomen tudi zaščita kritične informacijsko komunikacijske infrastrukture, ki med drugim podpira tudi delovanje in upravljanje ostale kritične infrastrukture.

Kateri so po vaši oceni tisti ključni izzivi, ki se jim boste morali na UVTP v prihodnje posebej posvetiti?

Ključni izzivi UVTP-ja v prihodnosti - ohranjanje nacionalne kibernetske suverenosti je neločljivo povezano z zagotavljanjem nacionalne kibernetske varnosti. Z razvojem in naraščanjem pomena omrežij, informacijskih sistemov in komunikacijskih povezav je postajala suverenost nad nacionalnim kibernetskim prostorom vse pomembnejša. Države, ki se zavedajo suverenosti nad svojim kibernetskim prostorom, le tega varujejo in branijo. Navadno temu namenjajo na prvi pogled nesorazmerno velika sredstva. Vzrok za to je, da je zaradi globalne prepletenosti nacionalnih informacijskih sistemov in omrežij, zagotavljanje nacionalne kibernetske varnosti resnično zahtevna naloga. Problem je tako kompleksen, kot je zapleten preplet velikega števila informacijskih sistemov in komunikacijskih povezav oziroma sam kibernetski prostor. Nedvomno najpomembnejši in tudi najočitnejši vidik nacionalnega interesa suverenosti nad nacionalnim kibernetskim prostorom je suverenost nad nacionalno kritično informacijsko-komunikacijsko infrastrukturo, ki je še posebej pomembna, saj predstavlja podporno infrastrukturo vsem drugim kritičnim infrastrukturam.

Zagotavljanje kibernetske varnosti na državni ravni je močno povezano z izboljševanjem kibernetske varnosti na globalni ravni. Ker gre za skupen cilj, se države, med njimi tudi Republika Slovenija, povezujejo v varnostne integracije. Varnostne integracije zagotavljajo kolektivno kibernetsko varnost, ki je večja kot je kibernetska varnost posameznih, v integracijo vključenih držav. Po drugi strani pa je kolektivna kibernetska varnost v integracije vključenih držav zelo odvisna od kibernetske varnosti vsake posamezne države. Vključenost v določeno varnostno integracijo države v nobenem primeru ne razbremeni odgovornosti in skrbi za lastno kibernetsko varnost, le izboljša jo. V varnostne integracije vključene države, ki ne skrbijo dovolj za svojo kibernetsko varnost, so navadno deležne stopnjujočih se opozoril in drugih spodbud k ukrepanju, saj z nezagotavljanjem svoje kibernetske varnosti ne ogrožajo le sebe, temveč kibernetsko varnost celotne integracije, še posebej na področju nacionalne varnosti in gospodarstva.

Moderno dinamično varnostno okolje prinaša nove grožnje med katerimi so še posebej izpostavljene kibernetske grožnje. Nam lahko zaupate v katero smer boste v prihodnosti na uradu izvajali aktivnosti za obvladovanja teh tveganj?

Obvladovanje kibernetskih groženj oziroma za učinkovito izvajanje kibernetske varnosti je ključnega pomena sodelovanje vseh relevantnih deležnikov v okviru javne uprave in zasebnega sektorja. Pri tem je izrednega pomena zagotavljanje povezanosti oziroma sinergije med državnimi organi, zasebnim sektorjem in kibernetsko varnostjo. Vzpostaviti je potrebno sodelovanje z vsemi deležniki (industrija, raziskovalne inštitucije, združenja...). To se bo doseglo z vzpostavitvijo širšega foruma oziroma delovne skupine, v kateri bodo lahko sodelovali vsi pomembni deležniki s področja kibernetske varnosti. Da bi dosegli učinkovito medresorsko koordinacijo in sodelovanje z ministrstvi, agencijami in ostalimi, slednji določijo osebo za koordinacijo kibernetske varnosti v svoji ustanovi. UVTP predstavlja ključni in povezovalni element državnih zmogljivosti na področju kibernetske varnosti. Kot tak je odločilnega pomena za pripravljenost, ukrepanje, koordinacijo, izmenjavo informacij, usklajevanje in odzivanje na kibernetske grožnje oziroma incidente. Spremljal bo stanje na področju kibernetske varnosti vključno s poenotenim razumevanjem minimalnih standardov. Pri tem bo sodeloval z drugimi državnimi organi in koordiniral njihovo delo na tem področju. Organom bo predlagal ukrepe za izboljšanje kibernetske varnosti, jim svetoval, organiziral izobraževanja, odgovarjal na strokovna vprašanja ter v skladu s predpisi in sklepi Vlade RS opravljal druge naloge s področja kibernetske varnosti.

V okviru varnosti omrežij in informacijskih sistemov ter zagotavljanju obvladovanja incidentov na kibernetske grožnje ima velik pomen tudi zaščita kritične informacijsko komunikacijske infrastrukture, ki med drugim podpira tudi delovanje in upravljanje ostale kritične infrastrukture. Prekinitev delovanja ali uničenje kritične informacijsko komunikacijske infrastrukture neposredno ogrozi nacionalno varnost, kar ima lahko resne posledice za splošno varnost, gospodarstvo, ključne družbene funkcije, zdravje ter družbeno blaginjo. Zaradi tega je potrebno, da se predstavniki UVTP-ja vključijo tudi v zaključek usklajevanja osnutka Zakona o kritični infrastrukturi v Republiki Sloveniji.

Področje kibernetske varnosti je ključno za delovanje vseh sistemov in podsistemov – lahko rečemo ekosistema - moderne družbe, zato ga bo potrebno neprekinjeno spremljati in nadgrajevati v skladu s hitro spreminjajočim se okoljem. Priprava pravnih podlag za vzpostavitev nacionalnega organa za kibernetsko varnost je tako samo prvi korak v nizu ukrepov, ki bodo potrebni za zagotovitev višjega nivoja kibernetske varnosti, dolgoročno pa bodo potrebna znatno večja vlaganja v nacionalni sistem kibernetske varnosti. To so razlogi, da bo prva naloga UVTP-ja, da ob pomoči delovne skupine za prenos NIS direktive 2016/1148 z dne 6. julij 2016, ki jo ustanavlja Ministrstvo za javno upravo, in medresorske projektne skupine, pripravi Akcijski načrt izvajanja Strategije kibernetske varnosti, ki bo, poleg strokovnih rešitev in načrta izdelave pravne podlage, vseboval tudi predvidene kadrovske in finančno-materialne posledice pri vseh deležnikih. UVTP bo tako pripravil akcijski načrt in ga posredoval v potrditev Vladi RS. V akcijskem načrtu se bodo opredelile tudi prednostne naloge za obdobje do konca leta 2020.

Sprejeta je bila Strategija o zagotavljanju kibernetske varnosti. Kje v tem okviru vidite pomembno vlogo vašega urada?

Z vzpostavitvijo nacionalnega organa za kibernetsko varnost bo Republika Slovenija pričela izpolnjevati dano zavezo zvezi NATO o prioritetni krepitvi državnih zmogljivosti kibernetske varnosti (obrambe), ki jo je dal predsednik Vlade RS, ter v svoj pravni red pričela prenašati zahteve, ki jih nalaga Direktiva o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Evropski uniji (NIS direktive). V okviru NATO procesa obrambnega načrtovanja je Slovenija sprejela cilj zmogljivosti E5308, ki se nanaša na informacijsko varnost in kibernetsko varnost, ter cilj E6202, ki se nanaša na kibernetsko varnost in politiko zveze NATO o kibernetski obrambi. Republika Slovenija mora tudi kot članica Združenih narodov (OZN), Organizacije za varnost in sodelovanje v Evropi (OVSE) in Organizacije za ekonomsko sodelovanje in razvoj (OECD) izpolnjevati zahteve s področja kibernetske varnosti, za katere te organizacije predvidevajo oziroma pričakujejo, da jih bomo kot polnopravni člani spoštovali.



Področje kibernetske varnosti je ključno za delovanje vseh sistemov in podsistemov – lahko rečemo ekosistema - moderne družbe, zato ga bo potrebno neprekinjeno spremljati in nadgrajevati v skladu s hitro spreminjajočim se okoljem.

S tem se v skladu s Strategijo kibernetske varnosti vzpostavlja osrednjo koordinacijo nacionalnega sistema kibernetske varnosti in ravno tako se začenja vzpostavljati pogoje za njegovo stabilno delovanje. UVTP bo na strateški ravni koordiniral zmogljivosti za zagotavljanje varnosti omrežij in informacijskih sistemov ter obvladovanja incidentov na vseh ravneh v državi, predstavljal enotno kontaktno točko v okviru mednarodnega sodelovanja, zagotavljal usklajeno delovanje in partnerstvo vseh pristojnih deležnikov v javni upravi, spodbujal in podpiral sodelovanje z znanstveno-raziskovalnimi inštitucijami, spodbujal sodelovanje z gospodarskimi družbami in zagotavljal povezovanje in sodelovanje z ustreznimi partnerji na mednarodni ravni.

Trenutno so operativne zmogljivosti za odzivanje na kibernetske grožnje porazdeljene v SI-CERT. Kako v prihodnje vidite razvoj vladnega centra (SI-GOC CERT)? Bo imel po vaši viziji UVTP mesto v zgodbi vzpostavljanja tega vladnega centra?

Pomembno je sodelovanje in medsebojna podpora s Slovenskim centrom za posredovanje pri omrežnih incidentih SI-CERT na ARNES-u, razvijajočim se vladnim CERT-om ter ostalo mrežo CERT-ov kot tudi z Agencijo za komunikacijska omrežja in storitve Republike Slovenije (AKOS), Institutom „Jožef Stefan“ in ostalimi znanstveno-raziskovalnimi in izobraževalnimi institucijami ter subjekti kritične infrastrukture, ki se po potrebi vključujejo v načrtovanje in izvajanje dejavnosti kibernetske varnosti.

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

UVTP bo na strateški ravni izvajal in koordiniral zmogljivosti za zagotavljanje kibernetske varnosti na nižjih ravneh v državi, obenem pa predstavljal enotno kontaktno točko pri mednarodnem sodelovanju. Sodeloval bo z ustreznimi organi Evropske unije, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrbel za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb na področju kibernetske varnosti.

Izobraževanje in usposabljanje sta ključa procesa za zagotavljanje in dvigovanje ustrezne stopnje varnostne kulture in zavedanja med organizacijami javnega in gospodarskega okolja ter preko tega tudi širšega družbenega okolja. Kako ta segment glede na omejene kadrovske vire v vašem uradu še okrepiti?

Kot že rečeno - vzpostaviti je potrebno sodelovanje z vsemi deležniki (industrija, raziskovalne inštitucije, združenja...). Z razširitvijo pristojnosti UVTP-ja bo slednji lahko pričel s pripravo programov ozaveščanja državljanov o nevarnostih in tveganjih v kibernetskem prostoru ter izvedbo posvetov v zvezi z vključevanjem vsebin s področja kibernetske varnosti v šolski kurikulum in v učne programe izobraževalnih ustanov na vseh, še prav posebno pa na nižjih (osnovnošolska in srednješolska) ravneh izobraževalnega sistema.

Menite, da so lahko ustrezne referenčne institucije kot na primer Institut za korporativne varnostne študije, tisti dejavnik, ki bi v tem procesu izobraževanja in usposabljanja s področja tajnih podatkov in informacijske varnosti nudili tisto dodatno kvaliteto in zmogljivost, predvsem na področju gospodarskega in korporativnega okolja?

ICS je vsekakor dejavnik, ki na varnostnem področju generalno kot tudi na specifičnih področjih prispeva h krepitvi varnosti in varnostne kulture. Predstavlja namreč okolje, ki predstavlja platformo sodelovanja med javnimi in zasebnimi akterji ter s tem ponuja dodano vrednost, predvsem ko govorimo o korporativni varnosti. ICS z vpetostjo in sodelovanjem v regionalnem in mednarodnem okolju omogoča prisotnost in možnosti afirmacije naših najboljših varnostnih standardov in praks tudi širše od meja Republike Slovenije, kar je v današnjem dinamičnem okolju praktično nujno.

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

Pojem industrijska varnost v ožjem smislu zajema zagotavljanje varnostnih postopkov in ukrepov, potrebnih za doseganje ustrezne ravni varnosti tajnih podatkov, ki jih država izmenjuje z gospodarskimi družbami. Gre za vzpostavitev takega sistema varovanja, ki učinkovito preprečuje nepooblaščeno razkritje, uničenje, odtujitev, spreminjanje ali kakršno koli drugačno zlorabo tajnih podatkov, opreme, objektov oziroma kakršnega koli premoženja, ki ga želi država zavarovati. Področje industrijske varnosti je multidisciplinarno, saj prepleta elemente s področja osebne, fizične, tehnične, dokumentacijske in informacijske varnosti. Za doseganje ustrezne ravni varovanja tajnih podatkov so zato potrebni organizacijski, administrativni in drugi postopki, ki omogočajo celostno oziroma integralno varovanje. V širšem smislu lahko pri industrijski varnosti govorimo tudi o sposobnosti države, da vzpostavi ustrezno ravnovesje med zaščito lastnih gospodarskih, političnih ali varnostnih interesov ob hkratnem spodbujanju gospodarske konkurenčnosti.

Da lahko neka gospodarska družba dostopa do tajnih podatkov, katerih lastnik je Republika Slovenija, mora pridobiti ustrezno varnostno dovoljenje. Varnostno dovoljenje je administrativna potrditev, da gospodarska družba izpolnjuje pogoje za varno obravnavanje tajnih podatkov od najnižje do vključno tiste stopnje tajnosti, do katere ji je bilo varnostno dovoljenje izdano. V zadnjih nekaj letih je na tem področju opazen znaten premik oziroma vedno večje število gospodarskih subjektov, ki so v možnosti sodelovanja v projektih, ki zahtevajo ali vključujejo dostop do tajnih podatkov, prepoznali poslovno priložnost. V Sloveniji je danes tako že skoraj dvesto gospodarskih družb z varnostnimi dovoljenji, ki jim omogočajo sodelovanje pri tajnih naročilih.

Posedovanje varnostnega dovoljenja gospodarski družbi odpira tudi možnost sklepanja komercialnih pogodb, katerih izvedba pogojuje dostop do tajnih podatkov, z gospodarskimi družbami drugih držav, pri čemer pa je temeljnega pomena pogoj, da ima Republika Slovenija z zadevno državo sklenjen in veljaven varnostni sporazum.



Dvostransko sodelovanje in meddržavni dogovori o vzajemnem varovanju tajnih podatkov so ena od pomembnih vlog nacionalnega varnostnega organa, katerega naloge opravlja UVTP. Število gospodarskih družb s pridobljenimi varnostnimi dovoljenji za dostop do tujih tajnih podatkov vsako leto narašča, vendar številka še zdaleč ne kaže dejanske konkurenčnosti slovenskega gospodarstva. UVTP si zato v sodelovanju s pristojnimi resorji zelo prizadeva, da bi gospodarske družbe spodbudil k pridobivanju teh dovoljenj. S pridobljenim varnostnim dovoljenjem za dostop do tujih tajnih podatkov se gospodarskim družbam namreč odprejo tudi vrata za sodelovanje v razpisih zveze Nato in Evropske unije.

Zaradi nenehno spreminjajočega se globalnega varnostnega okolja je področje industrijske varnosti eno najbolj razvijajočih se in intenzivnih področij delovanja in sodelovanja nacionalnih varnostih organov, hkrati pa se na tem področju vsake spremembe tudi najhitreje pokažejo. Prožnost in prilagodljivost vseh sodelujočih sta zato izjemnega pomena. Zaradi usklajevanja dejavnosti, razreševanja odprtih vprašanj in sprejemanja usmeritev na področju industrijske varnosti se pristojni organi na nacionalni in mednarodni ravni povezujejo v različne oblike sodelovanja. Na nacionalni ravni je treba omeniti medresorsko projektno skupino za industrijsko in fizično varnost, v kateri sodelujejo predstavniki različnih resorjev, ki so vključeni v proces industrijske varnosti, na mednarodni ravni pa je poleg delovnih odborov in teles EU in Nata, ki ustvarjajo varnostno politiko tega področja, treba omeniti delovanje skupine MISWG.

Danes so za prepoznavanje raznih vrst ogroženosti in obvladovanje tveganj potrebna specifična znanja. Da bi UVTP dvignil raven varovanja tajnih podatkov in spodbudil razmišljanja o pomenu krepitve varnostne ozaveščenosti, je leta 2009 začel posebna usposabljanja vodilnih in za varnost odgovornih oseb iz gospodarskih družb z varnostnim dovoljenjem.

Poleg krepitve vezi med državo in gospodarskim sektorjem, ki je na področju varnosti tajnih podatkov ključnega pomena, je glavni namen takega usposabljanja približanje razumevanja koncepta varovanja vitalnih državnih interesov subjektom, ki se v procesu svojega delovanja srečujejo s tajnimi podatki. Poleg tega naj bi udeleženci navedenega usposabljanja pridobili tudi boljšo ozaveščenost o zaščiti lastnega znanja, inovacij in idej. Na tak način urad neposredno prispeva k zaščiti konkurenčnosti slovenskega gospodarstva, posredno pa k njegovi hitrejši gospodarski rasti in razvoju.

UVTP je eden izmed najbolj aktivnih korporativnih članov Slovenskega združenja korporativne varnosti. Kaj so po vaši oceni dodane vrednosti tovrstnega sodelovanja tudi v luči javno zasebnega sodelovanja?

Varovanje tajnih podatkov in kibernetska varnost ter trend naraščanja s tem povezanih varnostnih tveganj je realnost - izziv, kako se uspešno s tem soočati pa prav gotovo eden največjih izzivov državnih organov, poslovnih subjektov in uporabnikov v želji zavarovati podatke zaradi zakonskih, osebnih ali poslovnih razlogov pred nepoklicanimi osebami in posegi.

In prav tu nam korporativno članstvo v Slovenskem združenju korporativne varnosti predstavlja dodano vrednost, zlasti na segmentih javno zasebnega partnerstva.

Tudi na tem področju namreč velja pregovor Winstona Churchilla: »Attitude is a little thing that makes a big difference« (v prevodu: Odnos je majhna stvar, ki pomeni veliko razliko).

Naj zaključim s spoznanjem, da je v današnjem svetu intenzivno in kooperativno vseobsegajoče sodelovanje v odgovor gornjemu izzivu praktično nujnost. ■

Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij.

»Ab uno disce omnes (po enem spoznaj vse)«
»Ustvarjamo vezi, ki bogatijo
ter tako gradimo pot do uspeha!«

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.

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

SKUPAJ SMO MOČNEJŠI!

www.ics-institut.si

Avtor: izr. prof. dr. Denis Čaleta / Inštitut za korporativne varnostne študije*



KOLUMNA

denis.caleta@ics-institut.si

NUJNO SPREJETJE PARADIGME O CELOVITOSTI PRISTOPOV OBVLADOVANJA TVEGANJ

Ob vedno bolj zahtevnem varnostnem okolju si upravičeno zastavljamo vprašanje kdaj bomo sposobni dojeti potrebo po spremembi vzorcev odločanja in stopiti z odločnejšimi koraki v smeri celovitosti sistemskih pristopov obvladovanja tveganj.

Dnevno smo soočeni z varnostnimi tveganji, ki se vedno bolj dotikajo tudi našega okolja in na njih nismo več imuni. Primeri hekerskih vdorov v informacijske sisteme, odtekanje ključnih informacij iz naših organizacij, do zadnjega primera požara v podjetju Kemis kažejo na to, da strateška vodstva še vedno razpolagajo s premalo varnostnega zavedanja in prepuščajo delovanje svojih organizacij igri na srečo. Seveda v javnem sektorju stanje ni nič boljše. Sicer pa danes v tem kompleksnem globalnem okolju težko potegneš jasno mejo ločnico med javno in zasebno odgovornostjo za še vedno nizko stanje na področju varnosti. Zato se upravičeno lahko vprašamo, kako poenotiti sistemske ukrepe, ki bodo v prihodnje stanju varnosti v naši državi dale pomemben zagon in predstavljale korak v pravi smeri. Poglejmo si dva najbolj očitna primera, kje so, tako na javnem kakor tudi gospodarskem področju, bistvene rezerve.

Na področju strateškega vodenja v javnem sektorju Vladi Republike Slovenije nikakor ne uspe poenotiti sistemskih korakov, ki bi pripeljali do ustreznejšega zakonskega okvira na področju zagotavljanja nacionalne varnosti. Le ta bi v pomembnem delu prisilil tudi strateški management v tistih gospodarskih okoljih, ki upravljajo s ključnimi infrastrukturnimi zmogljivostmi, k treznejšemu in odločnejšemu zagotavljanju predpogojev za zagotavljanje učinkovitejšega obvladovanja tveganj. Občutek razpršenosti korakov in idej, brez jasnega skupnega cilja, se kaže v pristopih pri pripravi nujno potrebnih zakonskih okvirov na področju zaščite kritične infrastrukture, informacijske in posledično kibernetske varnosti, zamujanja z implementacijo skupaj dogovorjenih varnostnih rešitev na evropskem nivoju, da stanja na področju obveščevalno-varnostne dejavnosti sploh ne omenjamo. Vsi ti procesi priprave posameznih predpisov nam jasno kažejo, da je nacionalna varnost v Republiki Sloveniji razdeljena med posamezne resorje, ki zaradi različnih dejavnikov in vzrokov med seboj niso sposobni ali pripravljeni sodelovati. K doseganju parcialnih ciljev jih vodijo ozki interesi, ki pa niso nujno tudi interesi usmerjeni v skupno zagotavljanje nacionalne varnosti. Vsekakor pa manjka strateški pogled in sposobnost poenotenja vseh parcialnih rešitev v skupno smer zagotavljanja nacionalnega strateškega interesa, na drugi strani pa racionalizacija in preprečevanje podvajanja določenih pristojnosti in odgovornosti. Vsekakor je to v prihodnosti ključnega pomena, še posebej v državi kot je Republika Slovenija, kjer je zaradi omejenosti ključnih virov, to nujno potrebno. Zadnja od nerazumnih korakov pa je vsekakor nezmožnost ureditve ovrednotenja poklicnih struktur na področju nacionalne varnosti. Nedopustno je, da se zaradi nesposobnosti celovitega urejanja tega sistema ponovno neti spor med ključnimi institucijami na področju nacionalne var-

Vsekakor pa manjka strateški pogled in sposobnost poenotenja vseh parcialnih rešitev v skupno smer zagotavljanja nacionalnega strateškega interesa, na drugi strani pa racionalizacija in preprečevanje podvajanja določenih pristojnosti in odgovornosti.

*avtor je član Slovenskega združenja korporativne varnosti



Vsak del integralnega varnostnega sistema, ki se nam na prvi pogled zdi še tako nepomemben, lahko v določenih izrednih situacijah prepreči velike škodne dogodke. Človeški potencial pa še vedno ostaja osrednji del, ki s svojim delovanjem bistveno vpliva na učinkovitost takega sistema.

nosti. Dolžnost vseh, še posebej pedsednika Vlade republike Slovenije je, da nemudoma poseže v te aktivnosti in se z vsemi udeleženimi za zaprtimi vrati uskladi o ustreznem vrednotenju poklicev policista, vojaka in drugih na tem področju pomembnih poklicev. Tisti z malo daljšim zgodovinskim spominom, kot je zadnji mandat te vlade, se še spomnimo kako katastrofalne posledice je tej mladi demokraciji prinesel spor med ministrstvoma za notranje zadeve in obrambo, takoj po nastanku naše države. Kompleksnost groženj, s katerimi smo soočeni, od vseh institucij zahteva skupno delovanje, ki ne bo zastrupljeno s sencami dvoma, kdo je bolje plačan in bolj pomemben za to državo. Na žalost je v državi s tako omejenimi viri pomemben prav vsak del tega sistema, ki bo v celoti lahko zagotovil ustrezno varno okolje za nadaljnji razvoj družbe in posledično tudi gospodarstva.

Če pogledamo samo primer iz gospodarskega okolja, ki v zadnjem obdobju odpira žolčne javne razprave o ustreznem obvladovanju tveganj. Seveda ob tem ne moremo zaobiti primera tragičnega požara v Kemisu. Vendar se zaradi omejenosti prostora ne bomo dotikali nadzornih institucij in zakonodaje ter vprašanj, kako je možno, da je na tako občutljivem naravnem in vodovarstvenem območju sploh možno dobiti dovoljenje za opravljanje take gospodarske dejavnosti, kot je predelava nevarnih odpadkov. Predvsem se bomo dotaknili pomanjkanja celovitih ukrepov na področju zagotavljanja korporativne varnosti, ki jih lahko najdemo v velikem številu ostalih gospodarskih organizacij v naši državi. Ne moremo trditi, da podjetje ni vlagalo v posodobitev svojih prostorov, saj so bili proizvodnji prostori relativno novi in moderno opremljeni. Seveda pa je potrebno vsako stvar pogledati bolj podrobno in se vprašati ali so bili visoki vložki v modernizacijo infrastrukture in varnostnih sistemov ustrezni in predvsem sistemski. Po zdaj zbranih podatkih, ki so prišli v javnost s strani strokovnjakov iz različnih institucij, ki so raziskovali vzrok za nastanek požara, lahko potegnemo določene zaključke, ki potrjujejo našo bojazen, da je bil sistem zagotavljanja tehnične in fizične varnosti, v povezavi s protipožarnimi ukrepi nezadosten in v reakciji ob začetku požara ni odreagiral tako kot bi bilo potrebno. Seveda bodo dokončni podatki dali več informacij, ki bodo omogočile temeljito analizo, iz katere upam, da bodo vsi odgovorni potegnili ustrezne izkušnje in zaključke. Včasih ni dovolj, da za vzpostavitev tehničnih sistemov strateško vodstvo nameni samo dovolj finančnih sredstev, temveč mora zagotoviti, da se v podjetju vzpostavi integralni varnostni sistem. Ob tem je potrebno takoj jasno povedati, da imamo v naših organizacijah velik problem zagotoviti ustrezne korporativno varnostne strokovnjake, ki so sposobni takega sistemskega pogleda in same vzpostavitve tega sistema. Če pa se k vzpostavitvi takega sistema pristopi skozi parametre najnižje cene ali pa, da take sisteme dizajnirajo sami ponudniki varnostnih storitev in tehničnih sistemov, največkrat dobimo finančno predimenzioniran sistem, ki pa ne zadosti niti minimalnim kriterijem integralnosti. Posplošeno bi lahko ocenili, da investitor za relativno visoke finančne vložke dobi zelo nizek in močno pomanjkljiv integralni varnostni sistem, ki ni sposoben učinkovitega obvladovanja celega niza tveganj, katerim so danes izpostavljene naše organizacije. Seveda je potrebno jasno priznati, da tudi gospodarski sektor ni imun na vrtičkarstvo pristojnosti in odgovornosti posameznih struktur znotraj poslovnih organizacij, ki omejujejo hitrejšo pot do celovitih in učinkovitih pristopov na področju obvladovanja tveganj.

Zgoraj navedena sta samo dva primera, ki smo jih, kot opozorilo na neustrezne slabe prakse varnostnega zavedanja strateških vodstev v javnem in gospodarskem okolju podali v razmislek in razpravo strateški in strokovni javnosti. Vsak del integralnega varnostnega sistema, ki se nam na prvi pogled zdi še tako nepomemben, lahko v določenih izrednih situacijah prepreči velike škodne dogodke. Človeški potencial pa še vedno ostaja osrednji del, ki s svojim delovanjem bistveno vpliva na učinkovitost takega sistema. ■

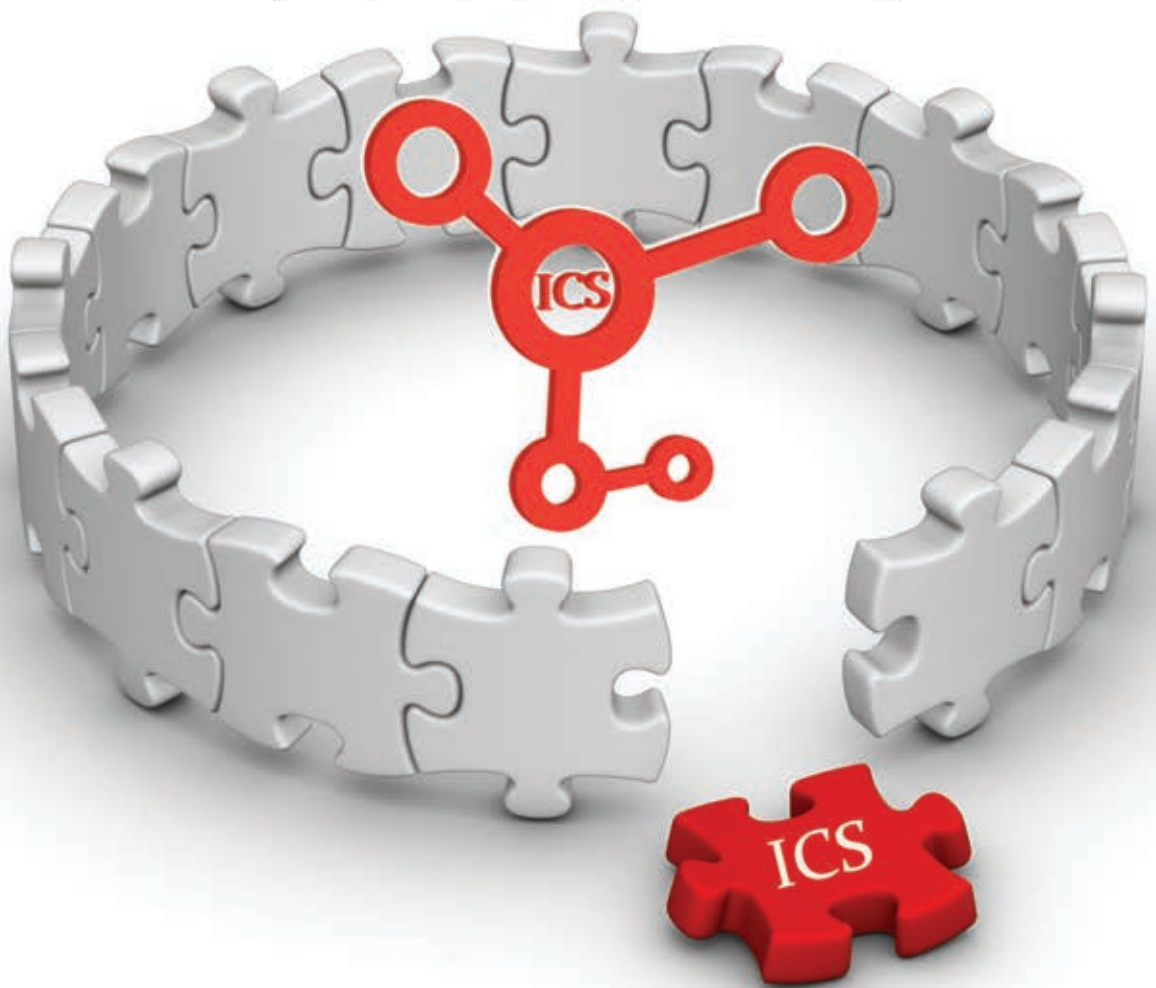
9. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 14.—15. marec 2018

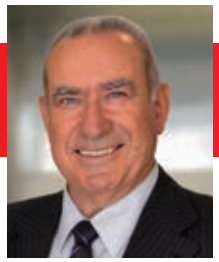


DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

SPROŠČENO VZDUŠJE, ODLIČNI PREDAVATELJI, MEDIJSKA ODZIVNOST,
IZMENJAVA NAJNOVEJŠIH SPOZNANJ IN DOBRIH PRAKS.
STROKOVNJAKI KORPORATIVNE VARNOSTI,
KI VLAGAJO V ZNANJE, BODO Z NAMI.
PRIDRUŽITE SE NAM TUDI VI!

WWW.ICS-INSTITUT.SI

Avtorja: doc. dr. Milan Vršec, mag. Miran Vršec /
Inštitut za korporativne varnostne študije*





REVIZIJA VARNOSTNIH SISTEMOV V KRITIČNI INFRASTRUKTURI

Morda je sedaj, ko je Zakon o kritični infrastrukturi v fazi obravnave in sprejemanja in ko so podane že skoraj vse evropske in nacionalne pravne podlage za upravljanje evropske in nacionalne kritične infrastrukture pravi čas, da naredimo korak k implementaciji sprejete regulative.

Ugotavljamo namreč, da vse aktivnosti, ki se nanašajo na izboljšanje zaščite in neprekinjenega delovanja kritične infrastrukture potekajo relativno počasi - tako na evropski kot tudi na nacionalni ravni. To ima do neke mere za posledico, da so tovrstne aktivnosti tudi v Sloveniji (pre)počasne. Poleg tega lahko rečemo, da izredni dogodki – tako teroristični in kriminalni kot tudi naravne nesreče – prehitevajo aktivnosti, ki se nanašajo na strategije, cilje in metodologije izboljšanja zaščite kritične infrastrukture. Poznavalec upravljanja korporativne varnosti v kritični infrastrukturi - ob povedanem - dobi občutek, da malokoga prav resno skrbi prenova varnostnih mehanizmov in zagotavljanje neprekinjenega poslovanja sektorjev kritične infrastrukture. Tako v tem kontekstu naletimo na dve vprašanji: Prvo se nanaša na pripravljenost Vlade RS ter nosilcev in lastnikov kritične infrastrukture na prenovo varnostnih sistemov v posameznih sektorjih kritične infrastrukture, drugo pa se nanaša na vprašanje, kako pristopiti k reviziji varnostnih sistemov vzpostavljenih na področju kritične infrastrukture.



Odgovor na obe vprašanji se v temelju ponuja v smeri vzpostavitve: prvič, vladnega projekta »*Prenova varnostnih sistemov v kritični infrastrukturi*«; drugič, »*Imenovanje prodorne ter z znanjem, izkušnjami, delovno vnemo in odgovornostjo pripravljene projektne skupine*« in tretjič, »*Sprejetje ustrezne metodologije za oceno ranljivosti, ogroženosti in varnostnih tveganj za celovito in dolgoročno zagotavljanje neprekinjenega poslovanja in za oblikovanje učinkovitih varnostnih in drugih ukrepov*«. Potemtakem gre za projekt, ki bi pokazal na učinkovitost obvladovanja ranljivosti, varnostnih groženj, varnostnih tveganj in obstoječih varnostnih mehanizmov, kot nadgradnja pa bi sledilo oblikovanje učinkovitejših stalnih in dodatnih varnostnih ukrepov, ki bi prispevali k vzdrževanju procesov neprekinjenega delovanja in poslovanja posameznih sektorjev kritične infrastrukture. Pred Vlado RS, nosilci, lastniki in upravljavci kritične infrastrukture je torej zahtevna in odgovorna naloga; kajti od te naloge je odvisno ali bo prišlo do dodane vrednosti (dviga ravni varnosti in zaščite) v že vzpostavljenih varnostnih sistemih kritične infrastrukture. Izboljšanje zaščite kritične infrastrukture pa je navsezadnje pomembno tudi z vidika doseganja višje ravni nacionalne varnosti in suverenega obvladovanja kriznega upravljanja.

*avtorja sta člana Slovenskega združenja korporativne varnosti



Pravna in druga izhodišča

Temeljno in vsebinsko pravno podlago predstavlja evropska regulativa urejanja zaščite kritične infrastrukture ter Resolucija o strategiji nacionalne varnosti Republike Slovenije (Ur. l. RS, št. 27/2010), ki določa varnostno politiko in varnostno strategijo zagotavljanja nacionalne varnosti. V tej resoluciji je kritična infrastruktura opredeljena takole: »*Različnim virom ogrožanja je v sodobnem času še posebej izpostavljena kritična infrastruktura, ki s svojim delovanjem zagotavlja izvajanje ključnih funkcij države. S tega vidika lahko tudi ogroženost kritične infrastrukture vpliva na nacionalno varnost Republike Slovenije. S terorističnimi napadi in drugimi grožnjami, motnjami, blokadami in povzročeno škodo na področju kritične infrastrukture se lahko resno ogrozi zdravje, varnost ali blaginja državljanov ter nemoteno delovanje države in javnih službe*« (člen 4.3.5). »*Republika Slovenija bo zaradi zagotovitve učinkovitega delovanja kritične infrastrukture vzpostavila enotno načrtovanje ukrepov za njeno zaščito v različnih razmerah. To načrtovanje bo temeljilo na medresorsko usklajenem zaznavanju ogrožanja kritične infrastrukture države in zagotavljanju ustreznega odzivanja na te grožnje*« (člen 5.4.5). Temeljno pravno izhodišče pa bo predstavljal Zakon o kritični infrastrukturi in podzakonski akti izdani na njegovi podlagi. Ta zakon ne bo »zaključek«, temveč šele pravi začetek skrbi za kritično infrastrukturo tako z vidika izboljšanja varnostnih mehanizmov, kot tudi z vidika izboljšanja poslovne učinkovitosti in konkurenčnosti sektorjev (berimo gospodarskih družb) kritične infrastrukture. To bi moral biti strateški interes Vlade RS, nosilcev, lastnikov, upravljavcev in konkretnega menedžmenta kritične infrastrukture.

Poleg temeljnega pravnega izhodišča je treba povedati, da je za varnostne mehanizme v kritični infrastrukturi pomembna tudi druga zakonodaja, kot denimo: Zakon o varstvu pred naravnimi in drugimi nesrečami, Zakon o varstvu pred požarom, Zakon o varnosti in zdravju pri delu, Zakon o varstvu okolja, Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih, Zakon o zasebnem varovanju in še mnogi drugi zakoni. Prav tako ne smemo zanemariti uvajanje varnostnih in drugih standardov v poslovne procese kritične infrastrukture.

V izhodišča revizije varnostnih sistemov v kritični infrastrukturi uvrščamo tudi nekatere projekte (tiste, ki so navedeni v virih tega prispevka in druge), v katerih je veliko koristnih ugotovitev in usmeritev, kako izboljšati zaščito, varnost in neprekinjeno delovanje kritične infrastrukture. Kar nekaj ugotovitev in napotkov pa izhaja tudi iz projektov obeh avtorjev tega prispevka, ki so se nanašali na projektiranje integralnih varnostnih sistemov v nekaterih gospodarskih družbah, ki so pomemben del kritične infrastrukture.

Kritična infrastruktura državnega pomena

Sektorji kritične infrastrukture Republike Slovenije (sklep Vlade št. 80200-2/2013/3, z dne 9. 1. 2014), so naslednji:

- *Sektor kritične infrastrukture, ki zagotavlja energetsko podporo,*
- *Sektor kritične infrastrukture, ki zagotavlja prometne povezave,*

- *Sektor kritične infrastrukture, ki zagotavlja preskrbo s hrano,*
- *Sektor kritične infrastrukture, ki zagotavlja preskrbo s pitno vodo,*
- *Sektor kritične infrastrukture, ki zagotavlja zdravstveno oskrbo,*
- *Sektor kritične infrastrukture, ki zagotavlja finance,*
- *Sektor kritične infrastrukture, ki zagotavlja varstvo okolja,*
- *Sektor kritične infrastrukture, ki zagotavlja informacijsko in komunikacijsko podporo.*

V predlogu Zakona o kritični infrastrukturi / 6. člen) pa beremo: »*Sektorji kritične infrastrukture so preskrba z vodo, preskrba s hrano, preskrba z energijo, zdravstvena oskrba, finančni sektor, promet, varstvo okolja, delovanje organov oblasti na državni ravni in informacijsko-komunikacijska podpora*«. Poleg določitve sektorjev kritične infrastrukture je Vlada RS določila tudi prioriteto delovanja sektorjev, ki izhaja iz soodvisnosti in medsebojnega vpliva sektorjev kritične infrastrukture, kajti motnje v delovanju enega sektorja lahko bistveno vplivajo na delovanje drugih sektorjev. Po prioritetah delovanja, oziroma neposrednem vplivu na delovanje drugih sektorjev, je kritična infrastruktura razvrščena po naslednjem prioritetnem vrstnem redu (sklep Vlade RS, št. 80200-2/2013/3, z dne 9.1.2014):

- *Zagotavljanje električne energije;*
- *Informacijsko komunikacijska podpora;*
- *Preskrba s pitno vodo;*
- *Preskrba s hrano;*
- *Zagotavljanje zdravstvene oskrbe;*
- *Preskrba z naftnimi derivati;*
- *Zagotavljanje železniškega prometa;*
- *Zagotavljanje letalskega prometa;*
- *Delovanje pristaniške dejavnosti;*
- *Preskrba s plinom;*
- *Delovanje plačilnega prometa;*
- *Zagotavljanje oskrbe z gotovino;*
- *Delovanje državnega proračuna;*
- *Varovanje zdravega okolja.*

Iz vladnih opredelitev kritične infrastrukture in določitvijo prioritet torej lahko sklepamo, da se ve v katerih gospodarskih in državnih področjih je treba zagotoviti trajnostni razvoj varnostnih mehanizmov in pogoje za neprekinjeno delovanje gospodarskih družb (z Banko Slovenije vred) in nekaterih državnih organov v vseh razmerah.

Pristop k reviziji varnostnih sistemov

Z revizijo varnostnih sistemov v kritični infrastrukturi mislimo na celovit pristop od Vlade RS imenovane projektne ekipe, izbranega referenčnega zunanjega izvajalca za revidiranje varnostnih sistemov in preglede urejenosti neprekinjenega delovanja posameznih sektorjev kritične infrastrukture. Ko govorimo o reviziji mislimo na izdelavo posnetkov obstoječega stanja na strateškem in operativnem nivoju upravljanja z varnostnimi tveganji, analizo stanja, oblikovanje ugotovitev, predstavitev predlogov rešitev in izboljšav ter načina njihove implementacije v obstoječe rešitve.



Ključna vprašanja pri tem so:

1. Ali je obstoječa varnostna dokumentacija skladna z veljavno evropsko in nacionalno regulativo in kot taka zagotavlja ustrezen pravni okvir za zaščito kritične infrastrukture?
2. Ali je potrebno izdelati vsebinski okvir za izdelavo (ali prenovo obstoječih) dokumentov načrtovanja zaščite kritične infrastrukture?
3. Ali je potrebno vzpostaviti projekt revizije obstoječih varnostnih sistemov v kritični infrastrukturi?
4. Ali je potrebno izdelati metodologijo za ocenjevanje in analiziranje ranljivosti, ogroženosti in varnostnih tveganj v kritični infrastrukturi?

Najin odgovor na prvo vprašanje je, da obstoječa varnostna dokumentacija v veliki meri ni ustrezna, ker je z vidika raznih zakonov in metodologij nepregledna, neusklajena, zelo slabo upravljana in daje zelo malo sinergijskih učinkov. Na drugo vprašanje se ponuja odgovor, da je potrebno pripraviti enoten vsebinski okvir prenove obstoječih varnostnih dokumentov, kjer je treba stremeti za tem, da se upoštevajo vse dobre rešitve in dosedanje prakse in povezane zakonodaje. Odgovor na drugo vprašanje je izhodišče za odgovor na tretje vprašanje, pri katerem se je treba sprijazniti z vzpostavitvijo vladnega projekta, ki bi zagotovil dvig ravni zaščite kritične infrastrukture in njenega neprekinjenega delovanja tudi v kriznih razmerah. Odgovor na četrto vprašanje daje podlago za enotno, celovito in dolgoročno upravljanje z varnostnimi tveganji v kritični infrastrukturi. Da, nujno je potrebno izdelati metodologijo za ocenjevanje in analiziranje ranljivosti, ogroženosti in varnostnih tveganj v kritični infrastrukturi, saj je to edini način, da bo Vlada RS na nacionalnem nivoju - ne glede na sektor ali dejavnost posamezne gospodarske družbe - zagotovila enotnost, preglednost, celovitost in dolgoročnost upravljanja z varnostnimi tveganji in posledično neprekinjenost delovanja kritične infrastrukture. V tem okviru predlagamo določene aktivnosti za Vlado RS kot glavnega usmerjevalca delovanja kritične infrastrukture, za ministrstva in Banko Slovenije, kot nosilce delovanja kritične infrastrukture in za upravljavce kritične infrastrukture kot neposredno odgovorne za delovanje posameznih sektorjev kritične infrastrukture.

> Revizija varnostnih sistemov v gospodarskih družbah, ki upravljajo s kritično infrastrukturo bi morala biti poslovni, ekonomski in strokovni interes, kajti med drugim gre za zagotavljanje neprekinjenega poslovanja in zakonitega delovanja tudi v kriznih razmerah. Z drugimi besedami gre za ohranjanje poslovne uspešnosti, vzdrževanje konkurenčnosti in za preprečevanje škod in izgub na dolgi rok.

VLADA RS:

- vzpostavi projekt revizije varnostnih sistemov v kritični infrastrukturi,
- imenuje projektno ekipo za vodenje projekta - ekipo vodi svetovalec vlade odgovoren za vodenje projektov, člani pa so državni sekretar v Ministrstvu za obrambo, Ministrstvu za notranje zadeve in v Ministrstvu za gospodarstvo,
- pripravi metodologijo za ocenjevanje in analiziranje ranljivosti, ogroženosti in varnostnih tveganj v kritični infrastrukturi - metodologijo lahko pripravi projektna ekipa,





- pooblasti enega od državnih sekretarjev v vsakem ministrstvu, da se aktivno vključi v izvedbo projekta prenove varnostnega sistema sektorja katerega nosilec je, pri čemer ima tudi nalogo, pooblastila, kompetence in odgovornost za upravljanje z varnostnimi dokumenti,
- izbere referenčnega zunanjega izvajalca, ki bo na podlagi pogodbe opravljal posnetke in analize stanja, podajal ugotovitve in rešitve ter izdelal varnostne elaborate z vsemi potrebnimi varnostnimi dokumenti,
- zagotovi finančne pogoje za izvedbo projekta.

NOSILCI KRITIČNE INFRASTRUKTURE – 14 ministrstev in Banka Slovenije:

- ministri in vodstvo Banke Slovenije podprejo projekt vlade, imenovanje projektne ekipe in izbor zunanjega izvajalca projekta,
- vsako ministrstvo in Banka Slovenije določi enega od državnih sekretarjev, da se aktivno vključi v izvajanje projekta ter medsektorsko sodelovanje v sistemu in procesih zaščite kritične infrastrukture,
- vsako ministrstvo v okviru nadzornega organa (inšpekcije ali drugega) vzpostavi učinkovit nadzor nad sistemi upravljanja z ranljivostjo, ogroženostjo in varnostnimi tveganji, vzpostavljenimi varnostnimi sistemi ter sistemi zagotavljanja neprekinjenega delovanja in kriznega vodenja.

UPRAVLJAVCI KRITIČNE INFRASTRUKTURE - gospodarske družbe, banke in druge organizacije v kritični infrastrukturi:

- v skladu z metodologijo, ki jo pripravi Vlada RS ter v skladu z napotki projektne skupine in zunanjega izvajalca zgoraj omenjenega projekta aktivno sodelujejo v ocenjevanju, analiziranju in prenovi obstoječih varnostnih dokumentov in varnostnega sistema kot celote,
- vodstvo posameznega upravljavca napoti vsaj enega ali dva iz obstoječega varnostnega menedžmenta v ustrezen magistrski izobraževalni program za pridobitev potrebnih znanj in kompetenc za upravljanje varnostnega sistema in korporativne varnosti na strateškem in operativnem nivoju,
- upravljavci morajo nosilce, projektno ekipo in zunanjega izvajalca izvedbe vladnega projekta o reviziji varnostnih sistemov obvestiti o tem, ali imajo kot zavezanci za obvezno organiziranje varovanja izdelano oceno tveganja ter programe in načrte varovanja po Zakonu o zasebnem varovanju in podzakonskih aktih izdanih na njegovi podlagi.

Revizija varnostnih sistemov v gospodarskih družbah, ki upravljajo s kritično infrastrukturo bi morala biti poslovni, ekonomski in strokovni interes, kajti med drugim gre za zagotavljanje neprekinjenega poslovanja in zakonitega delovanja tudi v kriznih razmerah.

Z drugimi besedami gre za ohranjanje poslovne uspešnosti, vzdrževanje konkurenčnosti in za preprečevanje škod in izgub na dolgi rok.

Zagotavljanje neprekinjenega poslovanja kritične infrastrukture

Iz predloga Zakona o kritični infrastrukturi je razvidno, da je temeljni namen zakona sistemsko urediti zagotavljanje neprekinjenega delovanja kritične infrastrukture RS, pri čemer se izhaja iz razumevanja, da zaščita kritične infrastrukture obsega vse aktivnosti, ki prispevajo k neprekinjenosti in celovitosti njenega delovanja (2.1 Cilji). Vlada RS, nosilci, lastniki in upravljavci kritične infrastrukture so torej dolžni poskrbeti za neprekinjeno poslovanje sektorjev kritične infrastrukture tako, da bodo delovali ob, med in po izrednem dogodku in tudi v morebitnih kriznih razmerah, ko se politika, država, gospodarstvo, civilna družba in prebivalstvo že sooča z nastalo ekonomsko, poslovno, človeško in moralno škodo in izgubo. K vzpostavljanju neprekinjenega poslovanja pa je treba pristopiti celovito. Vsaka nedoslednost se hitro maščuje, če ne prej pa ob nastanku konkretnega izrednega dogodka. Celovitost pristopa pa pomeni, da je treba v sklopu sistema kakovosti po ISO 9000 in po analizi ranljivosti, varnostnih groženj in varnostnih tveganj ter v okviru opredelitve kateri poslovni procesi so ključni za ohranitev neprekinjenega poslovanja, uvesti v poslovne procese primerne standarde, in sicer: standard ISO 22301 – prej BS 25999 (z Demingovo metodo vred), ki zagotavlja osnovno metodologijo vzpostavljanja neprekinjenega poslovanja, standard varovanja informacij ISO/IEC 27000, protipožarne standarde, standarde pristopne kontrole, protivlomne kontrole, videonadzora in druge varnostne standarde že sedaj predpisane standarde na področju zasebnega varovanja. Tista gospodarska družba v kritični infrastrukturi, ki stremi za poslovno odličnostjo, mora med drugim upoštevati tudi standarde družbene odgovornosti, standarde upravljanja s človeškimi viri in strankami, standarde na področju ekologije, morda pa tudi uvesti model 20 ključev in sistema uravnoteženih kazalnikov BSC. Za obvladovanje kriznega vodenja pa je potrebno pripraviti krizni načrt (z načrtom kriznega komuniciranja vred), določiti vsaj eno tajno rezervno lokacijo za vodenje neprekinjenega poslovanja in v okviru tega zagotoviti tudi neprekinjeno fizično in tehnično varovanje in druge oblike varovanja, ki zagotavljajo obvladovanje varnostnih tveganj (več o tem Vršec, 2011). Tiste gospodarske družbe, državni organi in druge organizacije s področja kritične infrastrukture, ki imajo pogodbeno angažirane zunanje izvajalce varovanja in zaščite, pa morajo od teh izvajalcev zahtevati, da se odgovorno vključijo v sistem neprekinjenega poslovanja in varovanja.

Vzpostavitev varnostnega menedžmenta

Če že govorimo o izboljšanju varnostnih mehanizmov v kritični infrastrukturi - kar v prvi vrsti zahteva že evropska regulativa - ne moremo mimo vprašanja kdo, kako in na podlagi česa ter kako kakovostno in učinkovito upravlja z varnostjo ter z neprekinjenim delovanjem in poslovanjem posameznih sektorjev kritične infrastrukture. Govorimo o kakovostnem varnostnem menedžmentu upravljanja s korporativno varnostjo v kritični infrastrukturi brez katerega si na dolgi rok ne moremo zamišljati pravočasnega in učinkovitega prepoznavanja ranljivosti, varnostnih groženj, varnostnih tveganj, profesionalnih odzivov na izredne dogodke in obvladovanja kriznega upravljanja. Nosilci in upravljavci kritične infrastrukture namenjajo premalo pozornosti tovrstnemu menedžmentu tako z vidika kadrovanja kot tudi z vidika izobraževanja in usposabljanja. Pri našem proučevanju varnostnega menedžmenta v kritični infrastrukturi opažamo, da je tovrstni menedžment močno podhranjen na točki ustreznosti izobrazbe in na točkah nedoraslosti poznavanja in obvladovanja celovite varnostne stroke, celovitih (integralnih) varnostnih sistemov, poznavanja široke palete varnostne zakonodaje, varnostnih standardov, standardov neprekinjenega poslovanja ter suverenega obvladovanja varnostnih groženj, varnostnih tveganj, odzivov na izredne dogodke in kriznega upravljanja. S tega vidika je kadrovanje v varnostni menedžment kritične infrastrukture za upravljavce oziroma za vodstva gospodarskih družb v kritični infrastrukturi izjemno pomembno in zahtevno opravilo, kajti imenovani posamezniki za to funkcijo prihajajo v zelo kompleksen sistem kritične infrastrukture. Zato je potrebno stremeti za kadri, ki imajo ustrezno izobrazbo in širino in so nato s strani - bodisi nosilcev, lastnikov ali upravljavcev - napoteni na izobraževanja za pridobitev ustreznih znanj. Kajti za napredek izboljšanja zaščite kritične infrastrukture so potrebni podiplomsko izobraženi varnostni menedžerji, ki so na strateški ravni in na nižjih ravneh sposobni obvladovati varnostna tveganja in upravljati integralni varnostni sistem. Ena od možnosti je vsekakor udeležba na magistrskem programu Management korporativne varnosti, ki nudi vsa potrebna znanja in dobro prakso za upravljanje celovitih varnostnih sistemov v kritični infrastrukturi ter v ostalem gospodarstvu in državnih organih. To dejstvo predstavlja preprosto potrebo za doseganje kakovostnejšega varnostnega menedžmenta, ki bo motiviran in sposoben upravljati z vsemi varnostnimi mehanizmi in izzivi, za katere je v prvi vrsti odgovoren najvišji menedžment v kritični infrastrukturi. S tega zornega kota je najbrž ta najvišji menedžment skupaj z lastniki zainteresiran tudi za kakovostno upravljanje korporativne varnosti. Gre torej za

Pri našem proučevanju varnostnega menedžmenta v kritični infrastrukturi opažamo, da je tovrstni menedžment močno podhranjen na točki ustreznosti izobrazbe in na točkah nedoraslosti poznavanja in obvladovanja celovite varnostne stroke, celovitih (integralnih) varnostnih sistemov, poznavanja široke palete varnostne zakonodaje, varnostnih standardov, standardov neprekinjenega poslovanja ter suverenega obvladovanja varnostnih groženj, varnostnih tveganj, odzivov na izredne dogodke in kriznega upravljanja.



upravljanje korporativne varnosti na bazi sprejetih varnostnih dokumentov kot so: varnostne politike, varnostne strategije, načrti fizičnega in tehničnega varovanja, načrti evakuacij, protipožarni načrti, načrti neprekinjenega poslovanja, krizni načrti, načrti kriznega komuniciranja in drugi specifični načrti glede na področje (sektor) kritične infrastrukture. To pomeni, da je treba 12. člen predloga zakona o kritični infrastrukturi razumeti v širšem kontekstu, to pomeni, da je treba v načrtovanje zaščite kritične infrastrukture - poleg ocene tveganja - uvrstiti vse ukrepe zaščite, od obvladovanja naravnih nesreč, požarov, nesreč in notranjih deviantnih pojavov vse do obvladovanja zunanjih izrednih dogodkov terorističnega in kriminalnega značaja.

Vlada RS, nosilci, lastniki in upravljavci kritične infrastrukture, še posebej pa varnostni menedžment bi se moral zavedati, da je pri načrtovanju zaščite kritične infrastrukture (pa tudi sicer) izredno pomembno poznavanje odvisnosti med ranljivostjo, varnostnimi grožnjami, varnostnimi tveganji in škodljivimi posledicami zanemarjanja tega vprašanja (več o tem Vršec in Vršec, 2016). Če varnostni menedžment v kritični infrastrukturi tega ne obvlada je neustrezno pripravljen pri načrtovanju varnostnih ukrepov in kriznega vodenja in ga je treba zamenjati ali napotiti na ustrezno izobraževanje ali usposabljanje. Da je to zelo pomembna premisa obvladovanja varnostnih mehanizmov pokaže (denimo) tudi obrazec »Risk = (function of) (CVT consequences-vulnerabilities--threat) (Cronin, Marion, 2012:9). Tudi obrazec »Tveganje = nevarnost oziroma grožnja (sprožilni dogodki) + Ranljivost (Hellstrom, 2006:6, v Prezelj in drugi, 2008), na splošen način definira, kaj je varnostno tveganje. Skratka, tuje literature o ranljivosti, varnostnih grožnjah in varnostnih tveganjih v kritični infrastrukturi je na pretek, zato jo priporočamo varnostnemu menedžmentu v slovenski kritični infrastrukturi.

Zaključek

Mislimo in verjamemo, da se bodo - takoj po sprejetju Zakona o kritični infrastrukturi – Vlada RS, nosilci, lastniki in upravljavci kritične infrastrukture lotili vseh potrebnih aktivnosti, ki izhajajo iz omenjenega zakona in drugih političnih, pravnih ter strokovnih izhodišč. Glavno besedo mora imeti Vlada RS kot gonilna sila implementacije zelo široke regulative pri vzpostavljanju trajnostnega razvoja varnostnih mehanizmov v kritični infrastrukturi. Ob tem ni morda odveč misel, da se v načrtovanju prihodnje zaščite kritične infrastrukture ni dobro opirati na oceno, da je Slovenija varna država, ki obvladuje globalno, regionalno in nacionalno varnostno okolje. S tega vidika lahko postavimo tudi drugo (sicer) drzno vprašanje: »*Ali se je Slovenija sposobna suvereno spoprijemati s prihajajočimi varnostnimi grožnjami in varnostnimi tveganji iz vseh okolij in na vseh ravneh?*«. Za ilustracijo utemeljitve tega vprašanja navajamo ugotovitev iz Sklepov strateškega pregleda obrambe 2016, kjer se postavlja vprašanje, kje so vzroki za to, »*da sposobnost za spoprijemanje s prihodnjimi varnostnimi tveganji in grožnjami ni na pričakovani ravni*« (Ministrstvo za obrambo - Sklepi strateškega pregleda obrambe, št. 80400-1/2016/6, z dne 22. 12. 2016). Če je to vprašanje aktualno na obrambnem področju, zakaj ne bi bilo aktualno tudi na širokem varnostnem področju. S tega vidika vse kaže, da čaka Vlado RS, nosilce, lastnike in upravljavce kritične infrastrukture, na področju izboljšanja zaščite kritične infrastrukture, še veliko dela.

Viri

- Cronin Kelley, Marion E. Nancy (2016). Critical Infrastructure Protection: Risk Management, and Resilience: A Policy Prspective,. CRS Press Taylor&Francis Inc.
- Projekt/raziskava: Prezelj, Iztok in drugi (2008). Definicija in zaščita kritične infrastrukture v Republiki Sloveniji. Končno raziskovalno poročilo. Ljubljana, oktober 2008. FDV.
- Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji. Vlada, 11. 7. 2014.
- Vršec Milan (2011). Pomen neprekinjenega poslovanja za poslovno učinkovitost organizacije, s poudarkom na kritični infrastrukturi. Ljubljana. Inštitut za korporativne varnostne študije.
- Vršec Milan, Vršec Miran (2016). Ranljivost, varnostne grožnje in varnostna tveganja si podajajo roke. Korporativna varnost, št. 12 2016. Ljubljana. Inštitut za korporativne varnostne študije.
- Zakon o kritični infrastrukturi. Predlog. Vlada RS, 30. 12. 2016-EVA 2015-1911-0001.
- Zakon o evidentiranju gospodarske infrastrukture. Osnutek. Vlada RS, 2. 2. 2016-EVA 2016-2550-0001. ■

V vsakem FORD-u je malo **MUSTANGA**.

SUMMIT AVTO
NAJVEČJI FORD SALON V SLOVENIJI



Ford
Go Further

Uradna poraba goriva: 8,0-13,6 l/100 km. Uradne specifične emisije CO_2: 179-306 g/km. Emisijska stopnja: Euro 6b, uradne emisije NOx: 0,0195-0,0183 g/km, specifične emisije trdih delcev: 0,00271-0,00222 g/km, število delcev: 2,8 x 10^{11}. Ogljikov dioksid (CO_2) je najpomembnejši toplogredni plin, ki povzroča globalno segrevanje. Emisije onesnaževal zunanjega zraka iz prometa pomembno prispevajo k poslabšanju kakovosti zunanjega zraka. Prispevajo zlasti k čezmerno povišanim koncentracijam prizemnega ozona, delcev PM_{10} in $PM_{2,5}$ ter dušikovih oksidov. Slika je simbolična.

SUMMIT AVTO d.o.o., Flajšmanova 3, 1000 Ljubljana
Telefon: 01 25 25 125, e-pošta: prodaja@summitavto.si

Avtor: mag. Anton Travner / direktor inštituta DCAF Ljubljana



IZZIVI NOVIH UKREPOV NA SCHENGENSKI MEJI

Uredba Evropskega parlamenta in Sveta o spremembi Uredbe 2016/399 (Zakonik Unije o pravilih, ki urejajo gibanje oseb preko meja - že dopolnjen in spremenjen Schengenski zakonik) je v javnosti dvignila veliko prahu, jeze, negodovanj, zanimanja in komentarjev.

Medtem, ko je večina slovenske laične javnosti (predvsem osrednji mediji) valila krivdo na bruseljsko administracijo, so hrvaški mediji, vključno s hrvaško politiko, v duhu siceršnjih medsosedskih odnosov zastoje na mejah pripisovali slovenski domnevni nefleksibilnosti in spoštovanje pravnega reda EU prikazovali kot namerno nagajanje Slovenije. Za razumevanje kaj uredba sploh prinaša je najprej treba pogledati kako in zakaj je do sprejema tako "drastičnih" sprememb Schengenskega zakonika sploh prišlo.

Že iz samega naslova uredbe je razvidno, da gre za pravni akt, ki sta ga sprejela Evropski parlament in Svet (torej države članice, kjer sta primerno zastopani tako Slovenija kot Hrvaška). Skladno z zakonodajnim postopkom je besedilo sprememb pripravila Evropska komisija, vendar predlog ni bil deležen bistvenih sprememb ne po razpravah v parlamentu, ne po razpravah na Svetu. Iz javnih nastopov političnih predstavnikov Slovenije je sicer moč razbrati, da naj bi Slovenija nasprotovala sprejemu besedila uredbe kot je bila na koncu sprejeta, vendar je iz javno dostopnih dokumentov o postopku sprejemanja uredbe, ki se nahajajo na spletni strani: http://eur-lex.europa.eu/procedure/EN/2015_307 moč razbrati, da sta tako Slovenija, kot Hrvaška zgolj opozorili na morebitne posledice[1], obe državi pa sta besedilo uredbe podprli in dne 7.3.2017 za sprejem tudi glasovali[2]. Iskanje grešnega kozla v Bruslju je torej zgolj metanje peska v oči in preprosto zavajanje javnosti. Kot je razvidno iz dokumenta o glasovanju, so besedilo uredbe soglasno podprle vse države članice, ki so glasovale (25), torej tudi Hrvaška in Slovenija.

Drugo vprašanje, ki se v zvezi s sprejetjem uredbe pojavlja pa je vprašanje, zakaj je do tako drastičnih sprememb sploh prišlo? Medtem, ko na eni strani strokovna in laična javnost v Sloveniji in Hrvaški ugotavlja, da je učinkovitost sprejetih ukrepov v nesorazmerju s posledicami, ki se manifestirajo v daljših, oziroma občasno zelo dolgih čakalnih dobah tako na meji med Slovenijo in Hrvaško, še bolj pa na mejah med Hrvaško in Srbijo, Hrvaško in BiH ter Hrvaško in Črno Goro, pa ima sprejeta uredba pozitivne (predvsem politične) učinke v državah EU, ki nimajo kopenske zunanje meje. Po podatkih EUROSTATa[3] se zelo varno počuti le 28,4% prebivalcev EU. V Sloveniji je ta odstotek občutno večji in znaša 44,7%, kar nas uvršča na sedmo mesto. Najbolj varne se počutijo na Malti (66,4) in najmanj v Litvi (9,8). Teroristični napadi in migracijski pritisk na občutek varnosti že v osnovi delujeta negativno. Predvolilni boji v Nemčiji, Franciji, na Nizozemskem in vrsti drugih evropskih držav pa so vprašanje varnosti povzdignili na piedestal brez primere. Medijske kampanje, v glavnem povezane z volitvami in vse večjim vplivom skrajno desnih ali celo radikalno desnih političnih strank so strah pred migracijami in v tej navezi tudi terorizmom posledično povezale z varovanjem zunanjih meja EU. Težišče dojemanja varnosti se je na splošno premaknilo v smeri, da varovanje zunanjih meja unije ni dovolj učinkovito in da so potrebni bistveno bolj drastični ukrepi. Zahte-

Po mnenju avtorja tega članka je bilo ravnanje držav v obdobju doslej največjega migracijskega vala na balkanski poti nedopustno, saj je v EU pod pretvezo humanitarne katastrofe vstopilo preko milijon tujcev, pri čemer identiteta večine teh ljudi ni bila nikoli ugotovljena, prav tako pa večina tujcev ni izpolnjevala pogojev za mednarodno zaščito, kar se je potrdilo kasneje.

vam in pričakovanjem po učinkovitejši kontroli meja so vlade (ne glede na politično usmerjenost levo – desno), večine držav sledile skoraj brez izjem. Pri tem se spomnimo postavitve tehničnih ovir (kar je v bistvu hudo olepšano ime za bodečo žico) na meji med Slovenijo in Hrvaško, še pred tem pa so na zunanji meji ograje postavile Madžarska, Bolgarija in Makedonija, kasneje pa so temu vzorcu sledile še nekatere druge države. Ko ravno govorimo o ograji je zanimivo, a redko omenjano dejstvo, da sta Ceuta in Maleila (španski mesti na afriški celini) že desetletja obdani z visokimi žičnimi ogradami, s katerimi se bolj ali manj uspešno blaži migracijski pritisk na kontinentalno Evropo.

Migracijski val po balkanski poti v letu 2015 in 2016 ter uvedba migracijskega koridorja sta splošno mnenje, da "schengen" ne deluje, samo še podkrepila. Po mnenju avtorja tega članka je bilo ravnanje držav v obdobju doslej največjega migracijskega vala na balkanski poti nedopustno, saj je v EU pod pretvezo humanitarne katastrofe vstopilo preko milijon tujcev, pri čemer identiteta večine teh ljudi ni bila nikoli ugotovljena, prav tako pa večina tujcev ni izpolnjevala pogojev za mednarodno zaščito, kar se je potrdilo kasneje. Zaradi migracijskega pritiska so celo skandinavske države, ki so bile tradicionalno naklonjene imigracijam, uvedle mejno kontrolo na notranjih mejah. Ad hoc so mejno kontrolo na notranjih mejah uvedle Avstrija, Nemčija, Danska, Švedska in Norveška. Kljub temu, da se je število migrantov, ki so v EU prihajali po balkanski poti od marca 2016 drastično zmanjšalo, je dvanajstega maja 2016 Svet na predlog Evropske Komisije sprejel sklep o uvedbi začasnega nadzora na notranjih mejah. Ta ukrep, ki predstavlja sicer dovoljeno a izjemo odstopanje od splošnih načel schengenskega pravnega reda, je še vedno v veljavi in je nedavno bil celo podaljšan za dodatnih 6 mesecev.

Uvedba mejne kontrole na notranjih mejah je najbolj radikalen ukrep, ki tako de iure kot de facto temeljito posega v "razkošje" neoviranega potovanja znotraj EU. Kljub temu, da vsi ostali atributi schengenskega pravnega reda ostajajo nespremenjeni, je ravno opustitev mejne kontrole in popolnoma neovirano prečkanje državnih meja znotraj EU privilegij, ki ga večina Evropejcev najbolje prepozna in ceni. Zdi se torej paradoksalno, da so državljani Avstrije, Nemčije, Danske, Švedske in Norveške pristali na ponovne mejne kontrole na svojih nacionalnih mejah in se odpovedali privilegiju

Uvedba mejne kontrole na notranjih mejah je najbolj radikalen ukrep, ki tako de iure kot de facto temeljito posega v "razkošje" neoviranega potovanja znotraj EU.

neoviranega prehajanja v sosednje države, ki so prav tako del schengenskega prostora. Razlog za pristajanje volilnega telesa na take ukrepe mora biti dovolj realen in otipljiv, nakazuje pa ga indikator padanja občutka varnosti, na kar vpliva prepričanje, da varovanje na zunanjih mejah ni zadostno in učinkovito.

Po mnenju avtorja tega članka je razlog za sprejetje sprememb Schengenskega zakonika predvsem v tem, da se omili občutek o pomanjkljivosti mejne kontrole na zunanjih mejah in da bodo spremembe, ki jih prinaša uredba pozitivno vplivale na stanje varnosti v celotni EU.

Za Slovenijo, državljane in prebivalce Slovenije je strateškega pomena, da mejnih kontrol na notranjih mejah ni. Ob resnem tveganju, da bi zaradi varnostnih izzivov, ki so jih neposredno, še bolj pa posredno (zaradi zlorabe vprašanja migracij v dnevno-politične interese) povzročila migracijska gibanja "padel schengen", je potrebno ponovno uvedbo mejnih kontrol na notranjih mejah in spremembo uredbe pogledati kot celoto. V kolikor bi Slovenija tvegala in ne bi podprla sprejema uredbe, bi jasno pokazala, da zunanje meje ni sposobna varovati, kot to zahteva večina prebivalcev EU, s tem pa bi odprla Pandorino skrinjico argumentov za potrebnost mejne kontrole na notranjih mejah schengenskega prostora.

Dejstvo je, da bosta uredba in z njo spremenjen režim mejne kontrole na zunanjih mejah ostala. Mejni prehodi med Slovenijo in Hrvaško so bili načrtovani skladno s takrat veljavno zakonodajo in takrat veljavnimi standardi. Temu primerno so bile prilagojene tudi kadrovske in tehnične okrepitve. Glede na število[4] potnikov, ki prečkajo mejo med Slovenijo in Hrvaško, ukrepov kot izhajajo iz zgoraj navedene uredbe niti teoretično, kaj šele praktično ni možno izvajati v celoti. Po mnenju avtorja obstaja vrsta možnih alternativnih rešitev, ki bi lahko ublažile negativne učinke spreme-



njenega režima mejne kontrole. Glede na to, da je malo manj kot tretjina vseh potnikov, ki so prečkali mejo s Hrvaško državljanov Slovenije (precej pa je tudi državljanov RH) bi z ustreznim obveščanjem in preusmerjanjem na manjše in manj obremenjene mejne prehode lahko ob konicah zmanjšali čakalne dobe na velikih mejnih prehodih. Z nekaj inovativnosti in v dobrem sodelovanju s hrvaško mejno policijo so možni še nekateri drugi ukrepi, medtem, ko je opuščanje mejne kontrole skrajni ukrep, ki ima lahko dolgoročno zelo hude in negativne posledice[5].

Dolgoročna in trajna rešitev je vstop Hrvaške v schengenski sistem in s tem odprava mejnih kontrol na slovensko-hrvaški meji. Hrvaška se intenzivno pripravlja za ponoven krog schengenskih evalvacij[6]. Če bodo obiski posebnih skupin visoko strokovno usposobljenih ocenjevalcev, ki bodo prihajali na Hrvaško od jeseni dalje potrdili, da sosednja država zadostuje vsem zahtevanim standardom, potem lahko v najboljšem in precej optimističnem primeru, vsaj teoretično, pričakujemo skorajšen vstop Hrvaške v schengensko območje. Zagotovo je to v interesu Slovenije. Zavedati pa se je potrebno, da je poleg izpolnjevanja tehničnih zahtev to tudi izjemno, ali celo predvsem politično vprašanje. Bolgarija in Romunija sta evalvacije uspešno prestali že pred leti, vendar države članice niso našle političnega soglasja, da bi sprejele ti dve EU članici tudi v schengensko družbo. Ob zgoraj navedenih političnih razlogih za uvedbo mejne kontrole na notranjih mejah in razlogih za sprejem sprememb režima mejne kontrole obstajajo resni pomisleki, ali bodo države članice uspele zbrati toliko zaupanja, da bodo sprejele tudi Hrvaško v prestižni schengenski krog. Pričakujemo pa lahko tudi pogojevanja vstopa Hrvaške z vstopom Romunije in Bolgarije. Takšna pogojevanja bi odločitev še dodatno otežila in po vsej verjetnosti precej zavlekla.

Časovna komponenta vstopa Hrvaške v schengenski prostor je torej negotova. Možnosti za vstop bi se lahko po optimističnem scenariju odprle ob koncu naslednjega leta, zaradi notranjepolitičnih razlogov držav članic EU pa bi se lahko uresničil tudi pesimistični scenarij, po katerem bo vstop zamaknjen v nedoločno prihodnost. Druge države zahodnega Balkana se intenzivno približujejo EU in izpolnjevanju standardom. Pomik schengenske meje na meje Srbije, Bosne in Hercegovine ter Črne Gore, bo pozitiven tudi za državljane teh držav, saj se bo območje brez kontrole povečalo. Izkušnje Hrvaške bodo zagotovo izjemno pomembno »učno gradivo« in pripomoček ostalim državam iz regije, v kolikor se zaradi drugih interesov proces širjenja EU ne bo ohlajeval še naprej.

1 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6570_2017_ADD_1&from=EN

2 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7067_2017_INIT&from=EN

3 http://ec.europa.eu/eurostat/web/gdp-and-beyond/quality-of-life/data/economic-physical-safety

4 v letu 2016 je zunanjo kopensko mejo v RS prečkalo 63.568.173 potnikov

5 Pogosto opuščanje mejne kontrole je lahko argument za podaljšanje mejne kontrole na meji z Avstrijo, lahko pa bi na podlagi tega argumenta kontrolo uvedle še Italija in Madžarska

6 V RH je bil že opravljen en krog evalvacij, vendar so strokovnjaki ugotovili, da RH ne izpolnjuje pogojev za vstop v schengensko območje. V nasprotju s Hrvaško, se je Slovenija v času pred prvo evalvacijo ustrezno pripravila in že po prvi evalvaciji dobila pozitivno oceno, zaradi česar popravnih evalvacij, ko je to v primeru sosednje države ni bilo. ■



Avtorji: Informacijski pooblaščenec RS, SI-CERT, ICS-Ljubljana

SLOVENIJA NUJNO POTREBUJE USTREZNO UREDITEV ODGOVORNEGA RAZKRIVANJA VARNOSTNIH RANLJIVOSTI

Informacijski pooblaščenec Republike Slovenije, nacionalni center SI-CERT in Inštitut za korporativne varnostne študije (ICS) so z namenom iskanja odgovorov na izzive, povezane s številnimi primeri razkritij ranljivosti informacijskih sistemov in omogočanja široke javne razprave o pomembnih vprašanjih informacijske varnosti organizirali posvet z okroglo mizo.

Gostje okrogle mize, ki jo je moderiral izr. prof. dr. Denis Čaleta (ICS) so bili Gorazd Božič (SI-CERT), dr. Sabina Zgaga (Ustavno sodišče RS), mag. Damijan Marinšek (Ministrstvo za javno upravo), Tadej Vodopivec (Comtrade d.o.o.), dr. Matej Kovačič (Institut Jožef Stefan/Slo–Tech) in Izidor Rojs (Specializirano državno tožilstvo). Uvodoma je informacijska pooblaščenka Mojca Prelesnik izpostavila ključna vprašanja, na katera bi organizatorji posveta želeli dobiti odgovore, nato pa so udeleženci okrogle mize vsak s svojega strokovnega vidika osvetlili problematiko (ne) odgovornega razkrivanja varnostnih ranljivosti.

Eno od izhodišč posveta je ugotovitev, da veljavna zakonodaja v Republiki Sloveniji področja odgovornega razkrivanja ranljivosti oz. t.i. etičnega hekanja izrecno ne ureja, hkrati pa upravljavci sistemov in velikih zbirk osebnih podatkov (tako v javnem kot tudi zasebnem sektorju) skrbi za varnost teh sistemov velikokrat posvečajo premalo pozornosti. To dokazujejo številni primeri razkritij varnostnih ranljivosti v zadnjem času.

> Absolutna kriminalizacija vsakršnega nenaročenega testiranja informacijskih sistemov (tudi odgovornega in dobronamernega) bi bila po mnenju mnogih zato celo nevarna, ker oteži hitro in učinkovito prepoznavanje varnostnih ranljivosti preden pride do resnega zlonamernega vdora.

Ni zanemarljivo, da so se države in korporacije razkritij varnostnih ranljivosti v preteklosti dolgo celo aktivno branile, s tem pa preprečevale, da se zaščiti tiste, ki ranljivost odgovorno razkrijejo, posameznike, ki jih ranljivost prizadene (ker so nezakonito razkriti npr. osebni ali drugi varovani podatki) ter upravljavce. Kot je opozoril eden od gostov, so kibernetski napadi za krepitev varnosti informacijskih sistemov primerljivi z blažjimi boleznimi, ki krepijo imunski sistem. Manjši napadi so zato posledično koristni, ker omogočajo izboljševanje varnosti in pravočasno odpravljanje ranljivosti ter boljšo odzivnost in pripravljenost na ukrepanje v primeru večjih, zlonamernih napadov. Absolutna kriminalizacija vsakršnega nenaročenega testiranja informacijskih sistemov (tudi odgovornega in dobronamernega) bi bila po mnenju mnogih zato celo nevarna, ker oteži hitro in učinkovito prepoznavanje varnostnih ranljivosti preden pride do resnega zlonamernega vdora. Udeleženci posveta so se upoštevajoč navedeno strinjali, da obstoja odgovornega razkrivanja varnostnih ranljivosti danes ne bi več smeli gledati zgolj čez prizmo kaznivega dejanja napada na informacijski sistem, kot ga določa 221. člen Kazenskega zakonika[1]. V svetu je namreč sprejeto, da pri *odgovornem* razkrivanju načeloma ne gre za kaznivo dejanje.

Kot okvirno definicijo etičnega hekanja oz. odgovornega odkrivanja varnostnih ranljivosti sta bila v okviru posveta izpostavljena dva temeljna pogoja: da ni protipravne koristi (lahko je pregled vnaprej naročen in plačljiv); in ni namena škodovati (namen je etična dejavnost).

Kot okvirno definicijo etičnega hekanja oz. odgovornega odkrivanja varnostnih ranljivosti sta bila v okviru posveta izpostavljena dva temeljna pogoja: da ni protipravne koristi (lahko je pregled vnaprej naročen in plačljiv); in ni namena škodovati (namen je etična dejavnost). V zvezi s tem je bilo v razpravi izpostavljeno, da odsotnost pravne ureditve pomeni tudi pomembna in zelo nevarna tveganja, da raziskovalec (nehote) poseže predaleč v sistem in posledično ogrozi sistem ali celo kritično infrastrukturo, če na strani tistih, ki iščejo ranljivosti ni nujnega zavedanja o vseh vidikih odgovornosti za morebitne posledice. Prav tako v takih primerih ni zavarovanja za morebitno nenamerno povzročeno škodo.

Pri urejanju odgovornega razkrivanja je treba upoštevati, da neurejeno stanje ovira, če ne celo kriminalizira tudi dobronamerne varnostne strokovnjake. Če bodo preveč v strahu za svoja ravnanja, potem ne bo odkrivanja varnostnih ranljivosti oz. še huje, te bodo izkoriščali subjekti iz javnega in zasebnega sektorja za svoje namene. Zanikanje obstoja varnostnih lukenj ne pomeni, da jih ni, temveč to, da za njih vedo osebe, ki z njimi nimajo legitimnih namenov. Na dolgi rok bo treba vplivati tudi na spremembo miselnosti upravljavcev sistemov, ki (tudi) odgovornega razkrivanja ne vidijo kot dobronamernega, temveč zanikajo varnostne pomanjkljivosti, se ob njihovem odkritju počutijo napadene in zoper prijavitelje sprožajo pravne postopke.

Razprava je pokazala, da ni enoznačnega odgovora na vprašanji, kdaj je ranljivost dopustno javno razkriti (upoštevajoč pravice prizadetih posameznikov ter dodatna tveganja in/ali škodo, ki jo takšna javna objava lahko povzroči) in kateri so primerni časovni okviri, ki jih morajo imeti na voljo upravljavci sistemov, da lahko ustrezno reagirajo na izpostavljeno ranljivost. Nobenega dvoma namreč ni, da v primeru velikih sistemov prepoznanih napak ni mogoče odpraviti čez noč. Obstaja pa različno razumevanje tega, kaj je skrajni rok, do katerega se mora upravljavec odzvati in poskrbeti za odpravo ranljivosti (različni standardi opredeljujejo rok 30/45/60/90 dni). Različna pa so tudi stališča o tem, kaj storiti, če upravljavec pozive preprosto ignorira. Izkušnje iz preteklih razkritij ranljivosti tako v Sloveniji kot drugih državah namreč kažejo, da marsikatero podjetje ali druga institucija brez javnega pritiska ne ukrepa dovolj resno, po drugi strani pa v primeru kompleksnih aplikacij lahko nadgradnja kljub hitremu odzivu traja tudi dlje kot 30 dni. Kot je bilo izpostavljeno v razpravi, se je informacijska varnost v državni upravi v zadnjih letih sicer izboljšala, vendar pa se vezanost na sistem javnega naročanja v teh primerih pogosto izkaže kot resna ovira pravočasnega ukrepanja. Prav tako pa bi morala država narediti več za stalno spremljanje informacijske varnosti. Za podjetja je v tem okviru pomembna



gospodarska priložnost razvoj zasebnosti prijaznih rešitev in izdelkov, ki imajo varstvo osebnih podatkov in širše zasebnosti vgrajeno že v osnovi.

Udeleženci posveta so bili soglasni, da je skrajni čas, da se tudi v Sloveniji naredi korak naprej tako na ravni pravne regulacije oz. postavitve pravnega okvira odgovornega razkrivanja varnostnih ranljivosti, kot tudi v smeri dviga ozaveščenosti odgovornih o nujnosti hitrega ukrepanja ob razkritju. Obstoječo definicijo kaznivega dejanja napada na informacijski sistem bi namreč dejansko lahko razumeli kot absolutno kriminalizacijo vsakršnega, tudi odgovornega prepoznavanja varnostnih ranljivosti informacijskih sistemov, ki pušča zelo majhne (tako rekoč nične) možnosti za izključitev protipravnosti v primeru naročenih testov ranljivosti ali obstoja skrajne sile. Pravnega instituta, ki bi posebej v teh primerih izključeval protipravnost, namreč ni. Zgolj na posameznem državnem tožilcu tako leži odgovornost za presojo ali obstajajo v posameznem primeru okoliščine, ki upravičujejo odločitev, da se kljub obstoju vseh znakov kaznivega dejanja bodisi kazenski pregon odloži, bodisi se kazenskega pregona ne začne ali se od pregona odstopi. To pa ne zagotavlja nobenih varovalk za zaščito posameznikov, ki so varnostne ranljivosti razkrili.

Tudi novi pravni okviri na ravni EU, ki že veljajo (t.i. NIS direktiva - o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov ter Splošna uredba o varstvu osebnih podatkov) zahtevajo odločnejše ukrepe za njihovo uveljavitev na nacionalni ravni in predvsem tudi ustrezno koordinacijo med različnimi organi, ki so pristojni za nadzor in ukrepe, ki jih ti instrumenti prinašajo. Čaka pa nas še uredba o zasebnosti v elektronskih komunikacijah, ki je v fazi priprave in se bo deloma tudi dotaknila tega področja.

Iz živahne razprave je mogoče izluščiti naslednje nujne spremembe predpisov, s katerimi bi morala država:

- Opredeliti, kdaj lahko sploh govorimo o odgovornem razkrivanju varnostnih ranljivosti (namen, premoženjska korist, odgovornost, dolžnosti glede nadaljnjega razkrivanja) in kdaj ne;
- opredeliti ustrezen pravni institut, ki bi določal, kdaj in pod katerimi pogoji bi v določenih primerih lahko šlo za izključitev protipravnosti dejanja odgovornega razkrivanja;



- zakonsko določiti, kakšni so možni ukrepi za zaščito posameznikov, ki so varnostne ranljivosti razkrili;
- opredeliti, kakšen in kako hiter mora biti odziv upravljavca sistema, na katerem so bile ranljivosti prepoznane;
- zagotoviti ustrezno statistično beleženje kazenskega pregona tovrstnih kaznivih dejanj s ciljem prepoznave pomanjkljivosti, vzorcev sistemskih težav in pogostosti teh pojavov;
- jasnejše opredelitve vloge upravljavcev, lastnikov sistemov pri izkazovanju ustrezne skrbnosti za redno preverjanje varnosti sistemov;
- nedvoumno opredeliti, komu morajo zavezanci glede na različne ureditve poročanja o varnostnih incidentih v različnih sektorjih in na različnih področjih poročati o posameznih kršitvah (Splošna uredba o varstvu podatkov, NIS direktiva (enako pa velja tudi za prihajajočo uredbo o zasebnosti v elektronskih komunikacijah).

Sklepno so udeleženci posveta soglašali, da posvet ne bi smel biti zadnji, saj so tovrstne široke razprave, na katerih sodelujejo predstavniki različnih deležnikov tako podjetij, varnostnih strokovnjakov, pravnikov, državnih organov in drugih zainteresiranih, nujne.

Na podlagi ugotovitev posveta so organizatorji z izpostavljenimi ugotovitvami in pozivom k čimprejšnji pravni ureditvi področja seznanili pristojni ministrstvo za pravosodje in ministrstvo za javno upravo ter jih pozvali k čimprejšnji pravni ureditvi področja. Udeleženci so se tudi strinjali, da bi organizatorji v prihodnje še naprej morali aktivno prispevati k nadaljevanju javne razprave o posameznih temah zagotavljanja varnosti informacijskih sistemov s sodelovanjem vseh deležnikov. ■

Avtor: Andrej Maslo / Pošta Slovenije d.o.o.*



POLOŽAJ IN VLOGA KRIZNEGA ŠTABA POŠTE SLOVENIJE PRI OBVLADOVANJU IZREDNIH DOGODKOV V POŠTI SLOVENIJE

V Pošti Slovenije smo izdelali Načrt kriznega delovanja v Pošti Slovenije, ki v primerih resnih nevarnosti in groženj v okolju, omogoča ustrezen odziv na nastale razmere in prehod podjetja v krizno, izredno delovanje ter uspešno obvladovanje razmer.

Izhodišča koncepta kriznega štaba in kriznega delovanja v Pošti Slovenije

Pošta Slovenije (v nadaljevanju: PS) je vpeta v dinamično in hitro spreminjajoče se okolje, zaradi česar je tudi podvržena številnim notranjim in zunanjim virom ogrožanja. Ti lahko predstavljajo nevarnost za zdravje in življenje zaposlenih v PS in njenih strank, nevarnost za premoženje PS, kot tudi nevarnost za nemoteno izvajanje procesov v podjetju. V PS so kot pomembni viri ogrožanja izpostavljene naslednje skupine groženj: naravne nesreče, kriminalna dejanja, tehnološke nesreče, izpadi in napadi na informacijske vire, zdravstvene nevarnosti ter družbeno-politične in socialne napetosti v PS in njenem okolju.

V pogojih resnih nevarnosti in groženj je ključnega pomena, da se sprejemajo ustrezne odločitve, hitro in pravočasno. Poslovodstvo PS je zato sprejelo odločitev, da se ustanovi Krizni štab Pošte Slovenije (v nadaljevanju: krizni štab), katerega glavna funkcija je, da v pogojih resnih nevarnosti in groženj, zagotavlja

V pogojih resnih nevarnosti in groženj je ključnega pomena, da se sprejemajo ustrezne odločitve, hitro in pravočasno.

načrtno in sistematično upravljanje z razmerami, skladno z vnaprej predvidenimi postopki in ukrepi.

Temeljna izhodišča koncepta kriznega štaba in kriznega delovanja v Pošti Slovenije so bila tako naslednja:

- Načrt kriznega delovanja v PS je krovni dokument na področju kriznega delovanja. Načrt predstavlja okvir organiziranega, nadzorovanega in usklajenega prehoda družbe na izredno delovanje.
- Namestnik vodje kriznega štaba je upravitelj in skrbnik Načrta kriznega delovanja Pošte Slovenije.
- V kriznem delovanju ima osrednjo vlogo krizni štab, katerega člani odločajo, koordinirajo, delegirajo, analizirajo in vrednotijo ukrepe in naloge za obvladovanje groženj v PS.
- Vloga kriznega štaba je, da se v času kriznega delovanja ukvarja izključno z nastalimi problemi, povezanimi z izrednimi dogodki, medtem ko poslovodstvo še naprej skrbi za normalno in tekoče poslovanje PS.
- Za delovanje kriznega štaba so pomembni vsi zaposleni v PS, kakor tudi zunanja javnost ter alarmni in nadzorni mehanizmi, ki so vzpostavljeni tako v PS kot tudi v njenem okolju. Pomembno vlogo pri podpori delovanja kriznega štaba imajo Nadzorni center PS, Forum za varovanje informacij (v zadevah informacijske varnosti) ter Svet za korporativno upravljanje s tveganji (telo, ki se v PS ukvarja s poslovnimi in operativnimi tveganji na različnih področjih). Prav tako je pri tem pomembno, da so pri delovanju kriznega štaba jasne komunikacijske poti, ki zagotavljajo (1) pravočasno zaznavo in prijavo virov ogrožanja, (2) nadaljnje procesiranje prijave na

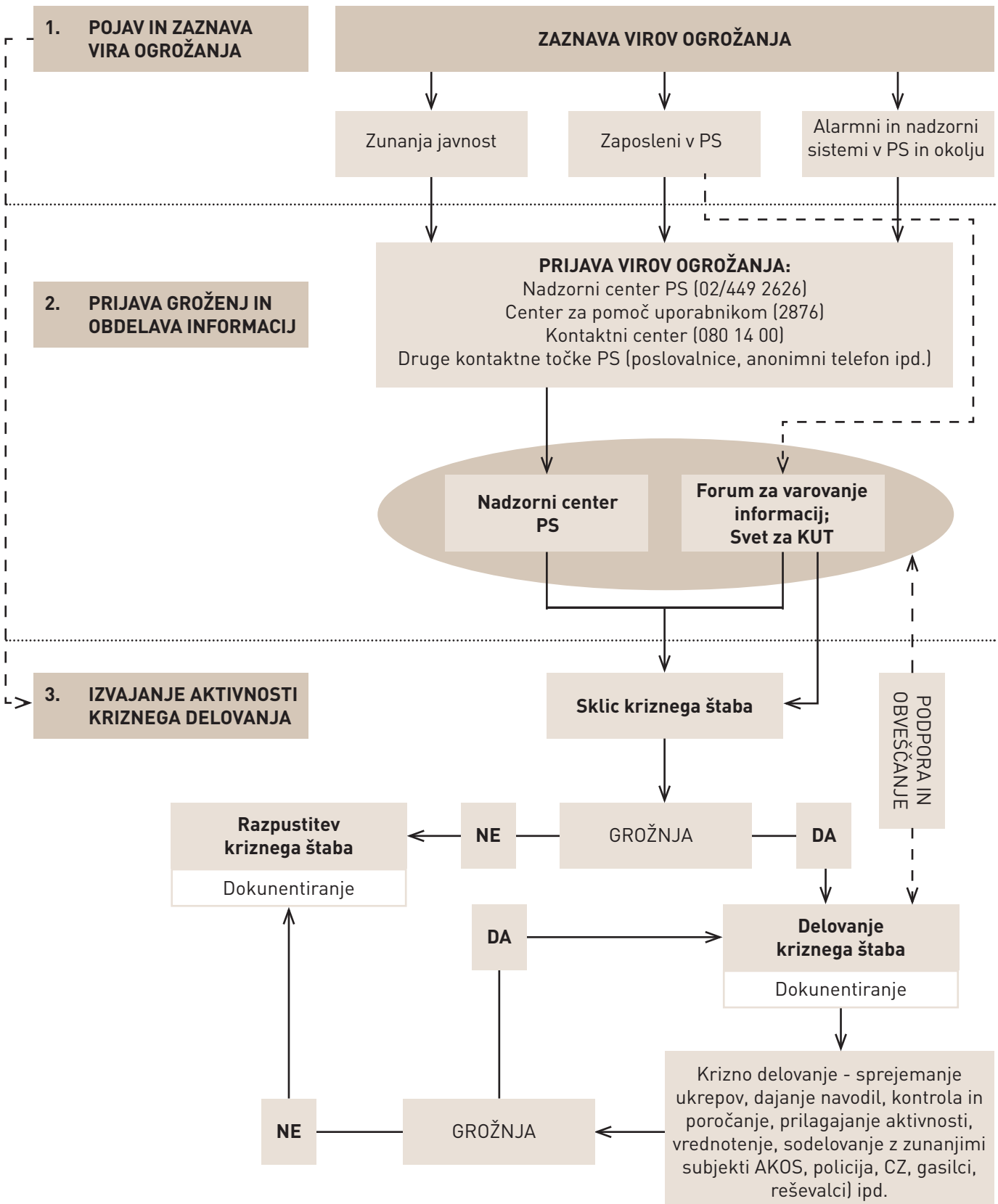
*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

ustrezne ravni, (3) obdelavo zbranih informacij na določeni ravni, (4) sprejemanje ukrepov in delegiranje nalog na določene ravni ter (5) nadzor in vrednotenje izvedbe ukrepov zaradi pravočasnega in učinkovitega obvladovanja izrednih, kriznih razmer.

- O delovanju kriznega štaba in sprejetih ukrepih za obvladovanje kriznega dogajanja je potrebno zagotavljati stalno obveščenost tako poslovodstva, kot tudi ostale notranje javnosti v PS ter skladno z ocenami tudi zunanje javnosti.

Shematičen prikaz koncepta kriznega delovanja v PS je prikazan v skici 1.

Skica 1: Shematičen prikaz koncepta kriznega delovanja





Krizni štab Pošte Slovenije

Krizni štab sestavljajo **stalni in nestalni člani**.

Stalni člani kriznega štaba so:

- vodja kriznega štaba, ki je generalni direktor družbe;
- namestnik vodje kriznega štaba, ki je direktor Področja korporativne varnosti in nadzora;
- direktorji področij in štabnih služb: kadrovskih in pravnih zadev, informacijske tehnologije, tehnologije in globalne logistike, službe korporativnega komuniciranja.

Nestalni člani kriznega štaba so:

- člani na poziv – zaposleni v PS, ki se v delu kriznega štaba vključujejo na podlagi poziva kriznega štaba.
- člani na povabilo – posamezni predstavniki drugih družb in institucij izven PS, ki se v delo kriznega štaba vključujejo na podlagi njegovega povabila.

Krizni štab je telo, ki bo v času izrednih razmer prevzel aktivnosti upravljanja, koordinacije in vodenja kriznega delovanja v PS. Krizni štab ima predpisane svoje naloge tako v mirnodobnem času kot tudi v času izrednih razmer v PS.

Vloga in pomen kriznega štaba v mirnodobnem času

Krizni štab se v mirnodobnem času sestaja redno ali po potrebi, pri čemer se krizni štab sestane redno enkrat letno.

V mirnodobnem času krizni štab skrbi za:

- pripravo kriznih scenarijev ter scenarijev odziva nanje;
- vzdrževanje in zagotavljanje pogojev za nemoteno izvajanje ukrepov, predvidenih z različnimi izvedbenimi dokumenti na področju kriznega delovanja;
- zagotavljanje pogojev za delovanje kriznega štaba v času izrednih razmer;
- usposabljanje članov kriznega štaba;
- letni pregled in ažuriranje načrta kriznega delovanja.

Krizni štab v času izrednih razmer
V primeru pojava izrednih razmer je delovanje kriznega štaba razdeljeno na tri glavne faze:

- sklic kriznega štaba,
- delovanje kriznega štaba in
- razpustitev kriznega štaba.

1. Sklic kriznega štaba
Vsak stalni član kriznega štaba lahko poda predlog, da se skliče krizni štab zaradi razmer, ki lahko predstavljajo resno nevarnost za zdravje in življenje ljudi, za premoženje PS in za pojav motenj v poslovnih procesih v PS. Predlog za sklic kriznega štaba lahko podata tudi Forum za varovanje informacij (v zadevah povezanih z informacijsko varnostjo) ter Svet za korporativno upravljanje tveganj.

Vodja kriznega štaba skliče krizni štab in v kolikor ta z večino prisotnih stalnih članov sprejme in potrdi oceno, da so podane okoliščine za njegovo delovanje, razglasi krizno delovanje in določi območje kriznega delovanja, za katerega bodo tudi veljali sprejeti ukrepi kriznega štaba. O sklicu in razglasitvi kriznega delovanja se obvešča poslovodstvo in ostala notranja javnost v PS ter skladno z ocenami tudi zunanja javnost.

V primeru, da krizni štab ne razglasi kriznega delovanja, se razpusti.

2. Delovanje kriznega štaba
Krizni štab skrbi, da je poslovanje PS v razmerah kriznega delovanja čim manj moteno ter da so posledice izpostavljenosti grožnjam obvladljive.

Glavne pristojnosti in naloge kriznega štaba so:

- razglasitev in preklic kriznega delovanja;
- določitev in spreminjanje območij kriznega delovanja;
- koordinacija in izvajanje aktivnosti za uspešno obvladovanje groženj in nevarnosti;
- odrejanje nalog, navodil, ukrepov in usmeritev;
- obveščanje notranje in zunanje javnosti;
- odločanje o posebnih ukrepih, ki se nanašajo na izvajanje poštnih storitev v pogojih groženj in nevarnosti (zapiranje pošt, začasna reorganizacija poštnega omrežja, prerazporeditve zaposlenih in materialnih sredstev, določanje prednostnih dostav ipd.).

Odločitve se v kriznem štabu sprejemajo in potrjujejo s strani vodje kriznega štaba, ki tudi vodi in koordinira delo kriznega štaba. Sprejete odločitve kriznega štaba so dolžni spoštovati vsi zaposleni. Pri delovanju kriznega štaba vodji kriznega štaba pomagajo stalni in nestalni člani kriznega štaba.

3. Razpustitev kriznega štaba
Krizni štab se razpusti in preneha z delovanjem, ko večina prisotnih stalnih članov kriznega štaba sprejme in potrdi oceno, da ni več okoliščin, zaradi katerih je bilo razglašeno krizno delovanje. S tem tudi preneha razglašeno stanje kriznega delovanja v PS na območjih, ki jih je določil krizni štab, kakor tudi vsi ukrepi, ki jih je krizni štab sprejel. O razpustitvi kriznega štaba se obvešča poslovodstvo in ostala notranja javnost v PS ter skladno z ocenami tudi zunanja javnost.

Po razpustitvi kriznega štaba se o delu kriznega štaba pripravi poročilo za poslovodstvo.

Zaključek

V Pošti Slovenije se je krizni štab od njegovega formiranja v letu 2016 pa do danes sestal dvakrat, in sicer:

- V primeru požara v poštnem logističnem centru v Ljubljani, v juliju 2016. Krizni štab je v primeru požara koordiniral aktivnosti na terenu, ki so se nanašale na obvladovanje obstoječih razmer ob nastanku požara, čimprejšnjo vzpostavitev delovnih procesov v logističnem centru, takoj ko je bilo to izvedljivo ter komunikacijo z javnostjo.
- V primeru povečanega absentizma pri zaposlenih v dostavi po več različnih poslovnih enotah PS, v januarju in februarju letošnjega leta ter sočasno napovedano belo stavko zaposlenih. Povečan absentizem pri zaposlenih je bil posledica virusnih oboljenj ter poškodb pri delu zaradi neugodnih vremenskih razmer v državi. Krizni štab se je sestal, ker je število bolnih in poškodovanih zaposlenih v dostavi že predstavljajo težave pri nemotenem izvajanju procesov v družbi. Krizni štab je odredil izvajanje ukrepov, katerih cilj je bil obvladovanje nastalih razmer in njihovega vpliva na izvajanje procesov v PS.

V Pošti Slovenije smo trenutno v pripravi strategije in načrta upravljanja neprekinjenega poslovanja. V sklopu tega procesa bo svojo vlogo imel tudi krizni štab, ki bo skladno s svojim poslanstvom še naprej predstavljal kolektivni organ upravljanja izrednih razmer. Z načrtom upravljanja neprekinjenega poslovanja pa bo Pošta Slovenije še povečala svoje zmožnosti, da bo ustrezno pripravljena na morebiten pojav nevarnosti in groženj, ki imajo neposreden vpliv na nemoteno poslovanje, s čimer bo zagotovila ustrezen odziv nanje ter uspešno okrevanje podjetja, potem ko je bilo soočeno s posamično grožnjo. ■



Avtorja: Živa Jezernik in Tomaž Rozman / Zavarovalnica Triglav d.d.*



PRIPRAVLJENI NA NOVO DOBO

Poslovno okolje, v katerem poslujejo zavarovalnice, se opazno spreminja. Ob že znanih tveganjih se pojavljajo nova, ki izhajajo iz okolja in hitrega tehnološkega razvoja. Ocenjevanje verjetnosti prihodnjih dogodkov in njihovih posledic postaja zato še težje, hkrati pa se zavarovalnicam odpirajo nove poslovne priložnosti. Kaj v takih razmerah pomeni upravljanje tveganj?

Tveganje pomeni nezmožnost pravilne napovedi prihodnjih dogodkov oziroma nezmožnost popolnega nadzora nad dejanskimi dogodki glede na pričakovane. Zunanji dejavniki povzročajo odstopanja od načrtovanih aktivnosti, ki vplivajo na uspešnost poslovanja. O tveganju govorimo tudi, kadar ne moremo z gotovostjo napovedati prihodnjih poslovnih rezultatov oziroma odstopanj od načrtov.

Tri obrambne linije

Skupina Triglav je v zadnjih letih vzporedno s prilagajanjem svojega poslovnega modela in sistema upravljanja gradila in dopolnjevala tudi sistem upravljanja tveganj. Cilj je zagotoviti uresničevanje strateških ciljev, poslanstva, vizije in vrednot družbe, kot sta strokovnost in varnost.

Sistem upravljanja tveganj je v Skupini Triglav zasnovan na trinivojskem modelu obrambnih linij.

Prvo obrambno linijo predstavljajo poslovne funkcije, ki s svojimi poslovnimi odločitvami aktivno prevzemajo in upravljajo konkretna poslovna tveganja.

Drugo obrambno linijo sestavljajo poslovne funkcije (funkcija upravljanja tveganj, funkcija skladnosti poslovanja, aktuarska funkcija) in odbori v okviru sistema upravljanja tveganj, kar vključuje postopke prepoznavanja, merjenja in spremljanja izpostavljenosti tveganjem.

Tretja obrambna linija obsega funkcijo notranje revizije, ki izvaja procese in aktivnosti, povezane z rednimi pregledi učinkovitosti notranje kontrolnega okolja na posameznih poslovnih področjih, ter skrbi zanje in za učinkovitost sistema upravljanja tveganj.

Uprava in nadzorni svet družbe nista neposredno del omenjenih treh obrambnih linij, njuna vloga v sistemu upravljanja tveganj pa je ključna. Sta namreč primarna deležnika, ki ju servisirajo vse tri linije, in sta odgovorna za delovanje sistema treh obrambnih linij znotraj sistema upravljanja tveganj in kontrolnih procesov.

Vstopamo v novo fazo tehnološkega napredka, ta pa bo prinesel nove oblike izpostavljenosti, ki jih ne predvideva in ne vsebuje nobena od današnjih zbirk podatkov. Zavarovalnice bomo morale zato razviti modele, ki bodo temeljili predvsem na ocenah in predpostavkah ter ne več toliko na preteklih izkušnjah.

Ključna tveganja

Pri poslovanju prevzema zavarovalnica naslednja pomembnejša tveganja:

- **zavarovalna tveganja** so tveganja nastanka izgube ali neugodne spremembe v vrednosti zavarovalnih obveznosti zaradi neustreznih premij in neustreznih predpostavk, upoštevanih v izračunu zavarovalno-tehničnih rezervacij;
- **tržna tveganja**, ki so posledica sprememb tržnih vrednosti sredstev, obveznosti in finančnih instrumentov;
- **likvidnostna tveganja**, ki pomenijo nevarnost, da zavarovalnica ni sposobna poravnave svojih obveznosti ob njihovi zapadlosti oziroma v primeru nastanka obveznosti iz naslova večjih škod;
- **kreditna tveganja** kot tveganje izgube zaradi neizpolnitve obveznosti nasprotne stranke;
- **operativno tveganje**, ki nastane zaradi neustreznega ali neuspešnega izvajanja internih procesov, ravnanja zaposlenih, delovanja vzpostavljenih sistemov ali obvladovanja zunanjih dogodkov in njihovih vplivov;
- **nefinančna tveganja**, pri katerih so z vidika poslovanja zavarovalnice pomembna strateška tveganja, tveganje izgube ugleda in kapitalsko tveganje.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Nova tveganja na obzorju

To so tveganja, ki jih že poznamo in vemo, kako se nanje najbolje pripraviti. V zadnjem času se v zavarovalniškem svetu čedalje več govori tudi o t. i. »novih tveganjih«. Ena največjih svetovnih zavarovalnic **Allianz** je v svoji že šesti raziskavi Allianz Risk Barometer – Top Business Risks 2017 med največjimi poslovnimi tveganji za zavarovalnice, ki poslujejo v evropskem prostoru, izpostavila (Allianz, 2017):

- prekinitve poslovanja,
- tržne razmere (nestabilnost, povečana konkurenca, stagnacija trgov, M&A),
- kibernetska tveganja.

Najpomembnejša tveganja glede na lansko letno raziskavo ostajajo nespremenjena (Allianz, 2016). Poleg njih omenja tudi spremembe regulative, makroekonomsko okolje, naravne nesreče, tveganje ugleda in izgube dobrega imena pa še nevarnost požara in eksplozij, uvajanje in vpliv novih tehnologij ter politična tveganja, vključno z nevarnostjo vojn in terorizma. To kaže na izredno hitro spreminjajoče se okolje, kar zahteva fleksibilnost in prilagodljivost zavarovalnic. Klasična zavarovalna tveganja (naravne nesreče, nevarnost požara in eksplozij) postajajo v zavarovalništvu deležna vse manj pozornosti. Zato po oceni strokovnjakov z vseh področij zavarovalništva iz leta v leto izgubljajo mesta na lestvici najpomembnejših tveganj.

Podobno v svojem pregledu najpomembnejših tveganj iz februarja 2017 ugotavlja tudi evropski regulator **EIOPA**. Zaradi tržnih razmer makroekonomskega okolja in rekordno nizkih obrestnih mer postajata najpomembnejši skupini tveganj tržna in makroekonomska ter manj skrb vzbujajoča zavarovalna in kreditna tveganja (EIOPA, 2017).

Učinkovito obvladovanje tveganj

Odgovori na spremenjene okoliščine so bili tudi podlaga za novo strategijo Skupine Triglav. Ta vključuje prenovljen poslovni model Skupine in posameznih družb, dodaten tehnološki razvoj ter poudarja pomen sistema upravljanja tveganj v Skupini Triglav. Pomen razumevanja tveganj in širitev kulture aktivnega upravljanja tveganj se povečujeta na vseh ravneh delovanja Skupine.



Eden glavnih kriterijev dolgoročno vzdržnega poslovanja je kapitalska ustreznost matične družbe in Skupine Triglav. Od januarja 2016 je v veljavi enotna evropska regulativa **Solventnost 2**, ki se osredotoča na prepoznavanje, merjenje in proaktivno upravljanje tveganj. Ta pravila od zavarovalnic zahtevajo, da ob sprejemanju poslovnih odločitev upoštevajo tudi njihov vpliv in vpliv drugih zunanjih dejavnikov na nivo prevzetega tveganja ter s tem na kapitalsko moč zavarovalnic.

Upravljanje tveganj zahteva obravnavo Skupine Triglav kot celote. Zato vzporedno z nadgrajevanjem sistema upravljanja tveganj v Zavarovalnici Triglav v vse odvisne družbe Skupine prenašajo tudi dobre prakse, znanje in usmeritve s tega področja.

Nova tehnologija – nove nevarnosti in nove priložnosti

Nadaljnji koraki vodilne zavarovalno-finančne skupine v Sloveniji in regiji Adria bodo morali biti nadvse premišljeni, saj se bodo spremenili poslovni modeli zavarovalnic, v okviru katerega se bo spremenilo kaj, kako in komu bodo zavarovalnice prodajale. Ob nevarnostih novih poslovnih modelov pa tehnologija prinaša tudi nove priložnosti. Nova tehnologija tako za podjetja pomeni celo več priložnosti kot stroškov, povezanih s prehodom na digitalno ekonomijo (Svetovna banka, 2017), ob tem pa prinaša tudi priložnosti v obliki novi trgov, novih prodajnih kanalov in novih produktov.

Uporaba tehnologije se povečuje tako rekoč na vsakem koraku, kar bo vodilo v zmanjšanje določenih vrst tveganj (npr. zmanjšanje nesreč v prometu), hkrati pa bo prinesla nova tveganja, kot so informacijska oziroma t. i. kibernetska tveganja.

Izpostavljenost tveganjem se bo v vse bolj digitalizirani družbi pomembno spremenila. Vstopamo v novo fazo tehnološkega napredka, ta pa bo prinesel nove oblike izpostavljenosti, ki jih ne predvideva in ne vsebuje nobena od današnjih zbirk podatkov. Zavarovalnice bomo morale zato razviti modele, ki bodo temeljili predvsem na ocenah in predpostavkah ter ne več toliko na preteklih izkušnjah.

Povečana uporaba tehnologije bo med drugim vodila v povečan obseg ustvarjenih podatkov in s tem ustvarila priložnost za zavarovalnice, saj bodo lahko uporabile te podatke, da bolje spoznajo svoje stranke. Ob tem se pojavi priložnosti za ustvarjanje prilagojenih oziroma individualnih zavarovanj. Pri tem bosta zaznava in predvsem pravilna ocena tveganj, ki jih prinašata nova tehnologija in vsesplošen razvoj, priložnost za zavarovalnice, da se na tovrstne izzive odzovejo z razvojem novih produktov in storitev.

Spremenil se bo tudi način prodaje. Zavarovalnica Triglav že danes beleži rast internetne prodaje zavarovanj. Največja



sprememba bo prehod s prodaje, kjer se je zavarovalnica srečala s stranko enkrat v letu ob obnovitvi pogodbe, na način, ki bo temeljil bolj pogostejši interakciji. Glede na to, da zavarovalnice v družbi opravljajo tudi funkcijo ozaveščanja pred tveganji, bi lahko zavarovalnica komunicirala s strankami celo dnevno. Prišlo bo tudi do prehoda na večkanalno komuniciranje. Tako bo lahko komunikacija potekala prek telefonskega klica, aplikacij, e-pošte, družbenih omrežij itd. Pri tem pa bo potrebno poskrbeti tudi za varnost in zasebnost osebnih podatkov strank.

Pri pripravi novih zavarovanj bodo zavarovalnice izpostavljeni več negotovostim kot pri pripravi zavarovanj v preteklosti. Toda negotovosti, ki jih prinaša prihodnost, so ob zavedanju potencialnega tveganja za zavarovalnice lahko tudi priložnost. Na katerih področjih jo vidijo v Skupini Triglav?

1. Informacijska tehnologija
Uvedba zavarovanj za kibernetska tveganja, kot so tatvine in brisanje podatkov, blokade sistemov, tatvine denarja, oškodovanje ugleda podjetja, prevare, izsiljevanje. V dobi, ko bo vse stvarno povezano v medmrežje (t. i. internet stvari), se bodo kibernetska tveganja še stopnjevala. Vse večji je tudi trg zavarovanj za tehnologijo, ki je čedalje dražja, hkrati pa tudi čedalje bolj pomembna za naš vsakdan. Za primer lahko vzamemo mobilne telefone. Prihajajo pa tudi nove oblike prevoznih sredstev in še mnoge tehnologije, ki bodo zavzele prostor v naših domovih.

2. Letalniki
Uvedba zavarovanj za uporabo letalnikov, pri čemer je rizikov za uporabnike kar nekaj: možnost trčenja, padci, vprašanja kršenja zasebnosti, možnost ugrabitve letalnikov.

3. Nanotehnologija
Uvedba zavarovanja odgovornosti, ko bi se nanodelci izkazali za škodljive. Previdnost pri oceni izpostavljenosti bo tu za zavarovalnice ključna, da se ne bi ponovila povsem napačna ocena zavarovalnic glede obsega in posledic azbestnih obolenj.

Družba se je skozi celotno zgodovino spreminjala, z njo pa se so spreminjala tudi oblike zavarovanj in zavarovalnice. Trenutno se družba zopet močno spreminja, z njo pa tudi okolje, v katerih posluje Skupina Triglav. A spreminja se za vse, tudi za konkurenco. Pomagati ljudem razumeti tveganja, poiskati prave poslovne priložnosti in graditi odpornost družb v Skupini proti neugodnim vplivom so cilji upravljanja Skupine in tveganj, ki so (že) del našega vsakdana.

Viri

- EIOPA (2017): Risk Dashboard. Dostopno 3. maja 2017 na povezavi https://eiopa.europa.eu/Publications/Standards/EIOPA-BoS-17-022%20EIOPA%20RISK%20DASHBOARD%20February%202017.pdf.
- Allianz (2017): Allianz Risk Barometer: Top Business Risks 2017. Dostopno 3. maja 2017 na povezavi https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf
- Allianz (2016): Allianz Risk Barometer: Top Business Risks 2016. Dostopno 3. maja 2017 na povezavi http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf
- The World Bank (2017): Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia. Dostopno 3. Maja 2017 na povezavi https://www.worldbank.org/en/region/eca/publication/digital-dividends-in-eca ■

BTC CITY 360° LIVE
IZ MESTA 360° V ŽIVO



BTC CITY LJUBLJANA

450 TRGOVIN

70 LOKALOV IN RESTAVRACIJ

8500 BREZPLAČNIH PARKIRNIH MEST

VODNO MESTO ATLANTIS

BREZPLAČEN PANORAMSKI POGLED
NA LJUBLJANO S KRISTALNE PALAČE

KAKO DO NAS?

IZVOZ / EXIT
Ljubljana
Nove Jarše

www.btc-city.com

BTC CITY

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije

INTERVJU
g. Franci Petek, poveljnik Gasilske zveze Slovenije

POŽARNA ZAŠČITA KLJUČNI TEMELJ KORPORATIVNE VARNOSTI

Ustrezno načrtovan sistem požarne zaščite je za korporativno varnost v organizacijah izrednega pomena. Izkušnje iz realnega okolja nas vedno znova opozarjajo, da ima lahko zanemarjanje tega dejstva za posledico izgubo človeških življenj in uničenje materialnih zmogljivosti, ki so ključne za delovanje organizacije.

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

Osnovna naloga GZS je in bo, da zagotavlja pogoje za delo našega operativnega kadra. Lahko se pohvalimo, da nas je že več kot 160.000 od tega okrog 50.0000 operativnih gasilcev. Pri tem ne smemo pozabiti, da to delo opravljamo prostovoljno, kar pomeni veliko različnih dejavnosti, da lahko zagotovimo ustrezen kader. Z vzgojo in usposabljanjem začnemo že z našo mladino.
Usposabljanje je ena najpomembnejših nalog GZS. Prenova učnih programov je velik korak k boljši usposobljenosti naših gasilcev. Z izgradnjo regijskih poligonov (otvoritev prvega bo 27.5.2017 v Ormožu) bomo zagotovili kvalitetno vzdrževanje znanja pridobljenega v učnih centrih.
Ustrezna oprema in tehnika je druga pomembna naloga GZS. Tipizacija gasilskih vozil, tehnike in opreme zagotavlja, da so zagotovljeni minimalni pogoji- standardi za kvalitetno in varno delo. Tipizacija je v fazi posodabljanja. Komisija za tehniko je že potrdila osnutek sprememb, sedaj gre v širšo razpravo in v sprejem na Poveljstvo GZS.

Kljub gospodarski krizi si v prihodnje želim, da bodo pogoji za naše delo ostali vsaj na takšnem nivoju kod do sedaj. Predvsem dovolj operativnega kadra, primerno usposobljenega, z ustrezno tehniko in opremo.

Gospodarska kriza se prav gotovo pozna tudi pri gasilcih in delu GZS, vendar ne v takšni meri kot v gospodarstvu. Za gasilce je odgovorna lokalna skupnost – župan, manjši delež pri tem zagotavlja država (sofinanciranje enot širšega pomena in sofinanciranje gasilskih vozil, tehnike in opreme). Proračuni občin za gasilce so v različnih občinah zelo različni in kljub gospodarski krizi ostajajo v večini primerov približno v enakem obsegu. Tudi država je pri sofinanciranju enot širšega pomena ostala na istem, višina sredstev za sofinanciranje opreme pa se je leta 2015, po znamenitem amandmaju v parlamentu precej povečala. Imamo pa vedno večje težave pri zagotavljanju dejavnosti GZS, dela je vedno več, sredstev in delovne sile pa enako oziroma manj. Še najbolj se gospodarska kriza pozna pri industrijskih prostovoljnih društvih, ki so direktno odvisna od gospodarstva.
Kljub gospodarski krizi si v prihodnje želim, da bodo pogoji za naše delo ostali vsaj na takšnem nivoju kod do sedaj. Predvsem dovolj operativnega kadra, primerno usposobljenega, z ustrezno tehniko in opremo.

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

Naš sistem temelji na prostovoljnem gasilstvu. V Sloveniji imamo 14 poklicnih enot, ki so v večjih mestih in so po operativni moči zelo različne. Ljubljanska brigada ima v eni izmeni 28 gasilcev in lahko obvlada tudi malo večjo intervencijo, za razliko poklicne enote v Ajdovščini, ki ima v izmeni tri gasilce in nujno potrebuje pomoč prostovoljnih gasilcev pri vsaki malo večji intervenciji.



Ena od boljših stvari naše zakonodaje je, da se je odgovornost na področju zaščite in reševanje prenesla na lokalno raven. Tako je župan odgovoren za prostovoljne in poklicne gasilce. V Sloveniji smo zgradili sistem, ki nam ga marsikdo zavida. Poklicne enote v večjih mestih in močna prostovoljna društva. Kombinacija poklicnih in prostovoljnih gasilcev je pri nas pripeljana do zavidljivega nivoja, ko tudi prostovoljci delamo na profesionalni ravni. Del prostovoljnih gasilskih društev opravlja naloge širšega družbenega pomena. Imamo 33 prostovoljnih enot širšega pomena in 14 poklicnih enot, ki rešujejo ob prometnih nesrečah, reševanju iz vode in na vodi ter posredujejo ob nesrečah, kjer so prisotne nevarne snovi. Te enote pokrivajo območje cele Slovenije, tako da je vsak del oddaljen od lokacije enote največ 20 minut, s tem pokrijemo 93 odstotkov države. Aktivacija je urejena z alarmnimi načrti lokalnih skupnosti in to poteka avtomatično. Ob nesreči pokličete center za obveščanje (112) in operater točno ve kako mora ukrepati ob določeni nesreči in koga poklicati. Vse ostalo je stvar vodje intervencije, ki po potrebi zahteva dodatne sile. Gasilci smo edina sila, ki lahko v zelo kratkem času zagotovimo na neki lokaciji več sto ljudi.
Drugače zelo dobro sodelujemo s poklicnimi kolegi. Trenutno se spreminja Zakon o gasilstvu, kjer bi želeli to še nadgraditi. Želja je, da bi bila znanja prostovoljnih in poklicnih gasilcev primerljiva. Seveda tu ne gre za vseh 50.000 prostovoljnih operativnih gasilcev, gre za tiste, ki so se pripravljeni dodatno usposabljati. Poklicni gasilec pristopi k opravljanju zaključnega izpita po šest mesečnem usposabljanju v Gasilski šoli. Prostovoljni gasilec pa bi ustvaril pogoje za pristop k zaključnemu izpitu skozi več letno usposabljanje preko temeljnega in dopolnilnega usposabljanja ter izkušenj.

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

Že v prejšnjem vprašanju sem omenil, da je usposabljanje zelo pomembna naloga GZS. V letu 2016 smo usposobili 7728 gasilcev na nivoju GZ in regij in 5913 na nivoju GZS. V lanskem letu smo končali z velikim projektom prenove Temeljnih učnih programov za prostovoljne gasilce, še pred tem smo morali spremeniti Pravila gasilske službe prostovoljnih gasilcev, s katerimi smo ustvarili pogoje za prenovo. Zelo hitro smo ugotovili, da je potrebno prenoviti vsa temeljna usposabljanja, da naj bo razmerje med teorijo in vajami 50%/50%, velik poudarek posvetiti ciljem (informativnim- formativnim), približati izobraževalna programa poklicnih in prostovoljnih gasilcev, izločiti ponavljanja vsebine med predmeti in med tečaji, dvigniti kakovost posredovanja izobraževalnih vsebin, stremeti k poenotenju izvajanja tečajev po celotni Sloveniji. Novost so tudi zaključni izpiti, ki bodo pozitivno vplivali tudi na predavateljski kader, saj bo nad njimi še ena kontrola.

Kako se v ta sistem izobraževanja vključuje projekt Višje Gasilske šole?

Projekt Višje gasilske šole je trenutno ustavljen. Kar veliko je bilo narejenega na tem področju. Na koncu se je pojavilo vprašanje o smiselnosti same šole in zagotavljanju denarja. Slovenija je zelo majhna z veliko raznih višjih in visokih šol. Potrebe na tem področju so, vendar je vprašanje, v kakšnem obsegu.

Načrtno delo z mladimi se nam vedno bolj obrestuje saj smo ena redkih organizacij, ki se ji članstvo nenehno povečuje.



Samostojno preživeti na tako majhnem prostoru je težko. Po mojem osebnem mnenju je kombinacija Fakultete za kemijo, oddelka za tehnično varnost in Gasilske šole, prava stvar. Na fakulteti dobiš ustrezno teoretično znanje in verodostojno (cenjeno) diplomo, v Gasilski šoli pa kvalitetno praktično znanje.

Kako med mladimi zagotoviti ustrezno zanimanje za poklic gasilca?

Na GZS se zavedamo, da brez mladih ni napredka. Načrtno delo z mladimi se nam vedno bolj obrestuje saj smo ena redkih organizacij, ki se ji članstvo nenehno povečuje.
Pridobivanje novih mladih članov je naloga prostovoljnih gasilskih društev, gasilskih zvez in Gasilske zveze Slovenije in vseh struktur, ki delujejo znotraj teh organizacijskih oblik. Mladinske komisije na vseh nivojih, vodstva organizacij in mladinski mentorji imajo največjo vlogo pri oblikovanju smernic in programov za delo z mladimi, ki se lahko v vsakem okolju vključijo v prostovoljno gasilsko društvo in v eno izmed mladinskih aktivnosti, kot so spoznavanje gasilstva in gasilske preventive, gasilska in športna tekmovanja, letovanja in taborjenja, orientacija in gibanje v naravi, gasilski kvizi, prva pomoč, društva Mladi gasilec, kulturne in družabne prireditve, mednarodno povezovanje in udejstvovanje.
Za zahtevno delo v operativni enoti po dopolnjenem 18. letu starosti je mlade potrebno kvalitetno in uspešno izobraževati in usposobiti. Izobraževanja mladih gasilcev so usposabljanje za nazive, preventivne značke, gasilske veščine. Z novimi učnimi programi bodo naši mladi lahko osnovna operativna znanja pridobili tudi z usposabljanjem v mladinskih programih usposabljanja.
Mladinski svet Slovenije organizira poleg tečajev tudi posvete mladinskih mentorjev, kjer se poleg praktičnih vsebin udeleženci seznanjajo z aktualnimi dogodki v naši organizaciji, mladinsko problematiko in ostalimi pomembnimi vsebinami, ki so jim v pomoč za delo z gasilsko mladino.

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

Centralizacija ni nujno tudi slaba. V osnovi sistem zaščite in reševanja, še posebej pri gasilcih, temelji na lokalni skupnosti, se pravi zelo decentralizirano. Naša društva so zelo samostojna, kar prinaša dobre in slabe stvari, predvsem pa odgovornosti. Sistem jim pri tem samo pomaga. Za razliko od ostalih reševalcev (jamarji, gorski reševalci, posebne enote...), ki so organizirani na nivoju države, zelo centralizirano, kar je tudi prav. Vsako mesto ne potrebuje gorskih reševalcev, ali specialnih enot. Smo tako majhni, da v treh urah pridemo iz enega konca Slovenije na drugi konec. Menim, da se stvari premikajo v pravo smer. Še vedno pa imamo veliko balasta, ki je neučinkovit in v praksi ne deluje. Zelo pomembna je komunikacija med temi strukturami, prave informacije so v krizni situaciji zelo pomembne. Jasno se mora vedeti, kdo vodi in kdo je za kaj odgovoren.

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

Z nastankom novih občin se je stanje na področju opremljanja bistveno spremenilo. V zadnjih dvajsetih letih smo zamenjali veliko vozil, tehnike, še posebej velik napredek je v osebni zaščitni opremi. Zopet imamo tiste z zelo dobro opremo in takšne, ki dobesedno životarijo. Na splošno pa lahko rečemo, da smo dobro opremljeni, še posebej to velja za poklicne gasilske enote. Manjka nam še specialna oprema, ki je zelo draga, zato se trudimo zagotoviti tudi dodatni denar iz države. V preteklosti je bil to program Kras. Sedaj poteka program sofinanciranja gasilskih avto lestev, tako za poklicne kot prostovoljne enote.
Država vsako leto zagotavlja tudi sredstva iz proračuna za sofinanciranje vozil in opreme, ki pa ne preseže 20% vrednosti. Za nerazvite je ta procent nekoliko večji do 30%.

Prostovoljna gasilska društva so v tem okviru verjetno še bolj problematična in močno odvisna od finančne moči lokalne skupnosti?

Finančna moč občine in razumevanje župana je še kako pomembna. Že večkrat sem omenil, da so lokalne skupnosti glavni financer, ki s pogodbo določi višino sredstev in obveznosti. Na žalost si morajo društva v večini primerov polovico sredstev pridobiti sama. Načini pridobivanja sredstev so zelo različni in so povezani tudi s tradicijo.

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

Zelo pomembna je komunikacija med temi strukturami, prave informacije so v krizni situaciji zelo pomembne. Jasno se mora vedeti, kdo vodi in kdo je za kaj odgovoren.

Pri GZS deluje Komisija za industrijsko gasilstvo, ki si ves čas prizadeva za izboljšanje statusa industrijskega gasilstva. V ta namen je ob začetku delovanja, v novem mandatnem obdobju naredila analizo stanja industrijskega gasilstva. Analiza je pokazala, da stanje gasilstva v industriji ni zadovoljivo in zahteva nujno ukrepanje vseh organizacij, ki se ukvarjajo s področjem varstva pred požari in gasilstvom v industriji. Pomanjkljivosti se kažejo predvsem v usposobljenosti gasilskih in gasilsko-vodstvenih kadrov, pomanjkljiva pa je tudi opremljenost enot z gasilsko zaščitno in reševalno opremo. V nekaterih primerih je kategorija gasilske enote nižja, kot bi bilo pričakovati iz podatkov o vrsti dejavnosti podjetja. Število gasilcev večinoma ustreza predpisanemu s kategorizacijo, odstopanja pa so pri usposobljenosti kadrov, saj ima skoraj tretjina poveljnikov nižjo gasilsko izobrazbo od predpisane, pomanjkljiva je usposobljenost za nazive specialnosti. Pri tem je še posebej zaskrbljujoča opremljenost z osebno zaščitno opremo in z izolirnimi dihalnimi aparati. Tudi področje zdravstvenih pregledov gasilcev ni zadovoljivo, kar se še posebej kaže pri zdravstvenih pregledih po 4. členu pravilnika. Seveda pa obstajajo tudi svetle izjeme, kjer industrijsko gasilstvo dobro deluje.

Tudi s spremembo Zakona o gasilstvu želimo urediti področje industrijskih gasilskih enot. S pomočjo različnih ugodnosti bi lahko delodajalce nagradili za vložek na področju požarne varnosti in stimulirali zaposlitev prostovoljnih gasilcev.

Na žalost se pogosto srečujemo z ukinjanjem industrijskih gasilskih društev, kar je največkrat pogojeno z zapiranjem podjetij. Deležni pa smo tudi bolj veselih informacij o ustanavljanju industrijskih gasilskih društev. Tako se bodo v kratkem ustanovila tri nova industrijska društva.

Vsi našteti problemi so tudi izziv za prihodnje delo. Dobro organizirana gasilska služba v podjetjih je velika dodana vrednost, k požarni in splošni varnosti, tega se vse bolj pogosto zavedajo tudi delodajalci.

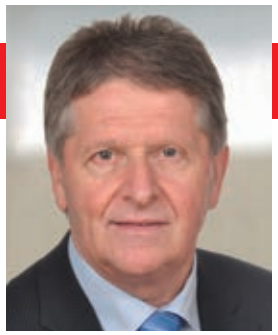
Dobro organizirana gasilska služba v podjetjih je velika dodana vrednost, k požarni in splošni varnosti, tega se vse bolj pogosto zavedajo tudi delodajalci.

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

Na žalost se vedno pogosteje srečujemo z zahtevnimi varnostnimi situacijami. V naši državi se skoraj nobena krizna situacija ne zgodi, da ne bi bili prisotni gasilci, tudi pri krizi z migranti smo sodelovali. Korporativna varnost je prav gotovo širši pogled na različne varnostne vidike. Nesporno je lahko GZS ustrezen in nujen partner. Pri našem delu posameznik ne pomeni veliko, je pa ključen člen. Samo skupaj smo lahko močni in uspešni. Še posebej to velja za industrijska okolja, kjer je potrebno združiti vse segmente varnosti in gasilci imamo tukaj zelo pomembno vlogo, še posebej na preventivnem področju. ■



Avtor: dr. Brane Bertoncelj / Slovensko združenje korporativne varnosti



NADZOR NA DELOVNEM MESTU: VEČ KOT JE OMEJITEV, VEČ JE KRŠITEV

Skladno z zakonodajo se delo opravlja po navodilih in pod nadzorom delodajalca, zato je ta upravičen tudi do nadzora nad zaposlenimi. Nadzor na delovnem mestu je legalna in legitimna pravica delodajalca.

Na delovnem mestu se praviloma soočata dva interesa, ki lahko prerasteta v konflikt, če nista ustrezno upravljana. Na eni strani imamo pravico zaposlenega do zasebnosti na delovnem mestu (obstaja odpor do tega, da se osebno integriteto zaposlenega postavlja pod vprašaj), na drugi strani pa upravičen interes delodajalca, da nadzoruje lastna sredstva, delo zaposlenega in ugotavlja odklone od norme. Toda delodajalec lahko kot »močnejša stranka« v praksi uveljavi več nadzora nad zaposlenim, kot je po naravi dela to še dopustno.

Pomembno je, da je zaposleni o kakršni koli obliki nadzora na delovnem mestu vnaprej seznanjen s pravili delodajalca glede dela, hišnega reda, prihoda na delo, gibanja po objektu, uporabi telefona, elektronske pošte, interneta ipd. in s tem, kdaj, kdo, kako in v kakšnih primerih ga lahko nadzira. Zaposleni se mora z nadzorom strinjati oziroma mora biti nadzor objektivno opravičljiv in zlasti mora biti sorazmeren.

Microsoft je izdelal programsko računalniško opremo za nadzor zaposlenih na delovnem mestu (vsebinsko nadaljevanje programa TrueActive Software, imenovan tudi kot »WinWhatWhere«). A tu ne gre za običajen nadzor, njihov sistem bo lahko v pravem »Orwellovskem stilu« nadzoroval zaposlenega z vrsto brezžičnih senzorjev, ki bi med drugim nadzorovali srčni utrip, obrazno mimiko, telesno temperaturo, možganske signale, krvni pritisk, telesne gibe ipd. Na podlagi teh meritev bi nato sistem lahko določil kdaj je zaposleni pod stresom ali nezadovoljen z delom in opozoril nadrejenega, da zaposleni potrebuje pomoč. Če je takšen sistem nadzora morda še upravičen za odgovorne operativne izvajalce nalog vitalne infrastrukture in za nekatere druge bolj tvegane poklice, pa vsekakor ni na splošno primeren.

> Koncept vodenja sloni najprej na zmožnosti voditi samega sebe in nato na veščini vodenja sodelavcev.

Izvajalci nadzora

Nadrejeni, tudi kot izvajalec nadzora na delovnem mestu, ima ključen doprinos pri razvoju konstruktivne organizacijske klime in pri doseganju poslovnih rezultatov. Izzivi in odgovornosti nadrejenega so številne, saj ima formalno moč nad zaposlenimi. Obvladovati mora tako odnose s svojimi predpostavljenimi kot tudi s svojimi podrejenimi, hkrati pa tudi z vodji na drugih poslovnih področjih. Dober nadrejeni ne nadzoruje le materialnih sredstev, denarja in zaposlenih, ampak mora predvsem razvijati sebe v smislu čustvene in socialne inteligence, saj bo le tako lahko pozitivno vplival na kakovost dela in življenja zaposlenih.

Koncept vodenja sloni najprej na zmožnosti voditi samega sebe in nato na veščini vodenja sodelavcev. Ključ do uspešnega vodenja je, da nadrejeni zna pritegniti sodelavce, izžarevati entuzijazem in navdušenje do dela ter da slednje prenese na sodelavce. Navdušenja sodelavcev in zadovoljstva pri delu pa ni mogoče kupiti, lahko si ga nadrejeni prisluži s svojim odnosom do njih. Najpomembneje je, da nadrejeni sodelavcem jasno pove, kakšna je strategija organizacije in cilj poslovanja ter da jim omogoči prostor za njihovo kreativnost. Upoštevati je potrebno tudi druge pomembne faktorje, kot so skupinska povezanost, komunikacija v skupini, kontekst, delovna usmerjenost, obstoječe skupinske norme ipd. Zaposleni niso roboti, in če jih bo nadrejeni utesnjeval z rutino, potem bo njihova kreativnost majhna.

Nadrejeni mora nadzirati delo in biti pozoren na možne odklone zaposlenih od

izvajanja navodil, ukrepov ter postopkov. Področja nadzora na delovnem mestu naj bodo določena v internih aktih, in sicer:
- funkcijsko določena (poslovni cilji morajo biti opravljeni v določenem času),
- poslovno določena (upoštevajoč specifično naravo poslovanja),
- tehnično določena (uporaba posebnih delovno - tehničnih pripomočkov) in
- organizacijsko določena (redni, občasni, izredni nadzor).

Izhodišča za nadzor so:
- pozornost nadzora mora biti usmerjena k realizaciji pomembnih poslovnih ciljev, nalogam in večjim problemom poslovanja,
- največ pozornosti naj bo namenjeno zlasti tistim ciljem, od katerih je odvisno uspešno upravljanje finančnih tveganj in tveganje zmanjšanja ugleda organizacije,
- vpeljati je potrebno take metode nadzora, ki ne zahtevajo veliko časa, a so kljub temu proaktivne, fleksibilne in učinkovite,
- zagotoviti je potrebno učinkovit pretok informacij med vsemi pomembnejšimi sodelavci,
- pomembna je izbira sodelavcev, ki so za delo kompetentni, usposobljeni in motivirani.

Varnostna politika organizacije mora z operativnim nadzorom in nadzornimi tehnikami povečati možnosti za neprekinjeno in uspešno poslovanje. Temeljna pravila so:
- zaposleni bi morali imeti dostop do materialnih sredstev ali podatkov, ki jih "morajo poznati in vedeti", da lahko opravljajo svoje zadolžitve,
- zaposleni bi morali imeti dostop do področij organizacije, za katera so pooblaščeni in »kamor morajo iti«,
- varnostna politika mora ustrezati zahtevam sredstev, ki jih je potrebno zavarovati,
- postopke bi morali redno pregledovati, posebno pri uvajanju nove opreme ali novih postopkov,
- nadzor določenih notranjih kontrol je treba ohranjati, da bi zagotovili, da se te opravljajo na ustrezen način,
- za vitalne poslovne procese bi morali opravljati naključne preglede (na preskok), da bi zagotovili, da se dosledno upoštevajo navodila za delo,
- preiskati bi morali vse nepooblaščene ali nenormalne situacije.

Noben zaposleni ne bi smel biti sam pooblaščen za opravljanje vitalnega poslovnega procesa, posebno ne na področjih z visokim tveganjem, tako da mora to delo zaposlenega nadzirati drugi sodelavec.

Noben zaposleni ne bi smel biti sam pooblaščen za opravljanje vitalnega poslovnega procesa, posebno ne na področjih z visokim tveganjem, tako da mora to delo zaposlenega nadzirati drugi sodelavec.

Problem pri opravljanju nadzora

Poseben problem nadzora predstavlja nadrejeni na določenih stopnjah hierarhije, ki je preveč izrazito naravnan k doseganju dobrih rezultatov poslovanja, kar sicer kratkoročno velja za eno od najmočnejših konkurenčnih prednosti v sodobnem managementu. Neusmiljena naravnanost na rezultate pa ima lahko tudi svoje temne strani in tudi destruktivne posledice. Nadrejeni s takšnimi motivacijskimi vzgibi kratkoročno sicer lahko poslovno uspeva, saj rastejo npr. storilnost, dobiček, tržni deleži ipd. Vendar pa mu manjka čustvena inteligentnost, ki je pomembna za uspešno vodenje. Nadrejeni lahko pretirano prekoračujejo sorazmeren nadzor na delovnem mestu zaradi neznanja, neizobraženosti ipd., lahko pa ima tudi vrsto lastnosti, ki sodijo na področje psihopatije (ta pojem se nanaša na trajen vzorec neupoštevanja in kratenja pravic drugih). Kot je zapisal K. Dutton v knjigi »Modrosti psihopatov« (2012) so ti uspešni tudi zaradi lastnosti, ki prispevajo k uspehu organizacije. Dutton celo zagovarja idejo, da kapitalistična družba potrebuje približno deset odstotkov psihopatov, a jih mora znati pravilno usmerjati in nadzorovati.

R. D. Hare (1991) je razvil klinično ocenjevalno lestvico psihopatije (PCL-R). Hare loči med antisocialno motnjo, kjer je v ospredju antisocialno vedenje, od psihopatije, kjer govorimo o specifičnih osebnostnih potezah. Psihopatija na le-



stvici PCL-R je seštevek lastnosti osebnosti in lastnosti socialno deviantnega življenjskega sloga: npr. zgovornost in površinskost, egocentričnost in aroganca, potreba po prejemanju spodbud in nagnjenost k tveganju, patološko laganje, sleparstvo in manipulativnost, pomanjkanje obžalovanja in občutkov krivde, čustvena plitkost, nezmožnost empatije in brezčutnost, odsotnost realnih in dolgoročnih ciljev, impulzivnost, neodgovornost in nezanesljivost, nezmožnost sprejemanja odgovornosti za svoja dejanja ipd. Med poglavitne skupne lastnosti, ki jih ta raziskovalec pripisal psihopatom z vrha družbene lestvice v korporativnih organizacijah, so pretirani šarm, karizmatičnost, odločnost, pogum, pretkanost, samozavest, zunanji ego, osredotočenost na uspeh in odpornost na občutek krivde.

Korporativnega psihopata zlasti privlačijo denar, ugled, privilegiji in moč. Psihopat svet okoli sebe razume predvsem kot zverinjak, v katerem velja boj za preživetje. Deluje v skladu z geslom: »Kdor ne bo zmagovalec, bo žrtev.« Na različne načine se poskuša preriniti v ospredje in karierno napredovati. Pri tem se lahko poslužuje spletk, diskreditacij, manipulacij, ustrahovanja, izsiljevanja in drugih znanih metod psihičnega nasilja. »Kompenziran« psihopat na vodstvenem položaju lahko ogrozi zdravje pri delu in blaginjo mnogih nič hudega slutečih in zaupljivih sodelavcev. Pri tem se verjetno sploh ni sposoben zavedati nemoralnosti in neetičnosti svojega početja. Prisotnost psihopatije v delovnem okolju pa ima uničevalni vpliv na dostojanstvo zaposlenih, dolgoročno zastruplja delovno okolje, uničuje timsko delo in zaupanje.

P. Babiak in R. D. Hare sta v knjigi »Kače v obleki: Ko gredo psihopati v službo« (2007) razložila, kako psihopati s pomočjo manipulacij napredujejo na hierarhičnih lestvicah, delujejo na svojih delovnih mestih, kakšen destruktiven vpliv imajo na sodelavce in na organizacije ter zakaj ne čutijo obžalovanja in krivde za povzročeno nasilje. Izpostavila sta komaj opazne, vendar ključne razlike med pristnimi voditeljskimi sposobnostmi in psihopatskimi lastnostmi. Možno je, da ima na videz uspešni vodja ali manager psihopatsko osebnostno strukturo, vendar mu jo uspeva uspešno nadzorovati, da ne prihaja v nasprotje z družbenimi normami in dobro prakso. Problem je, da so lahko disocialne osebnostne motnje globoko zakoreninjene v njem in se kažejo kot neupogljivi odziv na širok spekter medosebnih odnosov. Žal zdravljenje te osebnostne motnje ni preveč uspešno.

Ukrepi za boljši nadzor na delovnem mestu

Najuspešnejši ukrepi in postopki nadzora so tisti, ki zajemajo najširše vidike tveganj, in sicer:

Vodenje delovnega procesa
Zaposlenim je treba povedati (jih usposobiti), kaj od njih organizacija pričakuje in v čem se nanje zanese (zaupa). Kadar zaposleni ne stori, kar se od njega pričakuje, je to veliko pogosteje posledica napake , »šuma« v medsebojni komunikaciji kot pa kakršnokoli pomanjkanje motivacije, volje ali namena.

Vodstveni nadzor
Nadziranje izvajanja dela je ena od treh temeljnih nalog managerja. Nadrejeni mora nadzirati in opazovati odklone zaposlenih od izvajanja predpisanih navodil, ukrepov in postopkov ter v primeru potrebe pravočasno reagirati na to.

Pravni, organizacijski, kadrovski, fizični in tehnični ukrepi
»Utrjevanje« možnih področij preboja zaščite premoženja organizacije, omejevanje dobička kaznivega dejanja in povečanje tveganja za napadalca so tesno povezana s pravnimi, organizacijskimi, kadrovskimi, fizičnimi in tehničnimi ukrepi ter postopki za zaščito.

Nadzor nad dostopom
Omejiti je treba dostop do najbolj vrednih virov premoženja. Čim bolj je navedeni vir vreden, tem več naj bo stopenj nadzora in tem manj naj bo zaposlenih, ki bodo imeli dostop do njega.

Zaključek

Nadzor na delovnem mestu v organizacijah je v večini primerov že vzpostavljen, pri čemer pa niso vsi zaposleni ustrezno nadzorovani. Zlasti priviligirani so tisti, ki imajo pooblastilo, da vodijo in nadzirajo druge (vendar so tudi oni nadzirani s strani principalov: lastnikov ali ustanoviteljev). Poleg koristnih efektov nadzora, delodajalec na svojevrsten način izraža tudi nezaupanje do zaposlenih (več ko je omejitev, več je kršitev). Ob tem je ogrožena zasebnost zaposlenega, saj se ji mora marsikdaj odpovedati zaradi zagotavljanja lastnega obstoja, ki mu ga delo omogoča. Zato se utemeljeno postavlja vprašanje: »Ali je delo načeloma že ovira za posameznikovo svobodo?«

Delodajalčeva naravna težnja po večanju dobička in doseganju drugih ciljev poslovanja se odraža v vse večjih pritiskih na zaposlene, predvsem v smeri povečanja storilnosti. Neredko se zgodi, da je delodajalec v želji po večjem dobičku pripravljen poseči po kakršnemkoli ukrepu, ki vodi k temu cilju, pozabljajoč na psihologijo dela in moto, da je le zadovoljen zaposleni ustvarjalec dodane vrednosti.

Nadzor na delovnem mestu je še posebno zanimiv zato, ker se v zvezi z njim neposredno soočata dva pomembna interesa. Na eni strani je interes delodajalca, da zaposleni čim bolje in učinkoviteje dela, na drugi strani pa je interes zaposlenega, da ga zahteve delodajalca povsem ne razčlovečijo in mu tudi na delovnem mestu dopustijo nedotaknjen del njegove zasebnosti. Obstajajo mnenja, da so zaposleni nagnjeni k lagodju in nedelu, kar jih vse bolj ali manj »potegne« v absentizem ali zabušavanje. Danes tehnologija delodajalcu omogoča že skoraj popoln nadzor nad delom in (zunanjim) vedenjem zaposlenih. O tem, koliko je to dopustno, moralno in v skladu z deontološkim kodeksom, so mnenja strokovnjakov, delodajalcev in zaposlenih še vedno različna.

Medtem ko delodajalci, ki se odločajo za večanje vseh vrst in oblik nadzora nad zaposlenimi, izpostavljajo domnevne pozitivne učinke nadzora, obstajajo pa tudi mnenja kadrovskih strokovnjakov, da so pozitivni učinki nadzora le kratkoročne narave, celo več – na dolgi rok naj bi vodili k slabšim delovnim rezultatom. Npr. nasprotniki tehničnega nadzora zaposlenih dokazujejo, da večanje nadzora izkazuje nezaupanje delodajalca do zaposlenih, iz česar lahko sklepamo, da če delodajalec ne zaupa zaposlenemu, zakaj bi ta zaupal delodajalcu. Z večanjem nadzora naj bi hkrati upadala motivacija zaposlenih, saj ta ne temelji več na spodbudah in medsebojnem zaupanju, temveč zgolj na strahu pred morebitnimi sankcijami.

Izkušnje kažejo, da je treba vzpostaviti ustrezno kontrolo nad izvajalci nadzora na delovnem mestu, da ne bi ti popolnoma prevladali in ne bi bili edini, ki odločajo o tem, kaj je prav in kaj ni. Potrebujemo veliko več znanja in ozaveščanja o tem pojavu, obenem pa bi morali spodbujati v korporativnih okoljih sorazmernost, integriteto, družbeno odgovornost, empatijo in etiko soodvisnosti. Upošteva naj se latinski izrek: »Nikomur ni prepovedano delati sebi v korist, dokler ne škoduje drugim!« ■



POSVET

NADZOR NA DELOVNEM MESTU

27. septembra 2017, Ljubljana

Pridružite se nam na strokovnem posvetu z vrhunskimi strokovnjaki, ki prinaša:

- celovit pogled na obvladovanja tveganj pri delovanju organizacij v okviru odnosa zaposleni – delodajalec
- aktualne novosti s področja nadzora na delovnem mestu
- odgovore na kadrovske, pravne, varnostne in organizacijske vidike glede nadzora na delovnem mestu
- dobre prakse.

www.planetgv.si

ORGANIZATORJA POSVETA

PLANET GV

ICS
Institut za korporativne varnostne študije

BREZPLAČNA ŠTEVILKA
080 33 44

Avtor: Ingo Falk Pasch Wallersberg / Slovensko združenje korporativne varnosti



MONOPOL DRŽAVE NA PODROČJU ZAGOTAVLJANJA NACIONALNE VARNOSTI – ALI SPLOH ŠE OBSTAJA ?

Danes se sprašujemo, ali ta klasičen državni monopol na področju uporabe sile in ta klasična interna delitev področij zagotavljanja varnosti na omenjena njena državna sektorja še vedno velja.

Zagotavljanje varnosti je bil od nekdaj državni monopol – omejen na delo policije in vojske, katerih področji delovanja sta bili tudi od nekdaj strogo ločeni:
- delovanje policije na t.i. notranjo varnost v državi
- delovanje vojske na zagotavljanje varnosti države v zvezi z rizičnimi oz. agresorskimi izzivi iz tujine.



Še pred nekaj desetletji bi bila zastavitev takšnega vprašanja popolnoma nerazumljiva. Nasprotno danes, ko se na področju zagotavljanja varnosti pojavlja in etablira vrsta dodatnih subjektov, predvsem neposredno iz gospodarstva kot tudi iz področja znanstvenih dejavnosti in iz vrste družbenih organizacij. Varnost je postala ena izmed čedalje bolj iskanih tržnih storitev, čedalje bolj aktualnih znanstveno raziskovalnih področij in čedalje bolj številnih in specializiranih humanitarnih aktivnosti. Predvsem pa njeno zagotavljanje čedalje bolj izginja kot državni monopol. Nekdaj jasne opredelitve izključnega državnega monopola na tem področju postajajo čedalje bolj zabrisane, pa tudi sama nekdaj popolnoma jasna razmejitev področij delovanja obeh njenih glavnih državnih nosilcev vedno hitreje izginja, še posebej v kriznih situacijah.

Vse kaže, da smo na področju varnosti priča enemu izmed najbolj dinamičnih, silovitih procesov razvoja, v katerem se rušijo vsi nekdanji etablirani pojmi in omejitve – predvsem pa, da je zagotavljanje varnosti državni monopol.

Delovanje zasebnega varovanja v javnem interesu

Glede na aktualne podatke o številu policistov v primerjavi s številom varnostnega osebja lahko ugotavljamo, da je poklicni kadrovski potencial v obeh ključnih segmentih, tako na ravni države kot v zasebnem sektorju, dokaj izenačen. Po aktualnih objavljenih podatkih s strani MNZ znaša v Sloveniji število uniformiranih in neuniformiranih policistov skupno 7.044 oseb. Po podatkih, objavljenih na strani evropskega Združe-



nja CoESS, je v Sloveniji v letu 2013 znašalo skupno število varnostnega osebja 7.520 oseb. Za primerjavo naj navedem podatke za ZR Nemčijo. Po navedbah predsednika nemškega policijskega sindikata g. Oliverja Malchowa je bilo v Nemčiji leta 1990 cca 56.000 delavcev na področju zasebnega varovanja, po aktualnih današnjih podatkih pa jih je že cca 233.000. Gre za izjemno velik porast delavcev v zasebnem varovanju, pri katerem se že dosega aktualni številčni obseg pripadnikov nemške policije, t.j. 265.000 policistov.

Posebej pomembna je čedalje pogostejša zaznava, da se polje dejavnosti zasebnega varovanja **vedno bolj širi**. Dosedanja splošna politična, strokovna in zakonska omejitev pooblastil varnostnega osebja na obseg pooblastil, ki jih ima lahko tudi vsakdo, in s tem njihova nedvoumna ločnica od tistega obsega pooblastil, ki jih imajo pooblaščene uradne osebe, predvsem policija, se je v zadnjih dveh desetletjih močno razrahljala. Danes celo v državah, ki so vse do nedavnega strogo vztrajale na navedeni nedvoumni ločnici obsega pooblastil na področjih policije in zasebnega varovanja, še posebej v Nemčiji, prihaja do opaznega mehčanja te ločnice. Meje med obsegom pooblastil, ki jih ima policija, in tistim, ki se v ustreznih rizičnih razmerah omogočajo tudi varnostnemu osebju, so čedalje bolj zabrisane. Tako se danes v evropski strokovni javnosti čedalje pogosteje oglašajo vprašanja, ali se država umika iz področja zagotavljanja varnosti in, če je temu treba pritrditi, v kakšnem obsegu.

Pri obravnavi in razmejevanju področij pristojnosti policije in varnostnih služb pa ne smemo prezreti še vrsto drugih služb in pooblaščenih izvajalcev, predvsem občinskih redarskih služb, katerih delovno področje je vzdrževanje reda na javnih površinah. Delo teh služb se v praksi prav tako pogosto prepleta z delovanjem varnostnih služb – ne glede na to, da naj bi bilo področje slednjih služb – za razliko od redarskih – omejeno na zasebne površine. Določene posebnosti in razlike na tem področju obstajajo prav tako npr. v Nemčiji, kjer imamo ne le različne strokovne profile varnostnikov glede na obseg in stopnjo njihove usposobljenosti, marveč tudi glede na specifično področje njihovega delovanja in vnaprej predvidenega delodajalca, kar še posebej velja za t.i. strokovne delavce za zaščito in varovanje pri nemških železnicah. S tem pa področje dejavnosti in posebnih poklicnih profilov v okviru tega izjemno obsežnega in strokovno raznovrstnega področja varnosti še zdaleč ni izčrpano. Varnost je namreč kot kriterij in ena izmed najbolj ključnih zahtev povezana praktično z vsemi področji našega delovanja in z vsemi segmenti ter prostori našega bivanja. V današnjem času napredujoče kibernetike in robotizacije se zdi problematika zaščite elektronskih in računalniških povezav ter še posebej informacijske varnosti (ki jo je Zbornica za zasebno varovanje že pred dvema desetletjema brezuspešno skušala kot posebno področje uvrstiti v panožni zakon) že pretečena in zastarela. Verjetno pa bi se morali danes – prav zaradi naše čedalje večje globalne ogroženosti – veliko bolj usmeriti na proučevanje in preprečevanje naših današnjih bivanjskih stranpoti.

Zasebno varovanje tako po sili razmer že dolgo prevzema tudi naloge, ki sodijo na področje zagotavljanja javne varnosti in, ki naj bi bile sicer po tradicionalnem pojmovanju izključna domena državnih aktivnosti, predvsem Policije.

Privatizacija in s tem gospodarsko izvajanje nekdanjih izključnih državnih pristojnosti je v polnem teku.



Dejstvo je, da je danes v razvitem svetu - in tako tudi pri nas - zasebno varovanje sestavni del državnega varnostnega sistema. Najbolj nazorno je bilo to v zadnjem času vidno jeseni 2015 ob tako imenovani begunski krizi, ko so varnostne službe ob policiji in kasneje tudi vojski opravljale varnostne in redarske posle. Sicer pa dejstvo, da varnostne službe opravljajo redarske in varnostne naloge tudi na javnih površinah, zlasti v primerih varovanja javnih prireditev, ni nikakršna novost. Podobno velja tudi v Nemčiji (in z več ali manj izjemami tudi v drugih državah EU). Tako varnostniki tam varujejo, npr. tudi postaje podzemne železnice, ki so popolnoma javna površina, dostopna vsakomur. Zasebno varovanje varuje tudi ustavno zajamčene pravice in preprečuje izvršitev kaznivih dejanj, prav tako na javnih površinah. Dalje opravlja zasebno varovanje pri nas, pa tudi marsikje v tujini, potrebne storitve preverjanja potnikov in pregleda njihove prtljage na javnih letališčih in še vrsto drugih storitev na javnih površinah (npr. pri varovanju prevozov ali varovanju javnih zbiranj), pa tudi v javnem interesu, tako zlasti v zadnjem času še posebej v zaprtih ustanovah za nastanitev ilegalnih migrantov in pri njihovem vračanju v državo, iz katere so pripotovali. Vse to so storitve v javnem interesu in na površini, ki jo moramo označiti mnogokrat vsaj kot pol-javni, če ne velikokrat celo kot popolnoma javni ali po drugi strani tudi kot posebej zavarovan državni prostor.

V okviru tega silovitega razvoja zasebnega varovanja pa lahko beležimo tudi hude stranpoti, kaznive zlorabe te dejavnosti za huda kriminalna dejanja. V Sloveniji se lahko zlasti spominjamo še vedno ne popolnoma razčiščenega ropa SKB banke pred leti, pri katerem so sodelovali varnostniki družbe PCA (ki sicer ni bila članica ZRSZV). Na svetovnem prizorišču pa nam ostajajo pred očmi tudi grozljiva zločinska početja sodelavcev takratne ameriške zasebne vojaško varnostne službe »Blackwatter« po zasedbi Iraka v samovoljno sproženi vojaški invaziji (brez mandata UNO) s strani ZDA, Anglije in t.i. »koalicije voljnih« v zaporu Abu Ghuraib. V teh zločinskih dogajanjih je imela posebno vlogo prav omenjena zasebna firma (ki se je konec februarja 2009 nato preimenovala v družbo »Xe«, kasneje pa še enkrat v nadaljnjo novo firmo »Services LLC«, očitno iz razloga, da zabriše sledi svoje kriminalne preteklosti).

Zasebno varovanje tako po sili razmer že dolgo prevzema tudi naloge, ki sodijo na področje zagotavljanja javne varnosti in, ki naj bi bile sicer po tradicionalnem pojmovanju izključna domena državnih aktivnosti, predvsem Policije. Vzroka za takšen razvoj sta predvsem dva:

- s hitrim tehnološkim razvojem hkratno vedno večje širjenje nacionalno zelo pomembnih novih tehnoloških postopkov in produktov, ki zahtevajo ustrezen odziv policije in drugih državnih notranjih varnostnih struktur, s tem pa njihovo dodatno obremenjevanje;
- dolgoletno absolutno krčenje stroškov za vzdrževanje in razvoj državnih policijskih in vojaških kapacitet (z izjemo letošnjega leta zaradi nastalih izrednih razmer v posledici lanskoletnega emigrantskega na-vala).

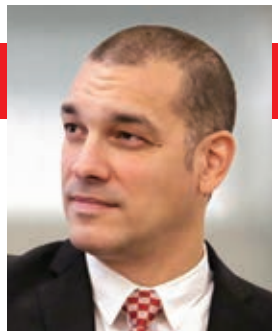
Varnost – državni monopol?

Po zgoraj navedenih ugotovitvah zagotavljanje varnosti znotraj civilne družbe **sploh ni več izključni monopol države**. Res imajo državni organi posebne pristojnosti in pooblastila na tem področju, res pa je tudi, da imajo tudi drugi organi in organizacije na tem področju prav tako določene pristojnosti in naloge, katerih kvaliteta in obseg sta se v zadnjih desetletjih vztrajno širila. Ali takšen razvoj daje potrebno jamstvo za ohranjanje oziroma celo izboljševanje pravne varnosti, je vprašanje, ki ga puščam odprtega. Sicer pa bi bil tudi nikalni odgovor brez učinka, ker je razvoj že šel v svoji smeri. Privatizacija in s tem gospodarsko izvajanje nekdanjih izključnih državnih pristojnosti je v polnem teku. Obseg te privatizacije je v različnih državah zelo različen – najbolj pa je viden tako v družbenih okoljih z nizkimi demokratičnimi standardi kot tudi v družbenih okoljih visokih socialno ekonomskih razlik. Gospodarska in s tem ciljno za doseganje čim večjega dobička usmerjena dejavnost varovanja postaja dvorezen meč – glede na dane okoliščine se vselej lahko odpre **vprašanje prevladujočega interesa: varnosti naročnika ali čim večje lastne koristi.** V teh danes prevladujočih pogojih varovanja sta odnos do naročnika in korektno strokovno izvrševanje dejavnosti stalno na preizkušnji. Bati pa se je, da je v danih okoliščinah zaostrene konkurence predvsem na določeni ravni, zlasti t.i. fizičnega varovanja, tudi odnos vodstva družbe do zaposlenega varnostnega osebja ambivalenten, t.j. po eni strani njegovega čim večjega delovnega izkoristka in po drugi strani njegovega čim nižjega plačila.

Ali so ti zakonsko nezadovoljivo opredeljeni odnosi med varnostno družbo in njenim naročnikom na eni strani in hkrati med njo in njenim varnostnim osebjem na drugi strani v dejavnosti, ki je v resnici zelo občutljiva in rizična ter temelji na razmerju medsebojnega zaupanja, dobra popotnica za uspešno izvajanje varovanja, je zelo veliko vprašanje.

Slej ko prej si bo morala država ponovno zelo resno zastaviti to vprašanje. ■

Avtor: Antun K. Buterin / Business Development Manager, Hikvision**



PAMETEN VIDEO NADZOR ZA MIRNEJŠA MESTA IN VARNEJŠE PREBIVALCE

Rešitve za videonadzor mest in drugih javnih območij – varnost po meri za manjša mesta in predmestja.

Mesta širom sveta so vsako leto pametnejša. Organe mnogih mest, zmeraj bolj privlači bližč sodobne informacijske in komunikacijske tehnologije, ki jim omogoča izboljšavo vsakodnevnega življenja prebivalcev. Hkrati je večja tudi potreba po tem, da bi se prebivalci na mestnih in predmestnih območjih počutili varne, zato vse bolj potrebujemo ukrepe za doseganje zadostne ravni varnosti. Tako je govora o popolnem spoju tehnologije in ljudske potrebe po varnosti. Cilj je jasen – narediti mesta in življenje v njih varnejše in lepše.

V podjetju Hikvision, kot vodilnem svetovnem proizvajalcu video nadzornih kamer in rešitev, katero že več kot 5 let drži 1. mesto v video nadzornih rešitvah, se intenzivno ukvarjajo z vsemi pogledi varnosti. Vsekakor to počnejo tudi ostala podjetja iz varnostne industrije. Kvalitetnejše rešitve za video nadzor zagotavljajo kakovostne in zanesljive sisteme, preproste za uporabo, ki jih je mogoče nadgrajevati ob naraščanju potreb, zaradi česar so dobra in dolgoročna naložba. Sistemi z visoko ločljivostjo zagotavljajo kristalno jasno sliko, ki zajame celo najmanjše podrobnosti v vsakršnih svetlobnih razmerah. Urbana varnost je področje, v katerem do izraza lahko pridejo samo kvalitetni izdelki. Zato je varnost mest, eno od mnogih vertikalnih tržišč, katerim so posvečene različne rešitve in inovativne ter pametne tehnologije strokovnjakov vseh svetovnih proizvajalcev varnostnih rešitev. Rešitev Pametno mesto ki, je sestavljeno iz širokega nabora izdelkov, kateri so zasnovani z enim samim namenom – pomagati mestnim oblastem v strateški implementaciji pametnih tehnologij.

Rešitev Pametno mesto nudi popolnoma vse, kar je potrebno:

- **Učinkovita zaščita stanovalcev ter javne in privatne lastnine;**
- **Učinkovito preprečevanje vandalizma in nepričakovanih napadov;**
- **Povečanje učinkovitosti preiskav in krajši reakcijski čas;**
- **Lažje in enostavnejše upravljanje s prometom.**

Rešitev Pametno mesto je zanesljiv IP sistem, posvečen splošni varnosti mesta, prebivalcev in poslovanja, ki ga odlikujejo naslednje lastnosti:



Izdelki kateri povezujejo ICT in ljudi na inovativen in koristen način

**Promocijske vsebine

HIKVISION



ŠT. 1 NA SVETU V VIDEO NADZORU

Hikvision Europe
Dirk Storklaan 3,
2132 PX Hoofddorp,
The Netherlands

Pooblaščeni distributer
Mars Commerce
Mirka Vadnova 19
4000 Kranj, Slovenija

www.hikvision.com

1. **NADZOR MESTNIH TRGOV IN PARKOV**: Različni modeli PanoVu kamer, ki omogočajo panoramski prikaz in brezkončne detajle, saj so ta območja noč in dan polna ljudi.
   - kamere DarkFighter: od 36x IR PTZ kamere do zunanje bullet kamere, te kamere omogočajo jasen pregled kljub slabi svetlobi;
   - kamere PanoVu s 4 ali 8 slikami naenkrat: panoramski prikaz 8MP ali 16MP, ter 23x 2MP PTZ kamera za prikaz najmanjših podrobnosti;
   - 4K Ultra HD kamere: v primeru potrebe po najvišji ločljivosti in mikroskopskih podrobnostih v sliki.

2. **NADZOR PROMETA IN JAVNEGA PREVOZA**: V sklopu sistema za obrambo pred terorizmom in žeparjenjem, razviti so posebni modeli mobilnih kamer in snemalnikov, za nadzor v avtobusih, tramvajih in vlakih, ter HD kamere za zaščito potnikov in postajališč, kakor tudi za spremljanje gibanja vozil po zastavljenih privzetih poteh. Poleg tega prometne kamere in radarji za merjenje hitrosti zagotovljajo forenzično natančnost posnetkov in video posnetkov prehitrih vozil in drznih voznikov, ki povzročajo nevarnost na mestnih cestah.
   - Sistem za namestitev v avtobuse: HD IP ali HD-TVI sistem, v kompletu s platformo GIS, za brezžično spremljanje videa v živo in vpogled v trenutno lokacijo vozila;
   - Sistem za namestitev v tramvaje in vlake: robustni mrežni snemalnik in kamere z IR-om in „ribjim očesom“ naredijo HD rešitev za javni promet in dvojne termalne kamere ter PanoVu kamere ščitijo območje in največje postaje.

3. **NADZOR JAVNIH PARKIRIŠČ**: Celovito rešitev sestavljeno iz razpoznave tablic (ANPR), samodejnih zapornic in štetja vozil, ter PanoVu kamer, za zaščito velikih odprtih območij, tudi v megli, dežju ali slabi vidljivosti. Poleg tega, platforma iVMS in LED oznake, prikazujejo prosta mesta na parkiriščih.
   - Panoramske kamere PanoVu: 4 različni modeli inovativnih in dizajnerskih atraktivnih kamer Darkfighter, nudijo panoramski prikaz in vrhunske podrobnosti, tudi v mraku.
   - ANPR kamere za samodejno prepoznavanje tablic: podpirajo Full HD video, povezujejo se z zapornicami, odporne so na vse vremenske pogoje, omogočajo belo in črno listo vozil, ter razna poročila.

Pametne funkcije kot dodana vrednost k varnosti prebivalcev in javne lastnine.

4. **NADZOR OBMOČJA**: Od morske ali rečne obale, do puščave ali zapuščenih mest. Mestne meje so pogosto na udaru ilegalnih migracij, tihotapljenj in drugih oblik kriminala. Za proaktivno varovanje območja, se priporočajo vrhunske termalne kamere in sistem z dvojnimi lečami, medtem ko laserski sistemi za sledenje in detekcijo, lahko že iz velike razdalje, zelo zgodaj odkrijejo vsiljivca in pravočasno preprečijo vdor.
   - Termalne kamere z dvema senzorjema: en senzor nudi termalno sliko za detekcijo iz razdalje, Darkfighter senzor pa omogoča normalno vizualno sliko za pregled in snemanje podrobnosti.
   - Laserski sistem za pozicioniranje: Full HD kvaliteta videa, 36x optični zoom, domet laserske svetlobe do 1km oddaljenosti.

5. **NADZOR VODNIH OBMOČIJ**: Za obalno stražo so najbolj primerne kompaktne antikorozivne HD kamere iz nerjavečega jekla, pri čemer se kamere lahko namestijo tudi na plovila, kjer kljubujejo vetru, soli, dežju in valovom.

6. **ZAČASEN POLICIJSKI NADZOR**: Za začasen policijski nadzor, v času protestov, parad ali koncertov, se kot enostavna in priročna rešitev uporablja mobilna HD PTZ kamera, katera se hitro in enostavno s pomočjo magneta ali trinožca namesti na streho policijskega vozila, v katerem je nameščen snemalnik. Policija lahko s tako hitro reakcijo prepreči nasilje in hitro odkrije povzročitelje. Isti cilj je mogoče doseči tudi s samostojno HD PTZ kamero, za namestitev na vozila z vgrajeno baterijo. Tukaj pa so tudi prenosne kamere za namestitev na telo policistov, ter prenosni snemalnik, ki omogoča povezovanje preko WiFi ali 3G/4G povezave.

7. **NADZORNI CENTER**: V centrih za nadzor in hrambo pomembnih podatkov, priporoča se uporaba centralizirane platforme za upravljanje z video nadzornimi sistemi (iVMS) ter »Video Wall« sisteme. Srce video nadzornega sistema je njegova upravljalna in nadzorna platforma: sistem za upravljanje videa. Programska oprema iVMS-5200 je namenjena preprostemu in učinkovitemu upravljanju vseh uporabljenih kamer (fiksno usmerjene kamere, vrtljive kamere za široka območja ali kamere za branje registrskih tablic). Zagotavlja sliko v živo, dostop do posnetkov, alarmna opozorila, ogled na več zaslonih z diagrami in pojavnimi okni za dogodke, ter oddaljeno pretakanje vsebine na mobilne naprave. Strežnik/platforma z odjemalci omogoča hkratno delo več uporabnikov, brez prekinitev, 24 ur dnevno.

Fiksne kamere za določena območja: kamere za nizko in zelo nizko osvetlitev s tehnologijo DARKFIGHTER



Milijoni kamer in snemalnikov širom sveta v manjših in velikih mestih vsakodnevno dokazujejo svojo stabilnost, vzdržljivost in koristnost



Ko si mestne oblasti pomagajo s sistemom - Pametno mesto, se v tej skupnosti, dokazano izboljšujejo vsakodnevne razmere za življenje.

Za nadzor nad občutljivimi lokacijami je najboljša rešitev kamera z box ohišjem polne visoke ločljivosti z več milijoni slikovnih pik in zamenljivim objektivom ali bullet kamera v obliki cevi z integriranim infrardečim elementom za osvetlitev in motoriziranim objektivom s samodejno ostritvijo in povečavo za dnevno/nočno snemanje. Če je osvetlitev zelo nizka, vendar pa kljub temu potrebujete barvne slike, za natančnejši pregled nad dogajanjem, je tehnologija DarkFighter na voljo pri mrežnih kamerah z občutljivostjo Ultra Low-Light.

Videokamere s polno visoko ločljivostjo in kamere za nizko osvetlitev: visoka ločljivost za ostro sliko podnevi in ponoči

Glavni namen video nadzornega sistema za mesta je nedvomno odpravljanje kaznivih dejanj, če pa jih le ni mogoče odpraviti, bo posneto gradivo neuporabno, če slika ni dovolj jasna. Namenska, visokokakovostna, posebej zasnovana oprema, je potrebna za zajem čiste slike registrskih tablic, vozil, obrazov in nezakonitih dejanj, pri čemer so razmere pogosto neugodne. Rešitve z več milijoni slikovnih pik v polni visoki ločljivosti (1.920 × 1.080 slikovnih pik) so popolne za ugotavljanje in prepoznavanje nezakonitih dejanj. Zagotavljajo jasne slike ne glede na svetlobne razmere, zahvaljujoč inovativni tehnologiji Low-Light in Ultra Low-Light, za snemanje ob nizki osvetlitvi. Pametne funkcije kot dodana vrednost k varnosti prebivalcev in javne lastnine.

Pametno zaznavanje kakovosti videa: Funkcija za nadzor kakovosti videa, kameri omogoča samodejno diagnosticiranje kakršnihkoli anomalij pri snemanju (izguba ostrine, premik kamere iz želenega položaja ali prekrivanje kamere za onemogočitev njenega delovanja), ter sproži lokalne in oddaljene alarme za sabotažo v nadzornem in upravljalnem središču.

Pametno izničevanje megle: S tem se lahko upravljavec, ki je odgovoren za nadzor nad območjem ali regijo, celo v nizki vidljivosti (megla, dim ipd.), zanese na instrument z izjemno sposobnostjo prilagajanja slike, ki izboljša kakovost in ostrino slike, ter zagotovi najboljše rezultate kamer.

Pametno zaznavanje prečkanja črte: Ta funkcija sproži alarm ob prečkanju vsaj ene predhodno nastavljene virtualne črte. Upravljavcem omogoča nadzor cestnih in prometnih predpisov, npr. prečkanje pešcev na prepovedanih mestih (obvoznice, avtocestni obroči) in vozila, ki na enosmernih cestah vozijo v napačno smer, polkrožno obračajo ali kako drugače kršijo prometne predpise.

Pametno zaznavanje vdora: Ta funkcija omogoča zaščito določenega območja z alarmom, ki se sproži samo, ko kakšen predmet, predhodno opredeljene velikosti, »nedovoljeno« prečka območje, pri čemer prečkanje traja določen čas. Tako je mogoče, v določenih časovnih obdobjih, nadzirati in upravljati dostop do zasebnih cest, javnih parkov, šol, spomenikov, odlagališč odpadkov ipd. z namenom nadzora nad javno lastnino in njene zaščite.

Prepoznavanje avtomobilskih registrskih tablic ANPR: Zahvaljujoč vgrajenemu algoritmu funkcija ANPR v kameri med snemanjem, samodejno prebere registrske tablice. Algoritem prepozna glavne formate evropskih registrskih tablic in jih lahko razvrsti glede na državo.
Ko se letos pametne IP kamere integrirajo z umetno inteligenco, bodo naša mesta postala še bolj varna. ■

Avtor: Andrej Drapal/ Consesus d.o.o.



OBVLADOVANJE TVEGANJ IN CELOVITO POROČANJE

Pri ocenjevanju organizacijskega tveganja obstoječa praksa izpostavlja finančna tveganja, tem pa sledijo preprečevanje tveganj za nesreče pri delu ter ocena in obvladovanje tveganj za fizično varnost, še posebej objektov, ki so ranljivejši kar zadeva vandalizme ali teroristične napade.

Za navedena tri področja tveganj obstajajo tri specializirane skupine strokovnjakov, ki se ukvarjajo s posameznimi tveganji. Ti vrednotijo ter pripravljajo in izvajajo ustrezne ukrepe za preprečevanje finančnih, delovnih ali fizičnih nesreč oziroma prilagoditev nanje. Od vseh treh področij so le finančna tveganja resnično integrirana v poslovne načrte, modele in poročila, medtem ko preostali vrsti tveganj lahko vidimo le v **izkazu poslovnega izida**, le redko pa sta omenjeni tudi v **bilanci stanja**, vendar vanjo nista res integrirani.

Ob redkih izjemah se večina organizacij z obvladovanji tveganj spopada na ravni ocenjevanja in preprečevanja, tako da so stroški ocenjevanja in preprečevanja različnih tveganj vključeni v izkaz poslovnega izida, ne pa tudi v bilanco stanja. Tveganja so ovrednotena kot strošek aktivnosti preprečevanja, ne pa tudi kot vrednost ali znižanje vrednosti na nivoju tržne vrednosti oziroma skozi bilanco stanja.

Poglejmo si recimo Investopedio (www.investopedia.com). Med obveznostmi, kjer lahko najdemo oziroma bi morali najti ocenjevanje tveganj, Investopedia navaja:

Kratkoročne obveznosti lahko vključujejo:

- *Kratkoročni del dolgoročnega dolga*
- *Dolg do bank*
- *Obveznosti iz obresti*
- *Najemnino, davke, komunalne storitve*
- *Obveznosti iz plač*
- *Predplačila strank*
- *Obveznosti iz dividend in drugo*

Dolgoročne obveznosti lahko vključujejo:

- *Dolgoročni dolg: obresti in glavnico na izdane obveznice*
- *Obveznosti iz pokojninske blagajne: denar, ki ga mora podjetje vplačati v pokojninski sklad za svoje zaposlene*
- *Odloženo davčno obveznost: davke, ki so bili obračunani, vendar še eno leto ne bodo plačani; poleg časovnega okvira ta številka usklajuje razlike med zahtevami glede finančnega poročanja in načinom ocenjevanja davka, kot so izračuni amortizacije*

In to je vse! Najdemo lahko le obveznosti, povezane s finančnim kapitalom, in finančne obveznosti, povezane s finančnim vidikom delovne sile, ni pa niti sledu o preostalih omenjenih področjih tveganj in obveznostih, povezanih s tveganji. Celo tveganja vezana na fizično varovanje niso niti omenjena. Preprosto lahko torej sklenemo, da obstoječa praksa ni sposobna integrirati ustvarjanja in tveganj vezanih na katerikoli drug kapital, razen finančnega.

Odgovoriti je torej potrebno na vprašanje, kako naj organizacije najdejo način vrednotenja ostalih kapitalov. Narediti je potrebno seznam možnih tveganj po različnih kapitalih. Pri tem je zanimivo, da vsak razumen vlagatelj intuitivno, če že ne racionalno, oceni vse takšne obveznosti – ne le finančnih – ko kupuje delnice ali sklepa druge posle z organizacijo. Vsi organizacije ocenjujemo celostno in poskušamo vzeti v obzir vsa možna tveganja na vseh možnih ravneh.

Poudariti želimo, da tveganj na vseh ravneh ne bi smeli obravnavati zgolj kot stroške, temveč tudi kot obveznosti, z besedami in številkami izražene v bilanci stanja, ki so bile predhodno zasnovane v postopku celovitega poročanja.

Na tem mestu ni mogoče našteti vseh možnih tveganj, saj jih je preveč. V nadaljevanju lahko z bežnim pogledom po dostopnih virih vidimo, da gre za izredno obširno tematiko.

Preprosto lahko torej sklenemo, da obstoječa praksa ni sposobna integrirati ustvarjanja in tveganj vezanih na katerikoli drug kapital, razen finančnega.

Poudariti želimo, da tveganj na vseh ravneh ne bi smeli obravnavati zgolj kot stroške, temveč tudi kot obveznosti, z besedami in številkami izražene v bilanci stanja, ki so bile predhodno zasnovane v postopku celovitega poročanja.

International Conference on Risk Assessment (in Health) (Mednarodna konferenca o oceni tveganja (v zdravstvu)). *Toxicology and Risk Assessment Conference* (Konferenca o toksikologiji in oceni tveganja). *Trust and Reputation Risks* (Zaupanje in tveganje izgube ugleda). *Defence &HLS conference* (Konferenca o obrambi ter zdravju in varnosti). *Cybersecurity* (Kibernetska varnost). *Workforce Legal Risks* (Pravna tveganja pri delovni sili). *Intelectual Property at Risk* (Intelektualna lastnina v nevarnosti). *Machine Safety Risk Assessments* (Ocene varnostnega tveganja pri strojih). *Safety Leadership Conference* (Konferenca o vodenju na področju varnosti). Itd. Itd.

Moj namen ni bil sestaviti izčrpen seznam, ampak opozoriti na obstoj številnih drugih možnih tveganj in tako narediti področje tveganj bolj otipliv. Nekatera tveganja so specifična za določene sektorje, mnoga pa so relevantna za vse tipe organizacij, četudi se njihove pojavne oblike med posameznimi organizacijami razlikujejo glede na poslovni model organizacije.

Seveda pa definiranje možnih tveganj za neko konkretno organizacijo še ni dovolj. Priti je potrebno do **celovite bilance stanja.** Postopek za vzpostavitev celovite bilance stanja opredeljuje nova praksa Celovitega poročanja (http://integratedreporting.org/). Ko soočimo sistem za celovito poročanje in **celovito bilanco stanja**, naletimo na dva izziva oziroma nalogi:

- Opredeliti grožnje/tveganja/obveznosti za vsak pomemben mehanizem poslovnega modela, ki poganja ustvarjanje vrednosti na kateremkoli od šestih vrst kapitala.
- Upoštevati, da posamezni mehanizmi ne delujejo izolirano, temveč so odvisni od rezultatov vseh drugih mehanizmov v poslovnem modelu.

Prva naloga je lažja. Morali bi se preprosto poglobiti v vsak postopek poslovnega modela in **odločiti o kritičnih točkah (*Critical Performance Indicator* – KPI)**, ki največ prispevajo k uspehu posameznega postopka in poslovnega modela kot celote.

Ni zunanjega pravila, kako izbrati najpomembnejše kritične točke, saj za to ni splošnega pravila, kot tudi ni splošnega poslovnega modela. Vsak poslovni model je edinstven, tako kot je edinstven vsak človek, čeprav nas ima večina dve nogi, pljuča in možgane. Na voljo ni nobene zunanje pomoči za opredelitev modela, po katerem se vsakdo od nas razvija kot človeško bitje. Praksa in teorija celovitega poročanja opozarjata le na najpogostejša mesta, kjer lahko najdemo KPI, vendar pa vsak kapital svojo vrednost dosega na svoj način. Šest vnaprej določenih vrst kapitala je tu samo zato, da nam pomagajo opredeliti celotno vrednost kapitala. Vendar pa še vedno nimamo zunanjega pravila niti število obstoječih vrst kapitala. Precej preprosto bi lahko število vrst kapitala povečali tako, da bi poiskali manjše podvrste kapitala znotraj šestih, opredeljenih v postopkih celovitega poročanja.

Za začetek torej vemo, da je treba v mehanizmih poslovnega modela definirati ne le finančni, ampak tudi proizvodni, intelektualni, človeški, družbeni in na-



ravni kapital, tako da se vsak mehanizem loteva vsaj enega od šestih vrst kapitala in da je na koncu vsak kapital opredeljen ali vključen v vsaj en mehanizem poslovnega modela.

Na tem mestu moramo opozoriti, da na poslovno modeliranje (obvladovanje tveganj je del tega modeliranja) ne bi smeli gledati tako mehanistično, kot je opisano zgoraj. Organizacija je veliko več kot le vsota različnih digitalno opisljivih postopkov. Toda zavoljo ocene in obvladovanja tveganja bi se morali vsaj pretvarjati, da imamo mehanski nadzor nad vsakim postopkom.

Odločilni trenutek prehoda v celovito obravnavo nastopi pri preoblikovanju obvladovanja tveganj, ki je prikazan kot **strošek**, v **odgovornost**, ki je v bilanci stanja prikazana kot **vrednost**. Prav to preoblikovanje dejansko spreminja digitalni/mehanistični pogled na organizacijo v analogno celostno gledanje na organizacijo kot na celostni organizem, ki se odraža skozi bilanco stanja.

Transformacija iz stroškov v vrednost, iz izkaza poslovnega izida v bilanco stanja, iz digitalnega v analogno, se zgodi z mehanizmi iz druge naloge oz. izziva: razumeti in (kolikor je mogoče) opisati **soodvisnost** vseh kritičnih točk.

Na primer: Fizična varnost jedrske elektrarne je odvisna od:

- Sposobnosti varnostnega osebja.
- Kakovosti izdelkov, vključenih v varnostne sisteme.
- Dodane vrednosti (dobička), ki jo obrat ustvari in je dodeljena varnostnim sistemom.
- Odnosov z lokalnimi skupnostmi, ki predstavljajo prvo stopnjo zaščite pri varnosti jedrske elektrarne.
- Spoštovanja naravnih virov, kot je na primer voda, ki hladi reaktor jedrske elektrarne.
- *Števila strokovnjakov, ki jih ustvari izobraževalni sistem in so na voljo jedrskim elektrarnam.*
- In tako naprej in tako naprej.

Precej očitno je, da je vsaka od omenjenih vrednosti/tveganj/vrst kapitala odvisna od vseh drugih omenjenih in neomenjenih vrst kapitala. Število soodvisnih povezav je tako veliko, da tvorijo kompleksni sistem (nelinearen, nemehanističen), v katerem zaradi kompleksnosti vznikajo mehanistično nepričakovani dogodki. Izredni dogodek je nujen rezultat katerega koli kompleksnega



sistema. Kompleksni sistemi kot na primer človek ali organizacije generirajo vznik (emergence) mehanicistično/digitalno nepredvidljivih dogodkov. Sistem vznika nepredvidljivih dogodkov pa lahko kompleksnosti primerno obvladuje le celovit oziroma integriran mehanizem upravljanja in poročanja.

Zdaj bi že moralo biti jasno, da je glavni izziv celovitega poročanja ne le **prepoznati** tveganja v zvezi z ustvarjanjem vrednosti vsakega kapitala, ampak tudi **poročati** o tveganjih tako, da upoštevamo kompleksnost odnosov, ki se na koncu odrazijo v bilanci stanja.

Posledično organizacije prav tako ne bi smele ločevati prepoznavanja in ocene različnih tveganj. Sicer morajo strokovnjaki tveganja **upravljati**, vendar pa je prepoznavanje in vrednotenje treba razumeti celostno. Jaz sam bi želel, da me pregleda zdravnik, ki dela po načelih celostne obravnave, nato operira visoko specializiran kirurg in na koncu še enkrat celostno pregleda prvi zdravnik. Jedrski reaktor mora varovati visoko specializirana varnostna služba, ki nima veliko časa za razmišljanje, saj mora delovati hitro in zanesljivo. Oceno zahtevnosti tveganj, povezanih z varnostjo jedrskih reaktorjev, in vrednotenje rezultatov pa prepuščamo strokovnjakom, ki razmišljajo celostno in celovito in, ki razumejo nepredvidljivost dogodkov, ki se že po definiciji dogajajo v kompleksnih sistemih. ■

Za začetek torej vemo, da je treba v mehanizmih poslovnega modela definirati ne le finančni, ampak tudi proizvodni, intelektualni, človeški, družbeni in naravni kapital, tako da se vsak mehanizem loteva vsaj enega od šestih vrst kapitala in da je na koncu vsak kapital opredeljen ali vključen v vsaj en mehanizem poslovnega modela.

9. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 14.—15. marec 2018



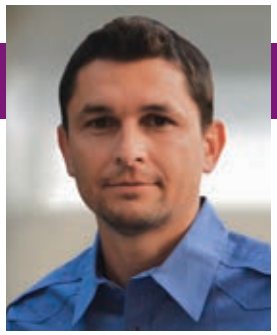
PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

PODELJENE BODO IZBRANIM INSTITUCIJAM IN POSAMEZNIKOM ZA NJIHOV INOVATIVNI PRISPEVEK NA PODROČJU RAZVOJA IN UVELJAVLJANJA VARNOSTI. NAGRADO PODELJUJE ICS-LJUBLJANA V SODELOVANJU S SLOVENSKIM ZDRUŽENJEM KORPORATIVNE VARNOSTI. NEODVISNA KOMISIJA OCENJUJE IN IZBIRA KVALITETO TER IZVIRNOST PRIJAVLJENIH UDELEŽENCEV V NASLEDNJIH KATEGORIJAH:

- NAJBOLJ VARNO PODJETJE
- NAJBOLJŠA KNJIGA S PODROČJA VARNOSTI
- NAJBOLJ VARNO MESTO/OBČINA
- KORPORATIVNO VARNOSTNI MANAGER LETA
- NAJBOLJ INOVATIVNA VARNOSTNA REŠITEV
- INOVATIVNA MEDIJSKA PROMOCIJA VARNOSTI

VEČ O NAGRADI IN NAGRAJENCIH NA SPLETNI STRANI INŠTITUTA WWW.ICS-INSTITUT.SI!

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



REPORTAŽA:
Mednarodna konferenca »Dnevi korporativne varnosti 2017«

PODELITEV NAGRAD »SLOVENIAN GRAND SECURITY AWARD 2017«

8. mednarodna konferenca »Dnevi korporativne varnosti 2017« je privabila več kot 200 udeležencev iz celotne regije JV Evrope.

Inštitut za korporativne varnostne študije (ICS) je ob so-organizaciji Slovenskega združenja korporativne varnosti in SE European Corporate Security Association (SECSA) v mesecu marcu organiziral tradicionalno mednarodno konferenco z nazivom »Dnevi korporativne varnosti«. Dogodek je utrdil sloves najpomembnejšega dogodka s področja korporativne varnosti v celotni regiji. To dokazuje več dejavnikov, od pomembnih gostov gospodarskega in javnega življenja, na sami otvoritveni slovesnosti, število zadovoljnih udeležencev, ki je letos preseglo številko 200, cel niz odmevnih tem, ki so nam jih predstavili vrhunski predavatelji iz Slovenije in iz tujine in nenazadnje prikaz celega niza najnovejših tehnoloških rešitev, katere so na konferenci predstavljali različni razstavljavci.

Konferenco so s svojimi svečanimi nagovori odprli izr. prof. **dr. Denis Čaleta**, predsednik organizacijskega odbora, **mag. Mitja Bervar**, predsednik Državnega sveta Republike Slovenije, **ga. Andreja Katič**, ministrica za obrambo in **g. Boštjan Šefic**, državni sekretar Ministrstva za notranje zadeve. V svojih nagovorih so poudarili zahtevnost varnostnega okolja, ki nas obdaja in pred naše organizacije postavlja kompleksne zahteve za obvladovanje tveganj, katerim smo izpostavljeni. Varnost je postala dobrina, katera je v trenutnih razmerah izredno izpostavljena. Omenjeni dogodek pa predstavlja odlično priložnost za izmenjavo izkušenj, dobrih praks in predvsem najnovejših spoznanj na področju korporativne varnosti.







*avtor je član Slovenskega združenja korporativne varnosti







Na otvoritvi mednarodne konference je potekala tudi podelitev »**Slovenian Grand Security Award 2017**« za dosežke na področju varnosti v preteklem letu. Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje Institut za korporativne varnostne študije, ICS-Ljubljana, v sodelovanju s Slovenskim združenjem korporativne varnosti.

Nagrada je namenjena procesom dvigovanja splošnega zavedanja in varnostne kulture v širši družbeni skupnosti, ki vsebuje poslovna in druga okolja. V šestih kategorijah neodvisna komisija izbira tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev. To kvaliteto nagrajujemo z uglednimi priznanji, ki so bila podeljena za dosežke na področju varnosti v letu 2016.

Nagrado v najbolj cenjeni kategoriji »**Najboljši korporativno varnostni manager**« je prejel **mag. Marko Potokar** iz podjetja Lek d.d., ki mu jo je podelil dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti. Nagrado **»Najbolj varno podjetje«** je tokrat prejelo podjetje **Eles d.o.o**., v imenu podjetja pa jo je sprejel g. Venčeslav Perko, direktor področja za informatiko in telekomunikacije. Ob tej priložnosti je dejal, da so v Elesu veseli, da je neodvisna komisija prepoznala prizadevanja družbe na področju krepitve korporativne varnosti. V družbi ELES, ki upravlja s ključno kritično infrastrukturo državnega pomena, se dobro zavedajo številnih varnostnih izzivov in tudi groženj v današnjem svetu, ki lahko negativno vplivajo na opravljanje svoje dejavnosti. Zato si že dalj časa prizadevajo za vzpostavitev integriranega sistema korporativne varnosti z integracijo korporativnega upravljanja in korporativne integritete.

Nagrado za **»Najbolj varno mesto«** je drugo leto zapored prejela **Mestna občina Ljubljana**. Podžupan g. Aleš Čerin je sprejel nagrado s strani mag. Mitje Bervarja, predsednika Državnega sveta Republike Slovenije. Gospod Boštjan Šefic pa je predal g. Srečku Ocvirku, županu **Občine Sevnica,** nagrado v kategoriji **»Najbolj varna občina«**.

Tokrat je nagrado »**Najbolj inovativna varnostna rešitev**« prejelo podjetje **Interblock d.d.** Nagrado je prevzel direktor informacijskih tehnologij, g. Dejan Dobrovoljc, ki mu jo je predal g. Tomaž Vesel, predsednik Računskega sodišča. Nagrada v kategoriji »**Najboljša knjiga s področja varnosti«** je bila letos podeljena **prof. dr. Bojanu Dobovšku**, ki mu jo je predal g. Andrej Slapar**,** predsednik uprave Zavarovalnice Triglav. **Informativna oddaja ODMEVI** je prepričala neodvisno komisijo in prejela nagrado v kategoriji »N**ajbolj inovativna medijska podpora«**. Nagrado je prevzela dr. Rosvita Pesek, voditeljica oddaje in sicer ji jo je predal mag. Miran Vršec**,** soustanovitelj Instituta za korporativne varnostne študije.









Predsednik organizacijskega odbora konference **dr. Denis Čaleta** je sicer v otvoritvenem nagovoru poudaril, »da gre v primeru nagrajencev za svetilnike odličnosti, ki se jim bomo trudili slediti tudi vsi ostali«.

Nagrade so priznanje vsem nagrajencem za njihov trud in dosežke na področju zagotavljanja visoke ravni varnosti in novih inovativnih pristopov na področju obvladovanja tveganj. Pomembnost nagrade se odraža tudi skozi izredno medijsko odzivnost podelitve in seveda visokih gostov, ki so prišli v imenu njihovih organizacij prejeti to cenjeno nagrado. Celotno obrazložitev nagrad si lahko preberete na spletnih straneh Instituta za korporativne varnostne študije www.ics-institut.si.

Po slovesnem delu je otvoritveno predavanje izvedel **veleposlanik g. Vojko Volk** in je bilo namenjeno predstavitvi geopolitičnim vidikom varnostnih tveganj v Evropi in implikaciji globalnih sprememb poslovnega okolja**.** Konferenca se je nadaljevala z odličnim mednarodnim strokovnjakom Dr. Fabiom Mulazzanijem (Head of Security and Business Continuity of European Food Safety Authority), ki je predstavil zelo aktualno vsebino s področja neprekinjenega poslovanja. Za tem se je zvrstilo še vrsto zanimivih predstavitev praktičnih izkušenj in novih tehnoloških rešitev na področju korporativne in informacijske varnosti. Skozi razpravo med strokovnjaki je bilo zaznati posamezne nove trende na področju celovitega zagotavljanja korporativne varnosti. Kako pomemben postaja proces obvladovanja tveganj kaže tudi podatek o udeleženosti predstavnikov strateškega managementa skozi celoten program konference **Dnevi korporativne varnosti 2017**.

Cel niz dogodkov, skozi dvodnevni program, je tudi tokrat omogočil tkanje novih strokovnih poznanstev, izmenjavo novih izkušenj in seveda strokovne afirmacije posameznih strokovnjakov ter ponudnikov varnostnih rešitev. Letošnja rdeča nit je bila vsekakor povezana z zaščito kritične infrastrukture in osnutkom zakona, ki se v tem trenutku nahaja v zakonodajnem postopku sprejemanja.

V okviru dogodka je bil podpisan tudi zelo pomemben sporazum o sodelovanju med **Slovenskim združenjem za korporativno varnost** in **Asociacijo za korporativno varnost iz Makedonije**.

Za konec velja še vabilo vsem, ki so pripravljeni vlagati v svoje znanje in potrebujete rešitve za celovito obvladovanje varnostnih tveganj na 9. Dneve korporativne varnosti, ki bodo v ustaljenem terminu v marcu 2018. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Management korporativne varnosti

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

Omogočiti obvladovanje poslovno varnostnih mehanizmov v gospodarstvu, industriji, državnih institucijah in civilni družbi.

Zakaj **Management korporativne varnosti**?

- **Študij za poklic prihodnosti.** Študij daje multidisciplinarna teoretična in praktična znanja s področja managementa in obvladovanja najrazličnejših tveganj v podjetju.
- **Nadgradnja širokega poslovnega znanja.** Študij omogoča spoznavanje vsebin, ki so značilne za korporativno varnost: geostrateški in politični vidiki varnostnih tveganj, varnostni standardi v poslovnih procesih, upravljanje varnostnih tveganj, načrtovanje in razvoj korporativne varnosti na vseh nivojih, procesi nadzora, gospodarsko poizvedovanje in mehanizmi za obvladovanje najrazličnejših tveganj.
- **Spoznavanje globalnega poslovnega okolja.** Tekom študija se obravnava številne primere iz domačih in mednarodnih podjetij, ki jih predstavljajo vrhunski strokovnjaki na področju varnosti v regiji.
- **Mreženje in osebni pristop.** Študij poteka v manjših skupinah, ki omogočajo neposredno sodelovanje predavateljev in študentov.

Komu je študij namenjen?

- Managerjem in strokovnjakom s področja korporativne varnosti, ki si želijo razširiti svoje poslovno znanje in pridobiti širšo perspektivo za dobro razumevanje globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja.
- Tistim, ki si želijo pridobiti znanje za vodenje oddelkov na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah.
- Podjetnikom in zaposlenim v sistemih, ki delujejo na področju energetike, telekomunikacij, informatike, transporta, financ in vsem, ki se srečujejo z vprašanjem varnosti ter tveganj v organizacijah.



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

- **RAZPISANE SMERI:**
  - **Korporativni varnostni manager**
  - **Korporativni varnostni manager - podjetnik**
- **POGOJI ZA VPIS:** diploma 1. stopnje ali starega visokošolskega strokovnega študijskega programa. Možen je tudi vpis neposredno v 2. letnik. Podrobnosti o vpisnih pogojih so na voljo na spletni strani: www.gea-college.si.
- **TRAJANJE ŠTUDIJA:** študij traja 2 leti in obsega 120 kreditnih točk po ECTS.
- **PRIDOBLJENI NAZIV:** magister/magistrica korporativne varnosti.
- **IZREDNI ŠTUDIJ:** izvaja se po razporedu, ki je prilagojen zaposlenim (študentom). Predavanja potekajo med tednom v popoldanskem času in ob sobotah dopoldne.
- **PRIZNAVANJE ZNANJ IN SPRETNOSTI:** na podlagi znanj, ki jih je posameznik pridobil s formalnim ali neformalnim izobraževanjem na tečaju, delavnici ali seminarju, se lahko prizna del študijskih obveznosti.
- **DODATNE AKTIVNOSTI IN PREDNOSTI:** mednarodna izmenjava (študij ali praksa) na več kot 30 partnerskih institucijah, podpora Kariernega centra, mednarodna konferenca, Alumni klub, ekskurzije in druge študentske aktivnosti. Študij je podprt tudi s sodobnim e-portalom, ki nudi študijske vsebine 24 ur na dan.



"Velika dinamika poslovnega okolja in stanje kriznih razmer sta danes postali stalnici. Tisti, ki tega ne razumejo, ostajajo v preteklosti. Ujemite prihodnost in dovolite, da vas s pomočjo interdisciplinarnih znanj, ki temeljijo na prenosu dobrih praks iz neposrednega poslovnega okolja, opremimo, da boste sposobni obvladovati tveganja in ustvarjati nove poslovne priložnosti."

izr. prof. Denis Čaleta, predavatelj, predsednik Slovenskega združenja korporativne varnosti

Predmetnik

I. LETNIK

Skupni obvezni predmeti

- *Management korporativne varnosti*
- *Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju*
- *Pravni vidiki korporativne varnosti*
- *Ekonomika obvladovanja tveganj v poslovnem okolju*

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

- *Varnostni standardi v poslovnih procesih*
- *Upravljanje varnostnih tveganj*
- *Načrtovanje in razvoj korporativne varnosti*

Smer Korporativni varnostni manager – podjetnik

- *Trženje/Marketing*
- *Finance*
- *Procesi nadzorstva v korporativnem varnostnem okolju*

Izbirni predmeti (študent izbere dva):

- *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 opravlja študent v 1. in 2. letniku*
- *Magistrsko delo*

GEA College je sodoben izobraževalni center in vodnik na poti k poslovni odličnosti.

GEA College nudi uporabna znanja s poudarkom na podjetništvu in managementu. Preko vpetosti v poslovno okolje spodbuja razvijanje inovativnih idej ter širjenje znanja in zavesti o tem, da je podjetništvo gonilna sila razvoja gospodarstva.

CENTER VIŠJIH ŠOL

Višješolski programi
(2 letni študij):
- Ekonomist
- Poslovni sekretar
- Informatika
- Organizator socialne mreže
- Gostinstvo in turizem

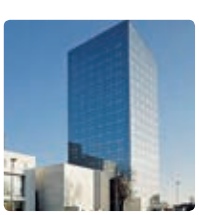
FAKULTETA ZA PODJETNIŠTVO

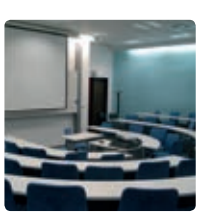
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

Magistrski programi
(2 letni študij):
- Podjetniški management
- Management korporativne varnosti

POSLOVNO-IZOBRAŽEVALNI CENTER

- Poslovni seminarji in delavnice
- Usmerjena poslovna izobraževanja
- Izobraževanja v podjetjih





GEA College - Fakulteta za podjetništvo
Dunajska cesta 156
1000 Ljubljana
T: (01) 588 13 00
F: (01) 568 82 13
E: podiplomski@gea-college.si
www.gea-college.si

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo



ELES

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.

Energija teče skupaj z nami. Kot sistemski operater slovenskega elektroenergetskega prenosnega omrežja skrbimo za njen varen, zanesljiv in neprekinjen prenos 24 ur na dan. Smo strokovnjaki z znanjem in izkušnjami, ki soustvarjamo energetsko prihodnost Slovenije na skrbno zastavljenih temeljih: odgovornosti, zavzetosti, znanju, zanesljivosti, sodelovanju in vztrajnosti. Strateško in trajnostno načrtujemo, gradimo in vzdržujemo prenosno omrežje Republike Slovenije. Za električno energijo na dosegu vaše roke.

Več kot 2550 km
prenosnega omrežja

Več kot 550
zaposlenih

V prenosno omrežje prevzamemo več kot 20.000 gigavatnih ur električne energije. S to energijo bi žarnica gorela več kot milijon let.

www.eles.si