Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2017, marec • št. 13

Podelitev nagrad »Slovenian Grand Security Award«

Ministrstvo za obrambo pomemben deležnik na področju zaščite kritične infrastrukture

Andreja Katič, ministrica za obrambo Republike Slovenije

BTC CITY 360º LIVE

MESTO PRILOŽNOSTI

BLAGOVNA ZNAMKA BTC CITY SI JE V DVAJSETIH LETIH IZBORILA SVOJE MESTO V SLOVENSKEM MARKETINŠKEM PROSTORU. DANES NE OZNAČUJE LE NAJVEČJE NAKUPOVALNO SREDIŠČE. BTC CITY POSTAJA POMEMBEN POSLOVNI CENTER, MESTO S ŠPORTNIMI IN KULTURNIMI VSEBINAMI TER PROSTOR USTVARJALNIH IN POSLOVNIH ZAMISLI. PRAV ZATO BO BLAGOVNA ZNAMKA BTC CITY V PRIHODNJE USMERJENA V USTVARJANJE PRILOŽNOSTI ZA KVALITETNO ŽIVLJENJE, NAPREDNE IDEJE IN NOVE VIZIJE.

BTC CITY

www.btc-city.com

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
marec 2017

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

Pred nami je ponovno največja in vsebinsko najbolj bogata regijska konferenca Dnevi korporativne varnosti. Razmah konference in vedno večje število udeležencev kaže na to, da se zavedanje o pomenu varnosti počasi a vendar vztrajno dviguje. Seveda k temu dejstvu največ pripomore zahtevno varnostno okolje v katerem organizacije danes delujejo in različna tveganja s katerimi so soočajo. Vendar učinkovitega poslovanja enostavno ni mogoče zagotavljati brez dejstva, da se pomemben fokus namenja tudi obvladovanju dinamičnih tveganj s katerimi se soočajo na globalnih trgih.

V zadnjem obdobju smo tudi v Republiki Sloveniji priča nekaterim pomembnim procesom, ki bodo v prihodnosti krojili okolje na področju korporativne varnosti in s tem povezanimi procesi. Eden izmed pomembnih projektov je vsekakor začetek postopka sprejemanja novega zakona o zaščiti kritične infrastrukture. Upati je, da bodo stališča in izkušnje upravljavcev kritične infrastrukture, v fazi dopolnil osnutka zakona, tudi upoštevane. Na tem mestu ima Slovensko združenje za korporativno varnost, ki združuje večino upravljavcev kritične infrastrukture, še posebej pomembno mesto. Drugi pomembni mejnik, ki bi ga želeli izpostaviti, pa je vsekakor, da smo na magistrskem programu »Management korporativne varnosti« dobili prvega diplomanta, ki bo nekako vrezal ledino razvoja profesije korporativne varnosti. No, posebej pa nas z optimizmom navdaja tudi dejstvo, da je kritična masa strateških managerjev, ki zaznavajo potrebo po učinkovitosti in urejenosti procesa korporativne varnosti v njihovih organizacijah, vedno večja. To pa pomeni, da bo v prihodnje temu pomembnemu področju, predvsem v poslovnih organizacijah, namenjeno več pozornosti.

V tokratni številki, ki je posvečena mednarodni konferenci Dnevi korporativne varnosti smo odprli cel niz aktualnih tem. V kolumni smo varnostne vidike postavili v širši geopolitični prostor regije v kateri živimo in poslujemo. K pogovoru smo povabili tudi ministrico za obrambo, ki vodi resor, kateri je zadolžen za pripravo novega zakona o kritični infrastrukturi, da nam globje pojasni namen in časovne okvire sprejema tega akta. Seveda smo odprli tudi cel niz vsebin povezanih neposredno s korporativno in informacijsko varnostjo in predstavljajo dobre prakse in rešitve, katere nam bodo olajšale delovanje v tem zahtevnem okolju. Posebej velja izpostaviti še oba intervjuja s cenjenima kolegoma iz dveg uglednih korporacij, ki delujeta na globalnem trgu in se vsebinsko dotikata tako informacijske varnosti kakor tudi neprekinjenega poslovanja. Glede na to, da je številka izšla ob pomembnem in že zgoraj omenjenem dogodku, je nekaj vsebine namenjeno tudi konferenčnim partnerjem, ki nam bodo predstavili nekaj dobrih praks in produktov. Tokrat izjemoma ponujamo tudi po obsegu večjo količino vsebinskih prispevkov.

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

izr. prof. dr. Denis Čaleta
Glavni urednik

ZAGOTAVLJANJE KORPORATIVNE VARNOSTI JE ZA DRUŽBO ELES IZJEMNEGA POMENA

ELES je pomemben predstavnik kritične infrastrukture v Republiki Sloveniji. Še posebej je ta pomembnost izražena zaradi dejstva, da je podsektor prenosa in proizvodnje električne energije tisti, ki ima neposreden vpliv na učinkovitost delovanja vseh ostalih delov kritične infrastrukture v naši državi in tudi širšem mednarodnem prostoru. S tega stališča je obvladovanje tveganj in s tem zagotavljanje neprekinjenosti delovanja sistema v ELES, ključni proces, ne samo v sami družbi, temveč v širši nacionalno-varnostni dimenziji.

16

INTERVJU
Dušan Dular, višji strokovni svetovalec generalnega direktorja pooblaščenec za informacijsko varnost in neprekinjeno poslovanje v Krki, d. d., Novo mesto

NEPREKINJENO POSLOVANJE POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

20

VARNOST V HOTELSKI INDUSTRIJI – Gradnik konkurenčne prednosti države in posamezne destinacije

Že dolgo je povsem jasno, da je varnost - poleg cene in kakovosti - sestavni del turistične ponudbe. V okoliščinah povečanja globalnih in regionalnih varnostnih groženj ter vse večjih težav obvladovanja varnostnih tveganj pa varnost postaja stalnica in dejanska potreba v posodabljanju varnostnih arhitektur v turističnih nastanitvenih objektih in v drugih turističnih storitvah in destinacijah. Kajti varnostne razmere so se začele spreminjati tudi v Evropi, ki je bila leta 2013 vodilna svetovna turistična destinacija, katero je obiskalo 560 milijonov mednarodnih potnikov.

29

INTERVJU
Dejan Dobrovoljc, direktor oddelka informatike v podjetju Interblock d.d.

INFORMACIJSKA VARNOST POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

38

PRIPRAVLJENOST VARNOSTNIH IN VODSTVENIH STRUKTUR NA AMOK SITUACIJO

V zadnjem obdobju smo tudi v Evropi soočeni s pojavom amok situacij, ki jih v najširšem obsegu lahko opredelimo kot dejanje, ko eden ali več storilcev, navidezno brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal.

44

Avtor: izr. prof. dr. Denis Čaleta / Institut za korporativno varnostne študije

INTERVJU
Andreja Katič, ministrica za obrambo Republike Slovenije

MINISTRSTVO ZA OBRAMBO POMEMBEN DELEŽNIK NA PODROČJU ZAŠČITE KRITIČNE INFRASTRUKTURE

Pogovarjali smo se z ministrico za obrambo Andrejo Katič, ki je bila na parlamentarnih volitvah leta 2014 izvoljena za poslanko Državnega zbora RS in bila do imenovanja na ministrski položaj tudi njegova podpredsednica. Ministrstvo za obrambo vodi od leta 2015. Dinamičnost varnostnega okolja in pomembnost ministrstva na področju priprave novega zakona o zaščiti kritične infrastrukture so bili razlogi za pogovor o odprtih izzivih in načrtih institucije, ki jo vodi.

Kompleksno varnostno okolje pred nas postavlja vedno nove grožnje, ki niso več tradicionalno vojaške. Kako vidite razvoj obrambnega področja glede na dejstvo, da so viri, ki jih Republika Slovenija namenja za obrambo, še vedno zelo omejeni?

Res je, da se Republika Slovenija sooča s poslabšanimi varnostnimi razmerami v regiji in širšem mednarodnem okolju. Sodobne oblike groženj, krize in oboroženi spopadi v soseščini EU ter migracijski tokovi pomenijo potencialno varnostno grožnjo tudi za nas. Nanjo se bo morala država ustrezno odzivati.

Na Ministrstvu za obrambo prepoznavamo spremenjene varnostne razmere, ki zahtevajo ustreznejše obrambne zmogljivosti za spoprijemanje s prihodnjimi viri ogrožanja in tveganji nacionalne ter mednarodne varnosti. V ta namen

Na Ministrstvu za obrambo prepoznavamo spremenjene varnostne razmere, ki zahtevajo ustreznejše obrambne zmogljivosti za spoprijemanje s prihodnjimi viri ogrožanja in tveganji nacionalne ter mednarodne varnosti.

smo med drugim opravili strateški pregled obrambe, ki nam je dal odgovore na vprašanja o aktualni obrambni sposobnosti Republike Slovenije. Z njim smo dobili podlago za usmerjanje nadaljnjega razvoja obrambnega sistema in njegovih zmogljivosti, da bo sposoben učinkovitega delovanja skladno s svojim poslanstvom.

Prepričana pa sem, da je zelo pomembno, da je vlada leta 2016 zaustavila nadaljnje zmanjševanje obrambnih izdatkov. Veseli me, da je ob seznanitvi s sklepi strateškega pregleda obrambe naložila Ministrstvu za finance, da pri pripravi prihodnjih proračunov upošteva zagotovitev nominalne rasti obrambnega proračuna za 20 do 30 milijonov evrov na leto in ciljno približevanje obrambnih izdatkov v višini 1,2 odstotka BDP v desetletnem obdobju. Odločitev vlade nam daje potrebne podlage za nadaljnji razvoj obrambnega sistema, povečanje obrambne sposobnosti države, izboljšanje pripravljenosti in vzdržljivosti Slo-

Kot enega izmed ciljev predloga zakona bi izpostavila, da je bilo vsem organom in organizacijam, ki delujejo na področjih, ki so za slovensko družbo posebno pomembna, naloženo, da pri svojem delu upoštevajo zahteve po zagotavljanju neprekinjenega delovanja kritične infrastrukture.

venske vojske ter ustrezno uresničevanje skupnih ciljev in zavez v Natu in EU.

Kako vam kot ministrici za obrambo uspeva obvladovati tako kompleksna področja na ministrstvu, ki so v bistvu zelo raznovrstna in imajo vsako zase zelo specifične zahteve in probleme?

Strinjam se, da je Ministrstvo za obrambo zelo kompleksen resor, saj združuje dva podsistema nacionalne varnosti – obrambnega in sistem varstva pred naravnimi in drugimi nesrečami. Zato delovanje v takšnem ministrstvu predstavlja poseben izziv in zahteva precej usklajevanja in tudi potrpežljivosti pri iskanju najboljših rešitev. Verjamem pa, da je na podlagi strokovnih in vodstvenih izkušenj, ki jih imam, podpore motiviranih sodelavcev, naše dobre volje in trdne naravnanosti delati dobro za Republiko Slovenijo, mogoče učinkovito upravljati ta resor in pri tem izboljšati razmere za delovanje Slovenske vojske.

Čeprav imata sistema različni poslanstvi in s tem povezane specifične zahteve, sta komplementarna in skupaj prispevata k varnosti ter zaščiti državljanov in države. Tudi ob zmanjšanih virih smo uspeli najti motive za iskanje možnosti za napredek in doseganje boljših sistemskih razmer za razvoj zmogljivosti ter povečanje učinkovitosti obeh sistemov. Letošnje leto bo nekakšen višek teh prizadevanj, saj pričakujemo konec prenove zakonov na področjih obrambe in kritične infrastrukture. Hkrati bomo pregledali in, če bo treba, prenovili nekatere temeljne dokumente, ki se nanašajo na nacionalno varnost. Povečanje izdatkov, namenjenih za obrambo in varstvo pred naravnimi in drugimi nesrečami, pomeni možnosti za večje zmogljivosti in boljše razmere za delo.

Učinkovito obvladovanje vseh procesov na ministrstvu temelji tudi na predanosti in motiviranosti zaposlenih, ki kakovostno opravljajo svoje delo. Sama vidim možnost izboljšav predvsem v večji funkcijski integraciji med organi v sestavi in upravnim delom ministrstva. Glede tega smo v preteklosti že naredili nekatere pozitivne korake, vendar ne do ravni, ki jo vidim kot potrebno.

Upravljanje procesov s področja sistemskih ukrepov na področju kritične infrastrukture tradicionalno in primerjalno ni umeščeno v Ministrstvo za obrambo. Zakaj menite, da je ta rešitev, ki jo poznamo v Republiki Sloveniji, primerna in predvsem učinkovita?

Da je takšna ureditev ustrezna, se je pokazalo že med predsedovanjem Republike Slovenije Svetu Evropske unije. V pripravah na predsedovanje je namreč v dogovoru z Ministrstvom za notranje zadeve naše ministrstvo prevzelo celotno področje zaščite kritične infrastrukture. Uspešni smo bili tudi pri predsedovanju svetu na tem področju in prav tako uspešno vodili in končali proces usklajevanja besedila *Direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite,* ki je bila pozneje tudi sprejeta.

Aktivnosti za zaščito kritične infrastrukture na nacionalni ravni so se sicer začele že z vodenjem Medresorske koordinacijske skupine za usklajevanje priprav za zaščito kritične infrastrukture v Republiki Sloveniji, ki jo je leta 2006 imenovala vlada. Vlada je skladno z direktivo sveta MO imenovala za kontaktno točko za področje varovanja evropske kritične infrastrukture v Republiki Sloveniji. Prav tako je MO uskladilo definicijo kritične infrastrukture državnega pomena ter osnovne in sektorske kriterije za njeno določanje, kar je vlada potrdila. Oblikovali smo tudi metodologijo za oblikovanje ukrepov za zaščito kritične infrastrukture in sodelovali z nosilci in nekaterimi upravljavci kritične infrastrukture pri njihovi pripravi.

Ob pripravi predloga zakona o kritični infrastrukturi smo umeščenost področja ponovno pretehtali. Po posvetovanjih je bilo doseženo soglasje, da vlogo usmerjanja na področju kritične infrastrukture še nadalje opravlja naše ministrstvo. Ta rešitev je vključena tudi v predlog zakona o kritični infrastrukturi, po katerem ima MO usmerjevalno vlogo na področju kritične infrastrukture.

V postopku obravnave je predlog novega zakona o zaščiti kritične infrastrukture. Kaj po vaši oceni lahko prinese zakonska ureditev tako zahtevne materije?

Najprej bi rada poudarila, da smo v pripravo predloga tega zakona vložili zelo veliko truda. Ocenjujem ga kot zelo pretehtanega. Njegov temeljni namen je sistemsko urediti neprekinjeno delovanje kritične infrastrukture Republike Slovenije. Izhajali smo iz razumevanja, da zaščita kritične infrastrukture obsega vse aktivnosti, ki prispevajo k neprekinjenosti in celovitosti njenega delovanja.

Kot enega izmed ciljev predloga zakona bi izpostavila, da je bilo vsem organom in organizacijam, ki delujejo na področjih, ki so za slovensko družbo posebno

Predvsem pa vidim velik prispevek v tem, da bo s tem zakonom narejen pomemben korak k povečanju odpornosti slovenske družbe na sodobne grožnje in varnostna tveganja.

pomembna, naloženo, da pri svojem delu upoštevajo zahteve po zagotavljanju neprekinjenega delovanja kritične infrastrukture. Pomembni sta tudi vzpostavitev primernih razmerij med organi in organizacijami, ki delujejo v sektorjih kritične infrastrukture, ter dopolnitev normativne urejenosti z vidika njene zaščite. Predvsem pa vidim velik prispevek v tem, da bo s tem zakonom narejen pomemben korak k povečanju odpornosti slovenske družbe na sodobne grožnje in varnostna tveganja.

Stroka očita zakonskemu predlogu, da zelo tehnokratsko ureja področja kritične infrastrukture, premalo pa je usmerjen k formiranju procesov, skozi katere bi država s svojimi viri na področju pomagala upravljavcem kritične infrastrukture.

S tem očitkom se ne morem strinjati. Prav tako pri obravnavi predloga zakona v javni obravnavi takšnih odzivov nismo dobili. Zavedamo pa se zaskrbljenosti posameznih podjetij, ki so ali bi lahko bila kritična infrastruktura, predvsem zaradi obsega dodatnih nalog, ki jih zakon prinaša. Temu smo se skušali izogniti že pri pripravi predloga.

V predlogu zakona o kritični infrastrukturi je tako predvideno, da se država vključi v njeno zaščito ob dodatnih ukrepih. Ti se uvedejo ob izrednem dogodku, krizi ali povečani ogroženosti kritične infrastrukture, če stalni ukrepi, tudi, če so stopnjevani, ne zadostujejo. Dodatni ukrepi, ki jih nosilci sektorjev kritične infrastrukture sprejmejo sami ali jih predlagajo v sprejem vladi, zakonsko niso obvezni, saj jih nosilci lahko sprejmejo oziroma predlagajo, če menijo, da so nujni.

O drugem očitku, ki ga navajate in ga v javni razpravi doslej prav tako ni bilo mogoče zaznati, je stališče Ministrstva za obrambo jasno. Menimo, da bi morebitna določitev takšnih procesov, prek katerih bi »država s svojimi viri na področju« pomagala upravljavcem kritične infrastrukture, presegala namen zakona o kritični infrastrukturi. Predvsem pa menimo, da takšnih procesov ni smiselno določati z zakonom, temveč se morajo postopoma razviti prek različnih oblik praktičnega sodelovanja med deležniki na področju zaščite kritične infrastrukture, zlasti med upravljavci kritične infrastrukture na eni in organi državne uprave na drugi strani. Za zdaj bo glavna pomoč države v tem, da bo s temeljnim sistemskim predpisom uredila področje, ki doslej zakonsko ni bilo urejeno.

Na področju učinkovite vzpostavitve sistema zaščite kritične infrastrukture bo imelo ključno vlogo javno-zasebno partnerstvo. Kako ocenjujete možnosti, ki bi v prihodnje krepile ta proces na omenjenem področju?

Menim, da je treba partnerstvo pri zaščiti kritične infrastrukture v najširšem smislu razumeti kot združevanje zmogljivosti, izmenjavo znanja in izkušenj ter posvetovanje in soodločanje. Torej ne zgolj v tradicionalnem ekonomsko-finančnem smislu kot sklepanje pogodb o sofinanciranju projektov v javnem interesu. Taka partnerstva moramo pri nas šele začeti razvijati, tudi na podlagi poznavanja in kritičnega upoštevanja tujih izkušenj in dobrih praks. Prve korake v tej smeri smo naredili že pri pripravi predloga zakona o kritični infrastrukturi, v katerem smo predvideli načelo (so)odgovornosti vseh pristojnih organov in organizacij pri zaščiti kritične infrastrukture, ne le gospodarskih družb in javnih zavodov, temveč tudi organov državne oblasti. Zelo pomembna je tudi izmenjava informacij med pristojnimi organi in organizacijami, ki temelji na medsebojnem zaupanju.

Večina upravljavcev kritične infrastrukture je združena v Slovenskem združenju korporativne varnosti. Menite, da bi lahko Ministrstvo za obrambo s formalnim vstopom v tako obliko združevanja napravilo pomemben korak k tesnejšim povezavam in približevanju procesov neposredne izmenjave dobrih praks in izkušenj na področju obvladovanja tveganj pri zaščiti kritične infrastrukture?

Rada bi poudarila, da MO že doslej v Republiki Sloveniji usklajuje in usmerja priprave za zaščito slovenske kritične infrastrukture državnega pomena, kot kontaktna točka za zaščito evropske kritične infrastrukture pa njenim nosilcem in upravljavcem zagotavlja izmenjavo informacij, dobrih praks, izkušenj ter možnost sodelovanja na vajah in usposabljanjih, povezanih z zaščito evropske kritične infrastrukture.

Slovensko združenje korporativne varnosti bo za MO, če bo z zakonom o kritični infrastrukturi določeno kot organ, pristojen za usmerjanje področja kritične infrastrukture, dobrodošel sogovornik pri izmenjavi dobrih praks in izkušenj, od obvladovanja tveganj do sistemskih in operativnih ukrepov za zaščito kritične infrastrukture. Polnopravno članstvo ministrstva kot organa državne uprave v tem združenju kot civilnodružbeni organizaciji pa je, če je sploh pravnoformalno dopustno, vsaj vprašljivo z vidika načelnega razmerja med državo in civilno družbo. Bodo pa z novo zakonsko obveznostjo nastale vsebinske priložnosti in potrebe za krepitev njegovega partnerskega odnosa z združenjem, v katerem že ima uradni status partnerja.

Sodobna informacijska družba pred nas postavlja tudi pomembna tveganja, ki se v zadnjem obdobju še posebej izražajo skozi kibernetske grožnje. Temu se ne more izogniti niti kritična infrastruktura. Kje lahko na tem področju najdemo vlogo Ministrstva za obrambo, ko govorimo o obvladovanju tveganj, ki jih kibernetske grožnje predstavljajo za nemoteno delovanje kritične infrastrukture?

Na področju kibernetske varnosti ministrstvo trenutno glavnino svojega dela usmerja v zaščito svojih komunikacijsko-informacijskih sistemov. Ker pa se zavedamo pomena kibernetske varnosti, strokovne službe ministrstva znotraj svojih pristojnosti in možnosti sodelujejo pri pripravi nacionalne normativne podlage, posredujejo nekatere informacije iz mednarodnega okolja in omogočajo možnost sodelovanja na vajah s tega področja. Naša vloga na področju kibernetske varnosti na nacionalni ravni se bo v prihodnosti še razvijala, saj je bila pred enim letom sprejeta nacionalna strategija kibernetske varnosti, akcijski načrt za njeno uveljavitev pa je v nastajanju.

V okviru ministrstva je pomemben proces zagotavlja tudi krizno upravljanje. Kako je po vašem mnenju pomemben ta proces in ali lahko ministrstvo s svojimi viri na tem področju ponudi logistiko za delovanje Sveta za nacionalno varnost?

V Republiki Sloveniji je v kriznih razmerah vsako ministrstvo do določene ravni odgovorno za izvajanje nalog na svojem področju. Glavni organ za usklajevanje kriznega odziva je vlada, ki je za zagotavljanje nacionalne varnosti ustanovila nekatera telesa. Svet za nacionalno varnost je njen posvetovalni in usklajevalni organ, Nacionalni center za krizno upravljanje (NCKU) zagotavlja vladi prostorsko in informacijsko-komunikacijsko podporo, Medresorska analitična skupina pa strokovno in analitično podporo v vojni, izrednem stanju ter ob kriznih dogodkih. Na ravni vlade so s tem zagotovljene možnosti kriznega upravljanja in vodenja, nujne za učinkovit krizni odziv. Vlada je prav nedavno potrdila zaključno poročilo projekta Sistem kriznega upravljanja in vodenja v Republiki Sloveniji, ki ga je vodilo in usklajevalo MO, kar je uspeh našega skupnega dela.

> Menim, da je treba partnerstvo pri zaščiti kritične infrastrukture v najširšem smislu razumeti kot združevanje zmogljivosti, izmenjavo znanja in izkušenj ter posvetovanje in soodločanje.

Menite, da bi lahko Nacionalni center za krizno upravljanje v prihodnosti organizacijsko postal neposredna podpora za delovanje Sveta za nacionalno varnost?

Skladno s trenutno zakonodajo center v organizaciji Ministrstva za obrambo zagotavlja prostorske, tehnične, informacijske in telekomunikacijske razmere za delo vlade ter državnega operativnega štaba obrambe predvsem v vojnem in izrednem stanju. Center zagotavlja informacijske in komunikacijske povezave za izmenjavo podatkov in informacij z državnimi organi, operativno-komunikacijskimi centri ter gospodarskimi družbami, zavodi in drugimi organizacijami, ki so po sklepu vlade posebnega pomena za obrambo.

Na podlagi tega je jasno, da NCKU že zdaj, še posebno pa v krizi, zagotavlja varne informacijsko-komunikacijske povezave ter v svojih prostorih omogoča neposredno komuniciranje in delovanje organov kriznega odzivanja, med katerimi je vsekakor tudi Svet za nacionalno varnost. ■

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!

ELEKTRO LJUBLJANA
GASILSKA ZVEZA SLOVENIJE
MARIBORSKI VODOVOD
BTC
PHILIP MORRIS LJUBLJANA D.O.O.
Ford SUMMIT AVTO
ZARJA ELEKTRONIKA
Slovenske železnice
CETIS
lek član skupine Sandoz
CINKARNA
Elita i.b. d.o.o.
KONTROLA ZRAČNEGA PROMETA SLOVENIJE
simobil.si
OBČINA SLOVENSKA BISTRICA
triglav
ELES
energetika ljubljana
hse Holding Slovenske elektrarne d.o.o.
TEŠ TERMOELEKTRARNA ŠOŠTANJ
NZS NOGOMETNA ZVEZA SLOVENIJE
LUKA KOPER Port of Koper
luka d.d.
Republika Slovenija
REISSWOLF secret. service.
Zanesljivo vsepovsod POŠTA SLOVENIJE
interblock LUXURY GAMING PRODUCTS
SIEMENS
TelekomSlovenije
DARS
Nova KBM PRIPRAVLJENI NA JUTRI
univerzitetni klinični center ljubljana
gorenjegroup
si·cert
INFORMACIJSKI POOBLAŠČENEC

www.ics-institut.si

Avtor: Vojko Volk / veleposlanik

KOLUMNA
vojko.volk@gov.si

NOVA BALKANIZACIJA BALKANA

Okoliščine in razlogi nastanka prve Jugoslavije ostajajo ena velikih skrivnosti zgodovine Evrope 20. stoletja; čigava je bila v resnici zamisel o združitvi šestih močno različnih narodov, petih jezikov in treh veroizpovedi brez skupne zgodovine in tradicije sobivanja v enovito državo? Je šlo za uresničitev želje ljudstev ali za načrt velikih sil?

Vsekakor je šlo za drzen poizkus, ki se je tragično končal in se na obroke končuje še danes. Bolezen Balkana je nenehno umiranje Jugoslavije, ki se kaže skozi neurejene odnose med državami naslednicami, odprta mejna in premoženjska vprašanja, skozi številne spore in blokade ter vedno bolj izrazito demontažo sporazuma o nasledstvu SFRJ. Mit o bratstvu in enotnosti jugoslovanskih narodov se je končal s krvavo vojno, upanje na mirno sožitje držav naslednic in stabilnost Balkana pa znova umira ob prebujanju skrajno nevarnih balkanskih atavizmov; četništva v Srbiji, ustaštva na Hrvaškem in skrajnega islamizma v BiH. Namesto, da se končno stabilizira se Balkan znova balkanizira. Slovenija je vsa leta svoje samostojnosti poskušala balkanskim državam pomagati in jim nuditi pomoč pri približevanju EU in NATO, v zameno za perspektivo boljšega političnega in gospodarskega sodelovanja. Slovenija je ena redkih evropskih držav, ki ima nacionalno strategijo do Zahodnega Balkana (2010). A zadnja leta je šel napredek rakovo pot, po Balkanu se namesto vesti o razvoju in gospodarskem napredku znova sliši sovražni govor in žvenketanje z orožjem. Balkan je znova tam, kjer je že bil. Čas je, da Slovenija na novo domisli svoj odnos in politiko do Balkana, ki iz nekdanje poslovne priložnosti znova postaja varnostni izziv.

Države razpadle Jugoslavije

Pet držav naslednic in sedmero držav, ki so nastale na ozemlju nekdanje SFRJ je doživelo zelo različne usode. Četrt stoletja od razpada skupne države sta razvojno napredovali Slovenija in Hrvaška, ki sta tudi edini doslej vstopili v NATO in EU, vse druge države pa so bolj ali manj stagnirale ali celo nazadovale. Vse od razglasitve neodvisnosti pa do gospodarske krize 2008 je bila Slovenija z veliko prednostjo vodilna med postkomunističnimi državami Evrope in imela med njimi najvišji BDP na prebivalca. Danes je Slovenijo že prehitela Češka,[1] dohitevajo pa jo tudi ostale države Višegrajske skupine. Hrvaška in BiH sta odtlej stagnirali ali nazadovali, še nekoliko bolj so nazadovale Srbija, Makedonija in Kosovo, ki skupaj z Albanijo in Moldovo sodijo med najrevnejše evropske države. Črna gora zadnja leta gospodarsko napreduje, vstopa v NATO in se pogaja za vstop v EU. Ob Črni gori sta Srbijo močno prehiteli tudi Romunija in Bolgarija, ki sta prej vedno krepko zaostajali za Jugoslavijo oziroma za Srbijo.[2] Baltske države, ki so padec komunizma pričakale kot najrevnejše, imajo danes 3 do 4 krat višji BDP od držav Balkana.

Države so bolj ali manj ohranile stopnje razvitosti iz časov skupne države, so se pa razlike med njimi močno povečale. Najbolj drastičen primer je Srbija, ki je bila v SFRJ tretja najbolj razvita republika,[3] zdaj pa zaostaja za Črno goro in je izenačena z Makedonijo.[4] V SFRJ je bil slovenski BDP na prebivalca zgolj dvakrat višji od srbskega, danes pa je več kot 4 krat višji. Države so ohranile tudi svoje tradicionalne trge in pretežno tudi politična zavezništva ter antagonizme. Dokler je privlačnost Evrope prevladovala so vse države, razen Miloševićeve Srbije, delovale v smeri evroatlantskih integracij. Takoj, ko je privlačnost NATO in EU upadla, so se pričele pričakovane težave; obujanje skrajnih nacionalizmov, verskih konfliktov in nazadnje tudi ozemeljskih pretenzij. Na Balkan se vračajo stara zavezništva in geopolitika hladne vojne. Rusija politično podpira in z orožjem oskrbuje Srbijo, ZDA pa enako počno na Hrvaškem. Nov igralec na Balkanu je Turčija, ki ima odločilen vpliv na muslimanske politike

v BiH, nov igralec so arabske države, ki financirajo islamski radikalizem povsod, kjer tradicionalno živijo muslimani.

Antagonizem Srbov in Hrvatov

Novejša zgodovina Balkana je v znamenju nenehnih napetosti in konfliktov med Srbi in Hrvati. Ostrina tega antagonizma je podobna tistemu med Izraelci in Palestinci in sodi v ti. fetišizem majhnih razlik, kjer se konflikt zaostruje zavoljo želje po razločevanju za vsako ceno in prevlado nad določenim, pogosto tudi istim ozemljem. Paradoks pri tem je, da sta državi kljub temu močno in celo usodno gospodarsko povezani. Koncern Agrokor, ki je pravi balkanski imperij, ima v vertikalni verigi večino živilskih podjetij Hrvaške in Srbije (tudi BiH) in združuje kar 64 tisoč delovnih mest. Morebitni razpad tega vse bolj zadolženega imperija, ki samo ruskim bankam dolguje milijardo evrov, bi bil hud šok za obe gospodarstvi. Tako Srbija kot Hrvaška že vse od razpada SFRJ sebe vidita kot regionalnega liderja, kar ju je v samo zadnjega pol stoletja vodilo do spopadov v dveh vojnah predvsem pa do nenehne ambicije po razdelitvi BiH. Po samo dveh desetletjih od zadnjega vojaškega spopada se obe strani znova približujeta razmeram, v katerih bo preskok s politične v vojaško konfrontacijo postal realna možnost.

Hrvaška je ob vstopu v EU v letu 2013 pomenila veliko upanje, da bo prispevala k stabilnosti na Balkanu in pomagala svoji soseščini pri približevanju in vstopanju v EU. V vsega dveh letih je Hrvaški uspelo razbliniti vsa tovrstna pričakovanja, v zadnjih dveh letih pa jih je celo postavila na glavo. Sodelovanje Hrvaške s Slovenijo, ki je po podpisu arbitražnega sporazuma in zagonu Brdo procesa postalo zgled za celoten Balkan, je bilo čez noč porušeno in praktično pozabljeno. Trenutno stanje v odnosih med Slovenijo in Hrvaško je do te mere poslabšano, da spominja na odnose med Hrvaško in Srbijo. Učinki hrvaškega izstopa iz sporazuma o arbitraži imajo daljnosežne posledice na celoten Balkan in v marsičem delujejo bolj uničujoče kot pa dejstvo, da je EU na Balkan domala pozabila. Tudi ZDA so svojo pozornost do Balkana znižale na minimum že kmalu po neuspešnem poskusu dogovora o ustavnih spremembah v BiH leta 2009 (ti.Butmirski dogovor). ZDA se odtlej posvečajo predvsem Hrvaški, kar je logična geopolitična odločitev že ob pogledu na zemljevid; Hrvaška je najbolj izpostavljena braniteljica meja zahoda proti negotovemu Balkanu in vselej nepredvidljivi Srbiji. V zadnjem letu se Hrvaška pospešeno oborožuje s podporo ZDA,[5] Srbija pa s pomočjo Rusije.[6] Hrvaško gospodarstvo je bilo eno zadnjih med članicami EU, ki je izšlo iz krize. Ključni razlog nove gospodarske rasti Hrvaške je bil predvsem vstop v EU, ob dejstvu, da sta uspešno poslovali vodilni hrvaški banki, ki sta v celoti v tuji lasti. Kljub vsemu Hrvaška ohranja velik razvojni zaostanek, med članicami EU po višini BDP na prebivalca za njo zaostajata samo Romunija in Bolgarija.

Hrvaška nazaduje tudi na področju splošnih svoboščin in demokratičnosti. Zaradi nesposobnosti soočanja z zločinsko preteklostjo NDH in vse bolj javne rehabilitacije ustaštva Hrvaška tvega, da bo znova postala „obrnjena“ podoba Srbije in njen večni rival v boju za prevlado na Balkanu. Hrvaški nacionalizem, tako kot srbski, postaja talec dogajanj v BiH, kjer tamkajšnji Srbi in Hrvatje vse bolj odkrito sodelujejo v političnem nasprotovanju muslimanski večini in izsiljujejo sicer nujne, nikakor pa ne edino možne spremembe daytonskega ustroja nesrečne BiH.

Takoj, ko je privlačnost NATO in EU upadla, so se pričele pričakovane težave; obujanje skrajnih nacionalizmov, verskih konfliktov in nazadnje tudi ozemeljskih pretenzij. Na Balkan se vračajo stara zavezništva in geopolitika hladne vojne.

Srbija je v zadnjih 15 letih kar trikrat vzbudila velika pričakovanja sveta. Najprej ob nastopu Vojislava Koštunice kot prvega predsednika po Miloševiću, potem v obdobju predsednika Borisa Tadića in nazadnje znova ob nastopu vladavine Aleksandra Vučića. Kljub vsem dobrim obetom Srbija ni izpolnila velikih pričakovanj in tudi Vučićevo obdobje ne prinaša napredka Srbiji. Ni ji uspel skok preko senc lastne zgodovine, v kateri ostaja ujeta z vsemi ostanki preteklosti in s še vedno popolno nezmožnostjo soočanja z realnostjo na Kosovu. Posledično stagnira tudi gospodarski in splošni razvoj Srbije. Kljub solidni gospodarski rasti v Srbiji realno upadata tako absolutni BDP [5] kot tudi povprečna plača [6], ki je višja samo še od povprečne plače v Albaniji in Makedoniji. [7]

Izjave vodilnih srbskih politikov o razmerah na Balkanu postajajo iz dneva v dan bolj radikalne in vse bolj zvenijo kot odkrit poziv k novim spopadom med izmučenimi in znova obubožanimi narodi Balkana. Bojevitega zunanjega ministra Ivico Dačića („Srbija je storila napako, ko je Makedonijo priznala pod njenim ustavnim imenom“. Ivica Dačić, januar 2017) vse bolj presega predsednik Tomislav Nikolić s poslej že povsem odkritim vojaškim hujskaštvom v odnosu do Kosova („Pripravljeni smo poslati vojsko na Kosovo“. Tomislav Nikolić, januar 2017). Vse manj obziren je tudi PV Vučić, ki z zadnjo epizodo pošiljanja srbskega vlaka na Kosovo posredno priznava, da volivcev ne more več motivirati z gospodarskimi in socialnimi obljubami lahko pa njihova srca zažge z vselej priročnim velikosrbstvom, militantnim antialbanstvom in pozivi k narodni enotnosti.

BiH, Makedonija in Kosovo

Tri najbolj zapletene države Balkana so v zadnjih letih najbolj nazadovale. Najtežavnejše razmere so trenutno v BiH in Makedoniji in nekoliko manj na Kosovu. Še leta 2009 je bila BiH razmeroma stabilna in je bila obetaven kandidat tako za NATO kot za EU. Makedonija bi v NATO morala vstopiti že leta 2008 a ji zaradi Grčije ni uspelo. Istega leta je Kosovo razglasilo samostojnost in presekalo gordijski vozel Balkana, kar je končno tudi Srbiji odprlo perspektivo evroatlantskih integracij. Zapletene politične razmere so imele neposreden vpliv tudi na gospodarstva držav, seveda pa tudi na njihovo stabilnost in varnost.

BiH se je z dogajanji v letu 2016 politično vrnila tja, kjer je bila v času razpadanja SFRJ. Srbi grozijo z odcepitvijo in priključitvijo Srbiji, Hrvatje - bolj ali manj upravičeno - zahtevajo zase posebno entiteto, muslimani pa kot večina težijo k unitarno urejeni državi. Srbe podpirata uradni Beograd in Moskva, Hrvate uradni Zagreb, muslimane pa Turčija in arabske države. Recept za katastrofo je spisan, obstoj BiH pa resno ogrožen.

Edina realna rešitev je ponovno in po možnosti takojšnje angažiranje EU in ZDA, a možnosti za to je malo.

Makedonija je svojo rakovo pot pričela že tistega večera, ko nek ameriški predsednik prvič v zgodovini NATO ni uspel prepričati ene od članic, da umakne svoj veto na širitev. Ko se je zadeva ponovila še z grškimi blokadami začetka makedonskih pogajanj z EU, je bilo jasno, da Makedonija postaja novo krizno žarišče Balkana. Medtem si je nakopala novega nasprotnika, Srbijo, ki po besedah MZZ Dačića obžaluje, da je Makedonijo priznala pod ustavnim imenom. Vsak konflikt z albansko manjšino prinaša negativne učinke za vse sosednje države, v katerih živijo Albanci. Makedonija je druga država na Balkanu, katere obstoj je lahko realno ogrožen.

Kosovo ostaja talec Srbije in lastne nesposobnosti, da se kot država uveljavi v mednarodni skupnosti. Ker niti ni popolna država tudi sam obstoj Kosova ni zares ogrožen. Edino, kar je zaradi Kosova zares ogroženo je evropska prihodnost Srbije. Srbija je z EU gospodarsko in politično povezana tako močno, da nima realne alternative, tudi zbližanja z Rusijo si ne more privoščiti brez ogromnih političnih tveganj in padca gospodarske rasti. Kosovo ima vselej udobno alternativo; če bo projekt države Kosovo tako kot zdaj zgolj vegetiral, se Albanci s Kosova še vedno lahko pridružijo Albaniji. Vojaške grožnje Srbije pa Kosovu že zdaj odpirajo pot k tesnejšemu političnemu in varnostnemu sodelovanju z Albanijo, ki je članica NATO.

Danes je vitalnost in pomen ohranila le peščica pobud med njimi, pa tudi nekoč najbolj obetavne, stagnirajo. Pogled za nazaj potrjuje, da brez urejenih bilateralnih odnosov države ne morejo imeti dobrega regionalnega sodelovanja.

Regionalno sodelovanje in regionalne pobude na Balkanu

Prvo desetletje po padcu Miloševića je bila na Balkanu „zlata doba“ regionalnega sodelovanja in pobud. Dobra dva ducata jih je bilo in so segale vse od že uveljavljenih srečevanj predsednikov držav JVE tja do RCC, ki se je s stalnim sedežem vzpostavila v Sarajevu. Danes je vitalnost in pomen ohranila le peščica pobud med njimi, pa tudi nekoč najbolj obetavne, stagnirajo. Pogled za nazaj potrjuje, da brez urejenih bilateralnih odnosov države ne morejo imeti dobrega regionalnega sodelovanja. To je tudi razlog, da uspešno deluje le nekaj redkih regionalnih povezav, kakršni sta denimo Baltska skupnost in pa Višegrajska skupina, V-4. Države lahko učinkovito povezujejo samo realni skupni interesi, ki niso samo dnevno politična potreba ampak odraz njihove družbene in gospodarske povezanosti in predvsem medsebojnega zaupanja.

Še dve leti nazaj so bili ob prvem sklicu ti. Berlinske pobude v Berlinu, na pobudo kanclerke Merklove, obljubljeni veliki infrastrukturni projekti v višini petine vrednosti od 12 milijard evrov, ki jih je Balkanu svečano zagotovil takratni predsednik EK Barroso.[8] Srbski PV Vučić je zelo pogumno napovedoval skupno gradnjo avtocestne povezave Niš-Priština, prikimaval mu je kosovski PV Thaci. Po dveh in pol letih se ne dogaja nič. Srbija ne zmore niti tega, da bi Kosovu dopustila članstvo v Unesco, kaj šele, da bi zmogla skupaj s Kosovom graditi ceste, ali pa bi odigrala vsaj nogometno tekmo sedaj, ko je tudi Kosovo član UEFA.

Regionalno sodelovanje postaja velik problem Balkana, ker je vse bolj protokolarno in formalno, z veliko družinskimi fotografijami in zaključnimi deklaracijami a z malo dosežki. Močno zgrešena je že politika srečevanja Berlinskega procesa v zahodnih prestolnicah namesto v prestolnicah Balkana, kjer bi imela taka srečanja večji odmev in najbrž tudi večji vpliv na lokalne javnosti.

Regionalno sodelovanje postaja velik problem Balkana, ker je vse bolj protokolarno in formalno, z veliko družinskimi fotografijami in zaključnimi deklaracijami a z malo dosežki.

Slovenija v razmerah obnovljenih balkanskih napetosti

Zgodovina slovensko-hrvaških odnosov priča o tem, kako je Hrvaška pogosto ovirala napredovanje Slovenije na poti v NATO in EU iz povsem jasnih razlogov; zmanjšati zaostanek Hrvaške na najmanjšo možno mero in preprečiti, da bi Slovenija postala del zahoda še preden bi se Hrvaška odtrgala od Balkana. Nekatera hrvaška lobiranja zoper „prezgoden“ vstop Slovenije v NATO so bila pred časom tudi javno razkrita, večina pa nam bo bržkone ostala prikrita.

Enako velja za čas vstopanja Slovenije v EU, kjer je bil najbolj eklatanten primer sporazum „Drnovšek-Račan“. Ta sporazum je Slovenija hrvaški strani predlagala po nasvetu ZDA in tudi EU z namenom, da meja (pa tudi vprašanje NEK in LB) ne bi več ovirala obeh držav pri sodelovanju in vstopanju v evroatlantske organizacije. Premier Račan je sporazum najprej sprejel, potem pa ga je pod pritiskom iz lastne stranke (Milanović) in celotne opozicije (Sanader) zavrnil. Prevladala je ocena še vedno vplivne Tuđmanove elite, da bo mejni sporazum Sloveniji omogočil „beg“ z Balkana, Hrvaški pa le dodatno otežil možnosti, da Sloveniji čim prej sledi.

Že vse od razpada SFRJ je bila nočna mora hrvaške politike to, da bi se Slovenija preveč oddaljila od balkanskih konfliktov in se odločneje priključila delovanju srednje in zahodnoevropskih držav, kamor sodi gospodarsko in bi z nekaj želje in volje sodila tudi politično. Hrvaška pa bi s svojimi zgodovinskim travmami, s svojimi etničnimi spopadi s Srbijo, s svojimi zahtevami do BiH ter liderskimi ambicijami na Balkanu ostala osamljena. Predvsem pa bi bila brez politične naveze na Slovenijo znova prepoznana kot del problematičnega in nemirnega Balkana, kar je najmanj, kar si katerakoli hrvaška politika želi. Za Slovenijo bi bila zato koristna načrtna in dosledna „depolitizacija“ bilateralnih odnosov s Hrvaško hkrati pa močno povečala politično sodelovanje z državami zahodne in srednje Evrope, še zlasti pri temah varnosti in migracij ter seveda prihodnosti EU.

Zaključek

Novim razmeram na Balkanu je potrebno prilagoditi zunanjo politiko Slovenije, še posebej na področju gospodarske diplomacije. Države Balkana so bile za Slovenijo dolga leta pomembna tržišča zato, ker je z njimi dosegala velike presežke v menjavi. Menjava Slovenije s Hrvaško je v zadnjih 5 letih narasla za več kot 40 odstotkov, od 2 milijard evrov 2010 do 3.3 milijarde evrov leta 2015, ob tretjinskem presežku v korist Slovenije. S preostalimi državami SFRJ in Albanijo pa je menjava v zadnjih 5 letih nihala, zrasla pa le malo, z 2.46 milijard evrov 2010 na 2.65 milijard v 2015, s prav tako velikim presežkom v korist Slovenije. Podatki so zgovorni sami po sebi in pričajo, da kapital na Balkanu postaja vse bolj previden. Slovenija je v zadnjih 5 letih močno povečala svojo blagovno menjavo s tujino, posebej z EU, zato je pomen držav Balkana upadel in predstavlja le še slabih 5 odstotkov blagovne menjave Slovenije s tujino.

Nastale razmere in povečana varnostna tveganja narekujejo previdnost v prvi vrsti pri novih investicijah slovenskih podjetij na Balkanu. Naslednji korak je boljše zavarovanje že obstoječih investicij in proizvodenj. Tretji in skrajen korak pa je lahko premislek o odprodaji investicij na potencialno najbolj ogroženih območjih. Še bolj pomembna je prilagoditev nacionalne strategije v smeri zagotavljanja več razvojne in tehnične pomoči državam Balkana in še več poudarka na sodelovanju držav na področju izobraževanja in sodelovanja mladih. Pomembna bi bila slovenska pomoč pri bogatitvi medijske ponudbe držav Balkana in delovanju lokalnih organizacij civilne družbe. V trenutne medijske razmere držav namreč posegajo predvsem politično-propagandne vsebine, ki prihajajo iz držav s posebnimi političnimi interesi, posebej iz Rusije, Turčije in arabskih držav. Pri tem bi bilo potrebno zagotoviti tudi pomoč EU.

Viri

1 http://ec.europa.eu/eurostat/statistics-explained/index.php/GDP_per_capita,_consumption_per_capita_and_price_level_indices

2 http://data.worldbank.org/indicator/NY.GDP.PCAP.CD

3 https://chnm.gmu.edu/1989/items/

4 http://www.tradingeconomics.com/

5 http://www.janes.com/article/62690/croatia-receives-first-oh-58-kiowa-helicopters

6 http://www.janes.com/article/66503/russia-to-donate-mig-29s-t-72s-to-serbia

7 http://www.balkaninsight.com/en/article/average-salaries-in-ex-yugoslavia-region

8 http://www.dw.com/sr/berlin-daje-tempo-evrointegracijama/a-17887856 ■

Nastale razmere in povečana varnostna tveganja narekujejo previdnost v prvi vrsti pri novih investicijah slovenskih podjetij na Balkanu. Naslednji korak je boljše zavarovanje že obstoječih investicij in proizvodenj. Tretji in skrajen korak pa je lahko premislek o odprodaji investicij na potencialno najbolj ogroženih območjih.

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

Avtorica: mag. Nadja Novak / ELES d.o.o.*

ZAGOTAVLJANJE KORPORATIVNE VARNOSTI JE ZA DRUŽBO ELES IZJEMNEGA POMENA

ELES je pomemben predstavnik kritične infrastrukture v Republiki Sloveniji. Še posebej je ta pomembnost izražena zaradi dejstva, da je podsektor prenosa in proizvodnje električne energije tisti, ki ima neposreden vpliv na učinkovitost delovanja vseh ostalih delov kritične infrastrukture v naši državi in tudi širšem mednarodnem prostoru. S tega stališča je obvladovanje tveganj in s tem zagotavljanje neprekinjenosti delovanja sistema v ELES, ključni proces, ne samo v sami družbi, temveč v širši nacionalno-varnostni dimenziji.

Družba ELES je sistemski operater prenosnega elektroenergetskega omrežja v Republiki Sloveniji, ki skrbi za varen, zanesljiv in neprekinjen prenos električne energije po Sloveniji in prek meja. Povezuje vse glavne udeležence v slovenskem elektroenergetskem prenosnem omrežju:

- elektrarne, ki v prenosno omrežje oddajajo električno energijo;
- pet distribucijskih podjetij;
- pet večjih porabnikov, t. i. neposrednih odjemalcev, ki električno energijo prevzemajo iz omrežja, ter štiri večje porabnike (železarne in Talum), s statusom zaprtega distribucijskega sistema.

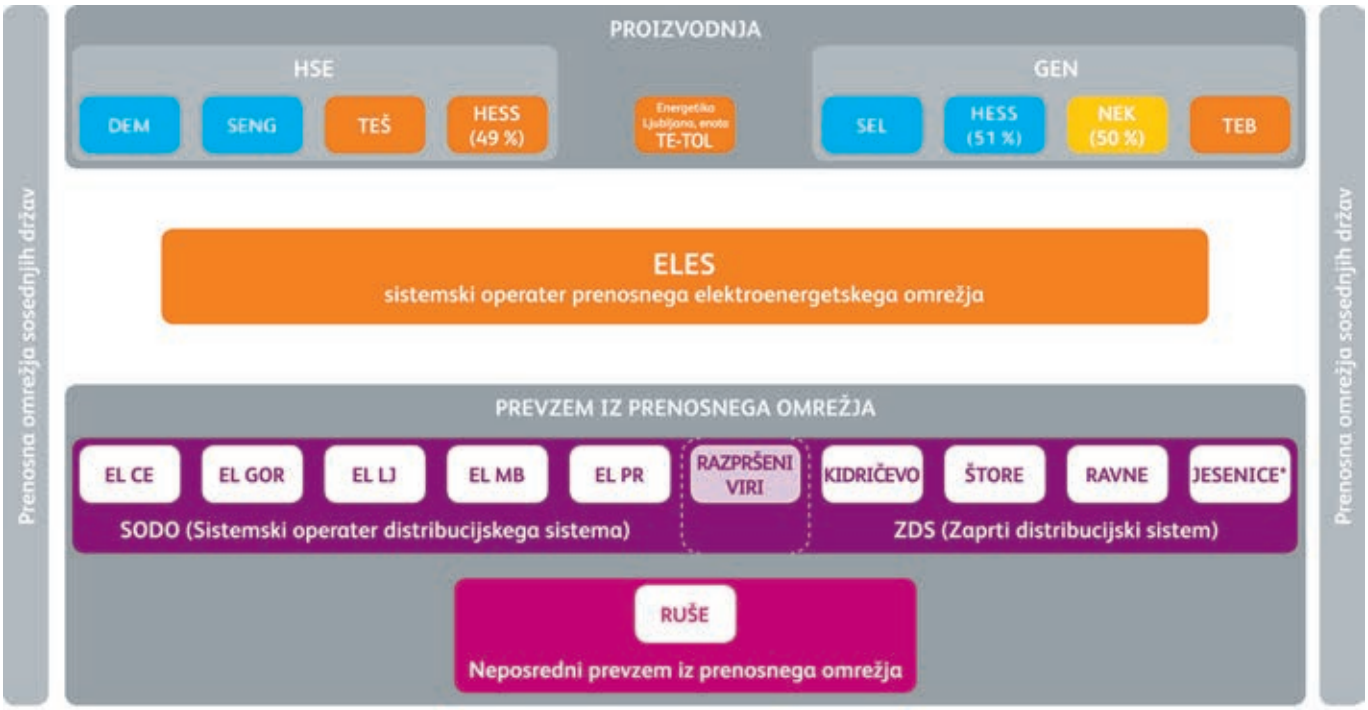
Za zagotavljanje zanesljivega in neprekinjenega prenosa električne energije v družbi strateško, odgovorno in trajnostno načrtujemo, gradimo in vzdržujemo slovensko visokonapetostno prenosno omrežje na treh napetostnih nivojih (400 kV, 220 kV in del 110 kV). Ker se infrastruktura za zagotavljanje električne energije uvršča na sam vrh kritične infrastrukture državnega pomena v Sloveniji, je skrb za zagotavljanje varnosti infrastrukture, ki je v lasti družbe ELES, izjemno pomembna.

Za korporativno varnost družbe ELES skrbi Služba za varnostni sistem in civilno obrambo

Korporativna varnost je za družbo ELES zelo pomembno področje, saj na delovanje podjetja vplivajo različni dejavniki ogrožanja, kot so na primer različni varnostni

Ker se v družbi zavedamo pomena krepitve korporativne varnosti in ker želimo slediti smernicam in trendom na tem področju, načrtujemo prenovo in krepitev omenjene službe ter njeno preimenovanje v Službo za korporativno varnost. V prihodnje si v družbi ELES želimo doseči boljšo sinergijo med tremi stebri za doseganje poslovne odličnosti – to so korporativna varnost, integriteta in upravljanje.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Slika 1: Vloga družbe ELES v slovenskem elektroenergetskem sistemu

dogodki v svetu in pri nas, naravne nesreče, državni predpisi in druga ravnanja oblasti ter najrazličnejša druga negativna odstopanja v družbi.

Za korporativno varnost v Elesu skrbi Služba za varnostni sistem in civilno obrambo, ki spada neposredno pod vodstvo družbe. Med najpomembnejše naloge te službe sodijo skrb za poslovno varnost družbe oziroma njeno neprekinjeno delovanje, kibernetsko varnost ter varnost zaposlenih in premoženja družbe. Sistem korporativne varnosti v družbi ELES obsega prepoznavanje vseh notranjih in zunanjih tveganj, ki bi lahko ogrozila varnost kritične infrastrukture državnega pomena ali zaposlenih in s tem ogrozila delovanje družbe, ter sistematično načrtovanje ter določanje pravnih, organizacijskih, kadrovskih in tehničnih ukrepov, ki so namenjeni ohranitvi reda, spoštovanju zakonov in internih predpisov ter varnosti zaposlenih in premoženja družbe. Urejen je tako, da ob skrbi za zagotavljanje dogovorjene varnosti v podjetju ne ovira izvajanja poslovnih procesov, ki potekajo v Elesu.

Ker se v družbi zavedamo pomena krepitve korporativne varnosti in ker želimo slediti smernicam in trendom na tem področju, načrtujemo prenovo in krepitev omenjene službe ter njeno preimenovanje v Službo za korporativno varnost. V prihodnje si v družbi ELES želimo doseči boljšo sinergijo med tremi stebri za doseganje poslovne odličnosti – to so korporativna varnost, integriteta in upravljanje.

Slika 2: Zaposleni v Republiškem centru vodenja 24 ur na dan in vse dni v letu skrbijo, da prenos električne energije poteka nemoteno.

Zagotavljanje varnosti kritične infrastrukture

Za opravljanje osnovne dejavnosti sistemskega operaterja prenosnega elektroenergetskega omrežja v Republiki Sloveniji, je zagotavljanje varnosti infrastrukture, opredeljene kot kritična infrastruktura državnega pomena, za družbo ELES izjemno pomembno.

Za učinkovito zaščito kritične infrastrukture je izrednega pomena dobro sodelovanje med upravljavci kritične infrastrukture in državnimi institucijami, ki na različnih področjih pripravljajo zakonski okvir za učinkovito delovanje tega sistema. Seveda s stanjem in pristopom državnih inštitucij včasih ne moremo biti v celoti zadovoljni. Upamo, da bo novi Zakon o zaščiti kritične infrastrukture nekatere stvari postavil bolj jasno in predvsem v smeri bolj usklajenih korakov vseh deležnikov na področju zaščite kritične infrastrukture. Vsekakor bi si v Elesu želeli, da je proces sodelovanja dvosmeren in da se v določenih normativnih aktih upošteva posebnosti in dobre prakse, ki jih kot najpomembnejši sistemski operater na področju kritične infrastrukture vsekakor imamo.

Posebej velja omeniti, da je nujno potrebno tako v družbi ELES in tudi v Republiki Sloveniji pristopiti k še aktivnejšemu upravljanju in obvladovanju kibernetskih in drugih s tem povezanih tveganj. Zaradi navedenega zelo veliko pričakujemo iz rezultatov evropskega projekta DEFENDER. Izkušnje in rešitve bodo vsekakor uporabne tudi za druge sistemske operaterje in upravljavce kritične infrastrukture v Republiki Sloveniji.

Seveda pa v družbi ELES nikakor ne zanemarjamo obvladovanja tveganj, ki jih prinašajo zunanji izvajalci določenih pomembnih procesov. Temu bomo predvsem na področju zagotavljanja varnostnih storitev v prihodnosti posvečali še dodatno pozornost. Zelo pomembno je, da se strateško vodstvo zaveda tveganj, ki jih prinaša »outsorcing« ključnih storitev. Zato bo v prihodnje razvoj teh ključnih procesov usmerjen v večje upravljanje z lastnimi viri.

Tudi zaposleni prispevajo k zagotavljanju korporativne varnosti

V družbi ELES se zavedamo, da so zaposleni najpomembnejši vir v družbi, zato predstavlja varovanje zaposlenih eno izmed osrednjih nalog Služba za varnostni sistem in civilno obrambo. Prav tako pa so zaposleni tudi pomemben steber za zagotavljanje korporativne varnosti in za uspešno delovanje družbe. Varnostna kultura v podjetju je povezana z zadovoljstvom zaposlenih ter z njihovim primernim usposabljanjem. Samo zadovoljen in primerno usposobljen delavec bo hkrati tudi primerno varnostno ozaveščen.

Dandanes, ko je mobilnost kadrov na številnih področjih zelo velika, si v Elesu na različne načine prizadevamo za ustvarjanje ugodnih delovnih pogojev in ohranjanje nizke stopnje fluktuacije zaposlenih. To nam tudi dobro uspeva, saj je stopnja nihanja števila zaposlenih v družbi izjemno nizka. Vsi zaposleni so pri svojem vsakdanjem delu dolžni upoštevati tudi načela poslovne etike in podjetniške kulture, ki smo jih že leta 2013 strnili v Etični kodeks družbe ELES ter seveda vse interne predpise.

Za dvigovanje oziroma krepitev zavedanja o pomenu korporativne varnosti, v družbi načrtujemo tudi usposabljanja za zaposlene. Zavedamo se namreč, da imajo družbe z visoko varnostno kulturo zaposlenih boljše možnosti in so na dolgi rok uspešnejše pri izpolnjevanju zadanih ciljev. V ta namen skladno s potrebami oziroma zahtevami večkrat letno organiziramo specializirane interne tečaje in seminarje, preko katerih ozaveščamo zaposlene na kakšen način ravnati, da bodo varnostna tveganja kar najmanjša. Ozaveščamo jih tudi o vlogi posameznika v organizaciji, kajti nezadovoljen posameznik je vedno najšibkejši člen v varnostni verigi.

Stanovsko združevanje je pomembno

Družba ELES je tudi eden izmed korporacijskih članov Slovenskega združenja korporativne varnosti. Ocenjujemo, da je stanovsko združevanje ter izmenjevanje dobrih praks in izkušenj med slovenskimi podjetji in organizacijami priložnost za napredek tako na področju lastnega dvigovanja korporativne varnosti kot na področju dvigovanja zavedanja o pomenu korporativne varnosti v širši družbi.

Evropski projekt »Defender« za zaščito elektroenergetske kritične infrastrukture

Družba ELES, Institut »Jožef Stefan« in Inštitut za korporativne varnostne študije so v okviru mednarodnega konzorcija, ki ga vodi italijansko podjetje Engineering, uspeli pridobiti približno milijon evrov evropskih sredstev za projekt na področju zaščite elektroenergetske kritične infrastrukture.

Cilj projekta Defender (Defending the European Energy Infrastructures) je vzpostavitev sistema ugotavljanja medsebojne odvisnosti in implementacija podatkov, ki se generirajo na vseh ravneh in vrstah infrastrukture in storitev družbe ELES (TSO, kritična infrastruktura, kritične storitve) ter na podlagi tega vzpostaviti model medsebojne odvisnosti podatkov, jih analizirati in vzpostaviti model kompleksnega reagiranja na dano situacijo z vključevanjem vseh dejavnikov družbe in vezanih deležnikov.

Družba ELES je v okviru prijave projekta postala eden od veznih članov med partnerji projekta in pomemben promotor projekta. Priprava prijave projekta pa je prispevala tudi k vzpostavitvi edinstvenega sodelovanja med družbo ELES, Institutom »Jožef Stefan« in Inštitutom za korporativne varnostne študije na področju kritične infrastrukture. ■

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

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije

INTERVJU
Dušan Dular[1] višji strokovni svetovalec generalnega direktorja pooblaščenec za informacijsko varnost[2] in neprekinjeno poslovanje v Krki, d. d., Novo mesto

NEPREKINJENO POSLOVANJE POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

Krka d.d. postaja s svojim širjenjem poslovanja globalna korporacija, ki je izpostavljena celemu nizu tveganj katerega pred njo postavlja dinamično varnostno okolje. Informacijska varnost in neprekinjeno poslovanje s tem postajata pomembno orodje v rokah strateškega managementa, ki mu omogoča učinkovitejše obvladovanje tveganj.

Krka d.d. je pomembno globalno podjetje. Kako pomembno je zagotavljanje neprekinjenosti vaše proizvodnje?

Kot verjetno v vsaki proizvodni organizaciji, je tudi v Krki zagotavljanje neprekinjenosti poslovanja ključnega pomena, saj vsak dan izgubljene proizvodnje, predvsem pa prodaje, ni več možno v celoti nadomestiti. Bolniki sicer neposredno ne bi bili ogroženi, bi pa Krka izgubila ugled in zaupanje svojih strank.

Nezmožnost dobave pa lahko pomeni tudi neposredno izgubo kupcev. Pogodbeni partnerji zaradi svojega zagotavljanja neprekinjenosti poslovanja to zahtevajo tudi od Krke in izvajanje teh zahtev tudi redno preverjajo. Zato smo zapisali, da je osnovni cilj, ki mu mora slediti UNP (upravljanje neprekinjenega poslovanja), da v izrednih oz. kriznih razmerah z obstoječim asortimajem, obstoječimi kapacitetami, obstoječimi dobavitelji, obstoječimi viri (človeški, finančni, energetski, informacijski, ...) zadovoljimo obstoječe kupce.

Kot verjetno v vsaki proizvodni organizaciji, je tudi v Krki zagotavljanje neprekinjenosti poslovanja ključnega pomena, saj vsak dan izgubljene proizvodnje, predvsem pa prodaje, ni več možno v celoti nadomestiti.

Pri zagotavljanju neprekinjenosti poslovanja je na prvem mestu izvajanje preventivnih ukrepov, da do katastrofalnih dogodkov sploh ne pride in vgrajevanje potrebne ravni robustnosti delovanja procesov, ki zmanjšuje občutljivost procesov na velike motnje, kot so npr. redundanca, zamenljivost kadra in podobno. Kljub temu prihaja do izrednih dogodkov, zato je zelo pomemben učinkovit odziv na nesrečo /katastrofo s ciljem zmanjševanja posledic. Šele nato pridejo na vrsto vnaprej pripravljeni načrti neprekinjenega poslovanja, ki z že omenjeno vgrajeno robustnostjo procesov in dodatnimi ukrepi omogočijo delovanje procesov v načrtovanem obsegu v času od »pogasitve požara« do normalizacije stanja.

Konkretno se ukvarjate z ocenjevanjem tveganj in zagotavljanjem ukrepov za neprekinjenost delovanja poslovnega procesa. Kako pomembna je standardizacija tega področja za obvladljivost delovanja tega kompleksnega procesa?

Vsaka standardizacija je posebno v velikih podjetjih še kako pomembna. Vsak proces je sicer odgovoren za obvladovanje svojih tveganj, je pa pomembno, da se vsi procesi tveganja obravnavajo stalno na podoben način da, jih merijo/ ocenjujejo z enakimi oz. vsaj primerljivimi merili. Le na ta način lahko na nivoju celotne organizacije določimo prave prioritete za zmanjševanje tveganj.

[1] Imenovani je član Slovenskega združenja za korporativno varnost.
[2] Imenovani se v okviru informacijske varnosti ponaša tudi z naslednjimi referencami CIS-SIQ Information Security Auditor, CIS-SIQ Information Security Manager in BSI-Business Continuity Management Systems Lead Auditor.

Ali lahko prekomerna standardizacija začne omejevati osnovni poslovni proces in prožnost sistema nepreki-njenega upravljanja v stalno spremi-njajočem varnostnem okolju?

Raziskave kažejo, da je podobno kot v Krki, obvladovanje tveganj v večini proizvodnih organizacij urejeno po področjih, t.i. silosih. Na ta način delovanja nas napeljujejo različni standardi in priporočila dobrih praks, ki nekako vsak po svoje zapovedujejo obvladovanje tveganj po posameznih področjih. Če pogledamo različna področja, kot so npr. tveganja s področja varnosti in zdravja pri delu, okoljska tveganja, tveganja informacijske varnosti in varovanja osebnih podatkov, finančna tveganja, tveganja zagotavljanja kvalitete končnih izdelkov, tveganja zagotavljanja medijev za proizvodnjo, tveganja dobave/dobaviteljev, splošna varnostna tveganja (npr. požar, eksplozija, vlom),... vse našteto je praktično nemogoče »stlačiti« v en koš, pod en standard, v eno metodologijo. Stopnje zavesti in načini upravljanja/ vodenja procesov s pomočjo obvladovanja tveganj so različni. Če bi stremeli k preveliki standardizaciji, lahko zavremo kreativnost v posameznih procesih ali posameznikih. Prevelika notranja reguliranost/ formalizacija podrobnih postopkov za obvladovanje posameznih tveganj je lahko ovira za uvajanje novosti, ali pa izgovor. Je pa zelo pomembno, da obstajajo zapisi o dejanskem izvajanju obvladovanja tveganj v procesih. Tu mislim na zapisane pristope/ metodologije, rezultate posameznih ocen tveganj, morebitne ukrepe in spremljanje izvajanja ukrepov.

Vse nove verzije ISO standardov postavljajo upravljanje tveganj kot eno od ključnih orodij za uspešno vodenje organizacij. Priporočajo uporabo nekaj osnovnih pristopov kot je npr. ISO 31000, sicer pa prepuščajo vsaki organizaciji, da na svoj način prepoznava tveganja, jih ocenjuje in obvladuje. V vsaki (uspešni) organizaciji obvladujemo tveganja pa če temu rečemo tako ali ne. Ko imamo npr. težave, iščemo vzroke (tveganja), ocenjujemo posledice (stopnje tveganja), sprejemamo ukrepe (zmanjšanje tveganj na sprejemljivo raven) in spremljamo njihovo realizacijo. Vse skupaj je lahko zapisano v različnih oblikah, od zapisnikov sestankov do projektne dokumentacije, odvisno od obsežnosti problema. Bistvo je pravočasno preventivno vpeljevanje ukrepov za zmanjševanje tveganj. Poleg nekaj generičnih/ tradicionalnih pristopov/ metod ocenjevanja tveganj poznamo tudi na desetine drugih metod (kvalitativnih, pol-kvantitativnih in kvantitativnih). Katera je najprimernejša? Odgovor ni enostaven. Morda je problem tudi v tem, da jih ne poznamo dovolj.

Moje mnenje je torej, da ne smemo pretiravati s standardizacijo, moramo pa imeti z najvišjega nivoja delovanja organizacije pregled nad tem, ali sploh oz. kako posamezni procesi obvladujejo tveganja, katerih lastniki so. V večjih podjetjih je slej ko prej za vse to potrebna posebna funkcija (organizacijska enota), ki celotno podjetje spodbuja k vodenju s pomočjo upravljanja tveganj, postavlja enotne kriterije za vrednotenje tveganj, skrbi za skupni katalog tveganj na nivoju podjetja, procesom pomaga pri izboru najbolj primernih metodologij in tehnik, ima nadzor nad izvajanjem vseh ocen

tveganj, ima nadzor na izvajanjem vseh ukrepov in učinkovitostjo izvedbe ukrepov, vodstvu zagotavljala ažurni pregled največjih tveganj,... seveda mora biti vse skupaj podprto s primernim orodjem za podporo sistemu obvladovanja tveganj.

Nam lahko zaupate kakšen pomen ima po vašem mnenju korporativna varnost v procesu zagotavljanja neprekinjenosti delovanja organizacije?

V Krki je služba, ki obvladuje korporativno varnost, globoko vpletena v neprekinjenost poslovanja predvsem na področju preventivnega delovanja pri preprečevanju katastrofalnih scenarijev, kot so npr. požari in eksplozije. V njihovi domeni je obvladovanje klasičnih tveganj, ki ogrožajo imetje Krke. Za cca 20 tveganj, kot so požar, eksplozija, vdori, vlomi, itd,, izvajajo oceno varnostne ogroženosti vseh stavb in delovnih procesov, predlagajo in izvajajo ukrepe za zmanjševanje tveganj, izvajajo izobraževanja/ usposabljanja in preverjanja zaposlenih glede poznavanja in izvajanja preventivnih varnostnih ukrepov. Zelo pomembna je njihova skrb za vzpostavitev in delovanje sistemov aktivne zaščite, ki npr. v primeru požara avtomatsko, brez prisotnosti gasilcev, gasijo požar.

Drugo pomembno področje pa je odziv na morebitno veliko nesrečo/katastrofo. Varnostna služba obvladuje celotni sistem alarmiranja in obveščanja ob nesrečah. V sklopu korporativne varnosti je tudi lastna poklicna gasilska enota, z ustrezno opremo in stalno pripravljenostjo, ki prva intervenira v primeru večjih nesreč. Korporativna varnost skrbi tudi za pripravo načrtov zaščite in reševanja, ki se lahko aktivirajo ob večjih nesrečah.

Ne smemo pa pozabiti tudi na zagotavljanje varnosti in zdravja pri delu, saj so zaposleni eden od ključnih virov pri zagotavljanju neprekinjenosti poslovanja.

Da, korporativna varnost ima veliko vlogo pri zagotavljanju neprekinjenosti poslovanja, predvsem v izvajanju preventivnih ukrepov s ciljem povečanja odpornosti na velike grožnje in na drugi strani pri odzivu na incidente/ nesreče s ciljem preprečevanja/ zmanjšanja posledic nesreče/ katastrofe.

Da, korporativna varnost ima veliko vlogo pri zagotavljanju neprekinjenosti poslovanja, predvsem v izvajanju preventivnih ukrepov s ciljem povečanja odpornosti na velike grožnje in na drugi strani pri odzivu na incidente/ nesreče s ciljem preprečevanja/ zmanjšanja posledic nesreče/ katastrofe.

Menite, da bi se morala za učinkovitejše obvladovanje varnostnih tveganj informacijska varnost tesneje povezovati s korporativno varnostjo?

Seveda, informacijska varnost in korporativna varnost morata tesno sodelovati. Če pogledamo standard ISO 27002 je za izvajanje zahtev v poglavju 11.1. Varovana območja odgovorna predvsem korporativna varnost. Tu mislim na fizično varovanje, pristopno kontrolo, varovanje pisarn, sob in naprav, zaščita pred zunanjimi grožnjami,... Vse je povezano tudi z zagotavljanjem varovanja informacij. V Krki pri varnostni oceni vsake stavbe, ki jo izvaja korporativna varnost, ocenjujemo tudi vpliv posameznih groženj na razpoložljivost, celovitost in zaupnost dokumentov/ informacij, ki se fizično nahajajo v stavbi ali posebej izpostavljenih prostorih z višjim varnostnim tveganjem.

Kako je po vaši oceni pomembna organizacijska in predvsem varnostna kultura pri zagotavljanju neprekinjenosti delovanja? Ali temu v organizaciji posvečate pomembno pozornost?

Kultura, tudi varnostna, je nekaj, kar ustvarjamo skozi leta. Zavedanje o pomenu predvsem zaščite, varovanja in zagotavljanja delovanja ključnih procesov je v Krki prisotna verjetno že od njene ustanovitve. Ko smo se odločili, da vzpostavimo sistem upravljanja neprekinjenega poslovanja v skladu s standardom, je bil prvi korak t.i. »analiza vrzeli«, ki je pokazala, da imamo vzpostavljene praktično vse zahteve standarda s področja preventivnega delovanja, ozaveščanja, povečevanja odpornosti na velike motnje, alarmiranja, ukrepanja ob velikih nesrečah, obveščanja javnosti, presojanja in verjetno še kaj. Tudi na področju načrtov neprekinjenega poslovanja, je bilo pripravljenih že veliko ukrepov, s pomočjo katerih bi lahko posamezni ključni procesi zagotavljali svojo neprekinjenost delovanja v primeru pojava velikih nesreč/ katastrof. To kaže na to, da je bila varnostna kultura tudi na področju neprekinjenosti poslovanja že od nekdaj na visokem nivoju. Skozi izvajanje projekta vzpostavitve sistema upravljanja neprekinjenega poslovanja se je to zavedanje zaposlenih in vodilnih v procesih še okrepilo predvsem glede smiselnosti priprave in testiranj samih načrtov neprekinjenega poslovanja.

Je vlaganje v izobraževanje in usposabljanje kadrovskih potencialov lahko tista potrebna kakovost, ki tudi na področju varnostnega zavedanja loči uspešna podjetja od povprečnih?

Izobraževanje kadrov je seveda predpogoj, da postaneš in ostaneš uspešno podjetje. V Krki v internem izobraževanju posvečamo veliko pozornost tudi izobraževanju in dvigovanju zavesti na raznih področjih povezanih z varnostjo, kot so npr. varnost pri zagotavljanju kakovosti končnega izdelka, varnost in zdravje pri delu, varstvo pred požarom in eksplozijo, informacijska varnost, okoljska varnost, itd. Zaposleni se morajo zavedati, da so ključni pri izvajanju varnostnih ukrepov oz. so največja nevarnost oni sami, če teh ukrepov ne izvajajo.

Seveda je pred tem potrebno zavedanje vodstva podjetja, ki mora tovrstne aktivnosti in pristope spodbujati, zagotavljati resurse in tudi kontrolirati.

Posebno področje izobraževanja in usposabljanja pa so znanja povezana z upravljanjem tveganj oz. neprekinjenim poslovanjem v procesih dela. Zaposleni običajno z lastno iniciativo in samo usposabljanjem pridobijo potrebna znanja o načinu obvladovanja in primernih metodologijah za obvladovanje tveganj v njihovih procesih. V primeru, da obstajajo možnosti izobraževanja in usposabljanja s tega področja zunaj Krke, spodbujamo in omogočamo tudi to obliko izobraževanja. V večjih podjetjih je smiselno razmišljati o specializiranih kadrih, ki s poznavanjem metodologij in orodij in poznavanjem dejanskih praks v samem podjetju lahko s prenosom dobrih praks (lastnih ali tujih) prispevajo k bolj učinkovitemu obvladovanju tveganj v procesih in s tem na splošno v celotni organizaciji .

Ste tudi eden od pomembnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebna in lahko prinesejo v naš prostor dodatno kvaliteto?

Prepričan sem, da so take oblike združevanja strokovnjakov v vseh strokah pomembne, drugače ne bi bil član združenja. Ko je ICS pred leti ustanovil v bistvu prvo združenje na področju korporativne varnosti, sem se mu kmalu pridružil, saj je predvsem neformalno izmenjevanje izkušenj s kolegi iz združenja zelo pomembno, da pridobiš nove ideje, znanja ali pa dobiš potrditev, da je tisto, kar delaš, deležno pozornosti in odobravanja tudi s strani stanovskih kolegov. Najdragocenejše pa so gotovo zgledne prakse, ki jih članom združenja omogočajo obiski organizacij, saj jih sicer nimamo priložnosti pogledati s tega zornega kota. ■

Izobraževanje kadrov je seveda predpogoj, da postaneš in ostaneš uspešno podjetje. V Krki v internem izobraževanju posvečamo veliko pozornost tudi izobraževanju in dvigovanju zavesti na raznih področjih povezanih z varnostjo. Zaposleni se morajo zavedati, da so ključni pri izvajanju varnostnih ukrepov oz. so največja nevarnost oni sami, če teh ukrepov ne izvajajo.

Varno v nov dan

Tel: +386 1 8317 488
Fax: + 386 1 8317 551
Service tel.: + 386 1 8317 452
Web: www.zarja.com
E-mail: info@zarja.com
prodaja@zarja.com

ZARJA ELEKTRONIKA

Avtorica: Nataša Klenovšek Arh, univ. dipl. ing. rač. in inf., mag. dr. inf*

SODOBNI SISTEMI UPRAVLJANJA Z ALARMI

"Optimizacija procesov, tehnični pregled in nadzor, možnost hitre prilagoditve, varnost in stabilnost velikih ali manjših objektov." Vse to so nujne zahteve današnjih vse bolj zapletenih sistemov, če želimo zagotoviti ustrezno tehnično varovanje. Zato smo v pregled vzeli enega izmed ponudnikov tovrstnih rešitev, to je alarmno-nadzorni grafični sistem Zarja AMS.

Organizirano vodenje, upravljanje in nadziranje si v današnjem času težko predstavljamo brez sodobnih informacijsko komunikacijskih tehnologij. Da lahko zagotovimo ustrezno kakovost in varnost celotnega sistema, je izrednega pomena zajemanje podatkov v realnem času, s pomočjo česa lahko nudimo celotno podporo procesu odločanja.

Vsaka organizacija, predvsem pa podjetja, kjer so visoka tveganja za napake, zaradi kompleksnosti proizvodnih procesov (kemična industrija, farmacija, proizvodnja električne energije, skladišča...), bi morala sistem upravljanja z alarmi, obravnavati z najvišjo možno prioriteto in kot sestavni del njihovega proizvodnega obrata.

Potrebam po celovitem nadzoru in upravljanju tehničnega varovanja sledi tudi podjetje Zarja Elektronika, ki je zahvaljujoč dolgoletnim izkušnjam na področju razvoja sistemov tehničnega varovanja, razvila napreden alarmno-nadzorni grafični sistem Zarja AMS.

V podjetju smo opravili osnovni varnosti pregled sistema Zarja AMS na podlagi smernic standarda ISO/IEC 27001, pri čemer smo uporabili različne tehnike tovrstnih varnostnih pregledov.

Alarmno-nadzorni grafični sistem Zarja AMS

Je produkt lastnega znanja in omogoča vsem deležnikom (operaterjem varnostnih nadzornih centrov, odgovornim v podjetjih ali ustanovah, gasilsko reševalnim službam...) prikaz statusa in upravljanje z integriranimi sistemi preko enotnega grafičnega vmesnika.

Sistem Zarja AMS temelji na SCADA sistemu, ki predstavlja glavne funkcije programske opreme Zarja AMS:

Alarmno-nadzorni grafični sistem Zarja AMS predstavlja celovito rešitev na področju tehničnega varovanja, ki pokriva širok spekter različnih sistemov.

S (Supervisiory) – nadzor
C (Contro) – kontrola
A (and) – in
D (Data) – podatkovni
A (Acquisition) – zajem.

SCADA preko različnih standardnih komunikacijskih povezav prejema podatke o stanju naprav ter jih ustrezno obravnava v smislu pregleda, razvrščanja in arhiviranja v kronološke liste dogodkov. Sistem Zarja AMS omogoča več nivojski grafični prikaz točnega mesta alarma na grafični mapi, mogoča je verifikacija, ki omogoča deležnikom primerno ukrepanje na podlagi informacij, ki jih sistem generira in takojšne izvajanje ustreznih postopkov.

Sistem Zarja AMS omogoča povezavo različnih naprav tehnične zaščite (javljanja požara, vloma, kontrole dostopa, registracije delovnega časa, video-nadzornih sistemov) v enoten sistem prikaza in upravljanja. Sistem je najpogosteje postavljen v varnostno nadzornem centru naročnika na centralnem računalniku in tako omogoča upravljanje in nadzorovanje sistemov tehnične zaščite z enega mesta. Zarja AMS omogoča prikaz žive slike in posnetkov digitalnih snemalnikov, krmiljenje video-nadzornega sistema vključno z obračanjem in

*avtorica je članica Slovenskega združenja korporativne varnosti

krmiljenjem objektiva kamer, kontrolo dostopa ob požarnih alarmih in vlomnih dogodkih ter povezovanje naprav tehnične zaščite različnih modelov in proizvajalcev ter priključitev in krmiljenje različnih sistemov upravljanja objektov (prezračevalnih in klimatskih sistemov, dvigal, toplotnih postaj, sistemov osvetlitve, svetlobnih znakov...) preko različnih standardnih povezav (ModBus , TCP/IP, Profibus DP...).

Varnostni vidik

V pogovoru z odgovornimi v podjetju Zarja Elektronika smo bili seznanjeni, da imajo v praksi največ sistemov Zarja AMS implementiranih v internih zaprtih sistemih naročnikov in niso dosegljivi preko interneta.

V času testiranja sistema Zarja AMS, smo do grafično-nadzornega vmesnika dostopali iz oddaljene lokacije preko spletnega brskalnika. Vmesnik je bil dostopen preko http protokola, pri čemer smo uspeli ujeti nekatere občutljive podatke v berljivi obliki, vendar pa podjetje za naročnika, v primeru zunanjega dostopa, poskrbi za https dostop, ki predstavlja varno različico http protokola, kjer je komunikacija med spletnim brskalnikom in spletno aplikacijo zaščitena, česar pa v tem primeru nismo testirali.

Uporabnik se prijavi z uporabniškim imenom in geslom, pri čemer se upošteva načelo »least privilege«, kar pomeni, da uporabnik dostopa samo do tistih funkcionalnosti, ki so potrebne za opravljanje njegovega dela. Testirali smo dostop z večkratnim poskušanjem naključnega uporabniškega imena in gesla, pri čemer nismo bili opozorjeni, da smo prekoračili dovoljeno število morebitnih napačnih prijav, s čimer bi lahko za krajši čas onemogočili ugotavljanje prijavnih podatkov in tako otežili izvedbo napada nepooblaščenega vstopa v sistem z ugotavljanjem prijavnih podatkov. Omenjena varnostna vrzel bi lahko postala tveganje v primeru možnosti dostopa iz svetovnega spleta, zato v Zarji že razmišljajo tudi o uvedbi politike upravljanja in varovanja gesel v grafično-nadzorni vmesnik Zarja AMS.

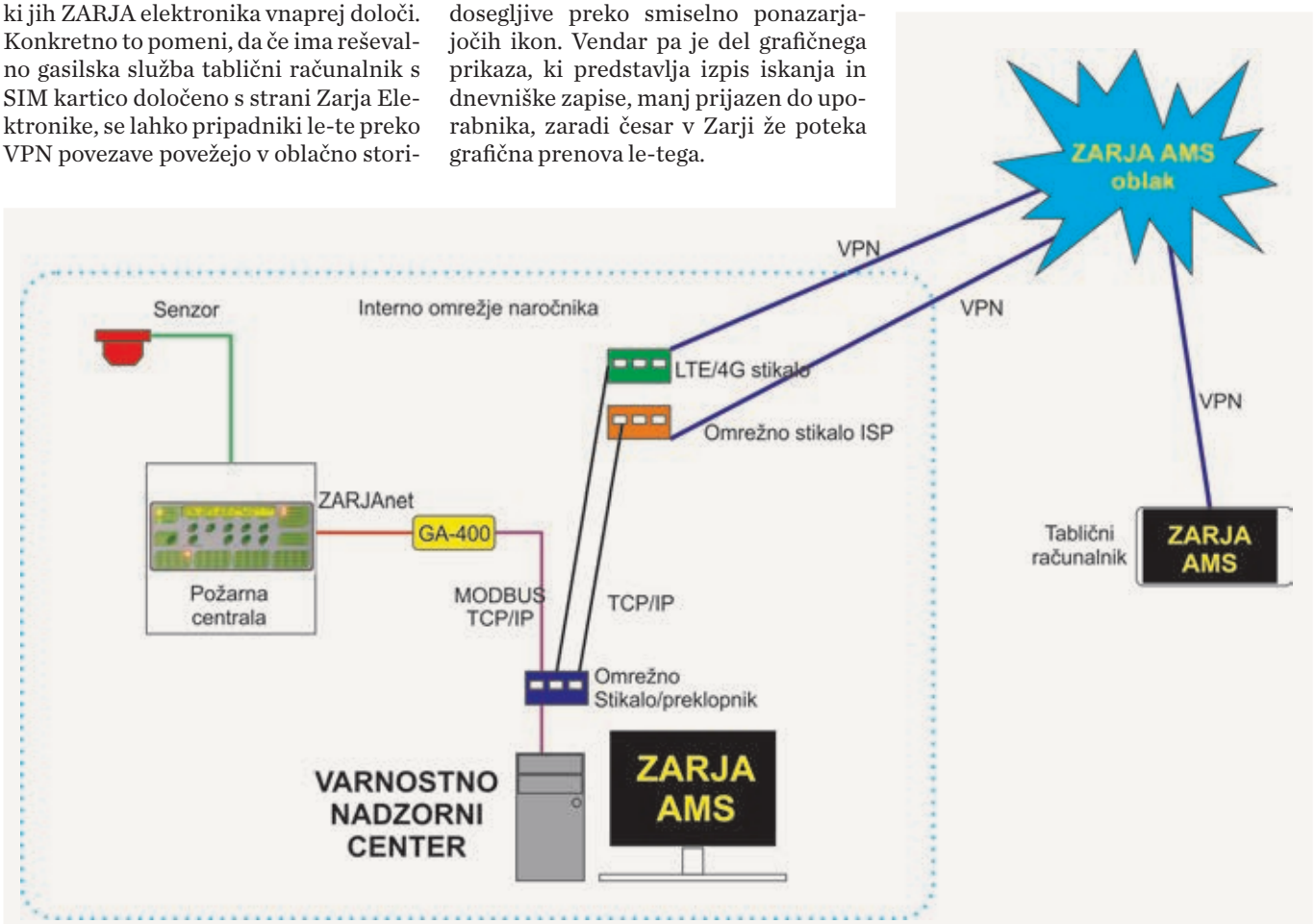
Varnost spletnega vmesnika smo preverili z vrivanjem stavkov SQL (ang. »SQL Injection«), pri čemer nismo bili uspešni. Po pregledu dnevniških zapisov, skupaj z odgovorno osebo podjetja Zarja Elektronika, smo ugotovili, da so poskusi bili zabeleženi, vendar pa administrator o tem ni bil posebej obveščen, kar pomeni, če administrator ne spremlja dnevniških zapisov, ne ve, da se je zgodil poskus napada. Vsekakor pa je tovrstna zaščita veliko bolj smiselna, ko bo omogočen dostop iz svetovnega spletna.

Če povzamemo…

Podjetje Zarja Elektronika je s svojimi storitvami na trgu prisotna že od leta 1969 in z izkušnjami iz terena in konzervativno varnostno politiko uspešno krmari med izzivi trga in potrebami naročnikov. Alarmno-nadzorni grafični sistem Zarja AMS predstavlja celovito rešitev na področju tehničnega varovanja, ki pokriva širok spekter različnih sistemov. Zarja AMS je odziv na sodobne čase, ko je potrebno združiti in optimizirati upravljanje več sistemov tehnične zaščite in upravljanja sistemov objektov v eno celoto in obenem omogočiti varen in učinkovit dostop do potrebnih informacij vsem deležnikom v sistemu. Menimo, da so z vidika informacijske varnosti na dobri poti, vendar se je potrebno zavedati vseh vidikov možnosti ogrožanja informacijske varnosti, zato je potrebno spremljati, nadzirati in se pravočasno odzivati na izzive, ki jim jih v prihodnosti vsekakor ne bo zmanjkalo. ■

Sistem Zarja AMS je mogoče povezati preko naročnikovih spletnih povezav ali preko mobilnega LTE/4G omrežja v ZARJINO oblačno storitev preko IP VPN storitev. Povezava se vzpostavi preko fiksnega ali mobilnega interneta, vendar skozi varen IPSec tunel. V primeru uporabe mobilnega interneta je dostop omogočen samo prek SIM kartic, ki jih ZARJA elektronika vnaprej določi. Konkretno to pomeni, da če ima reševalno gasilska služba tablični računalnik s SIM kartico določeno s strani Zarja Elektronike, se lahko pripadniki le-te preko VPN povezave povežejo v oblačno storitev in že med potjo na samo intervencijo dostopajo do potrebnih informacij (požarni načrt..). Je pa potrebno pri vzpostavitvi VPN povezav upoštevati vsa varnostna priporočila (265 bitno šifriranje, uporaba L2TP/IPsec protokolov...).

Iz uporabniškega vidika, je vmesnik dokaj razumljiv, kjer so funkcionalnosti dosegljive preko smiselno ponazarjajočih ikon. Vendar pa je del grafičnega prikaza, ki predstavlja izpis iskanja in dnevniške zapise, manj prijazen do uporabnika, zaradi česar v Zarji že poteka grafična prenova le-tega.



Skupina Triglav

triglav

Vse bo v redu.
www.triglav.eu

Avtor: mag. Miran Vršec / Institut za korporativne varnostne študije*

VARNOST V HOTELSKI INDUSTRIJI – Gradnik konkurenčne prednosti države in posamezne destinacije

Že dolgo je povsem jasno, da je varnost - poleg cene in kakovosti - sestavni del turistične ponudbe. V okoliščinah povečanja globalnih in regionalnih varnostnih groženj ter vse večjih težav obvladovanja varnostnih tveganj pa varnost postaja stalnica in dejanska potreba v posodabljanju varnostnih arhitektur v turističnih nastanitvenih objektih in v drugih turističnih storitvah in destinacijah. Kajti varnostne razmere so se začele spreminjati tudi v Evropi, ki je bila leta 2013 vodilna svetovna turistična destinacija, katero je obiskalo 560 milijonov mednarodnih potnikov.

Turisti so se v Evropi, s kakovostjo in varnostjo turističnih storitev, počutili varne in zadovoljne. Iz Zelene knjige Varnost turističnih nastanitvenih storitev je razvidno, da je Evropska komisija že leta 2010 za ohranitev in okrepitev svetovnega vodilnega položaja Evrope v turizmu sprejela sporočilo o celoviti strategiji za povečanje konkurenčnosti turistične industrije. Sestavni del ukrepov v tem sporočilu je tudi varnost turističnih nastanitvenih zmogljivosti. Kajti le ustrezna in učinkovita stopnja varnosti poveča zaupanje potrošnikov in okrepi rast z ustvarjanjem ugodnega okolja za bivanje in koriščenje celovite turistične ponudbe. Zagotavljanje varnosti hotelov je potemtakem ključna sestavina varnosti v turizmu kot prepoznavni in najbolj obsežni gospodarski dejavnosti.

V Evropi je Slovenija - z vidika terorizma - ena od najbolj varnih držav. To pa ni razlog, da bi varnost razumeli in obravnavali na lahkoten in samoumeven način, kajti varnostne razmere se tudi z vidika terorizma lahko v hipu spremenijo. Pa ne gre samo za terorizem. Varnost je treba razumeti zelo kompleksno (nesreče, klasični in organiziran kriminal, korupcija, afere, stavke idr.) kamor uvrščamo tudi katastrofalne in šokantne posledice kakšnega varnostnega incidenta oziroma izrednega dogodka. S tega zornega kota je treba obravnavati tudi varnost v hotelski industriji. Pri izboru turistične destinacije in konkretnega hotela ljudje vse bolj pogosto razmišljamo o varnostnem vidiku, ki predstavlja vse večjo težo pri končni odločitvi o izboru lokacije začasnega dopustniškega ali poslovnega bivanja. To je lahko eden od pomembnejših izzivov turističnih agencij in hotelirjev, kako varnostni vidik izrabiti za konkurenčno prednost in celovitost turistične ponudbe.

Pri izboru turistične destinacije in konkretnega hotela ljudje vse bolj pogosto razmišljamo o varnostnem vidiku, ki predstavlja vse večjo težo pri končni odločitvi o izboru lokacije začasnega dopustniškega ali poslovnega bivanja. To je lahko eden od pomembnejših izzivov turističnih agencij in hotelirjev, kako varnostni vidik izrabiti za konkurenčno prednost in celovitost turistične ponudbe.

Pri razmišljanju o varnosti v hotelih in hotelskih kompleksih, najprej pomislimo na analizo ogroženosti in varnostnih tveganj v makro in mikro okolju v katerem se hotel nahaja. Makro vidik analizira širše okolje (država, politična situacija, stopnja kriminalitete, zdravstvene razmere, podnebje, zračno, cestno in pomorsko infrastrukturo ipd.), mikro vidik pa ožje okolje hotela (lokalna skupnost, lokalna

*avtor je član Slovenskega združenja korporativne varnosti

stopnja kriminalitete, zdravstvena oskrba, lokalna infrastruktura, neposredna okolica in lokacija hotela, osebje ipd.). Že ta osnovna analiza lahko posamezniku zagotavlja ključne informacije o izboru lokacije njegovega začasnega bivanja. Izjemno pomembno je torej, kako je v ponudbi hotelirja predstavljen varnostni vidik in na kakšen način so obvladovana varnostna tveganja.

Za zagotavljanje optimalne stopnje varnosti hotela je potrebno vzpostaviti celovit sistem varnostnih ukrepov, ki je po eni strani »gostu prijazen«, po drugi strani pa zagotavlja optimalno obvladovanje ogroženosti in tveganj. Pomemben segment pri dolgoročnem zagotavljanju optimalne stopnje varnosti predstavlja krovna varnostna politika, politike za posamezna področja varnosti in uvedeni varnostni standardi. Pri načrtovanju optimalne varnosti moramo izhajati iz sistemskega pristopa in upoštevati čim širši nabor vidikov, ki vplivajo na varnost hotela. Pri tem je nujno upoštevanje zakonodaje, zahtev in podpore državnih organov in lokalne skupnosti (zdravstvena oskrba, policija, lokalno redarstvo, lokalne varnostne službe ipd.), makro in mikro okolje, kulturno in versko okolje, arhitekturne ureditve lokacije in objektov, dejavnosti, organizacije in ponudbe (osnovne in dodatne) hotela, strojnih, elektro in drugih inštalacij, energetske podpore, ciljnih skupin gostov in nenazadnje nabora možnih organizacijskih, fizičnih in tehničnih varnostnih rešitev. Zakonodaja, zahteve okolja in lokalne skupnosti, makro in mikro okolje ter kulturno in versko okolje predstavljajo temeljna izhodišča oziroma nujni okvir za vzpostavljanje in delovanje varnostnega sistema.

Arhitekturna ureditev lokacije in objektov lahko že predstavlja prvo oviro pri načrtovanju varnostnega sistema. Gre za problematiko nadzorovanja dostopov do lokacije in objektov, vhodov/izstopov v/iz lokacije in objektov, spremljanja gibanja vozil, blaga in oseb na lokaciji in znotraj posameznih objektov, nadzorovanja objektov in opreme, shranjevanja vrednosti, evakuacije v primeru izrednih dogodkov ipd. Pri iskanju ustreznega nabora varnostnih rešitev je iz tega vidika potrebno tudi upoštevati skladnost izbranih rešitev z arhitekturnimi rešitvami. Pri tem mislimo tudi na estetsko podobo elementov mehanske zaščite, elementov sistemov tehničnega varovanja, uniformiranost in delovna mesta varnostnega osebja ter zagotavljanje intervencijskih poti do hotela.

Iz **organizacijskega** vidika je potrebno upoštevati dejstvo, da sestavni del sodobnega poslovnega okolja predstavlja tudi področje varnosti, ki mora biti vpeto v strateški nivo vodenja in upravljanja hotela. Trendi in potrebe gredo v to smer, da turistične agencije že pri pripravi svojih ponudb angažirajo neodvisne strokovnjake, ki iz varnostnega vidika ocenijo in analizirajo ogroženosti in varnostna tveganja na neki lokaciji in na podlagi izdelane analize predlagajo ustrezne ukrepe za zagotovitev varnosti turistov, ki se bodo odpravili na oddih na konkretno lokacijo.

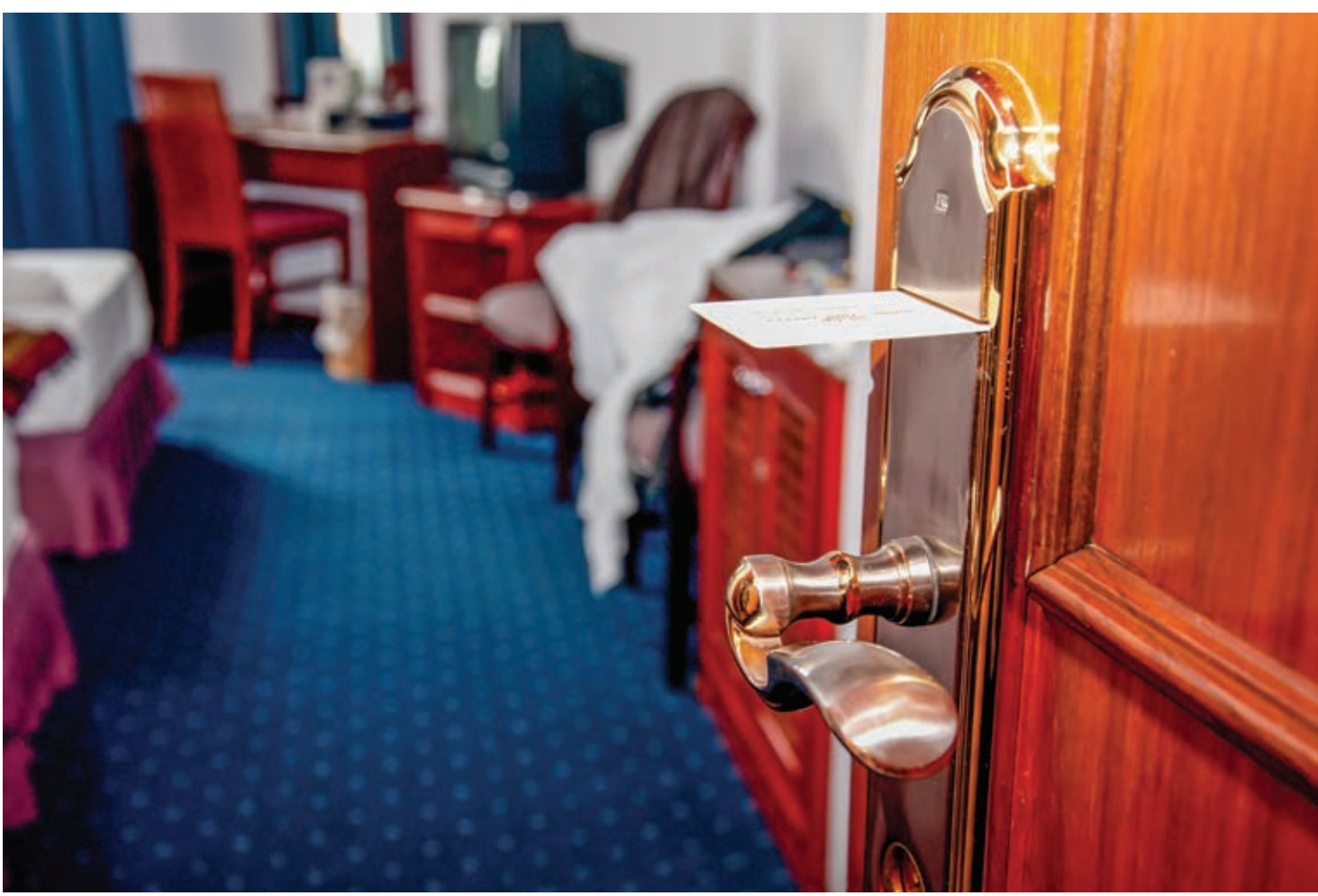
Iz **tehničnega** vidika za obvladovanje varnostnih tveganj uporabljajo različne kombinacije sistemov mehanske zaščite (npr.: varnostne ograje, varnostne zapornice, potopni stebrički, rolo in protivlomna vrata, trirogi, varnostna stekla in folije, varnostne blagajne in priročni sefi za osebno uporabo, sistem ključev ipd.) ter različne kombinacije sistemov tehničnega varovanja (npr.: sistemi aktivne požarne zaščite, sistemi za zgodnje odkrivanje in javljanje plinov, sistemi kontrole pristopa, sistemi za klic v sili v primeru zdravstvenih težav ipd.). Vsekakor je smiselno sisteme mehanske zaščite (tiste, ki so elektronsko krmiljeni) in sisteme tehničnega varovanja povezati v celovit sistem tehničnega varovanja, ki

je krmiljen preko centralnega nadzornega sistema s katerim upravlja operater v lastnem ali dislociranem varnostno (operativno) nadzornem centru, ki deluje 24 ur dnevno. Tak center se smiselno uporablja tudi kot komunikacijsko vozlišče za potrebe drugih služb in hkrati zagotavlja lokacijo za krizni štab v primeru nastanka izrednih varnostnih dogodkov (potres, izredne vremenske razmere, požar ipd.).
Iz vidika **neposrednega varovanja** lahko za obvladovanje tveganj organiziramo naslednje oblike fizičnega varovanja: neposredna prisotnost varnostnega osebja na lokaciji (stalna ali občasna - ob pomembnejših ali varnostno bolj izpostavljenih dogodkih), varnostni obhodi, intervencijsko posredovanje na alarmne situacije ali klice v sili ipd. Za najzahtevnejše ali bolj izpostavljene goste lahko hotelir ponudi tudi možnost najema osebnega varnostnika, ki bo skrbel za varno počutje gosta na lokaciji hotela in izven njega.

Z vidika **zakonodaje**, upoštevajoč tudi varnostne standarde v turizmu ter iz povsem praktičnih razlogov si mora menedžment hotela zagotoviti vse potrebne načrte in navodila, ki se nanašajo na varnost hotelskih zgradb, zaposlenega osebja, gostov in njihovega premoženja ter varnost celotnega hotelskega kompleksa. Govorimo o načrtu varovanja oseb in premoženja, ki obsega fizično in tehnično varovanje, protipožarni načrt, alarmno-odzivni načrt in načrt evakuacije. Za potrebe informiranja in usposabljanja za varnostno obnašanje in ravnanje pa je potrebno izdelati vsebinsko ustrezna varnostna navodila, posebej za zaposleno osebje, za goste, za vodnike izletov in drugih zunanjih hotelskih storitev in za zunanje pogodbene izvajalce. Vse to so varnostni dokumenti, ki v učinkovitem sistemu varovanja hotelskega kompleksa zagotavljajo visoko stopnjo varnosti, udobja in zadovoljstva.

> Občutek in dejanska stopnja varnosti je vse bolj pomemben faktor nakupnega odločanja posameznikov pri iskanju hotelskih kapacitet, kar še dodatno potrjuje naše dosedanje ugotovitve in ugotovitve konkretno predstavljene raziskave. Tudi zato se je potrebno zavedati, da visok nivo varnosti v hotelski industriji na dolgi rok zagotavlja pomembno konkurenčno prednost državi in posamezni turistični destinaciji na turističnem trgu.

Napovedovanje prihodnosti je precej tvegano opravilo. Za turizem, kot eno najhitreje rastočih panog, bi lahko rekli, da malce zaostaja za ostalimi gospodarskimi panogami, ko govorimo o področju obvladovanja varnostnih tveganj. Turizem je še posebej vpet v vse bolj globalna varnostna tveganja, zato je pri ocenjevanju tveganj tudi v tej panogi potrebno razmišljati globalno in delovati lokalno. V ta namen je na primer Sky Tuch razvil »Hotel security radar« kot orodje, ki



spremlja globalna varnostna tveganja in služi kot osnova za vzpostavitev sistema upravljanja s tveganji, izdelavo varnostne dokumentacije in usposabljanje osebja. Omenjeno orodje opredeljuje varnostna tveganja, ki so v letu 2015 vplivala na varnost hotelov. Pri tem je potrebno izpostaviti naslednjih pet dejavnikov:

Kraja identitete z namenom zlorabe kreditnih kartic

Varnost naše lastne identitete je bila v letu 2015 bolj kot kadarkoli prej najbolj izpostavljeno varnostno tveganje. Zlorabe kreditnih kartic, ki so posledica kraje identitete trenutno predstavljajo največjo grožnjo s katero se soočamo v hotelih. Kriminalne združbe ali posamezniki si z vdori v hotelski informacijski sistem ali neposredno krajo identitete gostov in krajo njihovih kreditnih kartic omogočajo dvigovanje gotovine in plačevanje blaga in storitev. Cilj bolj organiziranih kriminalnih združb ni le posamezni gost ampak skupine gostov, saj s tem dosegajo bistveno večje učinke svojega nezakonitega delovanja. Vse analize kažejo, da bo tudi v bodoče pričakovati porast omenjenih kaznivih dejanj.

Vdori v informacijski sistem

Kibernetska kriminaliteta hotelom predstavlja drugo največje varnostno tveganje. Hoteli imajo široko razvejani socialni inženiring zaradi katerega je izpostavljenost na tem področju toliko večja. Tu gre predvsem za izpostaviti tako imenovane APT (Advanced Persistent Threats), ki po svetu veljajo za najbolj nevarno obliko kibernetskih napadov na informacijske sisteme. Gre za prikrite in trajne napade na informacijski sistem s ciljem iskanja trenutnih varnostnih lukenj v zaščiti konkretnega informacijskega sistema in vdora v sistem. Napadi pa niso usmerjeni le na hotelski informacijski sistem, ampak so tarča napadov tudi gostje, ki preko hotelskega WI-FI vstopajo v omrežje. Praviloma so hotelski WI-FI bolj ranljivi, saj je njihova zaščita šibkejša in kot taka lažja tarča za napadalce. Gre za vdore v podatkovne baze gostov, ki se teh tveganj praviloma niti ne zavedajo in tako za napadalce postajajo lahek plen.

Preredke oziroma pomanjkljive revizije hotelske varnosti

Hotelska industrija sledi hitro rastoči panogi turizma. Skoraj vsak dan se nekje na svetu odpre nov hotel. Na svetu je okoli 1,26 milijona hotelov, ki se vsak po svoje ukvarja z varnostnimi vprašanji in izzivi prihodnosti ter obvladovanjem varnostnih tveganj. Z rastjo števila hotelov pa sorazmerno ne raste število varnostnih strokovnjakov (varnostnih revizorjev), ki izvajajo revizije varnostnih rešitev. Ta razkorak se iz leta v leto še povečuje. Na dolgi rok bo ta razkorak predstavljal vse večji problem, saj se revizije varnostnih rešitev ne bodo izvajale dovolj pogosto, strokovno in celovito, kar bo negativno vplivalo na varnost hotelov na dolgi rok. Pričakovati je, da se bo strošek revizij na dolgi rok dvigoval, kvaliteta pa padala. V praksi se ta problem kaže v tem, da nekateri hoteli podaljšujejo ročnost med posameznimi revizijami, spet drugi pa zaradi kratkoročnega prihranka stroškov izvedbe revizije le teh sploh ne izvajajo več. Ti trendi vodijo v povečevanje varnostnih tveganj tako na strani hotela kot tudi na strani gostov.

Fizični napadi

Kriminaliteta se po državah razlikuje. Vendar pa je, ne glede na navedeno dejstvo, v svetovnem merilu prepoznati splošno povečanje fizičnih napadov v hotelih. Tu gre predvsem za izvajanje vlomov v prostore hotelov in hotelskih sob ter razpečevanje drog v hotelskih sobah. Gostje vse bolj postajajo žrtve organiziranega kriminala in oboroženih napadov, predvsem v nočnem času. Hoteli so namreč v nočnem času lažje dostopni in manj varovani. V tem smislu se priporoča uvajanje programov ozaveščanja zaposlenih in gostov o nevarnostih, ki prežijo na njih v času delovanja ali bivanja v hotelu. V primeru povečevanja recesije in povečevanja socialnih razlik je v bodoče pričakovati porast tovrstnih kaznivih dejanj. V tem kontekstu moramo obravnavati tudi terorizem, kot globalno grožnjo varnosti, katerega dejanja se izvaja v lokalnih okoljih.

Zniževanje konkurenčne prednosti zaradi večjih varnostnih incidentov

Zavedati se je potrebno, da po daljšem časovnem obdobju, ko ni varnostnih incidentov in ko so varnostne revizije ohlapne, pozornost na varnostna vprašanja pada, s tem pa se lahko povečujejo varnostna tveganja, ki lahko negativno vplivajo na varnost hotela in njegovih gostov. Preventivno delovanje in nenehno vlaganje v posodabljanje varnostnih rešitev je torej na dolgi rok edina prava odločitev. Vlaganje v preventivne ukrepe je namreč na dolgi rok bistveno cenejše od stroškov, ki nastajajo zaradi škod in izgub do katerih prihaja zaradi šibkih in pomanjkljivih varnostnih mehanizmov.

Večji varnostni incidenti, to so incidenti, ki imajo za posledico omejeno delovanje ali celo zaprtje hotela za krajši čas, povzročijo izgubo poslov ter zahtevajo dodatna vlaganja v sanacijo posledic posameznega incidenta. Okrnjen ugled hotela ima zaradi večjega varnostnega incidenta lahko dolgoročne posledice na delovanje hotela, v nekaterih primerih lahko pripelje tudi do zaprtja hotela.

Dosedanje izkušnje so pokazale, da je v organizacijah, kjer imajo vzpostavljen celovit sistem varovanja in obvladovanja in vzpostavljen sistem upravljanja varnostnih tveganj na strateškem (korporativnem) nivoju (varnostno politiko, varnostno dokumentacijo, varnostne sisteme, učinkovit alarmni in odzivni sistem, redno vzdrževanje, servisiranje in posodabljanje sistemov varovanja, zagotavljanje neprekinjenega delovanja, izobraževanje in revidiranje), verjetnost nastanka varnostnega incidenta bistveno manjša, s tem pa je zagotovljena dolgoročna krepitev blagovne znamke in dobrega imena hotela.

Občutek in dejanska stopnja varnosti je vse bolj pomemben faktor nakupnega odločanja posameznikov pri iskanju hotelskih kapacitet, kar še dodatno potrjuje naše dosedanje ugotovitve in ugotovitve konkretno predstavljene raziskave. Tudi zato se je potrebno zavedati, da visok nivo varnosti v hotelski industriji na dolgi rok zagotavlja pomembno konkurenčno prednost državi in posamezni turistični destinaciji na turističnem trgu. ■

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

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

IZVIRNA MISEL

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

PRAVA IZBIRA

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

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

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

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

Integralni varnostni sistemi (celovito varovanje)

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

Varovanje oseb in premoženja

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

Kakovost in varnost

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

Krizno vodenje (krizni menedžment)

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

IZOBRAŽEVANJE

Varnostni menedžment

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

Avtor: dr. Brane Bertoncelj/Slovensko združenje korporativne varnosti*

ODLOČANJE IN KORPORATIVNA VARNOST: MED MOŽNOSTMI IN RACIONALNOSTJO

Življenje in delo posameznika je prepleteno z majhnimi in velikimi odločitvami. Odločanje je ena od najbolj značilnih mentalnih aktivnosti posameznika, ki se zgodi vsakih nekaj sekund (več tisoč dnevno), zavestno ali nezavedno.

V tem procesu prihaja do izbire med alternativami raznih prepričanj, možnih poti, aktivnosti ali dejavnosti, kar ustvari končno izbiro, odločitev. Obrobne odločitve sprejemamo hitro, kot po tekočem traku in z lahkoto. Povsem drugače pa doživljamo odločitve, ki bodo s svojimi, tisti trenutek posamezniku še neznanimi posledicami, bistveno vplivale na njegovo življenje ali delo. Vsa ta negotovost povzroča neprijetne emocije, napetost, tesnobo, frustracije in nelagodje. Pogosto je v ozadju tudi strah, da bo posamezniku kasneje žal, ker se je tako odločil. To nenehno tehtanje in izbiranje, pogosto med čustvi in razumom, povečuje razumski in psihični pritisk znotraj posameznika. V bistvu je odločanje potovanje iz nejasnosti v jasnost, iz teme v svetlobo. Kako torej izbrati pravo odločitev med možnostmi in racionalnostjo, je eno poglavitnih vprašanj tudi na področju korporativne varnosti. Ali smo pripravljeni sprejeti vse posledice odločitve, tako pozitivne kot tudi negativne?

Odločanje

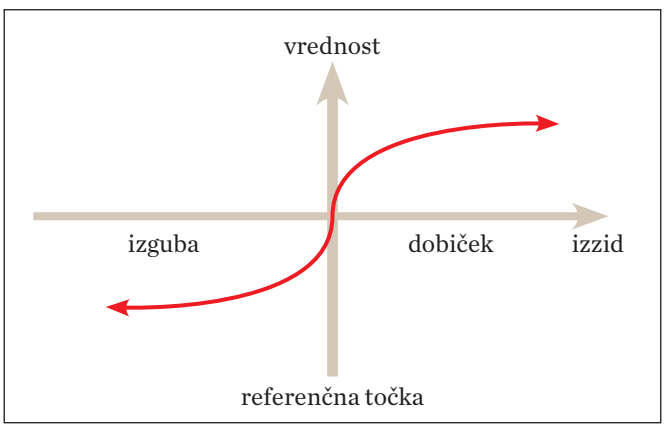
Večina odločitev je povezana z zadovoljevanjem potreb, med več možnostmi, v času in prostoru. Kaj imajo skupnega skrb za korporativno varnost organizacije: varnost poslovnih procesov, zaposlenih, sredstev, informacij, objektov, preprečevanje izgube informacij, notranjih prevar, obvladovanje varnostnih tveganj, preprečevanje notranjih in zunanjih ogrožanj? To so ODLOČITVE. Sprejemanje odločitev je eden temeljnih kognitivnih procesov, ki je široko uporabljen v določanju racionalnih, hevrističnih in intuitivnih selekcij v različnih situacijah, v vsakodnevnem življenju, poslovanju in tudi na področju korporativne varnosti. Odločanje na področju korporativne varnosti je danes zaradi številnih varnostnih izzivov in alternativ, ki so na razpolago, mnogo bolj kompleksno in zahtevno, kot je bilo v preteklosti.

Odločanje na področju korporativne varnosti je danes zaradi številnih varnostnih izzivov in alternativ, ki so na razpolago, mnogo bolj kompleksno in zahtevno, kot je bilo v preteklosti.

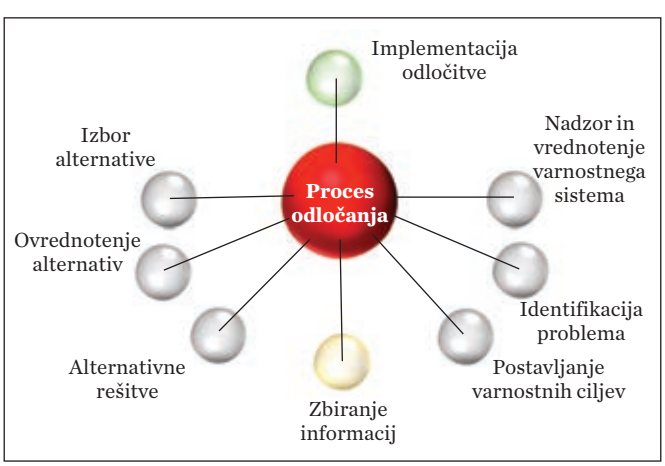
V skladu s teorijo neomejene racionalnosti, bi lahko vsak, ki se sooča s sprejemanjem odločitve, izmeril strošek in korist, ki bi jo ta prinesla. Tudi v razmerah negotovosti se lahko subjektivno oceni posledice odločitve. Raziskave kažejo, da je racionalnost odločanja relativno omejena, ker posameznik ne zna zaznati in izračunati vseh možnih izidov, zaradi nepopolnih informacij pa sprejema pogojno dobre odločitve. Nekatere odločitve so enostavne, pri teh lahko najdemo direktno povezavo med nekim dejanjem in posledicami ter kompleksne, s številnimi možnimi variablami. Posameznik ni najboljši ocenjevalec verjetnosti in lahko sistematično krši načela razumnega odločanja pri soočanju z dejavniki negotovosti. Njegova izbira ne ustreza osnovnim zahtevam doslednosti in skladnosti. Pogosto precenjuje verjetnost nedavnih, živih ali čustveno nasičenih dogodkov. Vse prevečkrat jih določa njihova neposredna preteklost, ki omejuje predvidevanja posameznika na poenostavljene konstrukte, v katerih je prihodnost zrcalna slika preteklosti. Raziskave kažejo, da so precenjeni dogodki dramatični in senzacionalni, podcenjeni pa praviloma nezanimivi.

*avtor je član Slovenskega združenja korporativne varnosti

Na spodnji sliki je prikazana funkcija hipotetične vrednosti odločanja (Kahneman in Tversky, 1992). Odločanje se začne s strukturiranjem problema, ki poenostavlja naknadno vrednotenje in izbiro, možni rezultati pa so dobički ali izgube glede na neko referenčno točko (običajno je to »status quo«, lahko tudi pričakovanje, želja ali potreba). Funkcija vrednosti je različna za dobičke in izgube, možni izid odločitve ali njegove posledice pa so pogojne verjetnosti, ki povezujejo rezultate z dejanji (funkcija je konveksna in razmeroma strma za izgube ter konkavna in postopna za dobičke). Posamezniku izguba prinese mnogo več neugodja, kot dobiček vzbuja zadovoljstvo.



Na spodnji sliki je prikazan proces odločanja (Florjančič in sod., 2004). Večina odločitev na področju korporativne varnosti je povezanih z zadovoljevanjem varnostnih potreb in zahtev. Varnostne dobrine so na razpolago v omejenih količinah (saj popolne varnosti ni), zato je možno doseganje le optimalne varnosti. Proces se začne z oceno stanja varnostnega sistema, identificiranjem varnostnih problemov in postavljanju varnostnih ciljev. Baza podatkov za zbiranje informacij je obsežna, sledi nabor raznih alternativ, njihovo vrednotenje in izbor. Zadnjo fazo pa predstavlja implementacija odločitve.



Stili odločanja

Stili odločanja so težnja k reagiranju na specifičen način, v odločitveni situaciji, pri čemer imajo na njih velik vpliv tudi značilnosti varnostnega problema. Več dejavnikov vpliva na sprejemanje odločitev: izkušnje (Juliusson in sod., 2005), kognitivne pristranskosti (Stanovich in West, 2008), starost in individualne razlike (Bruin in sod., 2007), prepričanje v osebno relevantnost (Acevedo in Krueger, 2004). Scott in Bruce (1995) sta definirala pet stilov odločanja (racionalni, intuitivni, odvisni, izogibajoči ali spontani). Racionalni stil je značilen za posameznika, ki podrobno išče in logično ovrednoti vse obstoječe alternative. Osredotoča se predvsem na logiko, red in sistematično analizo informacij. Intuitivni stil je značilen za tiste, ki namenjajo veliko pozornosti podrobnostim in upoštevajo svoje občutke o tem ali je neka odločitev pravilna ali ne, odvisni stil pa je značilen za tiste, ki iščejo nasvete in vodenje pri drugih. Izogibajoči stil je značilen za posameznika, ki se želi izogniti sprejemanju odločitve, spontani pa za tistega, ki ima občutek, da je v časovni stiski in želi odločitev čim hitreje sprejeti.

Posameznik ne uporablja samo enega stila odločanja, temveč uporablja kombinacijo stilov, pri čemer eden ali dva prevladujeta. Racionalni in intuitivni stil sta opredeljena kot funkcionalna stila odločanja, saj je posameznik, pri katerem ta stila prevladujeta, bolj prepričan v svoje sposobnosti, ima večji občutek samo-učinkovitosti in v večji meri upošteva sebe (Nygren in White, 2005). Intuitivni stil se v nasprotju z racionalnim stilom pozitivno povezuje tudi z višjo inovativnostjo (Scott in Bruce, 1995), medtem ko se racionalni stil, v nasprotju z intuitivnim, pozitivno povezuje z manjšo težnjo k sprejemanju tveganih odločitev (Baiocco in sod., 2009). Ravno nasprotno pa so rezultati raziskav pokazali za odvisni, izogibajoči in spontani stil. Posameznik, ki uporablja predvsem te tri stile odločanja, ima občutek, da usoda ni v njegovih rokah in je bolj nagnjen k sprejemanju tveganih odločitev (Baiocco in sod., 2009).

Poleg že navedenih stilov odločanja, obstajajo še drugi stili odločanja in so prikazani na spodnji sliki (naključno, rutinsko, sistematično odločanje).

Dejavniki, ki vplivajo na odločitev

Obstaja več dejavnikov, ki vplivajo na odločanje. Ti so pretekle izkušnje, različne kognitivne pristranskosti, starost, individualne razlike in prepričanja, pomembna za posameznika.

Pretekle izkušnje lahko vplivajo na prihodnje odločanje. Juliusson in sod. (2005) menijo, da pretekle odločitve vplivajo na odločitve tudi v prihodnosti. Bolj verjetno je, da se posameznik v podobni situaciji, po pozitivnih rezultatih predhodnih odločitev, odloči na podoben način tudi v prihodnje. Po drugi strani pa se posameznik izogiba ponavljanju preteklih napak (Sagi in Friedland, 2007). To je pomembno, če prihodnje odločitve, ki temeljijo na preteklih izkušnjah, niso nujno najboljše. Obžalovanje, občutek razočaranja in nezadovoljstva z odločitvijo, je lahko tudi potencialni rezultat odločanja. Po Abrahamu in Sheeran (2003) je obžalovanje prepričanje, da bo odločitev posledica neukrepanja.

Zaključek

Za kvalitetno odločanje moramo znati obvladovati in upravljati negotovost ter tveganja. Albertu Einsteinu pripisujejo citat: »Noro je ponavljati iste stvari in pričakovati drugačen rezultat.« Ali obrnjena misel – če so vse okoliščine enake, je smiselno pričakovati enak rezultat. In to je osnova napovedne varnostne analitike – iščemo miselne vzorce, ki so se že pojavili. Ob inovativnem pristopu storilcev kaznivih dejanj (čim bolj preprosto, tem bolj učinkovito) pa je lahko navedena trditev tvegana.

Racionalni posameznik postaja vse bolj pomemben dejavnik odločanja v kompleksnem varnostnem okolju. Faktorji, ki vplivajo na sprejemanje odločitve na področju korporativne varnosti so: strokovno znanje odločevalca, pretekle delovne izkušnje, starost, individualne razlike in prepričanje v osebno relevantnost. Kognitivne bližnjice lahko vodijo do slabših odločitev, vendar pa posamezniku omogočajo hitrejše odločanje ob podpori posebnih mentalnih strategij.

Učinkovito odločanje otežuje vrsta dejavnikov, in sicer: močno omejen razpoložljiv čas za odločanje, dopustnost napačne odločitve je minimalna, nepričakovano pojavljanje novih elementov za odločanje, odločanje v razmerah, ki so presenetile ali celo šokirale, ne poznamo vseh faktorjev situacije, ki vplivajo na odločitev, obstaja velika količina variant, vsi podatki niso dosegljivi ipd. Poseben problem predstavljajo nepoznavanje odločitvenega problema in ciljev odločitve, omejena sredstva (čas, denar, varnostni strokovnjaki ipd.) in možna nesoglasja med posamezniki, ki sodelujejo pri odločanju.

Racionalni posameznik postaja vse bolj pomemben dejavnik odločanja v kompleksnem varnostnem okolju.

Optimalno odločanje otežuje pretirana prepričanost o pravilnosti lastne sodbe. Posameznik prevečkrat pretirano zaupa lastnim, tudi napačnim sodbam. Osnova za to je verjetno neobčutljivost za pomanjkljivost domnev in predpostavk, na katerih slonijo njegove ocene. Najbrž noben dejavnik slabe odločitve ni bolj odločujoč kot pretirana samozavest. Narava problema in sodbe določa tudi raven samozavesti. Splošno strokovno znanje povzroča visoko stopnjo pretirane samozavesti, velja pa tudi obratna trditev.
Nekateri predlogi za dobro odločanje:

- osredotočite se na najbolj pomembne varnostne probleme (ki so se že zgodili, so pred tem, da se zgodijo, na kakšen način želite problem preprečiti?),
- ne odločajte se, če niste na to pripravljeni. Ne delujte impulzivno ali panično,
- bodite pozorni na pozitivne rezultate odločitve,
- resno razmislite o možnosti negativnega rezultata odločitve. Kateri je lahko najslabši možni scenarij, kako se ga lahko prepreči?
- odločitve usmerite v prihodnost. Kakšni bodo rezultati vaše odločitve v času in prostoru?
- zamenjajte število pomembnih odločitev za vrsto manjših sklepov,
- ne obstajata samo ena ali dve možnosti, ampak več. Proučite jih,
- odločite se za tiste, ki jih organizacija potrebuje, da bo poslovala varno. ■

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije

INTERVJU
Dejan Dobrovoljc, direktor oddelka informatike
v podjetju Interblock d.d.*

INFORMACIJSKA VARNOST POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

Interblock d.d. je s svojim širjenjem poslovanja že zdavnaj postalo globalno podjetje, ki je izpostavljeno celemu nizu tveganj, katere pred njega postavlja dinamično varnostno okolje. Informacijska varnost, sploh ko govorimo o igralniški industriji, s tem postaja pomembno orodje v rokah strateškega managementa, ki mu omogoča učinkovitejše obvladovanje varnostnih in informacijskih ter drugih s tem povezanih tveganj.

Korporativna varnost in še bolj specialno informacijska varnost je zelo pomembna nit vaše poslovne kariere. Nam lahko poveste katera so ključna področja pristojnosti, ki ste jih v svoji bogati karieri konkretno izvajali?

Odgovor na vprašanje bi vsekakor postavil v širši časovni okvir. Področja mojega strokovnega delovanja so bila že na začetku poklicne poti tako ali drugače povezana z informacijsko varnostjo.

Terminus kot tak v tistem obdobju vsekakor ni bil tako eksaktno definiran kot danes. Večino svojih dobrih praks in principov informacijske varnosti sem zato gradil vzporedno s potrebami in zahtevami takratnega časa ter dejanskih potreb klientele za katero sem delal.

Prelomna točka v mojem razvoju je bila povezana z igralniško industrijo. Potrebno je bilo na novo koncipirati in dejansko zgraditi strojno platformo, ki je izpolnila vse rigorozne in dokaj rigidne varnostne zahteve igralniškega regulatorja. 5 let kasneje se podobna rešitev pojavi na svetovnem IT trgu (TPM, Bitlocker in secure boot).

Realne izzive korporativne varnosti na globalnem nivoju sem spoznaval v korporaciji Siemens AG. S primarnega položaja Information Security Advisor-ja za Slovenijo sem napredoval v regionalni Security and Crisis Management oddelek. Odgovoren sem bil za neprekinjeno delovanje internih komunikacijskih sistemov ter satelitskih povezav v primeru kriznih situacij. Izjemno poučna izkušnja je bilo kasneje tudi delo za globalni oddelek CSO (corporate security office).

Globaliziran pristop je tudi v igralniški sektor prinesel popolnoma spremenjeno sliko. Trendi povezovanja različnih igralnih in multimedijskih naprav v neko celoto, souporaba novih tehnologij in pristopov ter povezljivost s korporativnimi zalednimi sistemi pa so to arhitekturo v pretežni meri spremenili. Iz navedenih razlogov je informacijska varnost postala eden od osnovnih in bistvenih elementov, ki se upoštevajo pri razvojnem in produkcijskem ciklu izdelkov.

Pridobljene izkušnje s pridom uporabljam pri izvedbi projektov na varnostno zahtevnem igralniškem področju.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

8. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 15.—16. MAREC 2017

PODELIJO SE 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!

Interblock d.d. predstavlja globalno podjetje, ki se ukvarja z zelo specifično dejavnostjo, kot je izdelava naprav za igralniško industrijo. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Globalna prisotnost seveda prinaša pozitivne učinke na delovanje in rast podjetja. Obenem pa zaradi različnih zakonodaj, regulative in nenazadnje lokalne specifike zahteva zelo multidisciplinaren pristop. Po mojih izkušnjah se percepcija tveganj tako pri zaposlenih kot tudi naših zunanjih partnerjih globalno precej razlikuje. Posledično izvajamo več ocen tveganja, ki skušajo zajeti lokalno situacijo. Ocene tveganj izvajamo tudi s pomočjo ustreznih lokalnih poslovnih partnerjev. Analize medsebojno primerjamo in klasificiramo ter skušamo izvesti čim bolj poenotene korektivne ukrepe.

Mogoč bistven vpliv ukrepov na poslovne procese se predhodno uskladi z vodstvom podjeta. Celoten cikličen postopek pa seveda zahteva ustrezno kadrovsko in finančno podporo katero je potrebno konkretno argumentirati.

Kako pristopate k prepričevanju strateškega managementa, da za delovanje procesov korporativne in informacijske varnosti nameni ustrezne organizacijske in finančne vire?

Način našega delovanja do določene mere regulirajo že lokalne zakonodaje, ki bolj ali manj specifično predpisujejo okvirne ukrepe informacijske varnosti. Govorimo seveda o osnovnem nivoju, po večini temelječem na uveljavljenih ISO standardih.

Oddelek Informatike je eden od kritičnih podpornih elementov delovanja naših poslovnih procesov. Operativne in razvojne potrebe ter vpeljava novih rešitev se generalno načrtuje skupaj z managementom ostalih oddelkov, skladno z njihovimi potrebami. Na osnovi specifikacij in uporabniških zahtev IT oddelek predlaga ustrezno rešitev ter okvirno ovrednoti potrebna sredstva, tako finančna kot tudi kadrovska, ter planiran časovni okvir implementacije. Izdelan projekt se vnese v planiran globalni IT budget, ki se zagovarja pred upravo podjetja. Glede na dinamiko poslovanja podjetja ali zaradi pojava ad hoc situacij pa je občasno določen del sredstev potrebno pridobiti tudi izven regularnih procesov planiranja. V takih primerih se managementu predstavi situacija, možen ali zaznan vpliv s stališča informacijske varnosti ali področja skladnosti, ter potrebni korektivni ukrepi.

Pri svojem delovanju imate pomembne specifike, ki se posebej odražajo v novih razvojnih produktih in ste globalno prisotni skoraj na vseh celinah. Kako so po vašem mnenju pomembne ključne informacije korporacije v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču? Nam lahko zaupate kako pomemben je v takih

primerih učinkovit sistem varovanja ključnih poslovnih informacij.

Podjetje Interblock d.d. na področju igralništva med drugim pokriva dokaj specifično in tehnološko izjemno zahtevno področje ETG (electronic table games). V primerjavi z ostalimi igralniškimi produkti tukaj ne govorimo o sto tisočih prodanih napravah ampak o »high end« izdelkih namenjenih za relativno ozek spekter igralniškega tržišča. Lahko rečemo, da je podjetje do neke mere globalni market leader, tako na področju inovativnega pristopa, uporabljenih tehnologij kot tudi novih oblik iger. Razvojni cikel produktov je primarno pogojen s potrebami in zahtevami tržišča. Časovni okvir od ideje, ustrezne certifikacije do realne implementacije na trgu je iz teh razlogov lahko merljiv tudi na letnem nivoju. Razkritje strateških informacij o naših novih produktih ali načinih uporabe bi lahko drugim proizvajalcem omogočilo zmanjšanje naše konkurenčne prednosti. Podobne produkte bi namreč lahko lansirali z manjšim zaostankom za nami.

Igralniški sektor je vedno bolj soodvisen od informacijske tehnologije. S tem se pred nas postavljajo tudi pomembna tveganja, ki jih prinaša ravno ta tehnologija. Zaupajte nam kako pomembna je informacijska varnost in kateri koraki so ključni za obvladovanje tveganj?

Modus operandi v igralniškem sektorju se je z leti prilagajal potrebam in zahtevam tržišča na katerem deluje. V pretekem obdobju je določen tip igralniških sistemov deloval kot zaključena celota v relativno izoliranem habitatu. Ta situacja je do neke mere dovoljevala arhitekturo, orientirano samo k svoji primarni nalogi, »entertainmentu«.

Globaliziran pristop je tudi v igralniški sektor prinesel popolnoma spremenjeno sliko. Trendi povezovanja različnih igralnih in multimedijskih naprav v neko celoto, souporaba novih tehnologij in pristopov, ter povezljivost s korporativnimi zalednimi sistemi pa so to arhitekturo v pretežni meri spremenili. Iz navedenih razlogov je informacijska varnost postala eden od osnovnih in bistvenih elementov, ki se upoštevajo pri razvojnem in produkcijskem ciklu izdelkov. Za uspešno obvladovanje tveganj pa samo ta element ni dovolj, potrebno je imeti vzpostavljen celoten proces.

Razvojni cikel produkta kot celote se začne z ustrezno razdelano produktno dokumentacijo. Vsebuje idejno zasnovo in v določeni meri tudi že krovno arhitekturo. Na dokumentu v tej fazi dela kar nekaj stakeholderjev oziroma deležnikov. Neavtoriziran dostop ali (ne)namerno razkritje vsebine že v tej fazi lahko pomeni izgubo konkurenčne prednosti ali odtujitev intelektualne lastnine. S stališča informacijske varnosti vsekakor lahko definiramo njegovo stopnjo zaupnosti, kje se dokument mora ali lahko hrani, kdo ga lahko obdeluje ali kako se prenaša med deležniki. Za informacijsko podporo temu procesu je danes na voljo velika večina potrebnih tehnologij in orodij. Vprašanje pa je ali so tudi pravilno in ustrezno

medsebojno integrirana in tako uporabniku še omogočajo enostavno delo. V kolikor ti pogoji niso izpoljneni, uporabniki v večini primerov poiščejo alternativne poti ter posledično celo kompromitirajo proces.

Podoben vzorec velja tudi za nadaljnje stopnje procesa. Razvoj programske kode in strojne opreme, beta testiranje, quality assurance, qualitiy control in nenazadnje proizvodni proces. Osebno smatram vlogo Informacijske tehnologije v vseh naštetih točkah procesa kot izjemno pomembno. Tako s stališča informacijske varnosti kot tudi apliciranja IT specifičnih znanj in dobrih praks v celoten razvojni proces.

Verjetno redno spremljate stanje na področju korporativne varnosti v slovenskem okolju. Kako bi ocenili zavedanje strateškega managementa v slovenskih podjetjih o pomenu korporativne varnosti in učinkovitega obvladovanja tveganj?

Težko bi podal neko realno oceno dejanskega stanja. Glede na izkušnje in izmenjavo mnenj v svojem krogu poslovnih sodelavcev in kolegov pa menim, da je situacija vsaj v določenem krogu podjetij dobra oziroma se hitro izboljšuje. Razlogov je sigurno več, morda lahko izpostavim vsaj dva na katera sem pretežno naletel. Izvozno naravnana in razvojna podjetja. Značilnost obeh je zavedanje o pomenu varovanja in obvladovanja informacij ter skladnost s standardi in poslovnimi procesi veljavnimi v razvitih ekonomijah. Vejamem, da management v slovenskih podjetjih temu področju daje večjo ali manjšo veljavo, pač skladno s trenutnimi realnimi kadrovskimi in finančnimi zmožnosti ter potrebami. Nenazadnje pa se postavlja tudi vprašanje ali imamo dovolj veliko kritično maso kompetenčnega kadra za to področje?

Je vlaganje v izobraževanje kadrovskih potencialov organizacij lahko tista potrebna kvaliteta, ki tudi na področju varnostnega zavedanja loči uspešna podjetja od povprečnih?

Vsekakor. Strokovno izobraževanje agilnih kadrov je bistvenega pomena za dolgoročni uspeh. Zaposleni namreč dobro poznajo notranjo strukturo in organizacijo podjetja, procese ter smernice razvoja, zato lažje najdejo potencialne pomankljivosti in predlagajo izboljšave. Glede na specifičnost določenih znanj ter nesorazmeren finančni vložek za pridobitev le teh, pa ne vidim bistvenih ovir tudi v občasnem povezovanju z zunanjimi konzultanti.

Kako uspete zagotavljati učinkovito izvajanje svojih strokovnih aktivnosti na področju varnosti skozi prizmo različnih kulturnih okolij in delovanja v različnih kontinentih?

Moram priznati, da govorimo o dokaj kompleksni nalogi. Percepcija informacijske (ne)varnosti in sprejemljivih metod varovanja korporativnih informacij se namreč med nacijami precej razlikuje. Kar je sprejemljivo (legalno ali osebnostno) za zaposlene v »Asia-Pacific« območju, se lahko na področju Južne Amerike izkaže za zelo kontradiktorno.

Prvi pogoj za učinkovito delo je predvsem razumevanje situacije in posledično prilagajanje določenih ukrepov. Pri tem mi je v bistveno pomoč nenehna komunikacija z zaposlenimi ter vzpostavitev medsebojnega zaupanja. Ukrepi se ne izvajajo brez predhodnega obveščanja lokalnega vodstva in zaposlenih. V veliki meri pomaga tudi laična, včasih pa bolj strokovna obrazložitev, kaj je namen ukrepov. Nenazadnje pa tudi priznam, če poslušaš in opazuješ, se lahko veliko naučiš od drugih.

Kakšno je po vaši oceni stanje kompetenc slovenskih strokovnjakov v globalnem okolju skozi vaš primer. Prihajate namreč iz majhne države. Imate zaradi tega kakšne težave pri uveljavljanju strokovnih zahtev na področju za katerega ste zadolženi?

Pri svojem delu imam priložnost sodelovati z nekaterimi vrhunskimi slovenskimi strokovnjaki, cenjenimi in priznanimi v svetovnem merilu. Menim, da lahko potegnem vzorčno paralelo med njihovimi izkušnjami ter situacijo katero bolj ali manj občutim tudi sam. Majhnost ali neprepoznavnost države na začetku verjetno odigra posredno vlogo. Včasih prisotno skepso lahko premagam samo z rezultati svojega dela, kompetencami in osebno integriteto. Normalno je, da se moram v stikih z novimi poslovnimi partnerji precej bolj potruditi in dokazovati kot sicer. V veliki večini primerov te sčasoma začnejo enakovredno obravnavati, ni pa temu vedno tako.

Vaše podjetje je tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebna in lahko prinesejo v naš prostor dodatno kvaliteto?

Združenje kot tako svojim delovanjem v lokalnem in regionalnem prostoru povezuje različne strokovnjake s področja korporativne varnosti. Multidisciplinarnost organizacij in podjetij iz katerih le ti prihajajo nam daje izjemno možnost formalne in neformalne izmenjave znanj in izkušenj. V tem kontekstu združenje opravlja pomembno vlogo o zavedanju pomena korporativne varnosti v današnjem globaliziranem prostoru.

Na osnovi preteklih izkušenj sem prepričan, da združenje kot tako lahko ponudi zelo strokovno podporo in pomoč pri izvedbi večjih in specifičnih varnostnih projektov s katerimi se naše organizacije ter podjetja srečujejo. ■

Avtor: mag. Marko Potokar / vodja varovanja Lek d.d.*

PRIPRAVLJENOST VARNOSTNIH IN VODSTVENIH STRUKTUR NA AMOK SITUACIJO

V zadnjem obdobju smo tudi v Evropi soočeni s pojavom amok situacij, ki jih v najširšem obsegu lahko opredelimo kot dejanje, ko eden ali več storilcev, navidezno brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal.

Uvod

Po vrnitvi iz vojne je Howard Unruh iz New Yerseya, čeprav je bil vojni heroj, ostal brezposeln. Živel je z mamo, ki ga je finančno podpirala, in tako postal tarča zbadljivk v stilu ‚mamin sinko'. Ko je tistega večera prišel domov iz kina, je opazil, da so izginila vhodna vrata, ki jih je pred kratkim sam naredil. To je bila kaplja čez rob. Naslednje jutro je vstal ob 08:00, si oblekel najlepšo obleko in pozajtrkoval z materjo. Nato je odšel. Oborožen z Lugerjem in 33 nabojniki. V dvanajst minut trajajočem pohodu je ustrelil 26 oseb, od tega 13 smrtno. Diagnoza: paranoidna shizofrenija. V zgodovino se je njegovo dejanje iz leta 1949 zapisalo kot začetek novega trenda imenovanega morilski pohodi.

Tistega dne se je Douglas Williams, proizvodni delavec v tovarni Locheed Martin, s še 13 sodelavci udeležil obveznega izobraževanja o etiki in raznolikosti. Kmalu po začetku sestanka je odšel do svojega vozila in se vrnil oborožen z dvema puškama. V desetminutnem pohodu je ubil 6 sodelavcev, 8 pa ranil. Nato je naredil samomor. Govorilo se je, da je bil Doug depresiven in da naj bi imel težave z vodstvom in sodelavci, saj naj bi po njegovem z njim neprimerno ravnali. Tega leta 2009 je bil to še eden izmed primerov morilskega pohoda na delovnem mestu.

Li Xianliang je bil delavec v premogovniku. Ko je ubil svojega nadrejenega, s katerim je bil v sporu zaradi denarja, je sedel na bager in v divjanju ter zaletavanju v avtomobile, motorje in avtobuse ubil 17 ljudi, 20 pa ranil. Kljub temu, da ga je mimoidoči poskusil zaustaviti tako, da je skočil na delovni stroj in ga zabodel. Za tem dogodkom iz leta 2010, znanem kot »hebejski pohod s traktorjem«, so sledili nepovezani morilski pohodi po šolah drugod po Kitajskem, zato so oblasti z interneta umaknile informacije v zvezi z dogodkom, saj so se bali t.i. copy--cat sindroma.

To pa ni bil prvi množični umor z uporabo vozila kot orožja. Na Češkoslovaškem je leta 1973 Olga Hepnarova v Pragi ubila 8 ljudi in ranila 12, ko je s tovornjakom zapeljala v skupino 25 čakajočih na tramvaj. Psihologi so zatrdili, da se je dejanja, ki ga ni obžalovala, v celoti zavedala. Po njenih besedah jo je vodila sovražnost do družine in sveta. Bila je obsojena na smrt. Kazen, ki je bila izvršena leta 1975, pa je bila zadnja izvršena smrtna kazen za ženske na Češkoslovaškem.

School shooting je pojem, ki označuje strelske morilske pohode v šolah. Eden najbolj krvavih je znan kot katastrofa v bathskovski šoli (orig.: Bath School disaster). Andrew Philip Kehoe, znan po svoji varčnosti, je bil s strani sokrajanov izvoljen za skrbnika denarja na šoli v Bathu. Zagovarjal je znižanje prispevkov in bil zato večkrat v navzkrižju s preostalimi člani šolskega odbora. Kratek čas je bil tudi občinski uradnik, a ga sokrajani kasneje niso več izvolili. Masovni poboj s 44 smrtnimi žrtvami in 58 ranjenimi (večina je bila otrok med 7. in 12. letom) je 18. maja 1927 izvedel z detonacijo več sto kilogramov eksploziva, ki ga je več mesecev skrivoma nameščal v kleteh šole.

Amok

Amok v indonezijski kulturi

Ko je kapitan James Cook objavil potopise s svojih obsežnih potovanj po svetu v času poznega 18. stoletja, se je zahodni svet prvič srečal s čudnim pojavom, ki naj bi obstajal med različ-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

nimi narodi malezijskega arhipelaga. Med prebivalci Malezije (Malay), ki so sicer sloveli po svoji miroljubnosti (Malay izhaja iz *malu = nežen, nežnost*), so se občasno dogajali primeri izbruha neobvladljivega nasilja, brez vidnega razloga ali opozorilnih znakov. V svojih zapiskih je Cook pisal o posameznikih, ki se obnašajo brezumno in nasilno, pri čemer brez razloga ubijajo in pohabljajo ljudi in živali. O pojavu, poznanem pod različnimi imeni, kot so *mengamuk, pengamok* ali pa preprosto *amok*, so poročali tudi še potem, ko je Malezija že postala britansko ozemlje. Eden tipičnih je bil primer iz leta 1891, ko je malezijski kmet Imam Mamat med popravljanjem ograje na svojem posestvu nenadoma pričel pobijati družinske člane in sovaščane. Med morilskim pohodom je Imam z *golakom* (*golak* je mačeti podobno orodje za sekanje) in kopjem ubil 6 ljudi, ranil pa 4. Za posledicami ran, ki jih je med dejanjem prejel tudi sam, je naslednji dan umrl. Sovaščani so o njem vedeli povedati, da je bil do tega dejanja eden najprijaznejših prebivalcev. Na vprašanje, zakaj je postal nasilen, so priče izjavile, da Imam ni vedel, kaj počne ter, da ga je obsedel hudič.

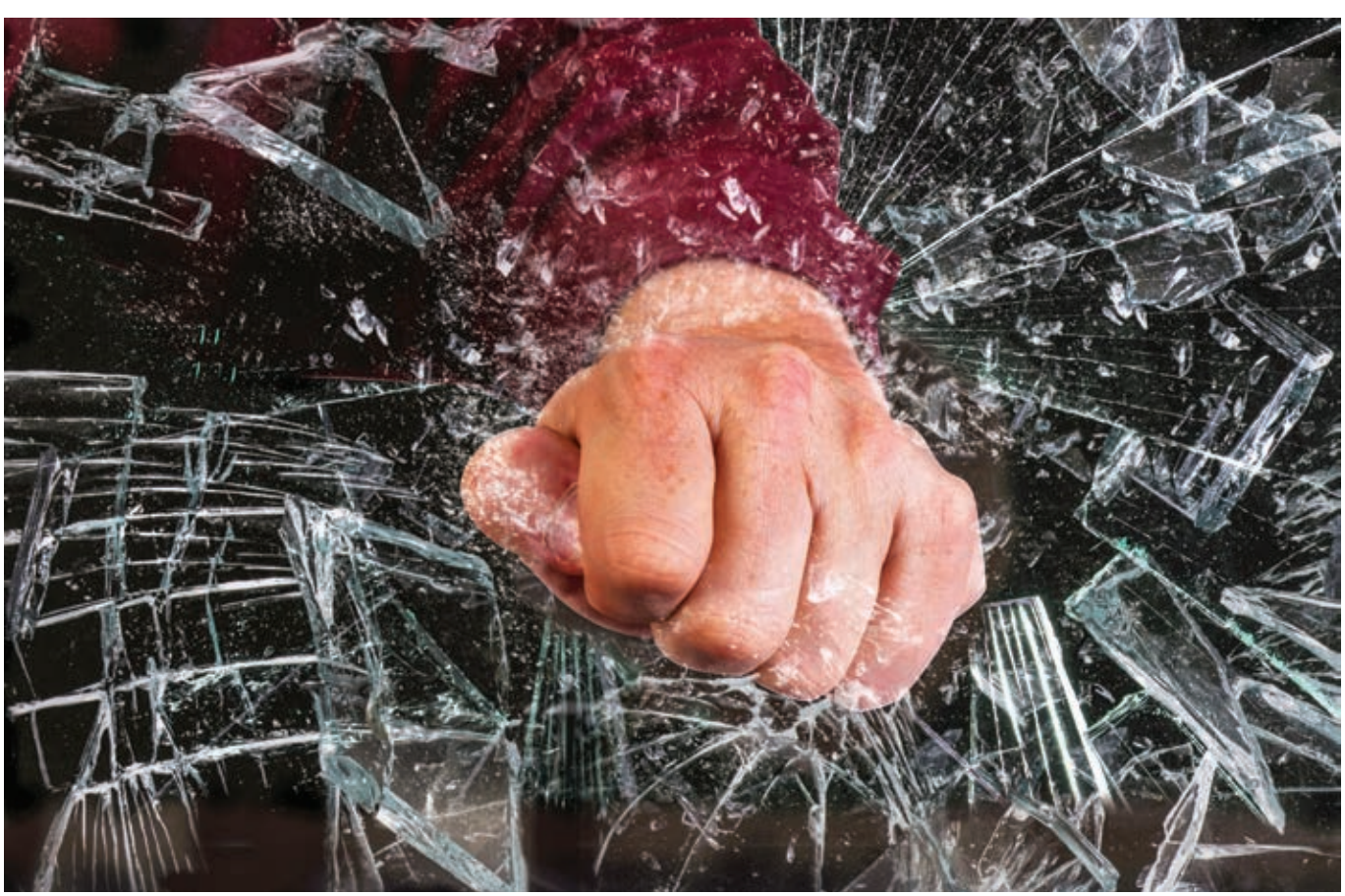
V malezijsko-indonezijski kulturi je *amok* (malez.: *norost z neobladljivo jezo*; indon.: *besno popasti*) zakoreninjen v globokem duhovnem prepričanju, da ga povzroča *hantu belian*, zli duh tigra, ki se naseli v telo storilca krvavega dejanja. Zaradi takega prepričanja se je v stari indonezijski kulturi amok napadalce toleriralo. V tipičnem primeru *amoka* posameznik (praviloma moški), ki prej ni pokazal nobenih znakov jeze ali nasilnosti, vzame orožje (tradicionalno meč ali bodalo, lahko pa tudi katerokoli drugo vrsto orožja) in v nenadnem izbruhu besa poskuša ubiti vsakega, ki mu prekriža pot. Dejanje se ponavadi zgodi na gosto poseljenih območjih oz. v gneči, napadalca pa na koncu ubijejo ali pa stori samomor. V primeru, da dejanje preživi, storilec izgubi zavest oziroma se ne spomni dejanja. Poznan je tudi t.i. *vojaški amok*, pri katerem so vojaki, soočeni z neizogibnim porazom, nenadoma planili v blaznost nasilja, ki je tako prestrašilo sovražnike, da so kljub slabšemu položaju zmagali oziroma so si vsaj zagotovili častno smrt v boju.

V sodobni Indoneziji se izraz *amok* (*amuk*) na splošno ne nanaša na nasilje posameznika, ampak se navezuje na mafijsko nasilje oz. nasilje združb. Za ‚klasični' *amok* Indonezijci danes pogosto uporabljajo izraz *gelap Mata* (dobesedno: *potemnele oči*), ki je v uporabi tudi na Sumatri in Javi.

Nekatere teorije trdijo, da je *amok* oblika namernega samomora predvsem v kulturah, kjer je samomorilno dejanje stigmatizirano. Ena izmed kontroverznih razlag povezuje *amok* z moško častjo (*amok* pri ženskah je skoraj neznan). Tako je lahko *amok* način pobega s sveta (storilci so običajno ubiti) in ponovna vzpostavitev lastnega ugleda, saj se takega človeka drugi bojijo in ga spoštujejo.

Zahodna opredelitev

Leta 1849 je bil *amok* na podlagi številnih poročil in študij primerov, ki so pokazali, da je bila večina posameznikov, ki so zagrešili *amok*, duševno bolnih, uvrščen med psihične motnje. Tako DSM-IV (Diagnostični in statistični priročnik duševnih motenj), ki ga je izdalo ameriško psihiatrično združenje, razvršča *amok* na dve uradni kategoriji: *amok* in *beramok*. *Amok* je redkejša oblika pojava in izvira iz besa, užaljenosti ali maščevanja proti posamezniku ali družbi in je tesneje povezan s psihozo, osebnostnimi motnjami, bipolarno motnjo in blodnjami. *Beramok* , ki je pogostejši, je povezan z depresijo in žalostjo, ki izhajata iz izgube, kot je smrt zakonca ali ljubljene osebe, ločitev, izguba delovnega mesta, denarja, moči itd. Povezan je z duševnimi težavami zaradi hude depresije ali druge motnje razpoloženja.



Kot je razvidno iz obravnavanih primerov, se AMOK situacije bistveno razlikujejo od klasičnih nasilnih situacij in dejanj oziroma kršenj javnega reda in miru. V primeru AMOK situacije gre namreč za dejanja, ki so neposredno usmerjena proti življenju posameznikov, storilec pa se ne oziroma se ni pripravljen pogajati, ampak izvaja pomor.

Simptomi, ki so navedeni v večini kliničnih opisov *amoka*, vključujejo:

- začetno obdobje umika iz družbe, ki traja več ur ali dni;
- nenadno, neizzvano nasilje, usmerjeno na vsakogar na dosegu roke, pa naj bodo to družinski člani, prijatelji ali pa popolni neznanci;
- napadi se nadaljujejo in lahko trajajo več minut, ur ali celo dni, dokler storilec ni ubit ali kako drugače onesposobljen;
- v primerih, ko storilec preživi, običajno pade v globok spanec ali zamaknjenost, ki lahko traja več dni;
- ko se storilec prebudi, je še naprej odmaknjen in nekomunikativen in se ne more spomniti, kaj se je zgodilo.

V klinični literaturi objavljene študije primerov *amoka*, ki zajemajo obdobje več kot sto let in posameznike od zgodnje odrasle dobe do srednjih let, nakazujejo, da pojav ni vezan na določeno življenjsko obdobje ali družbeni status. Medtem ko so bili v večini *amok* primerov storilci nepismeni kmetje ali ribiči, so zabeleženi tudi primeri, ko so bili napadalci uspešni trgovci, vojaki, obrtniki in celo člani kraljeve družine Malezije. V vseh primerih, kjer je uspelo storilcem preživeti in se izogniti zaporu, so se le-ti brez posledic vrnili v prejšnji življenjski tok z malo ali brez ponavljanja nasilja.

Vprašanje, kaj povzroča *amok* vedenje, je desetletja begalo psihiatre in medicinske raziskovalce. Sprva so *amok* povezovali s psihodinamskimi dejavniki, kot so izguba družbenega položaja, sovražnostjo in pripisovanjem krivde žrtvam, novejše raziskave pa pojav opisujejo kot vedenjski sindrom z različnimi možnimi vzroki, vključno z boleznimi, kot so malarija ali nevrosifilis. V nekaterih primerih je bila kot možen dejavnik predlagana tudi akutna zastrupitev. Ker je večina kliničnih amok primerov diagnosticiranih v zaporih in psihiatričnih bolnišnicah, ni presenetljivo, da so najbolj pogoste psihiatrične diagnoze za storilce shizofrenija in bipolarna motnja. Tako ostaja odprto vprašanje, ali se lahko te diagnoze uporabijo tudi za pojasnilo skrajnega nasilja v amok situacijah izven psihiatričnih in popravnih ustanov.

Poraja se tudi vprašanje, ali se je *amok* pojav sčasoma spremenil. Primeri v Maleziji in Indoneziji so bili pred angleško in nizozemsko zasedbo pogostejši, s pojavom psihiatričnega zdravljenja pa se je obravnava *amoka* in storilcev prenesla za zidove psihiatričnih bolnišnic in zaporov. Tudi uporaba izraza *amok* se je sčasoma spremenila. Čeprav še vedno prihaja do „klasičnih“ *amok* primerov, so Malezijci razširili uporabo izraza na kakršenkoli nenaden izbruh nasilja v Maleziji, povzročen s strani Malezijca ali tujca. Izraz *amok* se sicer drugje po svetu uporablja za označitev pojava množičnih umorov (mass murders, spree killing), vendar ne smemo prezreti, da med njimi obstajajo pomembne razlike. Čeprav se izbruhi nenadnega nasilja dogajajo po vsem svetu, pojav *amok* v svoji osnovi neposredno izhaja iz tradicij lokalnih kultur.

AMOK situacija

V policijskem žargonu *amok situacija* opisuje dejanje, ko eden ali več storilcev, navidez brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal. Uporablja se tudi *izraz aktivna strelska situacija*, ki označuje množični umor, pri katerem storilec uporabi strelno orožje. Za *množični umor* gre, ko je v krajšem času na omejenem geografskem območju ubito večje število ljudi. Navedene situacije se pojmujejo pod skupnim izrazom *aktivne življenju nevarne situacije*.

V angloameriški literaturi se za tovrstne primere uporabljajo tudi naslednji pojmi:

- MASS MURDERS: enkraten dogodek z več hkratnimi umori.
- SPREE KILLING: več umorov na dveh ali več lokacijah, med katerimi skoraj ni prekinitve.
- MASS SHOOTING: incident z več žrtvami, povzročen s strelnim orožjem.
- GOING POSTAL: izbruh ekstremnega in nekontroliranega besa, ponavadi v delovnem okolju.
- SCHOOL SHOOTING: oblika MS – napadi s strelnim orožjem na šolah in fakultetah.

Kot primer navedimo eno izmed najbolj znanih *amok situacij*, to je strelski pohod na ameriški srednji šoli Columbine leta 1999, na katerem sta srednješolca Eric David Harris in Dylan Bennet Klebold ubila 12 dijakov in 1 učitelja ter ranila še 24 dijakov. Prvi strel je bil sprožen ob 11:19, zadnji pa ob 12:08, ko sta storilca ubila še sebe. Ta primer množičnega poboja je pomenil spremembo v taktiki policijskega delovanja, saj se je pokazalo, da klasični način uporabe policijskih in specialnih enot za *amok situacije* ni primeren. Policija je namreč postopala po ustaljenih postopkih, ki se uporabljajo v primeru zajetja talcev, to je: zavarovanje okolice, blokada območja, čakanje na specialno enoto itd. Tako je v šolo vstopila šele uro po prenehanju napada in zaradi nepoznavanja objekta porabila vsaj še enkrat toliko za odkrivanje žrtev.

Je pa primerneje ukrepala finska policija v primeru iz leta 2008, ko je svoj smrtonosni pohod na zdravstveni šoli Kauhajoki pričel dvaindvajsetletni študent Matti Juhani Saari (10 mrtvih, 11 ranjenih). Streljanje se je pričelo približno ob 10:40, intervencijske službe pa so prvi klic dobile ob 10:46. Nekaj minut zatem sta na kraj dogodka prišla policista in takoj pričela ukrepati. Storilec jih je pričakal s streli. Ko so kasneje v objekt vstopili dodatni policisti in naleteli na storilca, se je ta zaprl v sobo in storil samomor.

Pripravljenost varnostnih in vodstvenih struktur na AMOK situacije

Naloge in pristojnosti za delovanje policistov so opredeljene v Zakonu o policiji, v katerem so med drugimi opredeljene tudi naloge varovanja življenja in osebne varnosti. Vsakdo, čigar

življenje oziroma osebna varnost ali premoženje so ogroženi ali kdor je žrtev kaznivega dejanja ali prekrška, sme zahtevati pomoč oziroma posredovanje policije. Na kraju posredovanja so policisti dolžni najprej vzpostaviti javni red in mir, če je ta ob njihovem prihodu še vedno kršen, in preprečiti morebitno nadaljnje ogrožanje varnosti oziroma izvajanje kakršnekoli oblike nasilja. Javni red in mir skušajo najprej zagotoviti s svojo navzočnostjo in z opozarjanjem oziroma ukazovanjem. Če to ne zadošča, morajo za vzpostavitev javnega reda in miru uporabiti prisilna sredstva. Policisti smejo uporabiti le tisto prisilno sredstvo, ki je sorazmerno načinu in moči upiranja ali napada. Pri uporabi prisilnih sredstev morajo spoštovati človekovo osebnost in njegovo dostojanstvo. Če smejo uporabiti več prisilnih sredstev hkrati, smejo hujše prisilno sredstvo uporabiti le, če je bila uporaba milejšega sredstva neuspešna ali če zaradi okoliščin in razlogov za varnost življenja, osebno varnost ali varnost premoženja ljudi ne bi bila mogoča. Za preprečevanje negativnih posledic takih protipravnih ravnanj je zelo pomembno, da so policisti ustrezno strokovno usposobljeni. Temu je namenjena redna vadba praktičnega postopka in samoobrambe, saj je treba prisilna sredstva uporabljati zakonito in strokovno, predpogoj za njihovo uporabo pa je, da se policisti znajo ubraniti napada nase in nato ustrezno ukrepati.

Kot je razvidno iz obravnavanih primerov, se AMOK situacije bistveno razlikujejo od klasičnih nasilnih situacij in dejanj oziroma kršenj javnega reda in miru. V primeru AMOK situacije gre namreč za dejanja, ki so neposredno usmerjena proti življenju posameznikov, storilec pa se ne oziroma se ni pripravljen pogajati, ampak izvaja pomor. Poraja se vprašanje, ali so policisti, ki prvi pridejo na kraj dogajanja, pripravljeni in ustrezno usposobljeni za ravnanje v tako kritični in življenjsko ogrožujoči situaciji. Imajo potrebno znanje in izkušnje, so dovolj izurjeni, vedo kako ukrepati in nenazadnje, je njihova oprema ustrezna?

Kaj pa varnostno osebje zasebnih varnostnih služb? Pravzaprav so varnostniki ‚prva bojna linija' za preprečevanje neprimernih in nezakonitih aktivnosti v organizacijah, kjer opravljajo svoje delo. Poleg vprašanja, ali so usposobljeni in primerno opremljeni tudi za ravnanje v izjemno nasilnih situacijah, obstaja tudi omejitev njihovih pooblastil. Podlaga za delovanje in ukrepanje varnostnika je namreč Zakon o zasebnem varovanju, ki ne vsebuje določil o ravnanju varnostnika v izrednih situacijah in ga k temu tudi ne zavezuje. Seveda mora varnostnik svojo službo opravljati vestno in pozorno spremljati okolico in dogajanje na varnostnem območju, preverjati prisotnost sumljivih predmetov in oseb ter ves svoj delovni čas preventivno delovati. Pa vendar je dovolj, da v primeru hujših oblik nasilja ‚samo' pokliče policijo ali pa intervencijsko službo, ki jo opravljajo njegovi kolegi? Tudi v tem primeru je na preizkušnji ustrezna usposobljenost, vključujoč znanje, izkušnje in izurjenost ter ustrezna opremljenost.

Kako pa je s pripravljenostjo organizacij v javnem in zasebnem sektorju? ZVZD-1 kot krovni predpis na področju varnosti in zdravja pri delu določa pravice in dolžnosti delodajalcev in delavcev v zvezi z varnim in zdravim delom ter ukrepi za zagotavljanje varnosti in zdravja pri delu. Določbe tega zakona se uporabljajo v vseh dejavnostih za vse osebe, ki so navzoče v delovnem procesu. Z vidika zagotavljanja osebne varnosti zaposlenih je pomembna določba, ki določa, da mora delodajalec načrtovati postopke za zmanjšanje nevarnosti za nasilje tretjih oseb. V prvem odstavku 23. člena ZVZD-1 je namreč opredeljeno, da mora delodajalec na delovnih mestih,

Pravzaprav so varnostniki "prva bojna linija" za preprečevanje neprimernih in nezakonitih aktivnosti v organizacijah, kjer opravljajo svoje delo.

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

Smo zaradi določil zakonov državljani res varni?

Zaključek

Katerakoli razlaga pojava izbruha nekontroliranega nasilja je že pravilna, je dejstvo, da imamo človeška bitja nasilje v sebi. Kdaj in na kakšen način nasilje izbruhne, je odvisno od vzgoje, situacije in samokontrole, zato bi se v družbi moralo poudariti širjenje znanja in zavedanja o varnostni kulturi ter vzgoji za nenasilje, ki je eden od mehanizmov, s katerim bi lahko povečali varnost. In ne glede na (ne)pripravljenost uradnih in neuradnih organov ter inštitucij, ne smemo pozabiti, da sta najboljša zaščita in obramba preprečevanje ter lastna ozaveščenost in skrb za varnost. Za lastno varnost smo namreč v prvi vrsti odgovorni sami.

Viri

- Boekler N., Seeger T., Sitzer P., Heitmeyer W. (2013). *School shootings: International Research, Case Studies, and Concepts for Preventions*. Springer, New York.
- Coester M, Marks E. (2009). *International Perspectives on Crime Prevention*. Forum Verlag Godesberg GmbH, Moenchengladbach.
- Čas T. (2012). *Policijsko pravo: izbrane vsebine za študente evropske pravne fakultete. Ljubljana.*
- Kobal, M. F. *Nasilje psihiatričnega bolnika kot urgentno stanje*. Pridobljeno na: http://www.pb-begunje.si/gradiva/Kobal1351439051132.pdf
- Revija VARNOST 3/2011. Ministrstvo za notranje zadeve Republike Slovenije Letnik LIX ISSN 2232-318X.
- Zakon o policiji, (Ur. l. RS, št. 107/2006, 66/2009 in 22/2010).
- Zakon o varnosti in zdravju pri delu (ZVZD-1). (2011). Uradni list RS, št. 43/2011.
- Zakon o zasebnem varovanju (ZZasV-1). (2011). Uradni list RS, št. 17/2011. ■

SISTEMSKE REŠITVE PRED POŽARI, – Z ENO BESEDO BONPET!

Samodejna gasilna ampula BONPET je najučinkovitejše gasilno sredstvo za gašenje začetnih požarov ter požarno zaščito manjših zaprtih prostorov brez stalne prisotnosti ljudi. Je tudi gasilni aparat estetskega izgleda. Nepogrešljiva je na vseh mestih, kjer predvidevate, da bo ob izbruhu požara temperatura najhitreje narasla (npr. na stropu ali zidu, najbližje mestu potencialnemu izbruhu požara).
Življenjska doba ampule je deset let brez vzdrževanja.

Pooblaščeni inštituti so potrdili učinkovitost in neškodljivost za človeka in okolje. Sodobna oblika in barva ampule zagotavljata tudi skladnost z ambientom.

NOVO
v ponudbi!
Bonpet gasilnik, specialist za olja in maščobe (F razred)

SAMODEJNE GASILNE AMPULE BONPET

priporočajo tudi **slovenske zavarovalnice** s popusti zaradi zmanjšanja rizika tveganja.

Bonpet® systems

Zanesljivi gasilni sistemi

Pot Vitka Pavliča 9,
1430 Hrastnik
e-pošta: info@bonpet.si
www.bonpet.si

Avtor: mag. Goran Čop / Pomočnik direktorja BONPET d.o.o.

GASILNI SISTEMI IN REŠITVE BONPET S PRIMERI DOBRIH PRAKS UPORABE V PODJETJIH

Požarna ogroženost je eden izmed dejavnikov tveganj, ki ima zelo velik vpliv na neprekinjenost delovanja naših organizacij. Pri analizi organizacij, ki so bile podvržene incidentom povezanih s požari smo ugotovili, da le te niso utrpele samo finančnih posledic temveč tudi dogoročne posledice v obliki izgube dobrega imena, ključnih partnerjev in zaupanja zaposlenih ter strank. To pa so dejavniki, ki lahko prinesejo tudi propad organizacije.

Samodejne gasilne ampule BONPET – sistemske rešitve za vaš posel

Samodejna gasilna ampula BONPET je najučinkovitejše gasilno sredstvo za gašenje začetnih požarov ter požarno zaščito manjših zaprtih prostorov brez stalne prisotnosti ljudi. Je tudi gasilni aparat estetskega izgleda. Nepogrešljiva je na vseh mestih, kjer predvidevate, da bo ob izbruhu požara temperatura najhitreje narasla (npr. na stropu ali zidu, najbližje mestu potencialnemu izbruhu požara).

Najboljši učinek samodejnega gašenja požara razreda A je dosežen takrat, ko vsaka ampula pokriva približno 8 m^3 površine s tem, da je nameščena v bližini (nad) potencialnim mestom izvora požara. Primerna je za gašenje vseh požarov razreda A, B in F. Življenjska doba izdelka je 10 let in ne potrebuje dodatnega vzdrževanja.

Skratka brez lažnih alarmov ter brez dodatne škode in vpliva na ljudi ali okolje.

Kako Bonpet ampula prepreči požar? Kako lahko samodejno deluje?

- Pri požaru v zaprtem prostoru se z naraščanjem temperature v prostoru segreje tudi gasilna tekočina, ki se v stekleni ampuli razteza.
- Pri temperaturi gasilne tekočine cca 85 °C +/- 5 °C njeno raztezanje povzroči, da se steklo zdrobi, tekočina pa pade v prostor, kjer se začne endotermni proces.
- Ta povzroči odvzem energije ognju oz. trenutno ohlajevanje v prostoru. Kot stranski proizvod endotermne reakcije se sprostita še majhni količini dušika in ogljikovega dioksida, ki preprečujeta dostop kisika do goreče površine.
- Na površini gasilne tekočine nerazpadle snovi tekočine tvorijo film, ki preprečuje ponovni vžig. V primeru, da ste ob izbruhu ognja prisotni v prostoru, lahko ampulo Bonpet **uporabite tudi ročno,** tako da jo vržete na gorečo površino. Ampula Bonpet se bo razbila in v trenutku zadušila ogenj.

Vgrajeni stabilni sistemi

Enostaven in zanesljiv način za zaščito premoženja pri večjih, odprtih in požarno močneje ogroženih površinah.

Vgrajeni gasilni sistem na tekoče gasilno sredstvo Bonpet projektiramo kot conski vgrajeni gasilni sistem za gašenje. Naprava je namenjena gašenju požarov razreda A, B in F. Vgrajeni gasilni sistem Bonpet poleg samodejnega delovanja omogoča tudi ročno aktiviranje gašenja. Sistem je primeren za požarno varovanje lakirnic, transformatorjev (zunanje in notranje), hidravličnih agregatov, strojev za preoblikovanje plastike (stroji za vakumiranje), skladišč vnetljivih tekočin, v lesnopredelovalni industriji (filtri itd.), skladišč, predorov (v preizkušanju), idr.

Način delovanja

Princip delovanja je gašenje z razprševanjem gasila. Ob tem upoštevamo postavitev cevovodov in razmeščanje šob kot pri sistemu za razprševanje vode, razlika je samo v količini gasil. Razprševanje vode ima predvsem nalogo, da omogoči posredovanje gasilcev, zato ima po normativu zahtevan tudi daljši čas razprševanja. Razprševanje gasilne tekočine Bonpet pa ima za glavno nalogo pogasitev požara, zaradi njene učinkovitosti pa zadošča bistveno krajši čas razprševanja tekočine (do 20 sekund) in ni potrebno zalivanje, kot pri vodi. Zaradi izrednih sposobnosti gašenja se zato v rezervoarju (po izračunu glede na površino gašenja) nahaja presenetljivo majhna količina gasilne tekočine Bonpet.

Dušik kot potisni plin gasilne tekočine preko pripravne grupe na jeklenki, tlačnega stikala in elektromagnetnega ventila ustvari tlak v rezervoarju z gasilno tekočino Bonpet. Izpust gasilne tekočine Bonpet v sistem cevovoda pa poteka preko avtomatiziranega krogelnega ventila. Ventil s pnevmatskim pogonom se odpira s signalom iz naprave za javljanje požara in s tem omogoči pretok gasilni tekočini do šob v coni gašenja, kjer je prišlo do odkritja požara.

Oprema

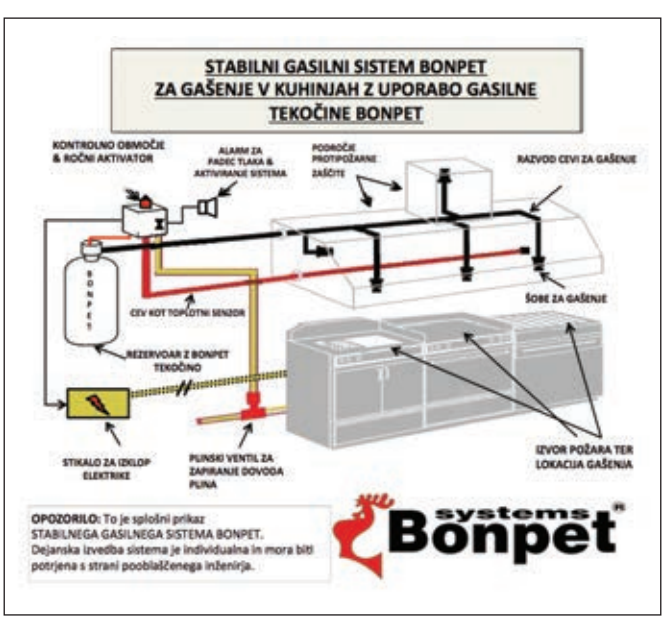
Vgrajena gasilna naprava je sestavljena iz elementov strojne in elektro opreme in se uvršča med nizkotlačne sisteme z delovnim tlakom gašenja do 5 bar, kar pomeni, da se za postavitev sistema cevovodov uporabljajo cevi in cevni priključki z nizkim preizkusnim tlakom 7,5 bar (vodovodna instalacija). Volumen rezervoarjev se določi glede na oceno požarne ogroženosti (do 600 litrov).

Prednosti

- Tekočina Bonpet ne povzroča dodatne škode, ostanek tekočine lahko pobrišete.
- Gasilna tekočina Bonpet je ljudem in okolju prijazna.
- Ob rednem vzdrževanju - neomejena življenjska doba.
- Stroške vzdrževanja določimo s pogodbo.
- Brezplačno svetovanje in ogled

Mini stabilni sistemi

Samodejno, učinkovito in enostavno gašenje požarov v kuhinjah in v manjših požarno ogroženih območjih. „Mini“ stabilni sistem je primeren za gašenje požarov tipa A, B in F, v prostorih, z velikim učinkom gašenja pri majhni količini tekočine BONPET.



Način delovanja

Princip delovanja temelji na posebni cevi, ki deluje kot toplotni senzor. Cev je upogljiva in elastična in se lahko instalira po vsej opremi, ki jo požarno varujemo. Na eni strani je cev priključena na posebni ventil z zaklopko, na drugi strani pa na ročni aktivator. Cev je pod pritiskom 18 bar, premer cevi je 6 mm, cev se deformira in aktivira pri temperaturi 160–180° C. V primeru požara zaradi povečane temperature in delovanja plamena na cev le-ta poči in tako pride do padca tlaka v cevi in delovanje na zaklopko, s čimer se aktivira avtomatsko gašenje.

Oprema

Na voljo sta dva rezervoarja za gašenje kuhinj in sicer 6-lit. in 11-lit., z različnimi tipi šob za gašenje fritez, grill plošč ter različnih kuhalnih plošč. Rezervoar mora biti pod tlakom 16 bar (pri temperaturi 20 °C). Delovna temperatura sistema je od 0 °C do 60 °C, za potisni plin pa se uporablja dušik (N2).

Prednosti

- Ni lažnih alarmov, sistem se aktivira samo ob porastu temperature.
- Pri gašenju ne povzroča dodatne škode (okolju prijazni medij), ostanek tekočine lahko pobrišete.
- Neomejena življenjska doba oz. 1-letna garancija (ob rednem vzdrževanju sistema).
- Gašenje brez tesnjenja prostorov (v primerjavi z gasilnim sredstvom CO2).
- Začetek gašenja ni pogojen z evakuacijo delavcev.
- Na zaščitni površini se tvori zaščitni sloj, ki preprečuje ponovni vžig.
- Neomejene možnosti za zaznavo in posledično gašenje požara v začetni fazi razvoja.
- Enostavna instalacija upogljive cevi za detekcijo požara; požar lahko zaznamo na vseh mestih z visoko stopnjo ogroženosti, kot tudi na nedostopnih lokacijah.
- Na zaznavo požara ne more vplivati noben zunanji dejavnik, kot so tresljaji, udarci, visoke koncentracije olja, masti in prahu.
- Na zaznavo požara, aktivacijo sistema in delovanje gašenja ne moreta vplivati ne vir ne napetost.
- Gašenje se lahko aktivira ročno s pomočjo aktivacijske tipke na koncu upogljive cevi za zaznavo požara. ■

Vgradnja ampul v elektro, razdelilne in komunikacijske omarice.

Področja vgradnje	**Proizvodni in pomožni prostori** **Industrijske naprave in stroji** **Transformatorske postaje, stikališča in kotlovnice** **Elektro in komunikacijske omarice**
Uporabljene rešitve	Samodejna gasilna Ampula BONPET Vgrajeni stabilni sistemi Mini stabilni sistemi

Vgradnja in postavite stabilnega sistema.

Avtorica: Dora Mezek Kukec / Slovenske železnice d.o.o.*

VPLIV MNOŽIČNIH MIGRACIJ NA NEPREKINJENOST DELOVANJA ŽELEZNIŠKE INFRASTRUKTURE

Migracijski val, ki je močno vplival tudi na Republiko Slovenijo je na področju zaščite ključnih infrastrukturnih sektorjev prinesel določena tveganja, na katera prej nismo polagali dovolj velike pozornosti. S tega stališča je vsaka izkušnja, ki nastane v procesu zagotavljanja neprekinjenosti delovanja kritične infrastrukture še dodatno pomembna. V nadaljevanju poglejmo nekaj izkušenj z migracijskim valom na zahodni Balkanski poti v letih 2015/2016.

Slovenske železnice (v nadaljevanju: SŽ)[1], kot masovni prevoznik, so podvržene izredno reguliranemu delovanju, ki zagotavlja varno izvajanje potniškega in tovornega prometa na javni železniški infrastrukturi. Eden izmed ciljev skupine je neprekinjeno delovanje in zagotavljanje rednega izvajanja železniškega prometa.

Veliko je dejavnikov, ki lahko vplivajo na redno delovanje SŽ. V prvi vrsti so to lahko naravno pogojeni vzroki (kot npr. žled v letu 2014), tehnične okvare ali človeški faktor, zaradi katerih lahko pride do posledic velikih razsežnosti.

Delujemo v varnostno negotovem sodobnem svetu, kjer so železniški sistemi lahko priljubljena tarča delovanja ekstremističnih in radikalnih skupin, ki smo jim bili priča v preteklosti (če omenim samo Bruselj 2015). Zaradi povezanosti v enoten sistem evropskega in panevropskega železniškega omrežja, zaznajo nacionalne železnice vsako prekinitev oz. motnjo izven nacionalnih meja. Kolikor prostorsko bližje je težava, toliko bolj vpliva na delovanje nacionalnih železnic.

Delujemo v varnostno negotovem sodobnem svetu, kjer so železniški sistemi lahko priljubljena tarča delovanja ekstremističnih in radikalnih skupin, ki smo jim bili priča v preteklosti

Ena izmed potencialnih groženj, ki jo lahko zaznamo ne le v železniškem okolju pač pa tudi na splošno v družbah razvitega sveta, so množične migracije pogojene iz najrazličnejših razlogov. V prispevku se ne bi rada spuščala v raziskovanje le teh, saj je bilo o njih že veliko povedanega in napisanega.

V nadaljevanju želim osvetliti nekatere posebnosti in orisati tok dogodkov, ki so bili, s pojavom množičnih migracij na zahodno balkanski poti, zabeleženi na SŽ.

Že v poletnih mesecih 2015 (julij in avgust) smo na SŽ intenzivno spremljali dogajanje pojava množičnih migracij, ki so se usmerile proti zahodni Evropi po tako imenovani Balkanski poti, ki nam ni bila več prostorsko odmaknjena, kot znana pomorska pot prek Apeninskega polotoka, saj so se dotikale tako rekoč našega praga[1]. Zaskrbljujoče je bilo izvajanje ukrepov madžarske vlade in njen izredno nehuman odziv do migrantov in samo vprašanje časa je bilo, kdaj bo Madžarska preprečila vstop na svoje ozemlje.

V začetku septembra smo na SŽ dali pobudo za srečanje s predstavniki Ministrstva za notranje zadeve in Policije, kjer smo drug drugega seznanili z osnovnimi principi sprejemanja migrantov in možnostjo prevoza le teh. Sledil je vsem znan tok dogodkov s končno eskalacijo, ko je Republika Hrvaška (v nadaljevanju RH) namenoma usmerjala tok migrantov na zeleno mejo.

Za boljše spremljanje situacije in množičnih prevozov migrantov, je bil na SŽ določen štab za spremljanje migrantske situacije[1], ki se je sestajal po potrebi, še

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

posebno pa takrat, ko se je bilo potrebno odločiti o zadevah, ki so bile vezane predvsem na spremembe od ustaljenega delovanja tehnološkega procesa, kar je bilo zelo pogosto. Štab je bil v nenehnih stikih s predstavniki MNZ in Policije.

Za obvladovanje nastale situacije je sledil odločen ukrep Slovenske vlade: sklep o zaprtju mejnih prehodov z RH[1].

V začetnem obdobju zaprtja mejnih prehodov za železniški promet, smo na SŽ za potnike v mednarodnem potniškem prometu organizirali nadomestni avtobusni prevoz – predvsem v smeri iz Slovenije proti RH. V celotnem obdobju od 17.9. do 30.9.2015 je veljala popolna zapora potniškega prometa z odpovedjo mednarodnih vlakov, ki vozijo direktno iz RH do zahodno-evropskih držav preko železniškega mejnega prehoda Dobova. Glede na možnost, da bi RH namesto mejnega prehoda v Dobovi za prevoz migrantov uporabila ob sotelsko progo ter progo preko Čakovca, so bili brez možnosti nadomestnega prevoza odpovedani tudi vsi vlaki iz smeri RH na mejnih železniških prehodih Rogatec in Središče ob Dravi[5].

Po prvem valu množičnih migracij, ki smo jih zaznali predvsem v prevozu migrantov z avtobusi[6], smo pristopili k intenzivnemu pripravljanju Pogodbe z MNZ o prevozu migrantov z vlaki in avtobusi[7]. Izkušnje iz leta 2014 – izvajanje potniškega prometa v času žleda ter nadomestnih prevozov potnikov z avtobusi[8] več kot pol leta, so v danih razmerah predstavljali osnovo za pripravo na prehod za delo v spremenjenih okoliščinah. Pogodba je zajemala med drugim določen način naročanja ter zagotovitev voznih sredstev[9] in vse do tedaj pričakovane posebnosti pri prevozu migrantov.

S pojavom drugega vala množičnih migracij ter vedno večjim številom migrantov proti koncu oktobra 2015, so se vedno bolj krepile ideje po kontroliranem vstopu preko mejnih točk, ki jih je možno tudi bolje varnostno nadzorovati, zagotoviti vse shengenske mejne formalnosti ter migrante oskrbeti z osnovnimi življenjskimi potrebščinami. Kot edina vstopna točka iz RH za sprejem množičnih migracij v železniškem prometu, je bil določen mednarodni železniški mejni prehod Dobova. V sodelovanju z MNZ je bilo dogovorjeno, da se na operativni ravni med SŽ in hrvaškimi železnicami vzpostavi stalno obveščanje o vlakovnih kompozicijah, ki smo jih na SŽ pripravljeni sprejeti in v najkrajšem možnem času prepeljati v Republiko Avstrijo[10].

Dogodki in rešitve iz množičnih migracij, kot tudi izkušnje iz drugih posebnih situacij, na podlagi katerih smo v tokratnih množičnih migracijah ukrepali, so dobra osnova za pripravo načrta neprekinjenega delovanja železniške infrastrukture.

MNZ se je prek štaba SŽ ves čas seznanjala s situacijo v železniškem prometu. Glede na stopnjevanje števila migrantov v oktobru 2015 (preko 12.000 migrantov v enem dnevu) z vlaki na mejni prehod Dobova, je Vlada RS sprejela sklep o posebnih razmerah na področju opravljanja železniškega prometa[11]. S sklepom so bili določeni prednostni prevozi v potniškem in tovornem prometu. Hkrati je sklep predstavljal osnovo za formiranje izrednih potniških vlakov za prevoz množičnih migracij v notranjem železniškem potniškem prometu. SŽ so, skladno s prednostnimi prevozi v potniškem prometu, namenile maksimalno število potniških vagonov in elektro motornikov za izredne prevoze. Prevozi pa so se tudi v tem obdobju še vedno izvajali z avtobusi.

Najmnožičnejše migracije po številu migrantov v enem dnevu smo na SŽ zabeležili v drugi polovici oktobra 2015, nato se je situacija stabilizirala vse do konca množičnih migracij v začetku meseca marca 2016.

Iz predstavljenih dogodkov bi želela za zaključek izpostaviti vpliv množičnih migracij na neprekinjeno delovanje železniške infrastrukture s poudarkom na nemotenem izvajanju železniškega prometa:

- Vpetost v mednarodne povezave in dostopnost železniških prevozov predstavljata osnovo množičnim migracijam. Hitra odzivnost ter usklajenost delovanja vseh vpletenih (nacionalnih železnic na poti, državnih organov, lokalnih skupnosti, prevoznikov in drugih) so bistvenega pomena za nadzorovan potek množičnih migracij ter čim manjši vpliv na mobilnost prebivalstva.
- Železniški promet je bil v določenem obdobju prekinjen, ko je bilo potrebno prekiniti množične migracije zaradi obvladovanja situacije. Z uvedbo izrednih vlakov ter dodatnih avtobusnih prevozov, kot tudi na podlagi kontroliranega vstopa množičnih migracij v Slovenijo preko ene točke in dogovorjenim izstopanjem proti zahodni Evropi smo ponovno vzpostavili neprekinjeno delovanje železniške infrastrukture.
- Dogodki in rešitve iz množičnih migracij, kot tudi izkušnje iz drugih posebnih situacij, na podlagi katerih smo v tokratnih množičnih migracijah ukrepali, so dobra osnova za pripravo načrta neprekinjenega delovanja železniške infrastrukture.

Opombe

1 V tem prispevku izraz Slovenske železnice pomeni skupino Slovenske železnice, d.o.o., med katerimi so se v migrantskih prevozih posebno angažirale: SŽ – Infrastruktura, d.o.o., SŽ – Potniški promet, d.o.o., SŽ – Železniško invalidsko podjetje, d.o.o. in SŽ – Vleka in tehnika, d.o.o..

2 V mislih imam migracije, ki so se dogajale preko Madžarske, s katero imamo SŽ dnevne vlakovne potniške povezave in je obstajala možnost, čeprav malo verjetna, da migranti izberejo prevoz z vlaki preko Slovenije za dosego končnega cilja v zahodni Evropi.

3 Člani so bili kompetentni predstavniki družb skupine SŽ. Štab je deloval od 16.9.2015 do 9.3.2016, ko so na SŽ, skladno s situacijo, prenehale aktivnosti vezane na množične migracije.

4 S Hrvaško so bili zaprti vsi železniški mejni prehodi, celo z Istro, kjer nismo beležili migracij.

5 Vir: SŽ – Potniški promet, d.o.o.

6 V celotnem obdobju smo Slovenske železnice prepeljale več kot polovico migrantov z avtobusi. Vir: SŽ – Potniški promet, d.o.o.

7 Pogodba št. C1714-15-460470 sklenjena 26.11.2015 med SŽ in Policijo.

8 V prvi vrsti smo koristili avtobuse iz lastnega voznega parka, ki jih uporabljamo za nadomestne prevoze ob obnovah prog.

9 Tako železniških kot avtobusnih.

10 V kolikor je Avstrija zahtevala, da se pritok števila migrantov zmanjša, smo lahko zaustavili sprejem vlakov - migrantov na naši mejni postaji Dobova, kjer poteka izmenjava prometa med SŽ in Hrvaškimi železnicami.

11 Sklep VRS št. 37000-4/2015/3 z dne 22.10.2015. ■

ID Shop
SISTEMI ZAKLEPANJA

Kako do učinkovitega nadzora in organizacije nad vašimi vrati...

Ali veste, da lahko ključ povozi še tako napredno varnostno kontrolo pristopa, če nimate nadzora nad izdelavo ključev?

– **To pomeni, da je lahko nekdo v vašem podjetju do sedaj naredil že 10 ključev, ker nimajo zaščitenega profila, vi pa o tem nič ne veste.**

Ali veste, da je teža enega ključa 14 gramov?

– **Pri 50 vratih to pomeni 1kg z obeski in kovinskimi obročki.**

Ali veste, da obstaja razlika med patentno in blagovno zaščito ključa?

– **Pri patentni zaščiti ključa imate mehansko zaščito, ki je ni možno narediti z navadnimi stroji v ključavničarski delavnici *(zelo visoka zaščita).***

– **Pri ključu zaščitenim z blagovno znamko, lahko ključ naredite z enostavnimi stroji v ključavničarskih delavnicah, z drugo obliko ključa in proizvajalca *(zelo majhna zaščita).***

SHOP ID

ID Shop d.o.o.
Litostrojska 44d, 1000 Ljubljana
T. 01 500 40 50 **F.** 01 500 40 51 **E.** info@idshop.si

www.idshop.si

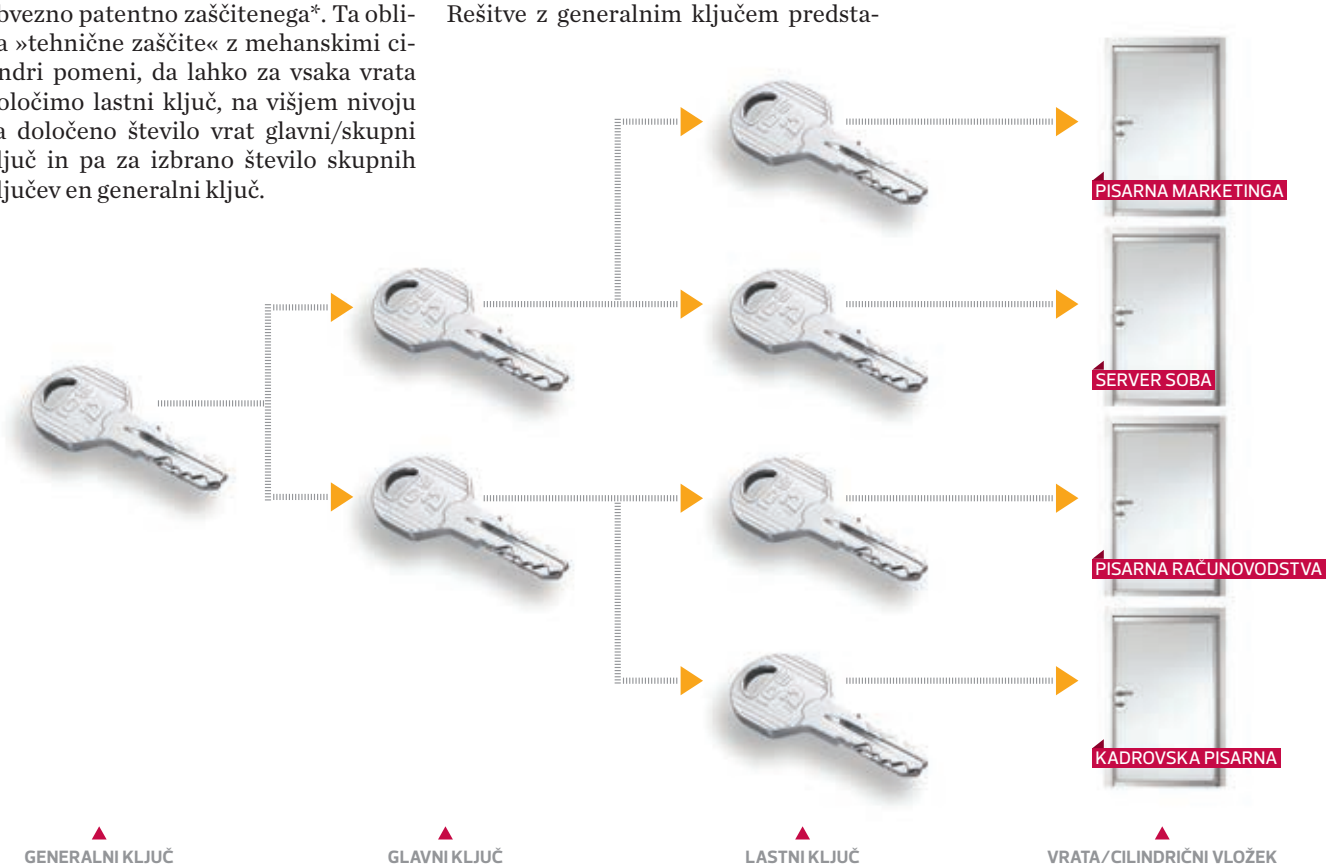
Avtorica: Mateja Mirtič / skrbnica ključnih kupcev, ID Shop d.o.o.

KAKO DO UČINKOVITEGA NADZORA NAD VAŠIMI VRATI?

Nove delovne prakse in zaposlovanja pomenijo z vidika varnosti nenehne spremembe in nadgradnje sistema fizičnega pristopa zaposlenih in obiskovalcev v organizacijah. V ta namen morajo biti varnostni sistemi v objektih in delovnih prostorih prilagodljivi in prožni brez kakršnihkoli večjih posegov. Popoln in učinkovit nadzor na področju varnosti in kontrole pristopa je možno doseči z mehanskimi in mehatroničnimi sistemi zaklepanja.

Osnova iz katere bi morale izhajati organizacije, ki želijo doseči višji nivo varnosti v smislu kontrole dostopa v njihove prostore, je vzpostavitev mehanskega sistema zaklepanja, obvezno patentno zaščitenega*. Ta oblika »tehnične zaščite« z mehanskimi cilindri pomeni, da lahko za vsaka vrata določimo lastni ključ, na višjem nivoju za določeno število vrat glavni/skupni ključ in pa za izbrano število skupnih ključev en generalni ključ.

Varnostne in organizacijske zahteve so različne glede na potrebe različnih industrij in tipov gradnje. Višji, kot je potreben nivo varnosti, večji morajo biti standardi kompleksnosti za generalni ključ. Rešitve z generalnim ključem predstavljajo dolgoročno, varno in premišljeno investicijo, hkrati pa so dizajnirani za dolgotrajno uporabo in z možnostjo razširitve oz. nadgradnje sistema.



Zakaj je tako pomembno zagotoviti zaščiten sistem zaklepanja prostorov?

Ker je še tako napredna kontrola pristopa brez pomena, če nimate pregleda nad tem koliko posameznih ključev imate v obtoku. Brez zaščitenega profila ključev je namreč nekdo v vašem podjetju do sedaj lahko naredil že 10 ključev, vi pa o tem ne veste ničesar. Manjše število ključev v obtoku omogoča večjo preglednost nad celotnim sistemom, manjša je verjetnost, da se bodo ključi izgubljali (posledično je varnost večja), poleg tega pa se na ta način izognemo 'šopom ključev' s čimer posledično tudi privarčujemo.

Obstoječi mehanski sistem zaklepanja lahko kadarkoli postopoma dopolnite oz. nadgradite z mehatronskim sistemom in na ta način še povečate varnost.

Za kombinacijo mehanske in mehatronske kontrole pristopa so se odločili v Medicinskem centru Iatros, ki ima sedež na Parmovi ulici v Ljubljani. Center je bil ustanovljen leta 1994 in že od vsega začetka deluje na principu dnevne bolnišnice, poleg tega pa opravljajo tudi male kirurške posege. Vizija MC IATROS je nuditi celostno podporo bolnikom na enem mestu, ob sodelovanju vrhunsko usposobljenih zdravnikov in drugega osebja v medicinsko vrhunsko opremljenih prostorih.

V arhitekturnem biroju Košorok Gartner arhitekti d.o.o., kjer so zasnovali preureditev novih prostorov, so med drugim želeli vzpostaviti kartično kontrolo pristopa, saj mora biti v zdravstvenih ustanovah z veliko obiskovalci in zaposlenimi na različnih nivojih, nadzor nad vstopanjem v prostore na zelo visoki ravni. Glede na to, da imamo v podjetju ID Shop d.o.o. specifično znanje in izkušnje ter smo ustrezen sogovornik že v fazah nastajanja projektov, so se projektanti s svojimi zahtevami in željami obrnili na nas.

Cilj je bil postaviti čim bolj enostaven, prefinjen in celovit sistem kontrole pristopa, ki bi temeljil na mehanskih in mehatronskih rešitvah in, ki bi ga po končani preureditvi lahko vključili v BIM (Building Information Modeling)** model, ki je opremljen z vsemi potrebnimi informacijami za upravljanje z objektom, kamor sodi tudi kontrola pristopa.

V MC IATROS je zaposlenih 30 ljudi, kar tehnično gledano pomeni veliko lastnih ključev ter veliko prostorov, ki jih je potrebno imeti pod nadzorom. Ponudili smo jim rešitve avstrijskega podjetja EVVA, ki je vodilno na področju mehanskih sistemov zaklepanja, vse bolj pa se s svojimi inovacijami prebija v ospredje tudi na segmentu mehatronike.

Ponudili smo rešitev, ki obsega več varnostnih nivojev: 1. cilindrične ključavnice, 2. mehanski sistem zaklepanja, 3. stand-alone mehatronski sistem kartičnega pristopa s čitalci. Ključna želja naročnika je bila, da se zagotovi tudi možnost nadgradnje tako mehanskega kot mehatronskega sistema, kar se z EVVA komponentami lahko doseže in zato predstavlja idealno rešitev za vsaka vrata.

Naročnik se je v prvi fazi odločil za mehanski sistem zaklepanja s cilindri EPS, ki izpolnjuje vse potrebne zahteve modernih varnostnih tehnologij (trikratna dodatna zaščita proti nedovoljenemu kopiranju ključev, ustreza požarnim varnostnim zahtevam, je odporen na korozijo, ima protivlomno zaščito, zaščito proti vrtanju ipd).

Na varnostno občutljivih prehodih smo mehanski sistem nadgradili s stand-alone mehatronskimi kljukami, ščiti, cilindri ter čitalci, ki delujejo z baterijskim napajanjem. V prostorih se nahajajo avtomatizirana steklena drsna vrata in klasična enokrilna lesena, steklena, aluminijasta vrata, ter vrata, ki ločujejo požarni sektor. EVVA mehatronske komponente so se izkazale kot prava izbira, saj je njihova montaža hitra, enostavna in ne zahteva predelave vrat ali ožičevanja in so primerne tako za zunanjo kot notranjo namestitev.

S to rešitvijo:

- so jasno določene pravice uporabnikov,
- izguba medijev ne predstavlja več stroška: medij lahko enostavno prekličete,
- v enem koraku imamo pregled nad mehatroniko in mehaniko,
- spomin dogodkov: pregled nad dogajanjem je na voljo v vsakem trenutku,
- cenejše upravljanje in vzdrževanje sistema: sistem mehatronike in mehanike vzdržuje ena oseba.

Evva stenski čitalec je vsestransko uporaben v zaprtih predelih poslopij kot tudi zunanjih. V kombinaciji s krmiljeno stensko čitalno enoto je primeren za nadzor vseh vrst elektronskega zaklepanja in še veliko več. Tako zaklepanje vključujejo drsna vrata, ograde in nihajna vrata z elektronskim značajem ter dvigala.

Vsa dovoljenja za dostop so odobrena preko Evva Xesar programske opreme. Podatki se preko namiznega čitalca prenesejo iz programske opreme na identifikacijske medije (kartice, čipe). Sinhronizacija programske opreme z bazami podatkov in posameznimi vrati, beleženje podatkov, dodeljevanje novih medijev, pravic in črne liste uporabnikov poteka preko tabličnega računalnika.

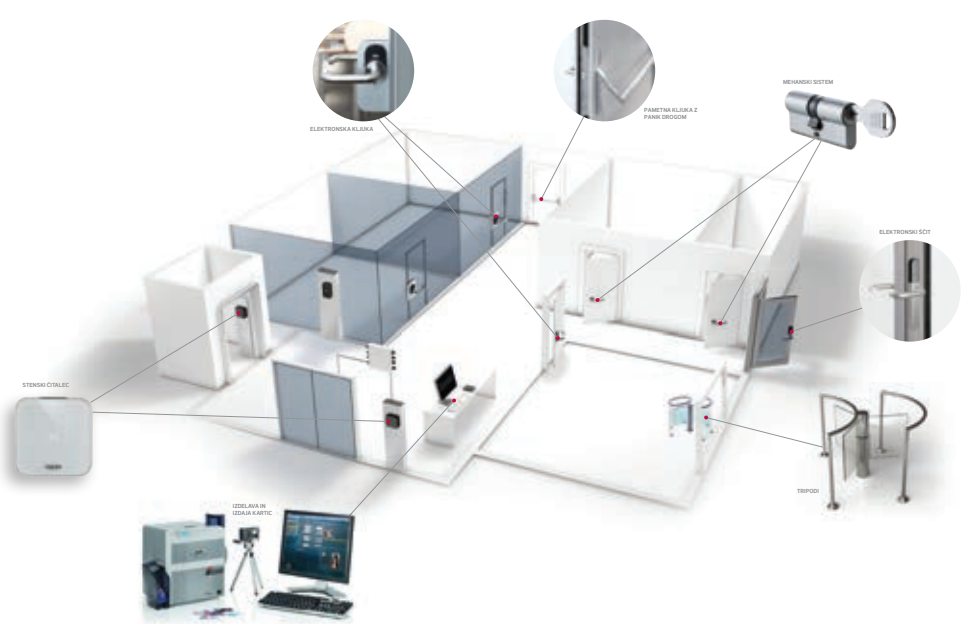
Mehatronski sistem zaposlenim v MC IATROS trenutno zagotavlja odpiranje vrat oz. vstopanje v prostore na podlagi pravic, ki so jim bile dodeljene. Ker pa je sistem zasnovan tako, da raste skupaj s potrebami strank, je že pripravljen, da preide v on-line svet. Zgolj z zamenjavo kontrolerja na vratih, lahko funkcije nadgradimo v EVVA Virtual Network model. Ta temelji na prenosu informacij direktno preko identifikacijskega medija od vrat do programske opreme, brez tabličnega računalnika . Ta model dodatno omogoča:

1 Dodajanje medijev na črno listo;
Zaposleni svojo ID kartico položijo na kontroler (update station) in črna lista se prenese na njihov ID medij. S tem medijem potem prenesejo to informacijo na vsaka vrata, ki jih odprejo. Nadgradnje se lahko še vedno izvajajo preko tabličnega računalnika.

2 Pregled nad varnostnim statusom;
Kadar nekdo poizkuša vstopiti v objekt z ukradeno kartico, ki jo je administrator že odstranil iz sistema, je ta medij že vključen na črno listo preko virtual network. Z ukradeno kartico vstop v prostore ni več možen. Programska oprema pa nudi pregled nad nadzorovanimi in nenadzorovanimi vrati in mediji.

3 Informacije o stanju baterij na komponentah;
Stanje polnosti baterij mehatronskih komponent je shranjeno na ID kartico in podatki se prenesejo na programsko opremo preko kontrolerja/updater-ja. Informacija o stanju baterij je potem na voljo v programski opremi.

4 Nova možnost filtriranja dogodkov;
Pregled vstopov se lahko od sedaj vodi ne le za posamezna vrata, temveč tudi po posamezni osebi, ki je vrata odprla.



Stranke pogosto kot težave pri obstoječih sistemih kontrole navajajo izgubo mehanskih ključev, kar iz vidika varnosti pomeni menjavo ključavnic in izgubo kontrole nad vstopanjem v prostor, to pa ponavadi vzame veliko časa in denarja.

Stranke pogosto kot težave pri obstoječih sistemih kontrole navajajo izgubo mehanskih ključev, kar iz vidika varnosti pomeni menjavo ključavnic in izgubo kontrole nad vstopanjem v prostor, to pa ponavadi vzame veliko časa in denarja. Težavo pri elektronskih kontrolah pristopa ponavadi predstavljajo predelave vrat, dodatna napajanja v primeru izpada električne energije in ožičevanje. Te predelave predstavljajo razmeroma visok strošek, še posebno za prostore, kjer takšna on-line kontrola pristopa ni potrebna, prav tako visok strošek predstavlja vzdrževanje teh sistemov.

Evva sistem kontrole pristopa je v takšnih primerih ustrezna rešitev. Nudi vse, kar pričakujete od mehatronskih sistemov, poleg tega pa ni potrebna nikakršna predelava vrat in ožičevanje, kar pomeni bistveno nižjo investicijo.

*Patentna zaščita ključa predstavlja mehansko zaščito, katero je možno narediti z običajnimi stroji v ključavničarskih delavnicah, medtem ko je možno pri ključu, ki je zgolj blagovno zaščiten, narediti duplikat z enostavnimi stroji in z drugo obliko ključa ter od drugega proizvajalca.

** BIM (Building Information Modeling) omogoča sodoben, pametnejši način gradnje in projektiranja. Omogoča možnost vključevanja različnih strok in delovnih procesov, ki tradicionalno obstajajo vsak za sebe. Implementacija BIMa, poleg 3D oblikovanja objektov, omogoča tudi izdelavo energetskih analiz, svetlobne, vetrovne in druge analize, izdelavo natančnih ocen investicij, terminskih planov, nadgradnjo BIM modela v model za upravljanje (Facility Management - FM) in več. ■

Avtor: Zvonimir Cvetko Damnjanović / Slovenska Policija

NAPADI NA INFORMACIJSKE SISTEME GOSPODARSKIH DRUŽB

Pri svojem delu se pogosto srečujemo z žrtvami napadov na informacijske sisteme, tako s fizičnimi osebami, kot z odgovornimi osebami v gospodarskih družbah, ki so oškodovane. Skupno jim je, da iščejo pomoč organov pregona pri reševanju težav, katere so v večini primerov povzročili oškodovanci sami. Posledica teh težav je velikokrat materialna škoda in pa tudi ugled.

V poplavi prijav težko opredelimo vse napade na informacijski sistem za klasično kaznivo dejanje po 221. členu Kazenskega zakonika – Napad na informacijski sistem (Ur. l. RS št. 50/2012). V praksi je ogromno tovrstnih škodljivih ravnanj opredeljeno kot kaznivo dejanje Goljufije, saj storilci z lažnivim prikazovanjem ali prikrivanjem dejanskih okoliščin spravijo v zmoto oškodovanca ali ga pustijo v zmoti in ga s tem zapeljejo, da le-ta v škodo svojega ali tujega premoženja kaj stori ali opusti (211. člen).

Navedeno izpostavljamo iz razloga, ker je zaradi tega samo s pomočjo statističnih podatkov zelo težko pridobiti realno sliko o številu napadov na informacijske sisteme. V letnem poročilu Policije za leto 2015 je pod rubriko Računalniška kriminaliteta navedeno sledeče:

AKADEMIJA

preskok digitalni

22. marec 2017, Planet GV, Ljubljana

So vaše ekipe res dovolj seznanjene s temeljnimi spoznanji delovanja in razvoja v času digitalne revolucije?

PREVERI ZNANJE IN PREJMI BON ZA **50€!**

PREVERITE SVOJE DIGITALNO ZNANJE!

73% sprememb, ki jih prinaša digitalizacija ni povezanih z IT oddelki, temveč z delovanjem vseh ostalih oddelkov in procesov. Ključ do uspeha in konkurenčnosti je najprej usposobiti zaposlene, da bodo razumeli svojo vlogo v upravljanju dinamike sprememb v okolju in možnih priložnosti.

www.digitalnipreskok.si

Tabela 1 - Statistika računalniške kriminalitete

Kazniva dejanja računalniške kriminalitete	Število kaznivih dejanj		Porast/ upad [v %]	Število ovadenih osumljencev		Porast/ upad [v %]
	2014	2015		2014	2015	
Zloraba osebnih podatkov	5	3	...	0	2	...
Zloraba informacijskega sistema	1	6	...	0	1	...
Kršitev materialnih avtorskih pravic na internetu	1	2	...	15	4	...
Napad na informacijski sistem	155	162	4,5	68	76	11,8
Izdelovanje in pridobivanje orožja ali pripomočkov za vdor v ali napad na informacijski sistem	6	1	...	6	1	...
Skupaj	**168**	**174**	**3,6**	**89**	**84**	**-5,6**

(vir: http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2015_popravljeno.pdf)

V istem poročilu najdemo podatke, da je bilo v letu 2014 podanih kar 3.567 in v letu 2015 kar 2.754 prijav v zvezi klasične goljufije. Nikakor pa iz navedenega poročila ni mogoče izluščiti podatkov, koliko od teh prijav, povezanih z goljufijo, je bilo storjenih preko spleta in s pomočjo različnih metod socialnega inženiringa (tudi tehničnih, z uporabo specializiranih programov).

Iz delnega poročila Policije za prvo polletje leta 2016 izhaja, da so v istem obdobju beležili 6,8% porast prijav kaznivega dejanja Napada na informacijski sistem, hkrati pa je za navedeno kaznivo dejanje beležen 19,7% upad v številu ovadenih osumljencev.

Hkrati v letnem poročilu za leto 2015, katerega je podal SI-CERT, opazimo, da so v navedenem letu beležili kar 1.924 incidentov. Od tega so razvrstili napade v štiri vrste, ki so številčno opredeljeni kot:

Tabela 2 - Statistika obravnavanih incidentov na SI-CERT

Vrsta napada	Število
Tehnični napad	732
Goljufije	618
Phishing	283
Vprašanja in poizvedbe	225
Skupaj:	**1858**

(vir: https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf)

Logično je, da prihaja do razhajanj v statistiki, saj vsi ne prijavijo dogodka Policiji oziroma SI-CERT-u. V praksi opaža avtor zaskrbljujoče podatke, da veliko število posameznikov in še več predstavnikov gospodarskih družb ne želi podajati nikakršne prijave in želijo dogodek čim prej prikriti. Še vedno ostaja prisotna mentaliteta sramu pred neuspehom in porazom, ki ga posamezniki neupravičeno doživljajo ob takšnem dogodku. Ključno je izmenjevanje podatkov o incidentih, saj se pred vse večjim številom raznolikih napadov najučinkoviteje zaščitimo z ozaveščanjem.

Avtorja Panagiotis Trimintzios in Gavrila Razvan v poročilu Agencije Evropske unije za omrežno in informacijsko varnost, National-level Risk Assessments, An analysis Report iz leta 2013 izpostavljata ključne dejavnike tveganja za kibernetično varnost:

- velik primanjkljaj znotraj nacionalnih okvirjev, na področju poenotenja strokovne terminologije iz področja informacijske varnosti,
- nedokončane in različne metode ocenjevanja tveganj,
- primanjkljaj celovitih metod za soočanje z grožnjami,
- potrebo po učinkovitem upravljanju s tveganji, kapaciteto pripravljenosti in potrebo po strokovnem znanju in še
- potrebo po večjem deljenju informacij med različnimi udeleženci, ki soustvarjajo oceno tveganja na nacionalnem nivoju.

Statistika je lahko v določenih primerih suhoparna ali celo zavajajoča, vendar se dani situaciji zgovornosti statistike in ugotovitev ne moremo izogniti. Velik dejavnik predstavlja indiferenca posameznikov do tveganj, ki jih prinaša informacijska doba. Posledično se ljudje premalo pogovarjajo o teh tveganjih, kar privede do napak, ki se prepogosto manifestirajo kot finančni udarec za gospodarske družbe.

Zavedati se moramo, da neposredni tehnični napadi na informacijsko infrastrukturo zahtevajo določeno stopnjo specifičnega znanja, katerega se ni lahko priučiti in, da učenje terja svoj čas. Kriminalcem pa je v interesu, da v čim krajšem časovnem obdobju zaslužijo čim več denarja na čim lažji način. Logična izbira je socialni inženiring, katerega se je relativno lahko priučiti, obstoječa orodja so preprosta za uporabo, učinkovitost pa je zelo velika. V praksi opažamo, da je večina napadov na gospodarske družbe izvršena z zlorabo zaupanja zaposlenih, tako da storilci zaposlene (tudi vodstveni in vodilni kader) prepričajo, da so zaupanja vredni in kredibilni. Posledica tega je v večini primerov drag finančni udarec za gospodarsko družbo.

V zadnjem času opažamo velik porast »vrivanja v komunikacijo« med dvema gospodarskima družbama, kjer se napadalci z različnimi tehnikami predstavljajo kot poslovni

partnerji ali celo vodstvo ene od korporacij, ki sodeluje v poslovnem procesu. Tako speljejo komunikacijo vstran od legitimnega poslovnega partnerja in preslepijo žrtev, da je prepričana, da dejansko komunicira s svojim poslovnim partnerjem. Pri tem zahtevajo plačilo na transakcijske račune, odprte v tujini, pogosto v državah, kjer za odprtje transakcijskega računa ni potreben osebni kontakt. V resnici gospodarske družbe le redko dobijo povrnjeno škodo, ki nastane ob takšnem nakazilu. Vsekakor gre pri teh zadevah za določeno malomarnost zaposlenih, saj ne preverjajo dejanskega naročila za nakazilo. Tovrstnih primerov in različnih izpeljank teh primerov je iz dneva v dan več.

Pogosti so primeri, kjer se s pomočjo »spoofinga«, oziroma prirejanja glave elektronskih sporočil, ali z zakupom domen s podobnim imenom poslovnega partnerja, kriminalci vrinejo v komunikacijo med naročnikom neke storitve ali blaga in dobaviteljem. V veliki večini primerov gre za mednarodno poslovanje, kjer storilci zagotovijo, da so naročeno blago že poslali oziroma ga bodo dobavili po ustaljenih poteh. Hkrati zahtevajo plačilo računa, vendar uporabijo enega izmed izgovorov, kot je na primer zaprtje računa, ali sprememba banke in s tem prepričajo naročnika, da nakaže denar na transakcijski račun neznane osebe.

Zaščita v tem primeru niso drage požarne pregrade, zaposlitev vrhunskih strokovnjakov s področja informacijske varnosti, plačljive protivirusne rešitve ali druge tehnične rešitve. Zaščita je precej bolj enostavna in preprosta. Komunikacija je ključnega pomena za ustrezno zaščito pred socialnim inženiringom.

Gospodarskim družbam, ki so žrtve teh različnih napadov je skupen primanjkljaj komunikacije med zaposlenimi. Pred dobrim socialnim inženiringom se je težko zaščititi, saj so omejitve socialnega inženiringa le plod različnih avtorjev, ki so zaradi lažjega razumevanja socialni inženiring razdelili na različne segmente, glede na način izvedbe napada. V resnici kriminalcem ni mar za razdelitev in morebitne omejitve, vidijo le cilj, t. j. materialno korist. Za njih ne obstajajo omejitve, so le začasne ovire, katerim se uspešno izogibajo. Edina omejitev je njihova iznajdljivost in domišljija. To jih dela izredno nevarne in učinkovite.

Zaščita v tem primeru niso drage požarne pregrade, zaposlitev vrhunskih strokovnjakov s področja informacijske varnosti, plačljive protivirusne rešitve ali druge tehnične rešitve. Zaščita je precej bolj enostavna in preprosta. Komunikacija je ključnega pomena za ustrezno zaščito pred socialnim inženiringom. V podjetju je potrebno vzpostaviti politiko odprtih vrat, znotraj hierarhičnega ustroja, ki omogoča odprte komunikacijske poti med vodstvom in zaposlenimi ter ustrezno ozaveščanje zaposlenih. Tako se bodo zaposleni zavedali tveganj, ki jih sami predstavljajo in bodo ob varnostnem incidentu znali ustrezno reagirati.

Pomanjkanje komunikacije ni le problem, ki se manifestira znotraj podjetij. Iz zgoraj navedenega poročila Agencije Evropske unije za omrežno in informacijsko varnost je razvidno, da se pomanjkanje učinkovite komunikacije manifestira tudi na regionalno, nacionalno in tudi globalno raven. To se predvsem opaža v nekonsistentnih varnostnih rešitvah in vzpostavljenih komunikacijskih kanalih znotraj javne uprave. Kritično pa je predvsem pomanjkanje komunikacije o varnostnih incidentih znotraj javnih inštitucij, kjer bi se lahko z izmenjavo podatkov preprečilo dodatne incidente. Posledice tega, skozi splošno znižano stopnjo varnosti na internetu, občutimo prav vsi uporabniki.

Problem, ki ga opažamo, da gleda večina ljudi na varnost kot strošek in ne kot investicijo v varno prihodnost. Ko škodna posledica že nastane, je njene učinke dosti težje upravljati. V konkretnih primerih govorimo o materialni škodi, ki presega tudi 300.000,00 €, kar predstavlja znaten nepredviden strošek za vsako gospodarsko družbo, ne glede na njeno velikost. Zato je ključnega pomena ozaveščanje in pogovarjanje na temo varnosti na splošno in ne samo na temo internetne varnosti. Vodstvo družb se premalokrat zaveda, da v njihovo kritično »infrastrukturo« spada ravno njihov kader, saj predstavlja veliko varnostno luknjo, ki jo kriminalci s pridom izkoriščajo.

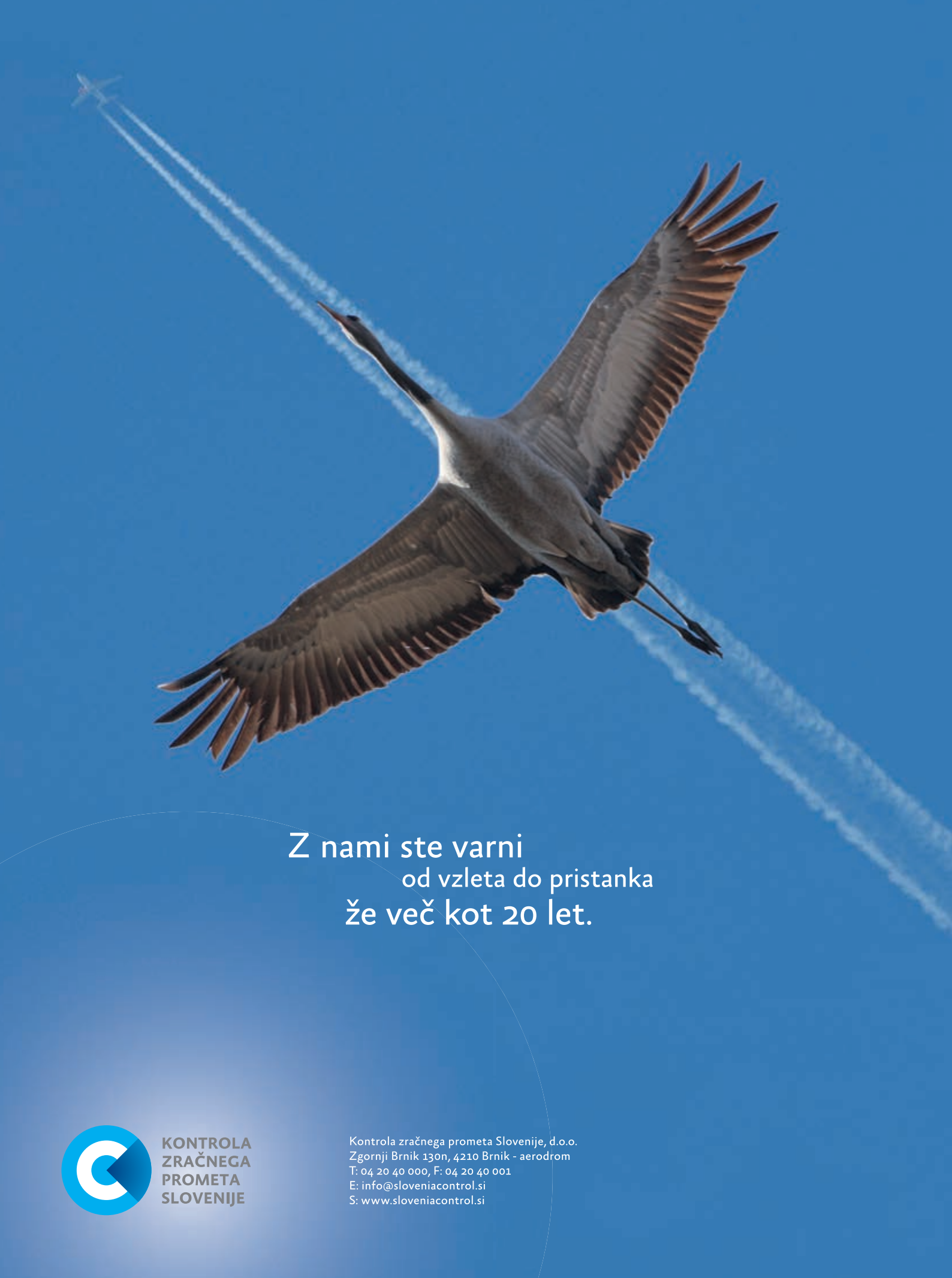
Obstaja dober razlog, zakaj je v Veliki Britaniji spletni kriminal že prevzel prvo mesto po dobičku v primerjavi s klasično kriminaliteto in zakaj je ta trend drugod po svetu v strmem porastu. Po podatkih angleške agencije National Crime Agency iz leta 2016 je razvidno, da splošna kriminaliteta obsega 47% celotne kriminalitete v Združenem kraljestvu Velike Britanije. Zloraba računalnikov zajema 17%, spletne goljufije pa 36%, skupno torej spletna kriminaliteta obsega kar 53% celotne kriminalitete. Zakonske omejitve pri mednarodnem sodelovanju varnostnih služb pa preiskavo tovrstne kriminalitete zelo otežujejo. Problem se pojavlja pri pridobivanju prometnih podatkov, ki so opredeljeni kot osebni podatki in je za to potrebna odredba sodišča, oziroma institut mednarodne pravne pomoči. Ti postopki se v praksi izvajajo, vendar trajajo predolgo. Prav tako je pridobivanje podatkov iz določenih držav zelo oteženo in še posebej dolgotrajno. Tukaj so zakonske omejitve, ki so postavljene z namenom varovanja osebnih podatkov posameznika, restriktivne do te stopnje, da ovirajo ali celo onemogočajo preiskavo.

Zaradi navedenega veljajo naslednja priporočila:

- vzpostavitev in vodenje jasnih in uporabnih varnostnih politik,
- politiko odprtih vrat, ki omogoča neovirano komunikacijo na vseh nivojih poslovne hierarhije (ne sme biti tabu, preverjanje odločitve o »nenavadnem« naročilu plačila),
- izobraževanje in ozaveščanje zaposlenih o nevarnostih spletnih goljufij (preverjanje zaglavja prejetih elektronskih sporočil z nenavadno vsebino in zahtevki o plačilu) in
- jasno postavljene smernice v zvezi ukrepanja ob morebitnem varnostnem incidentu (potrebno je vedeti, na koga se lahko obrnemo v primeru, ko zaznamo varnostni incident).

Viri:

- Pregled dela policije za prvo polletje 2016, spletno mesto Policije, http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/PorociloZaPrvoPolletje2016.pdf, pridobljeno 12. 2. 2017
- Letno poročilo o delu policije za leto 2015, spletno mesto Policije, http://www.policija.si/images/stories/Statistika/LetnaPorocila/PDF/LetnoPorocilo2015_popravljeno.pdf, pridobljeno 12. 2. 2017
- Poročilo o omrežni varnosti za leto 2015, Spletno mesto SI-CERT https://www.cert.si/wp-content/uploads/2016/06/SI-CERT_LP_2015.pdf, pridobljeno 12. 2. 2017
- Cybercrime vs. Non-Cyber Crime: What are the Comparative Effects?, spletno mesto Blue Coat, https://www.bluecoat.com/company-blog/2014-06-30/cybercrime-vs-non-cyber-crime-what-are-comparative-effects, pridobljeno 12. 2. 2017
- Cybercrime Overtakes Traditional Crime in UK, spletno mestp Krebson Security https://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk/, pridobljeno 12. 2. 2017
- Cyber Crime Assessment 2016, spletno metsto National criminal agency, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file, pridobljeno 12. 2. 2017
- Vodila varnega poslovanja, spletno mesto Varni na internetu, https://www.varninainternetu.si/article/vodila-varnega-poslovanja/, pridobljeno 12. 2. 2017
- Kazenski zakonik Republike Slovenije (Ur. l. RS, št. 91/2011 z dne 14. 11. 2011)
- Trimintzios P. in Razvan G., 2013, National-level Risk Assessments, An analysis Report, izdan s strani European Union Agency for Network and Information Security
- Lastni viri ■



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

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije

INTERVJU
Tilen Pahor, magister korporativne varnosti,
prvi diplomant magistrskega programa »Management korporativne varnosti«

MANAGEMENT KORPORATIVNE VARNOSTI POMEMBEN POKLICNI PROFIL PRIHODNOSTI

Pogovarjali smo se s prvim diplomantom magistrskega študija »Management korporativne varnosti«, ki se izvaja na GEA College/Fakulteti za podjetništvo. Kot prvi diplomant vsekakor pušča neizbrisen pečat vezan na uveljavljanje nove profesije v Republiki Sloveniji.

Ste prvi diplomant podiplomskega magistrskega programa Management korporativne varnosti«. Kako se počutite kot prvi med enakimi?

Počutim se odlično in prav lepo se sliši, ko ti nekdo reče, da si prvi med enakimi. Seveda pa to prinese tudi dodatno odgovornost in zavedanje, da je čas, da se še bolj povežemo in dvignemo zavedanje pomembnosti varnosti v slovenskem okolju.

Kakšni so vaši prvi vtisi o samem študijskem programu in vsebini študija? So bila dosežena vaša pričakovanja?

Predvsem bi rad izpostavil profesorje, ki v veliki večini prihajajo iz poslovnih okolij, kjer se dnevno srečujejo z različnimi varnostnimi tveganji in to znanje potem aplicirajo študentom. Biti manager korporativne varnosti še zdaleč ni le ozki pogled v varnosti. Ta oseba mora razmišljati kot finančnik, kadrovnik, pravnik in kot navadni delavec.

Kot študentje smo imeli možnost vpogleda v delovanje varnosti velikih slovenskih podjetij. Predlagali smo tudi nove varnostne postopke in poti ter analizirali kako bi delovali v poslovnem procesu. Z različnimi podjetji smo izmenjavali mnenja, znanja in izkušnje in velikokrat vse to primerjali s tujino.

Grožnje so vse okoli nas, treba jih je le prepoznati, zato študij vsebuje predmete vse od prava, financ pa do geopolitičnih vidikov in varnosti. S profesorji vzpostavimo močno vez, ki ne traja le med študijem ampak tudi po njem, kar je najpomembneje.

Katere so tiste ključne ugotovitve in napotila, ki jih lahko posredujete mlajšim generacijam ob razmišljanju za vpis na študij Managementa korporativne varnosti?

Velikokrat slišimo, da je manager korporativne varnosti poklic prihodnosti. S tem se strinjam, vendar bi rad poudaril, da ne gre le za varnost. Gre za svetovalsko funkcijo generalnemu direktorju, ki od vas pričakuje ne le načrtovanje, razvoj in uvajanje varnostnih standardov, ampak tudi stratega, skrbnika procesov in najpomembnejše, človeka na katerega se bo najprej obrnil, ko bo potreboval kakršenkoli nasvet. Zato tudi pravimo, da je manager korporativne varnosti človek štirih obrazov.

Sam študij je bil prepleten z različnimi dopolnilnimi možnostmi za izpopolnjevanje in preverjanje teoretičnih spoznanj v neposrednih praktičnih okoljih. Vam je ta možnost omogočila pridobitev ustrezne širine znanja, ki je aplikativen v realnem okolju?

Učenje v učilnicah je nekaj, pogled v realnost pa popolnoma nekaj drugega. Kot študentje smo imeli možnost vpogleda v delovanje varnosti velikih slovenskih podjetij. Predlagali smo tudi nove varnostne postopke in poti ter analizirali kako bi delovali v poslovnem procesu. Z različnimi podjetji smo izmenjevali mnenja, znanja in izkušnje in velikokrat vse to primerjali s tujino.

Nam lahko zaupate kakšni so vaši načrti za nadaljevanje karierne poti na področju korporativne varnosti?

Trenutno sem zaposlen v Univerzitetnem kliničnem centru Ljubljana, vendar se direktno s korporativno varnostjo ne ukvarjam. Dejstvo je, da so bolnišnice kritična infrastruktura, ki potrebuje vrhunsko varnost. Čez čas upam, da se bo tudi pri nas pokazala potreba po taki vrsti dela, ki bi ga sam z veseljem opravljal.

Ali se po vašem mnenju poslovno okolje bolj zaveda pomena celovitega obvladovanja varnostnih tveganj, kot v tistem obdobju, ko ste se odločali za začetek študija?

Upam si trditi, da še vedno premalo. Raziskave kažejo, da se podjetja odločijo za posodobitev varnosti šele po napadih na njihovo lastnino. Vlaganje

v preventivno varnost je vedno drago, zato se le malo podjetij odloči za ta korak. Zaradi pomanjkanja varnosti pa lahko pride do nepopravljive škode, velikokrat je že prepozno in so ključne informacije že bile odtujene iz podjetja. Šele takrat se podjetja zavedo, da bi nekaj dodatnega denarja v varnost lahko situacijo bistveno spremenilo. V informacijski dobi je informacija vredna več kot denar, zato bodo napadi na omrežja, kjer so shranjene informacije vedno pogostejši. To zavedanje pri slovenskih podjetjih bo treba dvigniti preden pride do nepopravljive škode.

Kako vidite vlogo Slovenskega združenja za korporativno varnost? Boste postali reden član omenjenega združenja z namenom izpopolnjevanja dobrih praks in druženja s strokovnjaki s področja korporativne varnosti?

Definitivno bom postal redni član in se skušal udeležiti čim več srečanj, ki jih združenje organizira. Mojo vlogo vidim predvsem pri dvigovanju zavedanja pomembnosti varnosti v bolnišnicah in uvajanju varnostnih standardov skupaj s Slovenskim združenjem za korporativno varnost. Menim, da so javni zdravstveni zavodi na tem področju zelo slabo poučeni in je treba dvigniti njihovo zavedanje, da se ne bodo ponovili dogodki iz SB Izole ali pa tisti in Nemčije, kjer so ukradli na tisoče zdravstvenih kartonov, s katerim so izsiljevali bolnike. ■

Od bodočega managerja korporativne varnosti se pričakuje ne le načrtovanje, razvoj in uvajanje varnostnih standardov, ampak mora biti tudi dober strateg, skrbnik procesov in človek, na katerega se direktor lahko obrne za nasvet. Zato tudi pravijo, da je manager korporativne varnosti človek štirih obrazov. Profesorji nas učijo, kako postati ta človek in pripravljajo na realnost. Najbolj pomembno pa je, da s profesorji vzpostavimo močno vez, ki traja tudi po končanem študiju.

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

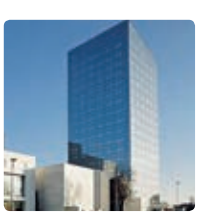
FAKULTETA ZA PODJETNIŠTVO

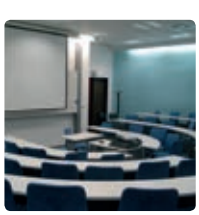
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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