Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2018, december • št. 18



Jubilejna 10. mednarodna konferenca »Dnevi korporativne varnosti 2019«

Kongresni center Brdo, 13.-14. marec 2019

Kako uspešna bo implementacija Zakona o informacijski varnosti?



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 središče delovanja smo postavili strateške inovacije, ki prinašajo nove rešitve za zagotavljanje zanesljivosti delovanja elektroenergetskega sistema.

www.eles.si



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
izr. prof. dr. Denis Čaleta

Trženje:
ICS-Ljubljana
info@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
december 2018

Izvod revije je brezplačen

Naslovnica in slike:
ID 68533754 © Sinemaslow | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

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

V zadnjem obdobju smo bili v Republiki Sloveniji priča pomembnim zakonskim mejnikom, za katere upamo, da bodo imeli pomembne posledice na področju obvladovanja tveganj. Govorimo o dveh pomembnih predpisih in sicer Zakonu o kritični infrastrukturi in Zakonu o informacijski varnosti. Oba prinašata v nacionalni prostor določene rešitve, ki pred upravljalce kritične infrastrukture in izvajalce bistvenih storitev postavljata določene obveze in pričakovanja, da bo obvladovanje v teh ključnih organizacijah ustrezno urejeno. Seveda pa se vsi zavedamo, da samo sprejetje osnovnih zakonskih predpisov še ni garant za uspešno izvedbo teh kompleksnih postopkov. Na podlagi obeh zakonov bo potrebno sprejeti cel niz pomembnih podzakonskih aktov in metodoloških izhodišč, ki bodo dala realne usmeritve in upajmo tudi poenotenje določenih procesov. No, na tej točki pa vsakič trčimo v oviro, ki se ji reče strateška podpora vsakokratne vladajoče politike za dokončno uveljavitev zakonsko predvidenih določil. Če ocenjujemo, kakšno prioriteto je temu področju namenila nova aktualna vlada, nas lahko začne skrbeti. Določeni podzakonski predpisi, posebej na področju Zakona o informacijski varnosti, zamujajo, ključni deležniki te vlade, kot na primer svetovalec za nacionalno varnost, pa temu področju ne posvečajo ustrezne pozornosti. Vse kaže, da bo pot uveljavitve učinkovitih ukrepov na področju kibernetske varnosti spet potekala od spodaj navzgor, kar pomeni, da bodo organizacije, ki poslujejo v zahtevnem globalnem varnostnem okolju, primorane svoje procese zavarovati na svoj lasten način. To verjetno ne bo v smeri neke enovite sistemske ureditve saj se bo vsak prilagajal svojim potrebam, znanju, sposobnostim in virom. Vendar lahko smatramo, da Republika Slovenija zamuja ključne trenutke za izvedbo usklajenih procesov, ki bi v končni posledici lahko racionalizirali kadrovske in finančne vire in tako prinesle učinkovitejše sinergijske učinke.

Na področju korporativne varnosti se pri obvladovanju informacijskih tveganj dogajajo spremembe, ki smo jih napovedovali že dalj časa. Informacijska varnost se iz sektorjev informatike organizacijsko vključuje v proces korporativne varnosti. Ta anomalija, kjer so tisti, ki so postavljali in skrbeli za delovanje informacijskega sistema, kontrolirali sami sebe, se je končno pričela urejati. To seveda na področje korporativne varnosti prinaša nove izzive in priložnosti.

V tokratni številki prinašamo cel niz aktualnih tem. Posebno pozornost posvečamo izzivom, ki jih prinaša kibernetska varnost in metodologija ocenjevanja tveganj, dotikamo se pomembnih tem iz korporativno varnostnega okolja, kot so pomen neprekinjenosti delovanja organizacij in procesi obvladovanja tveganj. Poseben del je tudi tokrat namenjen informacijski varnosti. K pogovoru smo povabili več zanimivih in izpostavljenih sogovornikov, ki so vsak iz svojega strokovnega stališča pomembno obogatili tokratno številko revije. Bralcem, ki niso imeli priložnosti sodelovati na odmevnem posvetu v Državnem svetu Republike Slovenije, na temo uveljavitve Zakona o informacijski varnosti in kibernetske obrambe, pa smo pobližje predstavili glavne zaključke tega odmevnega dogodka.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



KOLUMNA

KAKO RAZUMEMO NUJNOST IMPLEMETACIJE ZAKONA O INFORMACIJSKI VARNOSTI? 9



INTERVJU
Božidar Dajčman, direktor Sektorja za upravljanje fizične in informacijske varnosti, NKBM d.d.

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE 19



UPRAVLJANJE TVEGANJ V KRITIČNI INFRASTRUKTURI

Glavni namen tega prispevka je, da v okviru poslovnih, varnostnih, demografskih, globalnih in drugih izzivov, ki spremljajo kritično infrastrukturo, prispevamo nekaj misli, usmeritev in rešitev za celovito upravljanje tveganj in zagotavljanje neprekinjenega delovanja gospodarskih, javnih, državnih in drugih organizacij, ki upravljajo s kritično infrastrukturo. 24



VARNOST OBLAKA PREDSTAVLJA VARNOST NAŠIH APLIKACIJ IN PODATKOV

Varnost oblaka predstavlja varnost podatkov, aplikacij in infrastrukture vključene v oblak. Veliko varnostnih vidikov je vključenih v okolje oblaka, prav tako je veliko vidikov varnosti oblaka bodisi privatne, javne ali hibridne narave enakih, kot v lokalni prostorski IT arhitekturi. 44



STRELSKI NAPAD: PREŽIVI S TREMI »S« (STECI, SKRIJ SE, SPOPADI SE!)

Statistika kaže, da so strelski napadi v skokovitem porastu, niso izključeni tudi v Sloveniji. Korporativni varnostni managerji se srečujemo s številnimi izzivi pri načrtovanju za navedeni primer, zlasti na področju kritične infrastrukture, v smislu upravljanja aktivnosti, vzpostavitvi operativnega okolja in varovanja zaposlenih. 48

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

INTERVJU
g. Alojz Kovšca, predsednik Državnega sveta Republike Slovenije

DRŽAVNI SVET KLJUČNO STIČIŠČE INTERESNIH SKUPIN

Dinamično varnostno okolje pred širšo družbeno skupnost postavlja nove izzive in tveganja. O priložnostih za dvigovanje zavedanja o pomenu varnosti in tudi varnostnih izzivih, pred katerimi se nahaja Republika Slovenija, smo izkoristili priložnost in se pogovorili s predsednikom Državnega sveta Republike Slovenije g. Alojzem Kovšco.

Državni svet Republike Slovenije je ena od najpomembnejših državnih institucij, ki predstavlja stičišče različnih interesnih okolij. Nam lahko prosim pojasnite težišča delovanja tega vašega mandata.

Državni svet je pravzaprav stičišče civilne družbe s politiko. V njem so različni družbeni interesi, zastopani neposredno s predstavniki iz okolij, kjer ti interesi nastajajo in se artikulirajo. Državni svet ima torej neposreden vpogled v družbeno dogajanje na različnih področjih in lahko izpostavlja aktualne probleme, ter ponuja rešitve, še preden se v Državnem zboru oblikuje politična volja za naslavljanje taistih vprašanj.

Težišča delovanja Državnega sveta v aktualnem mandatu gredo večinoma v smeri:

- izboljšanja sodelovanja z Državnim zborom (izboljšanje sodelovanja Komisij Državnega sveta z analognimi Odbori Državnega zbora),

Državni svet bo v prihodnosti zagotovo posvetil veliko pozornosti varnostnim vprašanjem.



*avtor je član Slovenskega združenja korporativne varnosti

- povezovanja zastopnikov civilne družbe z Državnim svetom (Varuh človekovih pravic, Zagovornik načela enakosti, zastopnik pacientovih pravic, Komisija za preprečevanje korupcije, Informacijski pooblaščenec, Računsko sodišče, varuh konkurence) in vzpostavljanje periodičnega poročanja javnosti o stanju v družbi in državi,
- zunanjepolitičnih aktivnostih, ki pomenijo promocijo gospodarstva, znanosti, izobraževanja, kulture in športa,
- večanja prepoznavnosti Državnega sveta v javnosti in izboljšanja informiranja javnosti o vsebinah in rezultatih dela DS RS.



Varnost predstavlja eno od osnovnih dobrin in predpogojev za nemoten razvoj in delovanje družbe. Kako lahko Državni svet pripomore k dvigovanju varnostnega zavedanja o pomenu varnosti v slovenskem okolju?

Percepcija varnosti v slovenskem okolju je na dokaj nizki strokovni ravni. Slovensko volilno telo je praviloma apatično in varnostnih izzivov ne prepoznava, vse dokler ne preidejo v akutne oblike ogroženosti. Tedaj se začne družbena reakcija, ki je zaradi zapoznelosti praviloma nesorazmerna, ideološko spolitizirana in strokovno pomanjkljiva. Zgovoren primer, ki ilustrira takšno ukrepanje, je način reševanja migrantske krize.

Naloga Državnega sveta je hiter in kakovosten prenos informacij o problemih iz okolij, v katerih svetniki živijo in delujejo, do pristojnih delovnih teles DS, oblikovanje stališč in iskanje rešitev v dveh smereh: angažiranja vlade oziroma ministrstev ali neposredna akcija z oblikovanjem zakonodajnega predloga. Državni svet tudi redno organizira posvete na temo različnih družbenih problemov in za različne deležnike, najsi bo to na čisto praktični izvedbeni ravni ali na akademsko teoretični. Posveti s področja teorije varnosti, kot izvedbenih modelov za posamezne organe ali organizacije, so vsekakor dobrodošli.

Tudi vi ste, med drugim, po profesiji strokovnjak s področja obramboslovja. Kako osebno ocenjujete razvoj dejavnikov kompleksnega varnostnega okolja, ki nas obdaja?

Težko bi rekel, da sem po profesiji še vedno strokovnjak s področja obramboslovja. Življenje in delo me je zaneslo bližje gospodarstvu in politiki, pa vendar se nabere kar precej varnostnih vprašanj tudi v vsakdanjem delu politika. Varnostno okolje, ki nas obdaja, postaja vse težje in dražje obvladljivo. Postali smo globalna migrativna komunikacijska družba. Nesluten razvoj pretoka informacij nam na eni strani lajša in poenostavlja življenje in delo, na drugi strani pa nas umešča v sistem popolnega nadzora posameznikov in družbe s strani tistih, ki imajo možnost dostopa do podatkov in obdelave v realnem času. Če je vojna podaljšana roka ekonomije, potem je kibernetska vojna njena višja evolucijska stopnja. Prihajamo v obdobje vojskovanja brez jekla in smodnika, obdobje vzpostavljanja dominacije nad živčnim sistemom držav nasprotnic, brez povzročanja nepotrebnih izgub v živi sili in materialnih sredstvih... Vo-

jaške akademije evropskih držav že več let usposabljajo kadre za kibernetsko vojskovanje. Kje smo na tem področju v Sloveniji, težko ocenim.

Državni svet Republike Slovenije je v preteklosti zelo močno podpiral odpiranje strokovne razprave o perečih družbenih problemih. V tem so bile močno prisotne tudi teme, ki zadevajo varnostne procese. Bo tudi v prihodnje temu namenjeno dovolj prostora?

Državni svet bo v prihodnosti zagotovo posvetil veliko pozornosti varnostnim vprašanjem. Nova evropska finančna perspektiva naslavlja obrambno-varnostna vprašanja z vso resnostjo. Brexit in protekcionistični trgovinski ukrepi ZDA silijo EU v oblikovanje bolj samostojne in proaktivne varnostne politike. Ti procesi morajo postati sestavni del slovenske varnostne in gospodarske politike. Izgradnja evropskega obrambnega in varnostnega sistema ne sme postati ekonomsko breme, temveč ekonomska priložnost za Slovenijo. V tej smeri želimo v Državnem svetu organizirati posvete, s katerimi bi lahko čimprej mobilizirali domače strokovne in produkcijske kapacitete ter iskali priložnosti za sodelovanje z drugimi članicami evropske unije.

Menite, da bi se moral Državni svet RS na podlagi izhodišč in zaključkov, ki jih prinaša taka strokovna razprava, močneje vključevati v zakonodajne procese ob nastajanju določenih zakonskih okvirov?

Državni svet ima možnost implementacije zaključkov posvetov neposredno v zakonodajne predloge. V takšnih primerih se vsakokratna koalicija v Državnem zboru opredeljuje do predlogov Državnega sveta, kot do predlogov opozicije. V primeru, da nam uspe preboj na enem izmed težišč delovanja v tem mandatu, torej izboljšanju odnosov z Državnim zborom, je bolj smiselno ponujanje zakonodajnih predlogov koaliciji v »posvojitev«.

Gospodarstvo je interesno zelo močno zastopano v Državnem svetu. Katere bi bile po vaši oceni tiste priložnosti, ki bi ravno skozi te kanale gospodarstvu posredovale več informacij in znanj s področja boljšega obvladovanja varnostnih tveganj?

Gospodarstvo ima v Državnem svetu glede na celotno sestavo sorazmerno dobro zastopstvo. Dejansko gre za pet oseb, od katerih je ena zastopnica trgovinske,



druga gospodarske, tretja obrtno-podjetniške zbornice, dva sta pa zastopnika delodajalcev. Informacije za gospodarstvo o obvladovanju varnostnih tveganj je po svetnikih smiselno posredovati zbornicam. Prav tako so svetnice in svetniki tisti, od katerih se lahko pričakuje kakovosten »feed-back« iz zborničnih sistemov.

Slovensko združenje za korporativno varnost predstavlja eminentno združbo organizacij in posameznikov s področja korporativne varnosti. Izmenjava dobrih praks in informacij na področju obvladovanja tveganj je rdeča nit delovanja omenjene asociacije. Menite, da je v stičišču z Državnim svetom RS lahko to ena iz-

Slovensko združenje za korporativno varnost je zagotovo pomemben element podpore širšemu sektorju gospodarstva, ki v Državnem svetu lahko naslavlja tako državne organe, kot tudi gospodarstvo in civilno družbo.

med poti strokovne podpore širšemu sektorju gospodarstva?

Slovensko združenje za korporativno varnost je zagotovo pomemben element podpore širšemu sektorju gospodarstva, ki v Državnem svetu lahko naslavlja tako državne organe, kot tudi gospodarstvo in civilno družbo. Kot sem že uvodoma dejal, je slovenska družba precej inertna in na žalost reagira na ogrožanje šele ob ekscesnih dogodkih. Pomembno je, da se informacije o varnostnih tveganjih in možnostih zaščite pred njimi pojavljajo sistematično in trajno. Državni svet si z asistenco združenja utrjuje družbeno podobo organa, ki deluje v splošno korist družbe in države.

V tem okviru velja posebej izpostaviti malo gospodarstvo ali obrtnike, ki si v svojih organizacijah največkrat težko privoščijo postaviti osebe, ki bi se ukvarjale z varnostnimi procesi. Glede na to, da izhajate iz tega okolja, nas zanima vaše mnenje, kako bi lahko sistemsko in organizacijsko zagotavljali dovolj strokovne podpore na nivoju zborničnega združevanja ali drugih oblik, ki bi zagotovile, da imajo podjetniki na tej ravni dovolj informacij in podpore?



Ugotovitev, da mali obrtniki in podjetniki težko obvladujejo varnostne procese zaradi kadrovske podhranjenosti in ekonomske šibkosti, drži v celoti. Iz dolgoletne obrtniške prakse vem, da se malo gospodarstvo ukvarja z mnogimi nepotrebnimi administrativnimi zadevami, kar razume kot potrato časa in denarja. Za asistenco pri obvladovanju varnostnih tveganj se obrtniki težko obrnejo na njim neznane subjekte. Verjetno bi bil najboljši način organiziranja strokovne podpore skozi lokalne zbornice, katerim že tako zaupajo vpogled v svoje poslovanje. Zbornice na drugi strani iščejo vse storitve, s katerimi lahko dopolnijo svojo ponudbo in upravičijo naziv podjetniško-podpornega okolja. Od tu naprej je stvar identifikacije skupnih ciljev in dogovorov o sodelovanju.

Institut za korporativne varnostne študije in Slovensko združenje za korporativno varnost vsako leto podeljujeta prestižno nagrado Slovenian Grand Security Award. Nagrada je podeljena tudi v kategoriji najbolj varno mesto in najbolj varna občina. Menite, da to še dodatno stimulira lokalna okolja k boljšemu zagotavljanju varnosti?

Bolj kot kadarkoli poprej Slovenian Grand Security Award pomeni pomembno priznanje za kakovostno delo lokalnih oblasti. Starajoči se generaciji državljanov je varno okolje zelo pomembno. Prav ta generacija je volilno najbolj aktivna! Če malo špekuliram, bo imel župan »najbolj varnega« mesta v prihodnosti več možnosti za ponovno izvolitev, kot župan »najlepšega« mesta ...

Je za konec še kakšna misel, ki bi jo posebej želeli posredovati strokovnemu okolju revije Korporativna varnost?

Izpostavljajte probleme, ponujajte rešitve, vsekakor pa promovirajte strokovnjake in gospodarske družbe, brez katerih bi vse ugotovitve ostale zgolj ugotovitve in nikoli ne bi postale rešitve. ■

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



KOLUMNA

KAKO RAZUMEMO NUJNOST IMPLEMETACIJE ZAKONA O INFORMACIJSKI VARNOSTI?

Sodobno varnostno okolje je postalo zahtevnejše, kot je bilo v trenutku, ko so svojo mladost preživljali predstavniki trenutne strateške strukture, katera v zadnjih letih vodi Republiko Slovenijo. Ob tem se nam upravičeno postavlja vprašanje, ali se odgovorni sploh zavedajo, kako resne grožnje, kibernetsko okolje informacijske dobe 21. stoletja, postavlja pred našo družbo, ter pred javne in poslovne organizacije. Argumenti, ki jih bom navedel v nadaljevanju, nas lahko prej skrbijo, kot pa da bi nas pomirili.

Dejstvo je, da Slovenija v globalnem informacijskem okolju ni varna oaza. Verjetno je to postalo jasno tudi naši mladini, ki roko na srce, bolj razume informacijsko okolje v katerem danes živimo. Napadi na informacijska omrežja, tako javnih, kakor tudi poslovnih organizacij, so postali stalnica, ki medijske pozornosti sploh več ne pritegne. Tveganjem pa so izpostavljeni tudi navadni državljani. Torej je jasno, da so osnovni parametri zagotavljanja informacijske varnosti skupna skrb vsem predstavnikom naše družbe. Seveda je obseg odgovornosti različen in se neprimerno poglobi, ko začnemo govoriti o nacionalni varnosti, zaščiti kritične infrastrukture, zagotavljanju bistvenih informacijskih storitev, na katerih temeljijo ključni procesi delovanja te družbe. V mesecu maju 2018 je v veljavo stopil tako dolgo pričakovan Zakon o informacijski varnosti, ki bi poleg že prej sprejetega Zakona o zaščiti kritične infrastrukture postavil temelje za postavitev učinkovitih procesov zagotavljanja kibernetske obrambe in še širše ustrezne informacijske varnosti. Že pri sprejemu zakona je strokovna javnost pričakovala, da bo zakon nastajal na podlagi globokih strokovnih razprav, ki bi poleg procesov in mehanizmov, za učinkovito zagotavljanje informacijske varnosti, prinesel odgovore tudi na dileme, kako združiti in aktivirati že tako omejene vire, katere ima Republika Slovenija na tem zahtevnem področju na voljo. Kljub določenim naporom, ki so bili na področju odpiranja javne razprave v preteklosti že narejeni, tudi v okviru Slovenskega združenja za korporativno varnost, in s podporo posameznih pomembnih korporativnih članov, je bil Zakon o informacijski varnosti pripravljen in sprejet pod pritiskom nuje, ki jo je pred Slovenijo postavljala potreba sprejetja EU Direktive (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov (krajše direktive NIS). Določila omenjene NIS direktive je Slovenija, skozi omenjeni zakon o informacijski varnosti, v naš pravni red dejansko vpeljala v zadnjem trenutku. To je bil eden od zadnjih zakonskih aktov, ki ga je na predlog odha-

Napadi na informacijska omrežja, tako javnih, kakor tudi poslovnih organizacij, so postali stalnica, ki medijske pozornosti sploh več ne pritegne. Tveganjem pa so izpostavljeni tudi navadni državljani. Torej je jasno, da so osnovni parametri zagotavljanja informacijske varnosti skupna skrb vsem predstavnikom naše družbe.

*avtor je član Slovenskega združenja korporativne varnosti



jajoče vlade sprejel Državni zbor. Na opozorila, da so nekatere stvari terminološko in tudi vsebinsko nedorečene, ni bilo pravega odziva, kar je pod časovnim pritiskom tudi delno razumljivo.

Torej v veljavi imamo zakon, ki sicer ni idealen, prinaša pa nekatere jasne zaveze, določila, roke in predvsem pričakovanja, s strani neposrednih deležnikov informacijskega okolja. Imenovani so bili začasni organi, ki morajo zapolniti vrzeli do organiziranja pristojnega nacionalnega organa, ki bo zadolžen za koordinacijo ukrepov na področju informacijske varnosti. Začasno je bila ta pristojnost prenesena na Urad RS za varovanje tajnih podatkov. Do vzpostavitve nacionalnega CSIRT (skupine za odzivanje na incidente na področju informacijske varnosti) in CSIRT organov državne uprave bo njuno nalogo opravljal SI-CERT. Opredeljeni so jasni roki za pripravo strategije informacijske varnosti, metodologije za določitev izvajalcev bistvenih storitev in digitalnih storitev, določitev vsebine in strukture varnostne dokumentacije in varnostnih ukrepov in postopek obvezne in prostovoljne priglasitve incidentov v informacijskem okolju.

Trenutno pa, kljub temu, da so določeni roki zakona že pretekli, nimamo ustreznih dokumentov, metodologij in predvsem usmeritev, kako nadaljevati zapisane procese, ki jih predvideva Zakon o informacijski varnosti. Že dolgo je jasno, da nacionalna varnost, razen deklarativnega zavzemanja, ni bila v zadnjem obdobju na prioritetni listi nobene vlade. Signali iz praktično vseh institucij, ki predstavljajo sistem nacionalne varnosti, so zelo zaskrbljujoči. Organizacijske ter sistemske napake in načrtno siromašenje teh ključnih institucij kaže namreč svoje zaskrbljujoče posledice. Če poleg tega dodamo še strokovno-kadrovske težave, pa ta situacija predstavlja zelo resno stanje, ki bi terjalo nujno odzivanje vsake vladajoče elite. Razen, če le tej ni v interesu, da ima ključne institucije nacionalne varnosti pod neposrednim »političnim« vplivom, brez ustreznih zmožnosti realnega odkrivanja deviantnosti, ki jih v določenih primerih izvajajo ravno interesne skupine povezane z vladajočo elito.

Kako si lahko predstavljamo dejstvo, da je, kljub jasnemu zavedanju, podpora strateških odločevalcev na področju vzpostavljanja sistema informacijske varnosti in posledično kibernetske obrambe, mizerno nizka. Obe zgoraj navedeni organizaciji, UVTP in SI-CERT, ki opravljata in sta tudi po zakonu določeni kot ključna organizacijska dejavnika za nada-



ljevanje vzpostavitve sistema, praktično nista dobili novih kadrovskih in finančnih virov za izvedbo te kompleksne naloge. Tukaj se nam postavlja vprašanje, zakaj država ni sposobna centralizirati strokovnih kadrovskih virov v tiste centralne točke, ki bodo v prihodnje predstavljale temelj za izgraditev ustreznega in visoko strokovnega nacionalnega organa. Da o koordinaciji nacionalno varnostnega sistema sploh ne izgubljamo besed, saj je jasno, da potrebuje resne sistemske spremembe, ki bodo prinesle ustrezno učinkovitost in preseganje parcialnih interesov. Prav tako smo javno-zasebno partnerstvo v tej državi, kot eno izmed ključnih prioritet, zapisali v naše strategije. Tega procesa ne razumemo in se ne zavedamo, da lahko tako majhna država z omejenimi finančnimi viri izgradi uspešen sistem zagotavljanja kibernetske obrambe samo z vključevanjem vseh možnih resursov javnega in zasebnega okolja. Še več, državni organi in institucije, ki bi morale biti glavni motor na tem področju, se skrivajo za birokratskim dojemanjem okolja, ki pa največkrat privede do stanja, da le te postanejo ovira in ne dejavnik rešitve ter razvoja. Torej, že s kratkim površnim pregledom lahko ugotovimo, da Zakon o informacijski varnosti doživlja isto usodo, kot tudi ostala pomembna področja v okviru zagotavljanja nacionalne varnosti. Po sprejetju zakona in realizaciji zahteve EU po uveljavitvi določil NIS direktive si je politika ponovno zatisnila oči in ta problem za njo več ne obstaja. Na srečo je vedno več gospodarskih organizacij, tudi tistih, ki upravljajo kritično infrastrukturo, v katerih so se vodstva začela zavedati pomena neprekinjenosti delovanja, tudi v luči ustreznega obvladovanja informacijskih tveganj kibernetskega okolja. Brez ustreznega obvladovanja tveganj ni mogoče zagotavljati osnovnega poslanstva teh organizacij in to je zagotavljanje neprekinjenega poslovanja in ustreznih poslovnih ciljev. Razumevanje teh dejavnikov, na področju informacijske varnosti, se kaže v krepitvi le te, znotraj procesov korporativne varnosti in vedno večjih vložkov v zagotavljanje tega pomembnega segmenta. Pomembno vlogo na področju ozaveščanja in strokovne podpore, pa vsekakor ima tudi Slovensko združenje za korporativno varnost in Institut za korporativno varnostne študije. To morajo biti primeri dobre praske in svetilniki, ki nas bodo vodili do krepitve zavedanja o pomembnosti informacijske varnosti in kibernetske obrambe. V Republiki Sloveniji bomo pač morali ponovno po poti »bottom-up« pristopa, ki je nekoliko drugačen od večine držav, kjer se tega problema zavedajo z dosti večjo resnostjo. ■

Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij. Skozi združenje člani organizirano uresničujejo osebne in poslovne interese na področju korporativne varnosti.



Namen združenja je uresničevanje interesov članstva, ki so:

- združevanje znanja, izkušenj, interesov in razvojnih pogledov,
- pospeševanje razvoja izobraževanja in usposabljanja,
- razvoj mednarodno primerljivih korporativnih varnostnih standardov,
- izboljšanje kakovosti storitev na področju zagotavljanja korporativne varnosti,
- razvoj korporativnega varnostnega managementa,
- razvoj varnosti kot vrednote, ki izboljšuje pogoje dela in dviguje motivacijo.

Članstvo v združenju je prostovoljno. Združenje ima redne, korporativne in častne člane.

»Ab uno disce omnes (po enem spoznaj vse)«

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

CETIS · ELES · NZS · gorenje group VAROVANJE · Luka d.d. · hse Holding Slovenske elektrarne d.o.o. · TEŠ Termoelektrarna Šoštanj · LUKA KOPER Port of Koper · lek član skupine Sandoz · REISSWOLF secret. service. · A1 · BTC · Mariborski vodovod · Kontrola zračnega prometa Slovenije · Philip Morris Ljubljana d.o.o. · univerzitetni klinični center ljubljana · Gasilska zveza Slovenije · si-cert · Informacijski pooblaščenec

www.ics-institut.si

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih mesečnih strokovnih srečanjih,
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS-Ljubljana,
- popusti pri nakupu izdanih publikacij ICS-Ljubljana,
- brezplačna naročnina na revijo Korporativna varnost.

Dodatne ugodnosti za korporacijske člane združenja:

- postavitev logotipa na spletno stran ICS-Ljubljana in v reviji Korporativna varnost na straneh namenjenih združenju,
- popusti pri oglaševanju v reviji Korporativna varnost in na konferencah v organizaciji ICS-Ljubljana,
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS-Ljubljana za vse zaposlene v podjetju,
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij katere so korporacijski člani združenja,
- korporacijskega člana v združenju zastopata dve osebi,
- druge bonitete objavljene na spletnih straneh združenja.

Članstvo v **SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI**

vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

Občina Slovenska Bistrica

Pošta Slovenije

Informacijske storitve in inženiring, d.o.o. INFORMATIKA

triglav

PETROL Energija za življenje

Telekom Slovenije

AKRAPOVIČ

interblock Luxury Gaming Products

spica

Ford SUMMIT AVTO

ELEKTRO LJUBLJANA

Elita i.b. d.o.o.

SIEMENS

DARS

CINKARNA

UNISTAR PRO

Nova KBM Pripravljeni na jutri

LON

ZARJA ELEKTRONIKA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

Avtor: Gorazd Božič / vodja SI-CERT*



KAKO SLOVENIJA PRISTOPA K ODZIVANJU NA RAČUNALNIŠKE GROŽNJE? STRATEGIJA, DIREKTIVA, ZAKON

Državni zbor Republike Slovenije je na zadnji seji prejšnjega sklica aprila 2018 sprejel Zakon o informacijski varnosti (ZInfV), ki je pred tem brez težav šel skozi obravnavo na pristojnem odboru. S tem je naša država še pravočasno sprejela zakon, ki udejanja določila Direktive NIS Evropskega parlamenta. Kot samo ime direktive nakazuje, je njen cilj zvišati "raven varnosti omrežij in informacijskih sistemov v Uniji."

Direktiva želi ta cilj doseči z nekaj sorazmerno enostavnimi ukrepi: tako, da vpelje pojem bistvenih storitev za delovanje države in družbe, naloži članicam določitev *izvajalcev* bistvenih storitev, prepozna kot ključni člen delovanje odzivnih centrov CERT oz. CSIRT in državam članicam nalaga, da določijo vsaj enega takšnega, ki bo sprejemal prijave incidentov in nudil pomoč pri preiskovanju in obvladovanju incidentov. Vpelje tudi pojem *pristojnih nacionalnih organov*, ki med seboj znotraj EU sodelujejo v *Skupini za sodelovanje*, odzivni centri pa v *Mreži skupin CSIRT*.

Bistvene storitve

Če smo v prejšnjem obdobju govorili o ***kritični infrastrukturi,* se pojem s to direktivo razširja na *bistvene storitve.*** Direktiva določa sedem sektorjev, v katerih mora vsaka država članica identificirati te storitve in njihovim izvajalcem predpisati nekatere ukrepe, ki bodo informacijsko varnost izboljšali. Sektorji bistvenih storitev po direktivi so: *energija, promet, bančništvo, infrastruktura finančnega trga, zdravstveni sektor, oskrba s pitno vodo in njena distribucija, ter digitalna infrastruktura*. ZInfV to razširi še z dvema sektorjema: *preskrbo s hrano* in *varstvo okolja*. Poleg tega direktiva predpisuje ukrepe tudi *ponudnikom digitalnih storitev*, ZInfV pa doda še *organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti*. Kategorije zavezancev se sicer v zakonu nekoliko drugače obravnavajo, na hitro pa bi lahko rekli, da morajo vsi narediti naslednje:

- določiti kontaktno osebo za informacijsko varnost,
- opraviti analizo tveganj,
- sprejeti ukrepe za preprečitev in zmanjšanje vpliva incidentov, ter
- priglasiti vse incidente, ki imajo pomemben vpliv na izvajanje bistvenih storitev.

V urejenem okolju, kjer obstaja zavedanje o pomenu informacijske varnosti, so prve tri točke nekako razumljive takorekoč same po sebi. Nova zahteva pa je obveznost poročanja o pomembnih incidentih za zavezance. Ti bodo prijave pošiljali na SI-CERT, razen državnih organov, za katere bo poskrbela novoustanovljena vladna CSIRT skupina. Kako se to razlikuje od stanja, ki smo ga imeli pred sprejemom zakona? Poglejmo nekoliko nazaj, da si osvežimo spomin.

Direktiva določa sedem sektorjev, v katerih mora vsaka država članica identificirati te storitve in njihovim izvajalcem predpisati nekatere ukrepe, ki bodo informacijsko varnost izboljšali.

*Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij
*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Okvir: Sektor digitalne infrastrukture in ponudniki digitalnih storitev

Imena lahko nekoliko zavedejo: sektor digitalne strukture po Direktivi NIS je omejen na natančno določene storitve: *stičišča omrežij, ponudnike storitev sistema domenskih imen* in *upravljalce registra domenskih imen najvišje ravni.* V Sloveniji to pomeni SIX (Slovenian Internet eXchange) in register vrhnje Register.si, ki tudi upravlja z vrhnjo strukturo sistema DNS. Oba delujeta v sklopu storitev nacionalnega pomena javnega zavoda Arnes, kjer se nahaja tudi SI-CERT. Ponudniki digitalnih storitev pa tudi niso kar vsi ponudniki gostovanja in operaterji, ampak le mala množica: *spletne tržnice, spletni iskalniki* in *storitve računalništva v oblaku.*

Poročanje o incidentih je bilo ves čas obstoja SI-CERT prostovoljno. Vedno smo se trudili pokazati, da prijavitelj s sporočanjem incidenta lahko le pridobi.

Zgodovina

SI-CERT je pričel z delovanjem jeseni 1995 znotraj javnega zavoda Arnes, po vzoru drugih evropskih odzivnih centrov, ki so se v večjih državah pričeli oblikovati v tistem obdobju. Na začetku je bilo delovanje osredotočeno na podporo sistemskim administratorjem, ki so skrbeli za strežnike na takrat mladem internetu. Informacije o ranljivostih niso bile tako dostopne, kot so danes, in v strežnike so vdirali bolj ali manj hekerji iz stereotipov. Sledilo je obdobje črvov in IRC vojn na prelomu tisočletja, potem pa lahko rečemo, da so se prebudile vlade nekaterih držav in internet prepoznale kot orodje za dosego ciljev v mednarodni politiki. Od tedaj poznamo pojma *APT* (Advanced Persistent Threat) in *državno-podprte napade* (state-sponsored attack). Danes se pogovori vrtijo okrog *interneta stvari* in *SCADA* sistemov.

Že zelo zgodaj (primer Levjesrčni leta 1998) sta SI-CERT in slovenska Policija pričela sodelovati pri preiskovanju računalniškega kriminala. Če je bilo na začetku še nekaj nejasnosti okrog razdelitve vlog, danes teče sodelovanje gladko, tako kot tudi redna izmenjava praktičnih izkušenj med SI-CERT in Centrom za računalniško preiskovanje GPU MNZ. Na mednarodnem področju je SI-CERT že leta 1996 sodeloval pri EuroCERT mednarodnem projek-

tu, nato pa smo bili zelo aktivni tudi v skupini evropskih CERT centrov, ki sem ji tudi predsedoval med leti 2000 in 2008.

Leta 2010 je bil podpisan sporazum med Ministrstvom za javno upravo in SI-CERT, s katerim je slednji prevzel obravnavo incidentov v sistemih državne uprave, ter pomagal pri vzpostavljanju posebne "vladne CERT skupine", SIGOV-CERT, ki bo uradno pričel z delovanjem 1. 1. 2019. Nekaj let kasneje je bila podpisana tudi pogodba med SI-CERT in Ministrstvom za obrambo, po kateri je SI-CERT opravljal šestmesečna usposabljanja pripadnikov Slovenske vojske, ki naj bi nadaljevali z delom v kapacitetah za odzivanje SV in MORS. Vmes je SI-CERT prevzel tudi operativno preiskovanje incidentov, ki so jih dolžni po Zakonu o elektronskih komunikacijah operaterji poročati Agenciji za komunikacijska omrežja in storitve (AKOS), ter zagnal nacionalni program ozaveščanja širše javnosti na področju informacijske varnosti, *Varni na internetu*. Od leta 2012 naprej pa sodelujemo na evropskih vajah kibernetske varnosti Cyber Europe (v organizaciji agencije ENISA) in vajah Cyber Coalition zveze NATO.

Danes je SI-CERT umeščen v sektor za nacionalno internet infrastrukturo javnega zavoda Arnes, z Zakonom o informacijski varnosti pa je nedvoumno določen kot nacionalna CSIRT skupina Slovenije.

Obvezno poročanje

Poročanje o incidentih je bilo ves čas obstoja SI-CERT prostovoljno. Vedno smo se trudili pokazati, da prijavitelj s sporočanjem incidenta lahko le pridobi. Če malo raztegnem tisto znano analogijo z gasilci, ki jo vedno uporabim na predavanjih: vedno lahko poskusite požar pogasiti sami in v nekaterih primerih boste tudi povsem uspešni. Predvsem takrat, ko bo šlo za manjše incidente. Kadar pa bo v omrežnem napadu sodelovala naprednejša škodljiva koda ali pa boste potrebovali usklajeno sodelovanje v tujini, pa potrebujete znanje in povezave, ki jih nudi CSIRT.

Direktiva NIS izhaja iz predpostavke, da se v naštetih sektorjih nahajajo izvajalci bistvenih storitev, ki še niso sprejeli vseh nujnih ukrepov za izboljšanje svoje informacijske varnosti. Želi jih "poriniti" v pravo smer in jih povezati s CSIRT skupinami, to sodelovanje pa bo s primernim pristopom čez nekaj let lahko pokazalo napredek pri obravnavi incidentov. Zraven bodo nacionalne CSIRT skupine lahko sestavljale sliko zavedanja o stanju (angl. situational awareness) ter izboljšale izmenjavo informacij o incidentih med državami članicami. Del tega načrta je tudi obvezno poročanje o incidentih.

Kaj še manjka zakonu

Že med pripravo zakona je bilo na mizi več različnih idej o tem, kako urediti sistem odzivanja na incidente v državi in kam umestiti *strateški organ*, ki ga predvideva tudi Strategija kibernetske varnosti RS, sprejeta februarja 2016. Trenutna rešitev, kjer to vlogo prevzema do 1. 1. 2020 Urad





vlade RS za varovanje tajnih podatkov (UVTP), nato pa se bo njegov del preselil pod Ministrstvo za javno upravo kot Uprava za kibernetsko varnost, je res nenavadna. Morda bomo kmalu morali dodatno premisliti to rešitev in najti bolj učinkovito. Je pa to odvisno od politične volje in tudi zavedanja vrha politike o pomembnosti kibernetske varnosti.

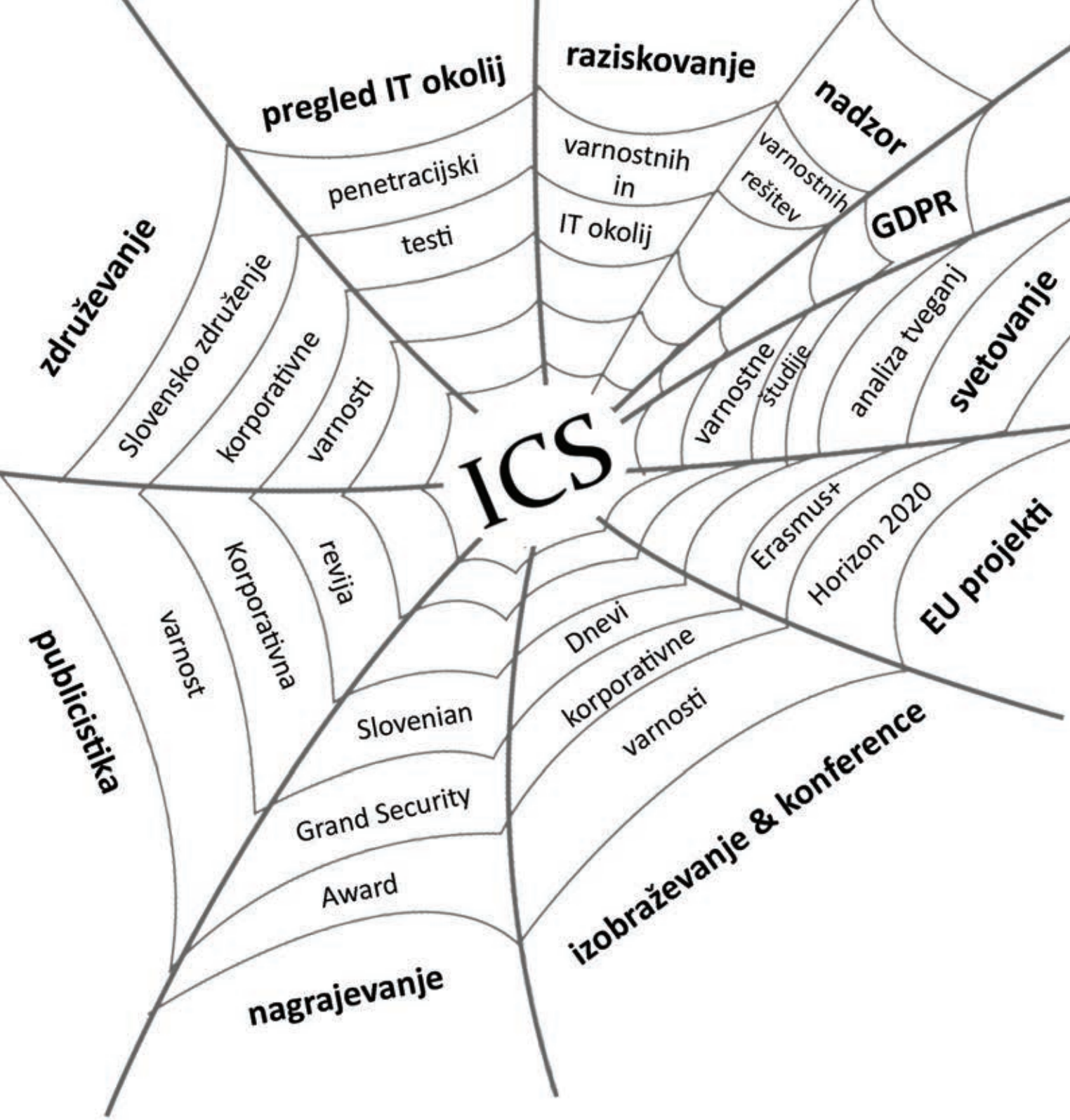
Osebno mi je žal tudi, da v zakon nismo uspeli spraviti člena, ki bi opredeljeval temo odgovornega razkrivanja ranljivosti. Čeprav seveda specialni zakon ne bi mogel razvrednotiti določil Kazenskega zakonika RS (in tega sploh ne bi želeli), bi lahko dal pomembna vodila tožilcem in sodiščem v primerih, ko gre za odgovorno razkritje. To bi lahko bil prvi korak pri ureditvi področja, žal pa je ta priložnost zamujena.

In še odgovor

Že pri prvih osnutkih zakona, skozi medresorsko usklajevanje, pa tudi po sprejemu zakona (nenazadnje tudi v tej reviji), smo lahko poslušali različne pripombe nad delovanjem SI-CERT s strani posameznikov, ki jih sicer prej nismo imeli priložnosti videti (in še manj poslušati) na strokovnih srečanjih. Ti so celotno področje opazovali zgolj skozi prizmo nacionalne varnosti in vojaškega delovanja v kibernetskem prostoru, zraven pa zanemarili množico težav, s katerimi se borijo podjetja in posamezniki, od kraj identitete, phishinga, do izsiljevalskih virusov. Kako le ne bi, saj so bili popolnoma novi v tej sferi. Pripombe so bile vedno splošne narave in nikoli nismo našli očitka na naše konkretno delovanje, kazale pa so včasih prav osupljivo pomanjkanje znanja.

Kako recimo odgovoriti očitkom, da ne bomo sposobni borbe proti kibernetskemu kriminalu, ko konkretni primeri sodelovanja z organi pregona skozi leta kažejo prav nasprotno, ko sodelujemo v projektih Europola in nam je zahvalo za sodelovanje izrekel tudi direktor ameriškega zveznega preiskovalnega organa FBI? Da ne moremo biti del sistema za odzivanje države, ko svoje znanje demonstriramo vsako leto na vajah iz kibernetske varnosti, ob ciljanih napadih na državno infrastrukturo in zaposlene v državni upravi pa s konkretnim delovanjem kažemo našo usposobljenost? Kako odgovoriti vojaku, ko se na lepem pojavi in zatrdi, da mora vse biti drugače, zraven pa ne ve, da smo iz vrha zveze NATO (kot verjetno eni redkih v državi) dobili priznanje za vzorno delovanje in priporočilo državi, naj gradi na tej dobri praksi? Ko zraven isti ljudje odločno trdijo, da problem odgovornega razkrivanja ne obstaja in da naj se vsi primeri lepo prijavijo kar policiji, zraven pa niti ne vedo, da smo tudi pri nas že imeli par okroglih miz na to temo?

Ne gre drugače, kot da upamo in verjamemo v to, da sistem odločanja v naši državi konec koncev vseeno upošteva ustrezne strokovne podlage in dokazane dobre prakse in da ne bomo deležni nespametnih rokohitrskih sprememb sistema, ki lahko v nekaj dneh ogrozi tisto, kar smo gradili desetletja. ■



ICS

INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE
CESTA ANDREJA BITENCA 68, LJUBLJANA
WWW.ICS-INSTITUT.SI

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Božidar Dajčman, direktor Sektorja za upravljanje fizične in informacijske varnosti, NKBM d.d.*

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

Bančni sektor je vseskozi izpostavljen celemu nizu varnostnih tveganj v poslovnem okolju, kar pred njega postavlja pomembno zahtevo po stalnem prilagajanju varnostnih procesov. Kako se z varnostnimi izzivi soočajo v NKBM, smo se pogovarjali z g. Božidarjem Dajčmanom.

NKBM predstavlja pomembno finančno institucijo v Republiki Sloveniji. Kateri so tisti ključni izzivi na področju varnostnih tveganj s katerimi se trenutno srečuje bančni sektor?

V bančnem sektorju varnostnih izzivov ne primanjkuje. Čeprav smo z eno nogo že v drugem, digitalno transformiranem svetu, nas redno ogrožajo tudi stoletja stare oblike kriminala, kot so ropi poslovalnic. Celovitih podatkov nimam, za slovenske banke pa si upam oceniti, da je bilo v zadnjih petih letih več izgub s klasičnimi prevarami ter odtujitvijo gotovine, kot s kibernetskimi napadi.

Po drugi strani med kolegi, ki se ukvarjamo z varnostjo v bankah, prevladuje mnenje, da grožnje kibernetske varnosti visijo nad nami kot Damoklejev meč, ki bo prej ali slej močno udaril po kakšni izmed slovenskih bank. Škoda, povzročena s takim napadom, bi bila lahko tudi znatno večja od tiste pri razvpitem ropu sefov leta 2005.

Poleg tveganja za nastanek varnostnih incidentov moramo upoštevati tudi vidik skladnosti z zakonodajo in zahtevami regulatorjev. V zadnjem času najbolj odmeva splošna uredba o varstvu podatkov (GDPR), ki velja od maja letos in med drugim predpisuje visoke kazni za primere, ko so osebni podatki nezadostno varovani. Zaradi te uredbe banke in druge organizacije nadgrajujejo svoje varnostne mehanizme za preprečevanje odtekanja podatkov.

Poseben poslovni in varnostni izziv za banke je direktiva o plačilnih storitvah PSD2, ki spodbuja, da na trg plačilnih storitev vstopajo nebančna podjetja, tudi velikani, kot so Apple, Amazon, Google in Facebook. Koncept odpiranja bank navzven pomeni večjo izpostavljenost podatkov o naših strankah zunanjemu svetu in prinaša dodatna tveganja. Direktiva predpisuje tudi določene varnostne ukrepe, ki jih bomo morali izvajati.

Vodite sektor za upravljanje fizične in informacijske varnosti, ki je že zaradi svojega poslanstva povezan s ključnimi procesi obvladovanja tveganj v

Če imamo ustrezno zavedanje na nivoju uprave, je to dober temelj za postopno izgradnjo varnostne kulture v organizaciji.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Izhodiščna lastnost za upravljanje varnosti je nesporna osebna integriteta in etika. Človek, ki etični kodeks organizacije sprejema zaradi prisile, ali kot nekaj nenaravnega, ni primeren za delo na področju varnosti.

organizaciji. Kako se s stališča strateškega managerja spopadate z uravnoteženjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj na področjih fizične in informacijske varnosti?

Poslanstvo našega sektorja je učinkovito zagotavljanje varnosti zaposlenih in naših strank, varovanje informacij in drugega premoženja banke ter zagotavljanje njenega neprekinjenega poslovanja. Znotraj tega okvirja več pozornosti in virov namenjamo točkam, kjer je tveganje višje. Pri tem sta področji fizične in informacijske varnosti obravnavani enakovredno.

Katere osebnostne in strokovne kompetence bi posebej izpostavili kot potrebo za dobrega strateškega korporativno varnostnega managerja?

Izhodiščna lastnost za upravljanje varnosti je nesporna osebna integriteta in etika. Človek, ki etični kodeks organizacije sprejema zaradi prisile, ali kot nekaj nenaravnega, ni primeren za delo na področju varnosti.

Pri strokovnih kompetencah so možni kompromisi. Ko sem pred petimi leti začenjal kariero na področju varnosti (šlo je za vodenje področja informacijske varnosti), sem imel z delodajalci in njihovimi tujimi lastniki zanimiv telekonferenčni intervju. Zastavili so mi tri praktične naloge, s katerimi so preverjali tri različne kompetence. Najprej so strokovno znanje s področja varnostnih rešitev preverili z nalogo, kjer sem moral predlagati arhitekturo za varnostno občutljivo informacijsko rešitev, potem so preverili sposobnost hitrega razmišljanja v primeru, ko je v teku incident in je potrebno predlagati ukrepe. V tretji nalogi je bilo potrebno prikazati, kako bi strokovno zapleteno temo predstavil najvišjemu vodstvu, ki praviloma ne pozna podrobnosti stroke, vendar potrebuje prave informacije za odločanje.

Zahtevali so torej poznavanje področja, dobro logično sklepanje ter sposobnost predstavljanja strokovnih tem laikom. Po svojih sedanjih kriterijih se nisem odrezal ravno briljantno, vendar je bilo v dani situaciji dovolj.

Navedene kompetence so res potrebne za managerja varnosti, vendar se lahko glede strokovnih kompetenc dopolnjujemo znotraj ekipe in z zunanjimi sodelavci, saj ni realno, da bi bilo vso potrebno znanje in spretnosti združene v eni osebi.

Vedno več storitev bančne institucije izvajajo v tesni povezavi z informacijsko komunikacijsko tehnologijo. Kako se lotevate obvladovanja tveganj, ki jih prinaša moderno kibernetsko okolje?

Banka je po naravi svojega posla organizacija, ki upravlja tveganje, zato je v bankah dovolj strokovnjakov, ki znajo ocenjevati tveganja in ukrepe za njihovo

znižanje. Ob krizi, ki smo jo doživeli pred desetletjem, se je žal pokazalo, da mnoge banke niso obvladovale kreditnih tveganj.

Upam, da se kaj podobnega ne bo zgodilo na področju kibernetskih tveganj. Tudi za kibernetsko varnost velja izrek Warrena Buffetta, da šele ob oseki vidimo, kdo je plaval brez kopalk.

V naši banki se ob podpori uprave sistematsko trudimo, da se črnim scenarijem izognemo.

Pri kibernetskih tveganjih si težko pomagamo s statističnimi modeli, ker ni na voljo dovolj podatkov, zato smo bolj odvisni od ocen čez palec in drugih metod, kot so npr. penetracijski testi. Najprej pa moramo poskrbeti za osnovno varnostno higieno, ki jo za naše potrebe primerno določa standard ISO/IEC 27001.

Imamo majhno vendar močno ekipo, ki mora ves čas podrobno spremljati razvoj na področju ranljivosti, groženj in varnostnih rešitev. Hkrati moramo razumeti tudi splošne trende na področju informatike in bančnega poslovanja.

V Slovenskem okolju do nedavno ni bila ravno praksa, da sta procesa fizične in informacijske varnosti združena v okrilju enotne službe, ki se strateško ukvarja s korporativno varnostjo. Kateri so po vašem prepričanju tisi dejavniki, ki so pripeljali do tega spoznanja, da informacijska varnost ne more biti del službe za informatiko?

Dobro poznam organiziranost varnosti v bankah, precej slabše pa v drugih organizacijah. Pri kakšni manjši banki se še najde vodja informacijske varnosti znotraj IT-ja, sicer pa je to preživet koncept, ki bo dokončno pokopan v kratkem, ko bo regulator z uredbo izrecno zahteval ločitev te funkcije od enot, ki jih nadzira - to pa je v prvi vrsti ravno IT.

Drugo vprašanje je, ali naj bodo v eni organizacijski enoti združeni informacijska varnost, fizična varnost, neprekinjeno poslovanje, odkrivanje notranjih in zunanjih prevar in še kakšno sorodno področje. Tu so možne različne rešitve, v vsakem primeru pa se morajo te funkcije povezovati vsaj matrično, če že hierarhično niso pod istim vodjem.

Pri nas združujemo fizično in informacijsko varnost ter zagotavljanje neprekinjenega poslovanja in skupaj delujemo zelo dobro. Velikokrat se področja med seboj



prepletajo. Dober primer je definiranje pravil in postopkov za upravljanje v krizni situaciji, kjer se srečajo vsa tri področja.

Ne glede na znanje in voljo, nam ne bi uspevalo brez dobrega sodelovanja z enotami, ki se ukvarjajo z informacijsko tehnologijo, digitalnimi storitvami, strateškim obvladovanjem tveganj, skladnostjo poslovanja, notranjo revizijo in drugimi.

Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od slabše uspešnih. Kako v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka, zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Ni lahko. Fraza, ki pravi, da so ljudje najšibkejši člen v varnosti, je oguljena, vendar resnična. Na nižji stopnji zrelosti je zavedanje zaposlenih hvaležno področje za doseganje hitrih zmag, kasneje je za majhne učinke potrebno vlagati veliko.

Če imamo ustrezno zavedanje na nivoju uprave, je to dober temelj za postopno izgradnjo varnostne kulture v organizaciji. Uporabljamo tako metode, ki v kratkem času dosežejo vse zaposlene (npr. e-učenje), kot tiste, ki zahtevajo več časa in so prilagojene posameznemu okolju (npr. obisk v poslovalnici).

Ne moremo si privoščiti, da bi zaposleni razumeli pomen varnosti šele, ko se zgodijo incidenti.

Združenje je zame pomembno kot stična točka, kjer se srečamo posamezniki, ki si želimo izmenjavati znanje in izkušnje, nedvomno pa združenje pozitivno prispeva tudi k razvoju korporativne varnosti kot stroke.

Nezadovoljni zaposleni lahko hitro postanejo tudi varnostni problem. Kako nameravate v prihodnje upravljati ta pričakovanja zaposlenih in vedno večji pritisk lastnikov na zmanjšanje stroškov dela?

Smernice Banke Slovenije narekujejo konsolidacijo bančnega sistema, saj se je bilančna vsota bank v zadnjih desetih letih iz prek 50 milijard zmanjšala na 40 mlrd. evrov, ena od posledic je zmanjševanje števila zaposlenih. Gre za proces, ki v večini bank traja že več kot pet let. Ob tem se bančništvo spreminja, digitalizira, vse bolj je v uporabi spletno bančništvo. Spremembe so tako za zaposlene, kot tudi stranke, v številnih primerih neprijetne, toda spremembe prinašajo tudi prednosti tako zaposlenim kot komitentom. Premoženje in informacije moramo v vsakršnih razmerah varovati tako, da so čimbolj varne pred zlonamernimi posamezniki, kar velja tudi za tiste, ki smo v banki zaposleni. Prav varnost je eden od segmentov, kjer so spremembe in prilagajanje na zahtevno okolje nujne. In v Novi KBM želimo pri tem slediti najboljšim praksam v panogi.

Kripto valute vedno bolj prodirajo v plačilne sisteme moderne družbe. Menite, da lahko njihova uporaba predstavlja določene varnostne izzive za bančni sektor?

Za banke kripto valute same po sebi ne predstavljajo ne poslovne ne varnostne grožnje.

Je pa uporabnost kripto valut kot plačilnega sredstva za izsiljevanje povzročila pravi val kripto virusov, oz. izsiljevalskih virusov. Ti povzročijo šifriranje podatkov, potem pa ponujajo dešifriranje za plačilo v kripto valuti. Ta vrsta virusov je očitno tako uspešna, da so druge vrste napadov začasno kar nekoliko usahnile, vključno s trojanskimi konji za uporabnike spletnih bank.

Banke imajo praviloma dobro urejeno varnostno kopiranje podatkov, zato niso izrazito občutljive na napade s kripto virusi.

Kako vidite vlogo Slovenskega združenja za korporativno varnost katerega korporativni člani ste v NKBM? Menite, da je to združevanje v Sloveniji prineslo pozitivne spremembe na področju korporativne varnosti?



Pri dosedanjem delu na področju varnosti in na drugih področjih sem se veliko naučil od kolegov iz drugih podjetij. Tudi, če smo na trgu konkurenca, smo zavezniki pri zagotavljanju varnosti in preprečevanju kriminala.

Združenje je zame pomembno kot stična točka, kjer se srečamo posamezniki, ki si želimo izmenjavati znanje in izkušnje, nedvomno pa združenje pozitivno prispeva tudi k razvoju korporativne varnosti kot stroke. ■



Vodilno globalno podjetje na področju varovanja

Dahua Technology se uvršča med vodilna podjetja na področju rešitev za videonadzorne sisteme.

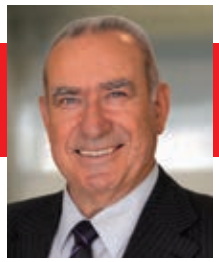
Zaposljuje več kod 13,000 ljudi na globalnem področju. Njene rešitve so v uporabi v več kot 180 državah.

CE FC RoHS ISO 9001:2000

www.dahuasecurity.com

DAHUA TECHNOLOGY
Cesta na Okroglo 7, 4202 Naklo, Slovenija
www.dahuasecurity.com

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





UPRAVLJANJE TVEGANJ V KRITIČNI INFRASTRUKTURI

Glavni namen tega prispevka je, da v okviru poslovnih, varnostnih, demografskih, globalnih in drugih izzivov, ki spremljajo kritično infrastrukturo, prispevamo nekaj misli, usmeritev in rešitev za celovito upravljanje tveganj in zagotavljanje neprekinjenega delovanja gospodarskih, javnih, državnih in drugih organizacij, ki upravljajo s kritično infrastrukturo. Kajti oboje, tako upravljanje tveganj kot tudi neprekinjeno delovanje, sta po najinih izkušnjah šibki točki v sistemu delovanja in razvoja kritične infrastrukture. Pristop k temu problemu je nakazan v prikazani shemi.

Metodološke podlage

Pri izdelavi prikazane sheme sistema upravljanja tveganj v sektorjih kritične infrastrukture (sektor energetike, sektor prometa, sektor prehrane, sektor preskrbe s pitno vodo, sektor zdravstva, sektor financ, sektor informacijsko-komunikacijskih omrežij, sektor varovanja okolja), sva izhajala iz metodoloških, pravnih in strokovnih podlag opisanih v nadaljevanju prispevka.

Metodološki okvir za upravljanje s tveganji je zelo širok. Iz številnih modelov in metod predlagava naslednji izbor: COSO (ERM), MOSAR, FMEA, COBIT, BIA, Delphy, model Andersen in še nekatere druge metode in modele, ki omogočajo snovanje osnovnega metodološkega skeleta za upravljanje tveganj v kritični infrastrukturi. Vse bolj pa se v praksi upravljanja tveganj poleg modelov in metod uveljavljajo standardi za upravljanje tveganj (ISO 31000:2018, ISO/IEC 31010:2018, ISO Guide 73:2009, ISO/IEC 51:2014, ISO/TC 262:2011) kot izredno pomembno orodje za upravljanje tveganj v gospodarskih in drugih družbah, ki upravljajo s kritično infrastrukturo. Ob teh standardih je nujno upoštevati še obvezne varnostne standarde na področju zasebnega varovanja (Odredba o določitvi standardov, ki so obvezni na področju zasebnega varovanja), varnosti in zdravja pri delu (OHSAS18000), varstva pred požari, varstva okolja, varnosti in sledljivosti živil (HACCP), neprekinjenega poslovanja (ISO 22301) in na področju varovanja informacij (ISO/IEC 27000). Uporaba navedenih standardov omogoča še bolj celovito in poglobljeno obvladovanje izrednih dogodkov, groženj in tveganj ter vzpostavitev zanesljivega in učinkovitega sistema neprekinjenega poslovanja in kriznega vodenja.

> Za pravilen pristop k celovitemu ocenjevanju tveganj je treba najprej izdelati, sprejeti in implementirati vladno politiko korporativnega upravljanja kritične infrastrukture in v tej politiki nakazati in v procese upravljanja ustrezno umestiti sistem in proces upravljanja tveganj.

Pravne podlage

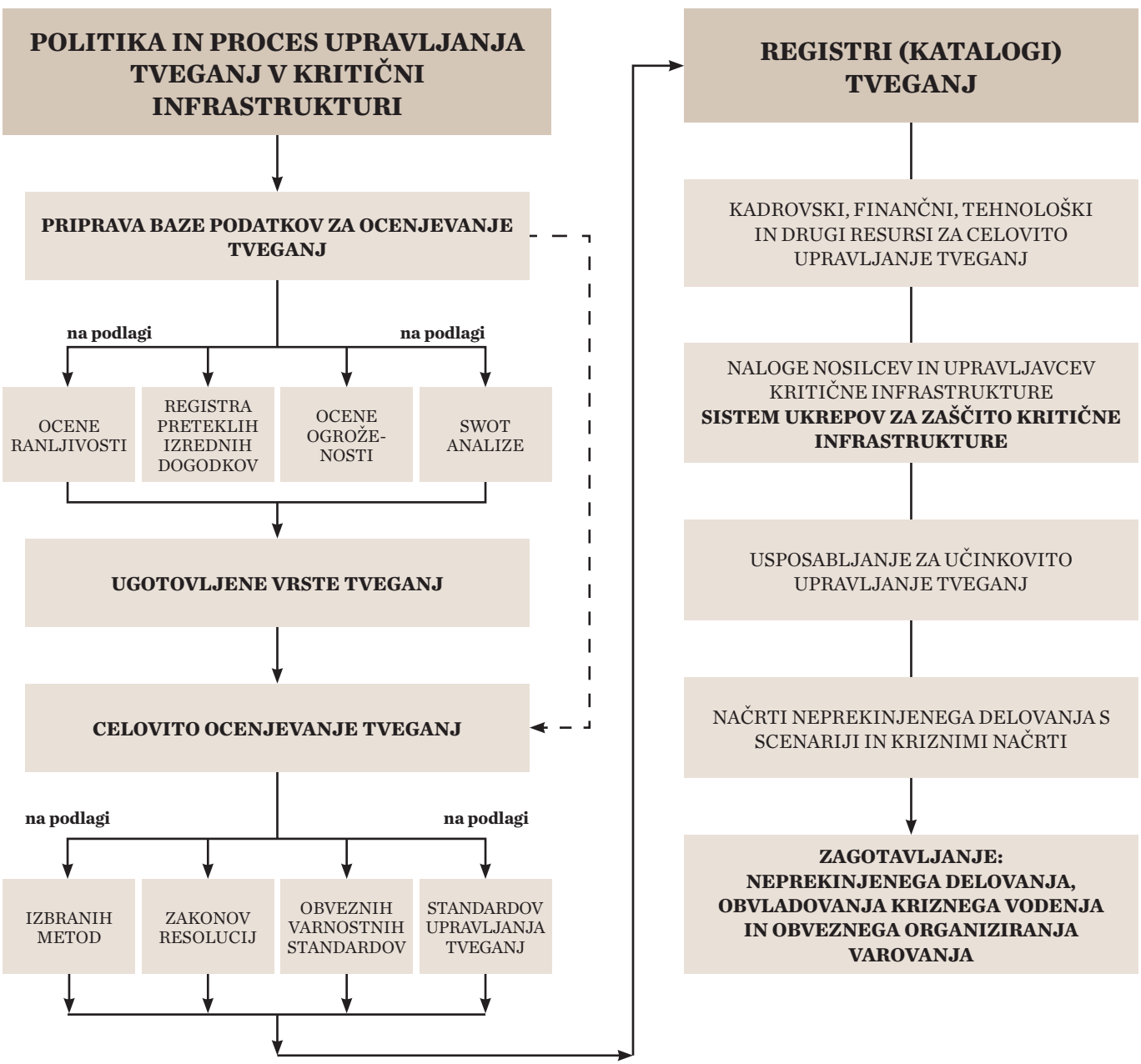
Osnova so pravne podlage za organiziranje, delovanje in razvoj kritične infrastrukture (smernice, uredbe, zakoni, podzakonski akti, resolucije idr.) tako na nivoju Evropske unije, kot tudi na nivoju države. Na nivoju države izpostaviva predvsem naslednjo zakonsko podlago: Zakon o kritični infrastrukturi, Zakon o gospodarskih družbah, Zakon o varstvu pred naravnimi in drugimi nesrečami, Zakon o varstvu okolja, Energetski zakon, Zakon o varnosti in zdravju pri delu, Zakon o varstvu pred požari, Zakon o informacijski varnosti, Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih, Zakon o zasebnem varovanju, Zakon o nevarnih snoveh, vnetljivih

*avtorja sta člana Slovenskega združenja korporativne varnosti

tekočinah, plinih ter drugih nevarnih snoveh, Zakon o kemikalijah in še nekateri drugi zakoni, ki se nanašajo na izvajanje dejavnosti v kritični infrastrukturi.

Strokovne podlage

V kritični infrastrukturi je bilo doslej izvedenih nekaj deset projektov, raziskav, študij in analiz v okviru katerih je bila proučevana ranljivost, ogroženost, tveganja in urejenost sistema upravljanja s tveganji, neprekinjenega delovanja in kriznega vodenja. Najina dognanja in spoznanja so take narave, da je kritični infrastrukturi namenjeno premalo pozornosti glede njene ranljivosti, ogroženosti in novih poslovnih in varnostnih izzivov ter prizadevanj za višjo stopnjo načrtnosti, organiziranosti in usklajenosti posameznih področij upravljanja s tveganji in neprekinjenega delovanja. V tem kontekstu si več pozornosti zasluži tudi krepitev konkurenčnosti naše kritične infrastrukture in skrb za zaščito informacijsko komunikacijskih sistemov, denimo z uporabo poslovnih orodij kot so Benchmarking, Business intelligence in sistem uravnoteženih kazalnikov BSC. V ta krog sodi tudi vzpostavitev sistemov šifriranja elektronskih sporočil zoper globalna tveganja prisluškovanja in prestrezanja občutljivih poslovnih informacij, ki se z elektronskim komuniciranjem pretakajo skozi sistem satelitskih navigacij.



Shema: Metodološko vsebinski pristop za vzpostavitev sistema upravljanja tveganj v kritični infrastrukturi (M. in M. Vrsec, 2018)



11. člen Zakona o kritični infrastrukturi (ZKI) določa, da dokumente načrtovanja zaščite kritične infrastrukture sestavljata dva dokumenta in sicer: Ocena tveganj in Ukrepi za zaščito kritične infrastrukture. V tem prispevku se ukvarjava samo z oceno tveganj in z zagotavljanjem neprekinjenega delovanja, katerega sestavni del je tudi ocenjevanje tveganj. Sistem ukrepov za zaščito kritične infrastrukture predstavlja izjemno širok vsebinski okvir, zato si zasluži posebno obravnavo. Nujno izhodišče za pripravo teh ukrepov pa je seveda poglobljena ocena vseh vrst tveganj v sektorjih kritične infrastrukture.

Za pravilen pristop k celovitemu ocenjevanju tveganj je treba najprej izdelati, sprejeti in implementirati vladno politiko korporativnega upravljanja kritične infrastrukture in v tej politiki nakazati in v procese upravljanja ustrezno umestiti sistem in proces upravljanja tveganj. Sledi priprava baze podatkov, ki so podvrženi ocenam in analizam tako, da je možno razkriti in ugotoviti vse vrste tveganj, tudi z ugotovitvijo specifičnih tveganj, ki so edinstvena za posamezne sektorje kritične infrastrukture. Ko imamo izdelano jasno sliko o ugotovljenih vrstah tveganj, se lotimo celovitega ocenjevanja tveganj, ki je podlaga za določitev stopenj tveganj in pripravo registra oziroma kataloga tveganj z vsemi potrebnimi elementi. Preden se lotimo ocenjevanja tveganj je ključnega pomena izbrati ustrezne kadrovske resurse, ki so kompetentni, imajo ustrezna znanja, izkušnje in sposobnosti in so tudi ustrezno umeščeni v organizacijsko strukturo organizacije, da lahko nemoteno in strokovno izvajajo vse potrebne aktivnosti v procesu izdelave ocene tveganj. Ob tej priliki naj izpostaviva tudi pomembnost zavedanja širine pristopa k izdelavi ocene tveganj, ki mora zajemati tako globalni, kot tudi lokalni vidik in mora v fazi ocenjevanja tveganj vključevati tudi vse strateške partnerje posameznega upravljavca kritične infrastrukture (strateške kupce, dobavitelje, inštitucije ipd.), ki so prav tako dolžni zagotavljati neprekinjeno delovanje in se vključevati v krizno vodenje v primeru pojava izrednih dogodkov in kriznih razmer.

Ko je ocenjevalni del v sistemu upravljanja tveganj (levi del zgornje sheme) dokumentiran, lastniki in upravljavci - ob pomoči nosilcev KI - zagotovijo potrebni organizacijski okvir, finančne, tehnološke in kadrovske resurse ter varnostne in nadzorne mehanizme za celovito (operativno) obvladovanje in upravljanje tveganj. To pa še ni zadostni pogoj za celovito obvladovanje in upravljanje tveganj na ravni upravljavcev kritične infrastrukture, saj je treba na podlagi ocene tveganj izdelati načrt ukrepov in vzpostaviti sistem izvajanja ukrepov za zaščito kritične infrastrukture. Vse to pa seveda ne gre brez usposobljenih in motiviranih človeških virov. Na podlagi vnaprej določenih programov izobraževanj in usposabljanj je torej potrebno usposobiti tiste, ki so v prvi liniji odgovorni za obvladovanje in upravljanje tveganj, vzporedno s tem pa še podati ustrezne informacije vsem zaposlenim, poslovnim partnerjem in pogodbenim izvajalcem, da v poslovnih procesih in vsak v svojem poslovnem in delovnem okolju pričakovano in v zadostni meri prispeva k obvladovanju tveganj. To pomeni, da nosilci kritične infrastrukture, pri sebi in pri upravljavcih kritične infrastrukture, najprej vzpostavijo proces usposabljanja odgovornih za obvladovanje in upravljanje tveganj, ki ga koordinira Ministrstvo za obrambo. Krona obvladovanja in upravljana tveganj pa je načrtovanje in izvajanje neprekinjenega delovanja gospodarskih družb, ki upravljajo s kritično infrastrukturo. Pri tem je ključnega pomena

pripravljenost na hitro in strokovno odzivanje na izredne dogodke ter pripravljenost (vaje na podlagi scenarijev) na razreševanje verjetnih kriznih situacij. Da bi se zagotovil čim bolj enoten in primerljiv pristop k obvladovanju neprekinjenega delovanja gospodarskih in drugih družb, zavodov in državnih organov, je priporočljivo uporabiti standarde za vzpostavljanje neprekinjenega delovanja kot so ISO 22301, ISO/IEC 27001 in 27005, ob tem pa še standarde obvladovanja tveganj ISO 31000 in ISO/IEC 31010. Tak pristop na eni strani terja nekaj več znanja in nekaj več sredstev, na drugi strani, pa zagotavlja učinkovitejše in uspešnejše upravljanje neprekinjenega delovanja ob nastanku izrednih dogodkov v morebitnih kriznih situacijah. Nosilci in upravljavci kritične infrastrukture se morajo namreč zavedati polne odgovornosti za morebitne napake, malomarnosti, slabih in pomanjkljivih ocen tveganj ter neustreznih in neučinkovitih ukrepov za zaščito kritične infrastrukture, ki lahko ohromi ali onemogoči delovanje celega sektorja in/ali določene gospodarske družbe, kar – z vidika soodvisnosti – lahko ohromi delovanje tudi drugih sektorjev, širšega gospodarstva, državnih in civilnih institucij ter prebivalstva.

V okviru zagotavljanja neprekinjenega delovanja in kriznega vodenja ter ocenjevanja tveganj izpostavljamo obvezno organiziranje varovanja, ki bi ga morale imeti vzpostavljenega vse gospodarske družbe, ki upravljajo s kritično infrastrukturo (zavezanci obveznega organiziranja varovanja) – konkretno denimo energetske in telekomunikacijske družbe, letališča, Luka Koper, zdravstvene, prometne in druge družbe, katerih dejavnosti so bistvene za delovanje ključnih družbenih funkcij, zdravje ter varnost in zaščito gospodarstva, civilne družbe in prebivalstva. Tudi po Zakonu o kritični infrastrukturi so gospodarske službe, ki upravljajo s kritično infrastrukturo zavezanci obveznega organiziranja varovanja (13. člen 6. točka ZKI). Torej morajo imeti izdelan načrt varovanja, ki poleg ocene stopnje tveganja vsebuje tudi program varovanja in načrt fizičnega varovanja.

Nosilci in upravljavci kritične infrastrukture se morajo namreč zavedati polne odgovornosti za morebitne napake, malomarnosti, slabih in pomanjkljivih ocen tveganj ter neustreznih in neučinkovitih ukrepov za zaščito kritične infrastrukture, ki lahko ohromi ali onemogoči delovanje celega sektorja in/ali določene gospodarske družbe, kar – z vidika soodvisnosti – lahko ohromi delovanje tudi drugih sektorjev, širšega gospodarstva, državnih in civilnih institucij ter prebivalstva.

Nujni koraki za prihodnost

Nekaj dokumentov za obvladovanje tveganj in neprekinjenega delovanja, ki kličejo po takojšnji izdelavi. Da bi stekel proces obvladovanja in upravljanja tveganj na strateški ravni (vladna raven in raven nosilcev KI) ter proces obvladovanja in upravljanja tveganj na ravni upravljavcev kritične infrastrukture, so pred kompetentnimi deležniki kritične infrastrukture naslednje naloge s ciljem izdelave naslednjih (nujnih) dokumentov, ki so:



- Vlada določi politiko korporativnega upravljanja kritične infrastrukture v kateri opredeli tudi določila o vzpostavitvi sistema upravljanja tveganj (17. člen ZKI);
- Ministrstvo za obrambo izdela politiko upravljanja tveganj, ki bo veljala in bo enotna za vse nosilce in vse upravljavce kritične infrastrukture;
- Ministrstvo za obrambo izdela navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture (12. člen ZKI), torej navodilo, ki bo enotno za vse sektorje kritične infrastrukture;
- Nosilci sektorjev kritične infrastrukture (ministrstva) izdelajo strokovne usmeritve za ocenjevanje tveganj v posameznih sektorjih in podsektorjih, v katerih delujejo določeni upravljavci kritične infrastrukture (12. člen ZKI);
- Upravljavci kritične infrastrukture najprej – na podlagi navodila in strokovnih usmeritev ter na podlagi lastnih ocen ranljivosti in ogroženosti ter SWOT analize - izdelajo oceno tveganj, na podlagi te ocene pa še ukrepe za zaščito lastne kritične infrastrukture (12, 13, 14, in 15. člen ZKI);
- Upravljavci kritične infrastrukture morajo zagotavljati neprekinjeno delovanje (3., 10. in 19. in 24. člen ZKI). V skladu s to zahtevo si morajo posamezni upravljavci kritične infrastrukture izdelati načrte neprekinjenega delovanja, katerega sestavni del je tudi krizni načrt z načrtom kriznega komuniciranja. Priporočamo neprekinjeno delovanje v skladu s standardom ISO 23001 in ISO/IEC 27005;
- Nosilci in upravljavci kritične infrastrukture določijo (imenujejo, op. avtorjev) kontaktno osebo ali več takih oseb za sodelovanje na področju kritične infrastrukture z drugimi upravljavci kritične infrastrukture, drugimi nosilci sektorjev kritične infrastrukture in Ministrstvom za obrambo (18. in 19. člen ZKI). Po naši presoji ne gre samo za sodelovanje, ki bi ga morale izvajati kontaktne osebe, temveč gre za odgovorne osebe, ki morajo obvladovati sistem upravljanja in obvladovanja tveganj na ravni nosilcev in na ravni upravljavcev kritične infrastrukture. Na ravni Ministrstva za obrambo je treba vzpostaviti neko organizacijsko obliko (denimo odbor za tveganja), ki bi ga sestavljale kontaktne osebe nosilcev kritične infrastrukture. Kajti tudi pri upravljanju tveganj je treba upoštevati medsebojno odvisnost sektorjev kritične infrastrukture.

Le v primeru, če bodo vsi nakazani dokumenti izdelani in implementirani v prakso, bomo lahko govorili, da ima kritična infrastruktura vzpostavljen učinkovit sistem obvladovanja in upravljanja tveganj in sistem neprekinjenega delovanja, tudi v kriznih okoliščinah.

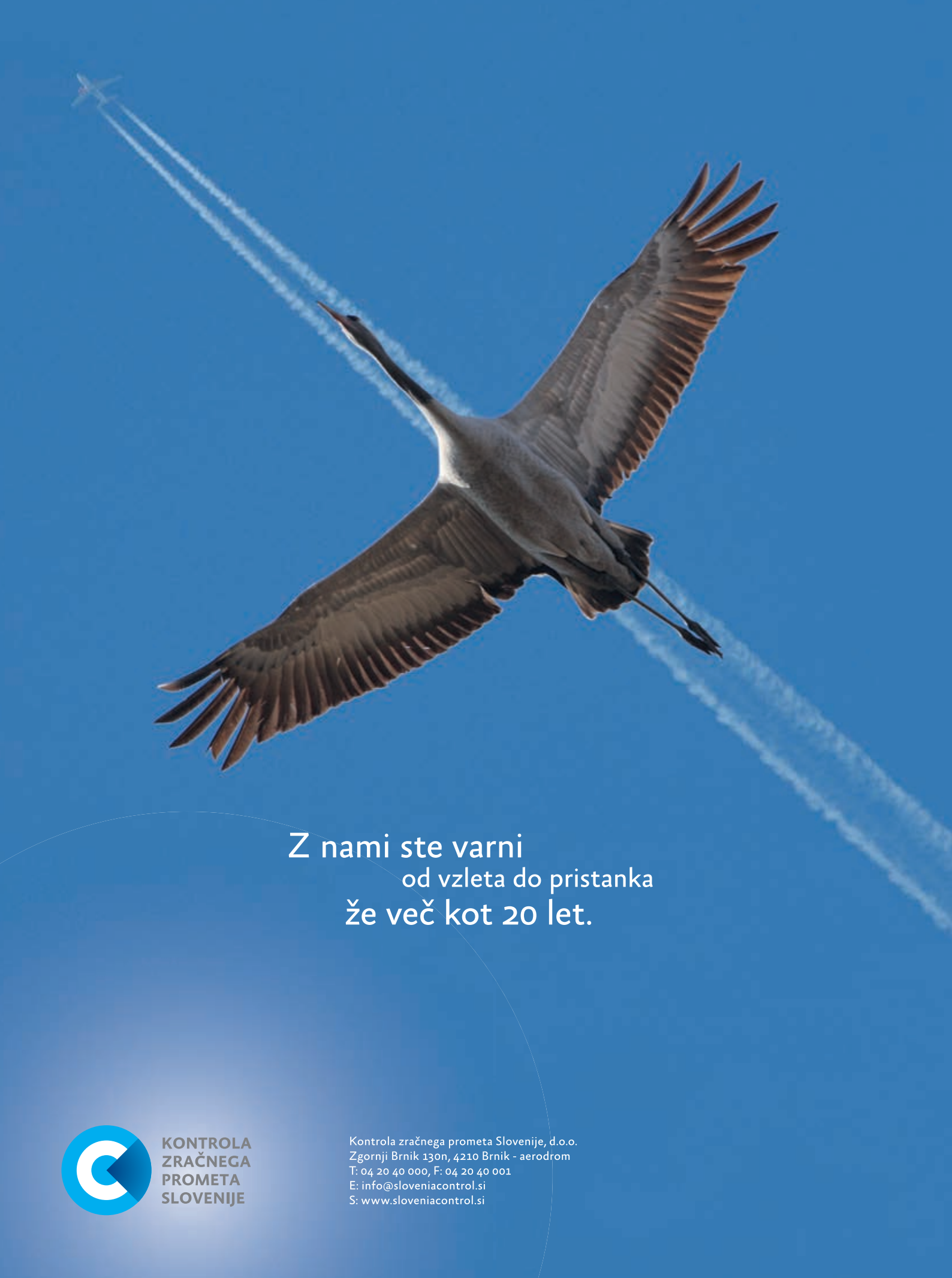


Zaključna misel

Vlada, kot strateški usmerjevalec delovanja in razvoja kritične infrastrukture, ter nosilci (ministrstva) in upravljavci (gospodarske in druge družbe) kritične infrastrukture, bi morali nameniti več pozornosti trajnostnemu upravljanju tveganj ter zagotavljanju neprekinjenega delovanja kot glavnima adutoma ohranjanja konkurenčnosti naše kritične infrastrukture nasproti kritičnim infrastrukturam sosednjih držav. Ta cilj kliče po tem, da bodo morali kompetentni v prihodnje na vseh ravneh narediti za (lastno) kritično infrastrukturo nekaj več kot doslej. Kliče tudi po tem, da bodo štele zasluge uspešnih razvojnih potez in nasprotno, iskala se bo tudi odgovornost za neobvladovanje tveganj, napak in stranpoti. Navsezadnje gre tudi za razvijanje višje ravni družbene odgovornosti nosilcev in upravljavcev kritične infrastrukture.

Glavni viri

- Modeli upravljanja s tveganji: COSO (ERM): 2018-Smernice za obvladovanje tveganj v korporativnem upravljanju podjetij, model MOSAR, model FMEA, model BIA in Model Andersen
- Projekti in raziskave v kritični infrastrukturi. Seznam projektov in raziskav je dostopen na Inštitutu za korporativne varnostne študije
- Resolucija o strategiji nacionalne varnosti Republike Slovenije in druge resolucije za posamezna področja (sektorje) kritične infrastrukture
- Sklep o določitvi nosilcev sektorjev kritične infrastrukture Republike Slovenije in z njimi sodelujočih državnih organov, Vlada, štev. sklepa 80200-1/2018/10, z dne 5. 7. 2018
- Standardi upravljanja tveganj: ISO 31000:2018, ISO/IEC 31010:2018, ISO Guide 73
- Standardi varovanja: ISO 14001, OHSAS 18000, HACCP, ISO/IEC 27000
- Standard neprekinjenega poslovanja ISO 23001
- Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture. Izvirna študija, 2018. Inštitut za korporativne varnostne študije, Ljubljana
- Vršec, Milan, Vršec Miran (2018). Načrti neprekinjenega poslovanja in krizni načrti v funkciji obvladovanja tveganj. Korporativna varnost, št. 17/2018.
- Zakon o kritični infrastrukturi, Ur.l.RS, št. 75/2017
- Zakon o informacijski varnosti, Ur.l.RS. št. 30/2018
- Zakon o zasebnem varovanju, Ur.l.RS, št. 17/2011, s podzakonskimi predpisi
- Zakonodaja, ki ureja: varstvo pred naravnimi in drugimi nesrečami, varstvo okolja, varnost in zdravje pri delu, varstvo pred požari, varnost živil, ter varstvo pred nevarnimi snovmi in kemikalijami s podzakonskimi predpisi ■



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: izr. prof. dr. Denis Čaleta, Institut za korporativne varnostne študije*



OCENJEVANJE TVEGANJ V KRITIČNI INFRASTRUKTURI – VPLIV IZOBRAŽEVALNEGA PROCESA NA KVALITETO IZVEDBE

Nujno je potrebno vzpostaviti ustrezno zavedanje, da je samo učinkovita ocena ogroženosti tista prava podlaga, za sprejemanje celovitih odločitev v procesu obvladovanja tveganj, za delovanje kritične infrastrukture. Postavlja pa se dilema ali bo za učinkovito izvajanje tega kompleksnega procesa dovolj samo ustrezno predpisana metodologija. Verjetno se strinjamo, da je to samo prvi korak, ki brez učinkovitega sistema izobraževanja neposrednih izvajalcev tega procesa v organizacijah, katere obvladujejo kritično infrastrukturo, ne bo dosegel željenega cilja.

Vpliv zaposlenega na delovanje kritične infrastrukture v sodobni državi je eden izmed najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanjo stalno nevarnost, ki je ne smemo podcenjevati. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile tehnološke in fizične sestavine kritične infrastrukture varnejše, po drugi strani pa, kako obravnavati zaposlenega pri upravljanju teh kompleksnih sistemov, saj ta postaja vse pomembnejši referent za njeno zanesljivo delovanje. Pri uveljavljanju skupnega pristopa na področju ocenjevanja tveganj, bo potrebno zagotoviti, da bodo strokovnjaki, kateri se bodo v okviru sektorjev kritične infrastrukture, in samih neposrednih upravljalcev kritične infrastrukture, ukvarjali s procesom analize tveganj, imeli določena predznanja s področja analiziranja tveganj. To pomeni, da bo potrebno za te strokovnjake izvesti različne oblike delavnic in usposabljanj, kjer se bodo v usposobili z metodološkim aparatom in procesi analiziranja tveganj, po predvidenem metodološkem pristopu.

Pri uveljavljanju skupnega pristopa na področju ocenjevanja tveganj, bo potrebno zagotoviti, da bodo strokovnjaki, kateri se bodo v okviru sektorjev kritične infrastrukture, in samih neposrednih upravljalcev kritične infrastrukture, ukvarjali s procesom analize tveganj, imeli določena predznanja s področja analiziranja tveganj.

Proces bo potrebno v organizacijah izvajati kot kontinuirano aktivnost, ki bo del celotnega procesa zagotavljanja neprekinjenosti delovanja kritične infrastrukture v Republiki Sloveniji. Še posebej velja poudariti, da je potrebno zaščito kritične infrastrukture in procese analiziranja tveganj, za delovanje le te, umestiti v celovit proces zagotavljanja neprekinjenosti delovanja ključnih nacionalnih sistemov in učinkovito krizno upravljanje v Republiki Sloveniji.

*avtor je član Slovenskega združenja korporativne varnosti



Usposabljanje za obvladovanje tveganj v kritični infrastrukturi

Ministrstvo za obrambo je v letu 2017 in 2018, v okviru evropskega projekta PROPU[1], izdelalo Predlog programa usposabljanja upravljavcev kritične infrastrukture. V zaključnem delu tega programa so predstavljeni predlogi usposabljanja za zaščito kritične infrastrukture z naborom potrebnih znanj. Navedeno je, da predlogi usposabljanja izhajajo iz prepoznanih tveganj za delovanje kritične infrastrukture s strani upravljavcev in zmožnosti odzivanja ob motnjah v delovanju oziroma prekinitvi delovanja infrastrukture, ki jo upravljajo. To bo posredno prispevalo k zagotavljanju neprekinjenega delovanja kritične infrastrukture, lažjemu spopadanju z grožnjami in predvidevanju nepričakovanih tveganj.

Navedeno je, da bi s predlagano vsebino programa usposabljanja dosegli enotno raven usposobljenosti zaposlenih pri različnih udeležencih, oziroma vsaj osnovno raven usposobljenosti za zaščito kritične infrastrukture. Poleg tega bi se zvišala raven zavedanja o potrebi po nenehnem usposabljanju na področju kritične infrastrukture, okrepilo pa bi se tudi sodelovanje med različnimi upravljavci v sektorjih kritične infrastrukture in širše.

Predstavljeni program je ovrednoten tudi z urami po tematskih sklopih (skupaj za vse tematske sklope 18 ur) ter z načini izvedbe usposabljanja (predavanja, delavnice, elektronski način). Izvajalci usposabljanja niso definirani.

Nekaj ključnih spoznanj iz praktičnega okolja delovanja KI

V nadaljevanju si oglejmo nekaj ključnih praktičnih spoznanj, ki jih je opredelila projektna skupina ICS za izvedbo projektne študije »Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture«[2]. Ni presenetljiva ugotovitev, da je naša kritična infrastruktura zelo šibka na segmentu ravnanja s tveganji v posameznih sektorjih - ali bolje - v posameznih gospodarskih družbah, ki upravljajo s kritično infrastrukturo. Za tako stanje je več razlogov. Po naši presoji so ključni naslednji razlogi:

Še posebej velja poudariti, da je potrebno zaščito kritične infrastrukture in procese analiziranja tveganj, za delovanje le te, umestiti v celovit proces zagotavljanja neprekinjenosti delovanja ključnih nacionalnih sistemov in učinkovito krizno upravljanje v Republiki Sloveniji.

- izobraževalni sistem RS in posamezni izobraževalni procesi na vseh ravneh izobraževanja ne daje(jo) dovolj znanja za področje upravljanja tveganj v gospodarskih in drugih družbah. Še tiste izobraževalne ustanove, ki se nanašajo na družbene, varnostne in podobne vede so šibke na tem segmentu korporativnega upravljanja. Smiselni in pogumen korak je naredila GEA College - Fakulteta za podjetništvo, ki je pred nekaj leti v sodelovanju z Inštitutom za korporativne varnostne študije pripravila in sprejela magistrski program z naslovom Upravljanje tveganj in korporativna varnost. Nekaj študentov in študentk je že končalo ta program in doseglo naziv magister/magistrica upravljanja s tveganji. Škoda je le, da nosilci in upravljavci kritične infrastrukture še niso prepoznali dodane vrednosti tega magistrskega programa, ki zares nudi kompleksna znanja za upravljanje tveganj na strateških in operativnih ravneh države, industrije, gospodarstva in civilne družbe,
- v gospodarskih družbah, ki upravljajo s kritično infrastrukturo je kar nekaj koristnih usposabljanj, zlasti na področju varstva pri delu, požarne varnosti, varstva okolja, informacijske varnosti in še česa, vendar je to razdrobljeno, nepregledno, neenotno, neusklajeno ter načrtovano in izvajano na podlagi različnih metodologij. Predvsem pa je tovrstno usposabljanje izvajano na podlagi zakonskih zahtev in veliko manj na podlagi ocen ranljivosti, ogroženosti in tveganj,
- odgovorni in kompetentni za upravljanje raznovrstnih tveganj nimajo potrebnega znanja o metodah ocenjevanja, politikah in procesih upravljanja tveganj, o zakonodaji in standardih, ki določajo načine ravnanja s tveganji ter o poslovnih orodjih in tehnikah, ki prispevajo k učinkovitosti ravnanja s tveganji,
- upravljanje tveganj je silno zahtevno opravilo, ki poleg potrebnega znanja in upoštevanja dobrih praks, terja od posameznika in skupine tudi pogum, vztrajnost, prodornost, voljo, vzdržljivost in odgovornost na dolgi rok. To še posebno velja za obvladovanje izredno kompleksnih in raznovrstnih tveganj v kritični infrastrukturi. S tega zornega kota ni vsakdo sposoben, uporaben in kompetenten za prevzemanje tovrstnih funkcij in nalog,
- ker še ni enovitega programa usposabljanja za potrebe upravljanje varnosti in tveganj v kritični infrastrukturi, se kaže potreba po pripravi in implementaciji tovrstnega programa. Nekaj osnov za tak program je v Predlogu programa usposabljanja upravljavcev kritične infrastrukture Ministrstva za obrambo, ki pa ga je potrebno vsebinsko dograditi. V nadaljevanju je podan naš predlog programa usposabljanja za obvladovanje tveganj v kritični infrastrukturi.

Nekaj od zapisanega velja še danes, kajti, kot je ugotovljeno, je izobraževanje, usposabljanje in izpopolnjevanje, z vidika ranljivosti, ogroženosti, tveganj in ukrepov zaščite, močno podhranjeno. Zato bo treba v prihodnje to vrzel zmanjšati ali celo odpraviti, sicer se lahko zgodi, da bo trajnostni razvoj kritične infrastrukture upočasnjen.

Poleg zgoraj navedenih ugotovitev lahko nakažemo še nekaj drugih vrzeli v korporativnem upravljanju kritične infrastrukture, zlasti z vidika upravljanja korporativne varnosti. Gre namreč za strateško pomembne segmente upravljanja z varnostjo in tveganji, ki se nanašajo na



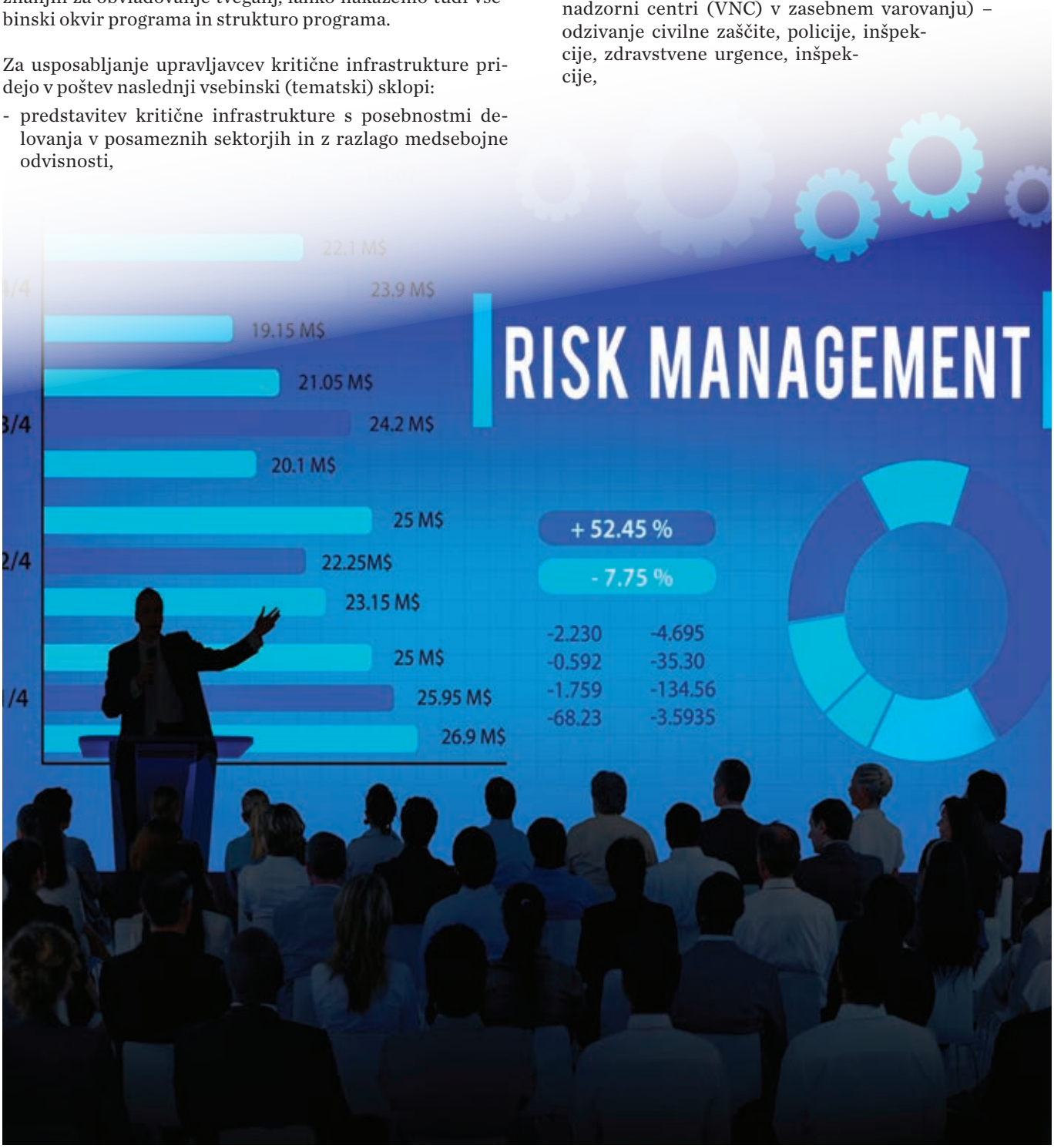
ocenjevanja ranljivosti in ogroženosti sektorjev kritične infrastrukture. Pri tem nas ne sme zavesti splošna ocena, da je Slovenija varna. Kajti do realne slike pridemo samo v primeru, ko profesionalno ugotovimo ranljive in varnostno zanimive točke v poslovnih in drugih procesih ter natančno ugotovimo varnostne in druge grožnje.

Predlog priprave ustreznega programa usposabljanja

Izhajajoč iz tujih izkušenj pri usposabljanju, za potrebe obvladovanja tveganj in ukrepov za zaščito kritične infrastrukture, ter iz ugotovitev projektne skupine ICS[1] o potrebnih znanjih za obvladovanje tveganj, lahko nakažemo tudi vsebinski okvir programa in strukturo programa.

Za usposabljanje upravljavcev kritične infrastrukture pridejo v poštev naslednji vsebinski (tematski) sklopi:

- predstavitev kritične infrastrukture s posebnostmi delovanja v posameznih sektorjih in z razlago medsebojne odvisnosti,
- oris zakonodaje, ki ureja delovanje sektorjev kritične infrastrukture,
- oris standardov kakovosti in varnostnih standardov,
- oris ključnih metod in standardov obvladovanja tveganj,
- ranljivost kritične infrastrukture – izdelava ocene,
- ogroženost kritične infrastrukture – izdelava ocene,
- tveganja v kritični infrastrukturi – izdelava ocene po navodilu in po sprejeti metodologiji,
- krovna varnostna politika in področne varnostne politike,
- politika in proces upravljanja tveganj,
- verjetni izredni dogodki v kritični infrastrukturi,
- odzivanje na izredne dogodke – alarmni sistemi (javni alarmni sistem, 112, 113, OKC Policijskih uprav, varnostno nadzorni centri (VNC) v zasebnem varovanju) – odzivanje civilne zaščite, policije, inšpekcije, zdravstvene urgence, inšpekcije,



Raznovrstni varnostni problemi ostajajo in jih moramo v nenehnem spremljanju aktivno analizirati. Vse to pred strokovnjake s področja korporativne varnosti postavlja dileme, kako mora biti korporativna varnost v takih razmerah, pri vodenju razvejanih organizacij, učinkovito orodje v rokah strateškega managementa.

- zagotavljanje neprekinjenega poslovanja posameznih gospodarskih družb, ki upravljajo s kritično infrastrukturo,
- delovanje kritične infrastrukture v kriznih okoliščinah – kritične poslovne funkcije, krizni štab, krizno vodenje, krizno komuniciranje, rezervna lokacija,



- notranji in zunanji nadzorni mehanizmi za ugotavljanje skladnosti delovanja na področju zaščite kritične infrastrukture,
- družbena odgovornost, organizacijska in varnostna kultura ter poslovna etika.

Nakazani tematski sklop zagotavlja celovito obvladovanje tveganj v kritični infrastrukturi, posledično pa tudi obvladovanje škod in izgub ter zmanjševanje stroškov delovanja in poslovanja gospodarskih družb, ki upravljajo s kritično infrastrukturo. Potrebno bo vložiti kar nekaj naporov za implementacijo tega ali pa dopolnjenega programa, kjer bo malo trši oreh izbor predavateljskega tima in priprava vsaj minimalnega učnega gradiva. Vsekakor pa bo vzpostavitev tovrstnega usposabljanja za upravljavce kritične infrastrukture in morebitne druge udeležence dodana vrednost pri pridobivanju znanja za obvladovanje groženj in tveganj v kritični infrastrukturi.

Zaključek

Raznovrstni varnostni problemi ostajajo in jih moramo v nenehnem spremljanju aktivno analizirati. Vse to pred strokovnjake s področja korporativne varnosti postavlja dileme, kako mora biti korporativna varnost v takih razmerah, pri vodenju razvejanih organizacij, učinkovito orodje v rokah strateškega managementa. Ravno pri strateškem managementu se varnostno zavedanje o pomenu korporativne varnosti, in varnosti nasploh, počasi dviguje in prihaja v ospredje. Vendar se prevečkrat dogaja, da strokovno znanje in sposobnost korporativno varnostnega managementa v organizacijah, ni na ustreznem nivoju, da bi izkoristil ta »zvezdniški trenutek« in se v določenih situacijah izkazal kot učinkovit mehanizem za ustrezno obvladovanje tveganj. Ta lažna zazibanost in samozadostnost je v svetu takih dinamičnih sprememb, kakršne se vsakodnevno dogajajo, praktično obsojena na takojšen neuspeh. Zaradi navedenega je potrebno, bolj kot kadarkoli do zdaj, vlagati v stalno izobraževanje in dograjevanje svojih znanj ter veščin. Ravno področje ocenjevanja tveganj bo v prihodnosti eno od tistih področij, ki bo podvrženo potrebi po neprekinjenem izvajanju usposabljanja ustreznih strokovnjakov, ki bodo v organizacijah izvajali te procese.

[1] Projekt PROPU – Predlog programa usposabljanja upravljalcev kritične infrastrukture (avtorici Alenka Čarni in Anica Ferlin) (financirano s podporo EU in sklada za notranjo varnost).

[2] Naročnik študije je MORS, **št. projekta 198/2018 – JNNV, študija SPOTKI** (financirano s podporo EU in sklada za notranjo varnost).

[3] Strokovne podlage za ocenjevanje tveganj za delovanje kritične infrastrukture. Izvirna študija, 2018. Inštitut za korporativne varnostne študije, Ljubljana. ■



Varno v nov dan

ZARJA ELEKTRONIKA

www.zarja.com

T: +386 1 8317 488 F: +386 1 8317 551 Dežurna služba T: +386 1 8317 452 E: info@zarja.com prodaja@zarja.com

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



VLOGA OUTSOURCINGA V PROCESU UPRAVLJANJA S TVEGANJI PRI UPRAVLJAVCIH KRITIČNE INFRASTRUKTURE

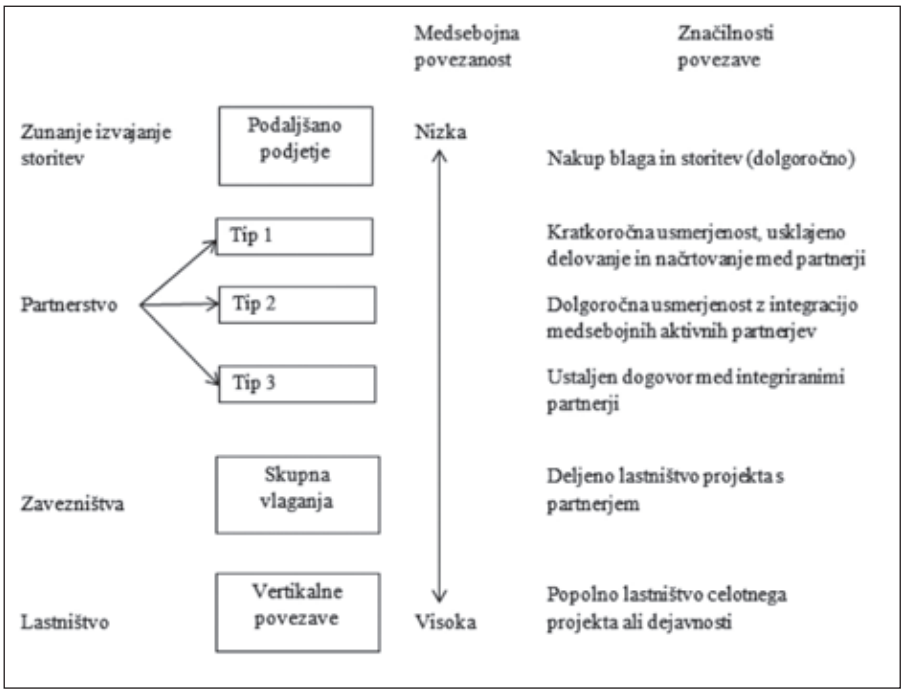
Povezovanje med gospodarskimi in drugimi organizacijami zagotavlja večjo učinkovitost, fleksibilnost, hitrejše in lažje prilagajanje spremembam na trgu, lažje izogibanje tržnim negotovostim ter s tem posledično povečevanje konkurenčnih prednosti na trgu. Med raznovrstnimi oblikami odnosov med organizacijami je tudi široko zasnovano zunanje izvajanje dobav in storitev (v angleškem prevodu: outsourcing). Gre za klasično obliko pogodbene nabave izdelkov in storitev, ki jih iz različnih vidikov ni smiselno izdelovati ali izvajati v lastni organizaciji.

Ko gospodarska in druga organizacija razmišlja katere izdelke in storitve bo zaupala zunanjim izvajalcem, se mora poleg zgoraj omenjenih prednosti, ki jih organizacijam prinaša outsourcing, zavedati tudi tveganj, ki jih prinašajo tovrstne oblike povezovanja. Naj izpostavim le nekaj glavnih tveganj, ki se jih je potrebno zavedati: poseganje zunanjih izvajalcev v osnovne dejavnosti organizacije, dolgoročna izpostavljenost odvisnosti organizacije od zunanjih izvajalcev, izguba dolgoročne prožnosti poslovanja zaradi odvisnosti od zunanjih izvajalcev, tveganja prekinitev dobav, slaba kakovost dobavljenih izdelkov in storitev, slaba morala in motivacija zaposlenih pri zunanjih izvajalcih, izguba notranje skladnosti poslovanja, tveganja zaupnosti poslovanja ter varovanja poslovnih skrivnosti in osebnih podatkov, izguba pravic intelektualne lastnine, nepredvideni in skriti stroški, tveganja ugleda in še mnoga druga tveganja.

Zunanji izvajalci so v pretekli praksi vse prevečkrat izpadli že iz samega procesa ocenjevanja tveganj, kar je v osnovi pomenilo njihovo pomanjkljivo angažiranje v izvajanju procesov upravljanja s tveganji, neprekinjenega poslovanja in kriznega upravljanja.

Ko obravnavamo vlogo outsourcinga v procesu upravljanja s tveganji pri upravljavcih kritične infrastrukture je zavedanje navedenih tveganj še toliko bolj pomembno. Po definiciji iz Zakona o kritični infrastrukturi so upravljavci kritične infrastrukture gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti ali upravljajo s kritično infrastrukturo, to je tisto infrastrukturo Republike Sloveniji, ki obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo, in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi.

*avtor je član Slovenskega združenja korporativne varnosti



Slika: Vrste partnerskih odnosov

Iz zgornje slike (povzeto po Mlakar, 2007, vir: Graham 1998, str. 187) je razvidna medsebojna povezanost med posameznimi oblikami partnerskih odnosov. Še posebej nas zanima zunanje izvajanje, za katerega, po omenjenem avtorju, velja nizka povezanost med zunanjimi izvajalci in organizacijo. Navedeno dejstvo nam mora služiti kot osnovno izhodišče za ocenjevanje tveganj pri tovrstni obliki partnerskega odnosa. Na prvi pogled bi lahko rekli, da nizka medsebojna povezanost že sama po sebi nakazuje na visoko stopnjo tveganja sodelovanja, zato moramo temu partnerskemu odnosu, pri ocenjevanju tveganj, nameniti posebno poglavje in mu posvetiti toliko več pozornosti.

V procesu ocenjevanja tveganj outsourcinga je potrebno najprej ugotoviti, kateri so tisti zunanji izvajalci, ki so za organizacijo strateškega pomena. Tu predvsem mislim na tiste dobavitelje izdelkov in storitev, ki so vitalnega pomena za delovanje organizacije, še posebej v primeru pojava izrednih dogodkov, to je tistih dogodkov, ki pri delovanju kritične infrastrukture predstavljajo resno motnjo v delovanju ali prekinitev delovanja kritične infrastrukture, ki vpliva ali bi lahko vplivala tudi na njeno varnost. V tej smeri je smiselna vzpostavitev registra zunanjih izvajalcev v katerem se posebej označi tiste, ki so strateškega pomena za upravljavca kritične infrastrukture.

Strateški zunanji izvajalci zaradi svoje pomembnosti za upravljavce kritične infrastrukture z vidika zagotavljanja neprekinjenega delovanja in dobav tudi ob izrednih dogodkih in v kriznih okoliščinah zahtevajo posebno obravnavo in jih je iz tega vidika nujno potrebno vključiti v procese upravljanja tveganj, izgradnje sistemov neprekinjenega poslovanja in kriznega upravljanja. Iz tega vidika predlagam postopno vključitev strateških zunanjih izvajalcev v omenjene procese. Postopnost uvajanja nakazujem v naslednjih korakih:





Ocenjujemo, da so tveganja outsourcinga strateške narave, zlasti, ko gre za zagotavljanje neprekinjenega poslovanja in obvladovanja kriznih poslovnih in varnostnih situacij.

- Vzpostavitev registra zunanjih izvajalcev.
- Določitev strateških zunanjih izvajalcev v registru zunanjih izvajalcev na podlagi kriterijev za izbor.
- Določitev zahtev o kakovosti, odzivnosti in sposobnosti zagotavljanja neprekinjenih dobav izdelkov in storitev.
- Izdelava pogodb z zunanjimi izvajalci.
- Izbor ekonomsko in kakovostno najugodnejših strateških zunanjih izvajalcev.
- Vzpostavitev dolgoročnega partnerskega odnosa s strateškimi zunanjimi izvajalci.
- Vključitev strateških zunanjih izvajalcev v proces ocenjevanja tveganj tako, da so določena tveganja zunanjih izvajalcev vključena v register tveganj.
- Vključitev izrednih dogodkov strateških zunanjih izvajalcev v register izrednih dogodkov
- Izdelava, izvajanje (vaje) in dograjevanje scenarijev izrednih dogodkov v katerih morajo sodelovati tudi strateški zunanji izvajalci.
- Odpravljanje neskladij ter uvajanje izboljšav v procese dobav izdelkov in storitev.
- Vključitev kadrovskih virov strateških zunanjih izvajalcev v procese izobraževanja na področju upravljanje tveganj.
- Vključitev strateških zunanjih izvajalcev v procese neprekinjenega poslovanja in v procese kriznega upravljanja.
- Vključitev strateških zunanjih izvajalcev v vodstvene in varnostne kolegije, ko gre za razreševanje poslovne in varnostne problematike ter načrtovanje vnašanja izboljšav v dobavne verige, ki morajo slediti zahtevam po hitrem odzivanju na izredne dogodke ter na zahteve neprekinjenega poslovanja in razreševanja. kriznih situacij.

Nakazani koraki v bistvu predstavljajo sistem uvajanja zunanjih izvajalcev v procese upravljanja tveganj, pri naročnikih njihovih izdelkov in storitev. Da bi se zunanji izvajalci (še posebej strateški) lahko vključili v zgoraj nakazan sistem upravljanja tveganj se morajo seznaniti z zakonom o kritični infrastrukturi, ki upravljavcem kritične infrastrukture med drugim nalaga tudi celovito upravljanje tveganj tako, da od njih zahteva izdelavo celovitih ocen tveganj in izdelavo ukrepov za zaščito kritične infrastrukture. Pri tem morajo upravljavci kritične infrastrukture v energetiki, informacijsko-komunikacijskih sistemih, prometu, zdravstvu, bančništvu in drugi kritični infrastrukturi identificirati, analizirati, oceniti in ovrednotiti različne vire tveganj med katere sodijo tudi tveganja outsourcinga. Ocenjujemo, da so tveganja outsourcinga strateške narave, zlasti, ko gre za zagotavljanje neprekinjenega poslovanja in obvladovanja kriznih poslovnih in varnostnih situacij.

Zunanji izvajalci so v pretekli praksi vse prevečkrat izpadli že iz samega procesa ocenjevanja tveganj, kar je v osnovi pomenilo njihovo pomanjkljivo angažiranje v izvajanju procesov upravljanja s tveganji, neprekinjenega poslovanja in kriznega upravljanja. Zaradi tega so bile organizacije še toliko bolj ranljive in izpostavljene tveganjem, kar bi lahko v določenih primerih izrednih dogodkov usodno vplivalo na poslovanje organizacije. Tega dejstva se moramo še posebej zavedati, ko govorimo o upravljanju s tveganji, neprekinjenem poslovanju in kriznem upravljanju pri upravljavcih kritične infrastrukture. Naj bo torej ta prispevek usmeritev za vse tiste, ki se ukvarjajo z upravljanjem tveganj, ob zavedanju, da so tudi zunanji izvajalci, še posebej strateški, pomemben člen pri zagotavljanju neprekinjenega poslovanja upravljavcev kritične infrastrukture.

Pomembno vlogo pri zagotavljanju učinkovitega upravljanja s tveganji, neprekinjenega poslovanja in kriznega upravljanja, pri upravljavcih kritične infrastrukture, predstavljajo tudi zunanje inštitucije in organi, ki so aktivno vpete v določene faze procesa upravljanja s tveganji, upravljanja z izrednimi dogodki, neprekinjenega poslovanja in kriznega upravljanja. Naj izpostavim le nekatere od njih: vlada in njene službe, agencije, policija, gasilci, reševalci, uprava za zaščito in reševanje s svojimi operativnimi enotami, inšpekcijski in nadzorni organi idr. Le ti imajo v določenih fazah omenjenih procesov celo ključno in vodilno vlogo, zlasti, ko gre za zakonodajne, usmerjevalne in nadzorne postopke ter za odzivanje na izredne dogodke in krize. ■

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 SAMODEJNI GASILNIK 2, 4, 6 ali 12L.

SAMODEJNE GASILNE AMPULE BONPET

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



Bonpet gasilnik, specialist za olja in maščobe (F razred)

Bonpet® systems

Zanesljivi gasilni sistemi

Pot Vitka Pavliča
1430 Hrastnik
Tel.: 080-26-63
e-pošta: info@bonapet.si
www.bonapet.si

Avtor: mag. Marko Potokar / Vodja varovanja, Upravljanje nepremičnin in storitve,
Novartis Business Services Lek d.d.*



VAROVANJE OSKRBOVALNIH VERIG

S pojavom širjenja svetovne trgovine so se povečale tudi priložnosti za kriminalna dejanja, ki so usmerjena v izkoriščanje ranljivosti globalnih oskrbovalnih verig. Zagotavljanje varnosti oskrbovalnih verigje bila od nekdaj ena izmed glavnih skrbi organizacij, ki se ukvarjajo s transportom, logistiko in proizvodnjo. Tveganja zaradi tatvin, povzročitve škode in zagotavljanja celovitosti pošiljk so v današnji dinamični in kompleksni družbi vse večja. Če k temu dodamo še grožnje organiziranega kriminala, piratstva in terorizma, postaja varnost oskrbovalnih verig ključnega pomena za preživetje podjetij.

Varovanje oskrbovalnih verig

Prevoz blaga v svetovnem gospodarstvu, ki ga poganja predvsem zunanje izvajanje storitev, še nikoli prej ni bilo tako kompleksno. Viri surovin, sestavnih delov in končnih proizvodov so globalne narave, zato so za njihovo distribucijo potrebne tudi globalne oskrbovalne verige. S povečanjem globalne odvisnosti se je povečala tudi vrednost dobavljenega blaga. Proizvodi z visoko vrednostjo, kot so elektronske naprave in zdravila, predstavljajo velik odstotek prepeljanega blaga. Nekaj deset kilogramska pošiljka mikroprocesorjev, vrednosti več deset tisoč dolarjev, pa je običajno zavarovana za manj kot tristo dolarjev.

Varnost in ranljivost oskrbovalnih verig je bila do terorističnega napada na Svetovni gospodarski center leta 2001 v veliki meri zapostavljena. S širjenjem terorizma, tihotapljenja drog, orožja in ljudi ter s potrebo po zagotavljanju integritete blagovne znamke so se povečale tudi zahteve po ureditvi področja varovanja oskrbovalnih verig in medsebojnem sodelovanju narodov. Zahteve Carinskega trgovinskega partnerstva proti terorizmu (C-TPAT - Customs-Trade Partnership Against Terrorism), Pobude za zaščito kontejnerjev (CSI – Container Security Initiative) in Transportnega združenja za zaščito sredstev (TAPA – Transported Asset Protection Association) so le nekateri primeri ureditve, namenjene obravnavi groženj oskrbovalnih verig.

Ranljivost oskrbovalne verige lahko razumemo kot njeno občutljivost na razne vrste motenj, ki jih je mogoče opisati kot nezaželene učinke ali kot negativne posledice, ki jih te imajo za oskrbovalno verigo. Če je tveganje, ki je posledica ranljivosti in motenj, za določen logistični proces previsoko, je potrebno vpeljati ustrezne kontrole za zmanjševanje tveganja oziroma spremeniti proces tako, da se doseže sprejemljiv nivo ranljivosti in motenj. V praksi to pomeni večji poudarek na varnostnih značilnostih manjših elementov oskrbovalne verige, kot so terminali, tovornjaki, zabojniki, pristanišča idr. Zaradi dinamičnosti oskrbovalnega procesa je zagotavljanje varnosti izjemno zahtevno. Odnos med vzrokom in posledico namreč v takem okolju ni linearen, kar pomeni, da tradicionalno obravnavanje tveganj praviloma ne zagotavlja dovolj učinkovitega mehanizma za ustrezno raven varnosti. Odnos med tveganjem in varnostjo mora biti zato analiziran tako z vidika subjektivne ocene, kot tudi s statističnega vidika. Uporaba komplementarnih metod namreč omogoča ugotovitev razlik med zaznano stopnjo tveganja in statistično pogojeno stopnjo tveganja.

Varnost logistike in tovora je bila dolgo časa premalo razvita. Z izboljšanjem varnosti terminalov so se varnostni incidenti preselili na povezave in lokacije med njimi. Medtem ko je varnost proizvodnih zmogljivosti po navadi relativno dobro zagotovljena, so ostali deli verige varnostno podhranjeni. Varnost med prevozom je potrebna za preprečitev neželene negativne motnje v toku blaga. Transportna varnost je kombinacija preventivnih

Obstoječe varnostne raziskave oskrbovalnih verig poudarjajo, da samo zagotavljanje preprečevanja kraje ni dovolj za celovito varovanje oskrbovalnih verig. Varnostni sistem mora upoštevati in vključevati tudi protiteroristične ukrepe.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

ukrepov za zagotovitev zaščite transporta, infrastrukture, vozil, sistemov in ljudi pred namernimi nezakonitimi dejanji. Za uspešno varovanje je ključno usklajevanje in sodelovanje vseh deležnikov, vključenih v transport.

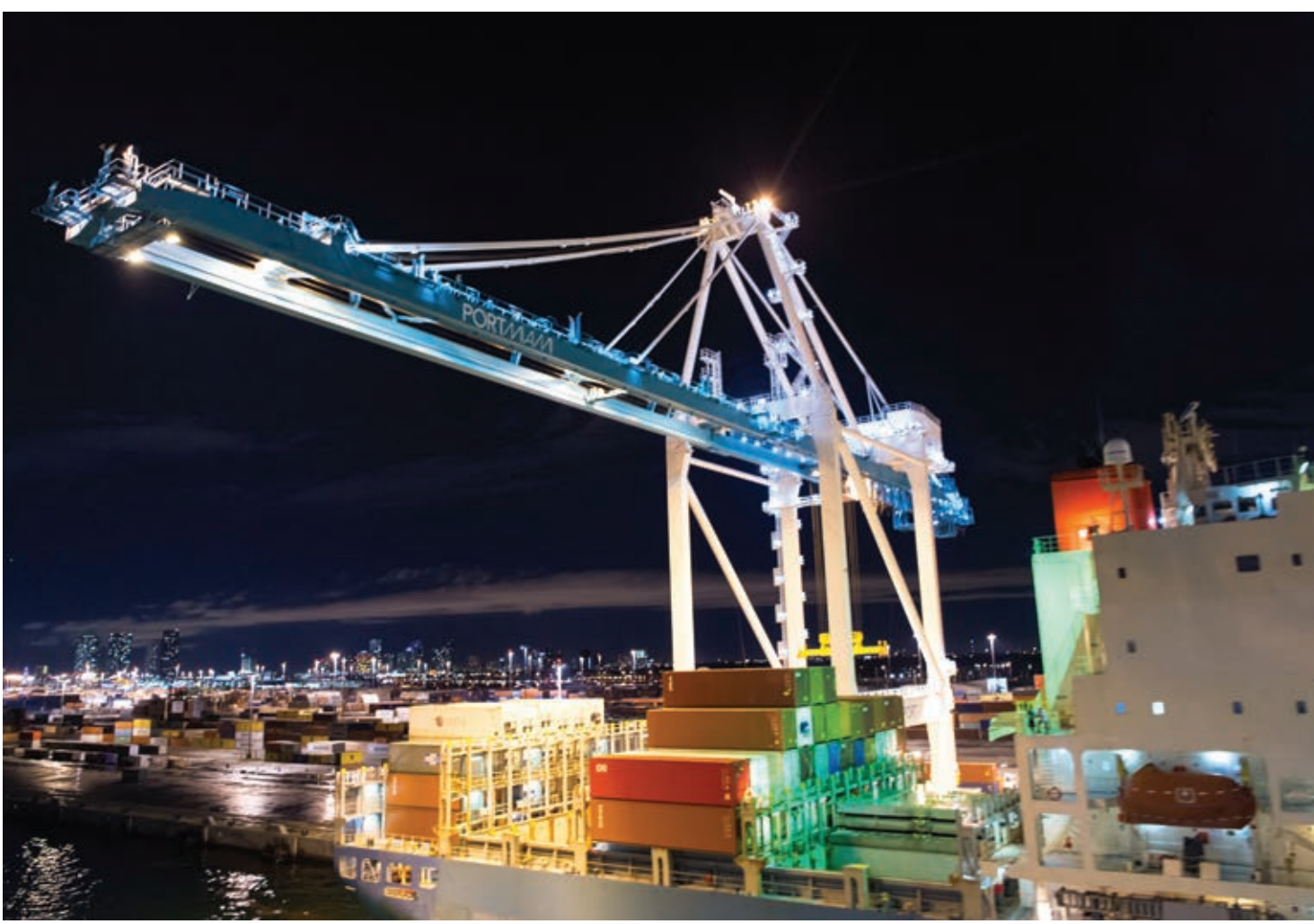
Dobavna veriga je avtonomna mreža poslovnih procesov, ki proizvajajo fizično blago ali storitve za stranke. Področje logistike se nanaša na vse dejavnosti od dobavitelja do stranke ter zagotavljajo pravi izdelek, ob pravem času, na pravem mestu. Namen transportnega omrežja je fizično premikati blago v določeni oskrbovalni verigi. To pomeni, da transportno omrežje fizično integrira oskrbovalno verigo z zahtevami. Transportni sistem sestavljajo trije elementi: vozila ali plovila, tovor in poti skupaj s terminali. Za prevoz izdelkov, ki so lahko ogroženi zaradi kraje, se lahko uporablja transportna veriga z lokacijami in prevozniki tovora, ki morda ne zagotavljajo zadostne stopnje varnosti za transport blaga od pošiljatelja do prejemnika.

Obstoječe varnostne raziskave oskrbovalnih verig poudarjajo, da samo zagotavljanje preprečevanja kraje ni dovolj za celovito varovanje oskrbovalnih verig. Varnostni sistem mora upoštevati in vključevati tudi protiteroristične ukrepe. Prav tako mora biti poudarek na globalnih vprašanjih in ne samo na lokalni ali regionalni ravni. Pri izvajanju načrtovanja ukrepov v nepredvidljivih okoliščinah je potrebno vključiti principe kriznega vodenja. In nenazadnje se je potrebno zavedati, da zagotavljanje varnosti ni samo notranja skrb podjetja, temveč zadeva vse deležnike v procesu oskrbovanja in mora biti vključena v celotno oskrbovalno verigo.

Zagotavljanje varnosti oskrbovalnih verig predstavlja enega izmed največjih izzivov za proizvajalce blaga visoke vrednosti ter za ponudnike logističnih storitev.

Kriminaliteta pri transportu blaga

Za ponazoritev zapletenosti logističnih dejavnosti lahko uporabimo model štirih logističnih tokov: materiala, virov, informacij in kapitala. Kraja blaga med logistično dejavnostjo se pojavi, ko tovorni tatovi izkoristijo pretok virov ali infrastrukturo. Z izkoriščanjem informacijskega toka lahko storilci dosežejo boljše udejanjenje načrta napada. Glede na cilj (tarčo) napada storilec izbere določeno vrsto napada. Tatovi tovora poskušajo odstraniti blago iz oskrbovalne verige z uporabo različnih metod za napad na različne lokacije znotraj oskrbovalne verige. Vse lokacije se lahko v različnih in kratkih obdobjih štejejo za geografsko fiksne lokacije. Vozila se sicer premikajo, vendar je gibanje predvidljivo – vsaj lokacijsko, če ne tudi časovno. Statistični podatki za krajo tovora kažejo, da se slaba polovica vseh incidentov zgodi med prevozom in vključuje grožnjo vozniku ali trganje platna na prikolicah s tovorom. V petnajstih odstotkih incidentov je tovor-





njak ukraden skupaj z blagom, naslednjih petnajst odstotkov pa predstavljajo ugrabitve in ropi. Običajno se kraje zgodijo na tovornjakih, ki so začasno parkirani na počivališčih ob cesti ali pa čakajo na možnost natovarjanja ali iztovarjanja.

Elementi kriminalnega dejanja

Glede na kriminološke raziskave vse vrste zločinov, od občasnega nasilja do naprednega in zapletenega gospodarskega kriminala, razkrivajo tri elemente: motiviranega storilca, tarčo in lokacijo, kjer se srečata storilec in tarča. Kaznivo dejanje se zgodi samo takrat, ko se vsi trije elementi združujejo istočasno in na istem mestu. Če eden od teh treh elementov manjka, ne more priti do kaznivega dejanja. Kombinacije lokacij in tarč imenujemo priložnosti za kriminalno dejanje. Storilec glede na vrsto priložnosti za kriminalno dejanje izbere določeno metodo za izvršitev kriminalnega dejanja. Ideja, da so možnosti za kriminalna dejanja odvisne od predvidljivosti znotraj določenih meja, je v kriminologiji znana kot perspektiva rutinske dejavnosti. Ključni element v tem pogledu je, da običajno gibanje in druge rutinske dejavnosti igrajo pomembno vlogo v zvezi z morebitnimi kriminalnimi dejanji. Potencialni storilci tako iščejo lokacije, kjer se nahaja veliko število razpoložljivih in primernih (ranljivih) tarč (žrtev). Izhajajoč iz opisanega koncepta lahko domnevamo, da je kraja tovora pogostejša v slabo upravljanih organizacijah z velikimi količinami blaga. Poznavanje infrastrukture in predvidljivost gibanja virov igra pomembno vlogo pri razumevanju različnih priložnosti za kriminalno dejanje. Geografske lokacije in koridorji, skozi katera teče blago, so po navadi zelo predvidljivi. Spremembe v transportni mreži tako pomenijo spremembe v možnostih tatvine; potencialni storilci morajo na novo spoznati in izkoristiti priložnosti za krajo in izvršitev kaznivih dejanj.

Vrste storilcev

Obstajata dve vrsti storilcev: profesionalni storilci in priložnostni storilci. Profesionalni storilec ukrade določeno blago v zameno za denar. Dejanje načrtuje tako, da identificira najšibkejši člen v varnostnem sistemu. Bolj ga skrbijo nepredvidljivi elementi varnostnega sistema (npr. drugi ljudje) kot pa varnostna tehnologija. Priložnostni storilec ukrade blago, ker je to zaželeno ali uporabno. Deluje impulzivno, brez vnaprejšnjega načrtovanja dejanja. Takšni storilci imajo malo ali nič znanja o varnostnih sistemih. Prisotnost vidnih varnostnih ukrepov pri njih povzroča strah. Ali gre za storilca ene ali druge vrste, je torej odvisno predvsem od posameznikovega poznavanja prednosti in pomanjkljivosti varnostnega sistema. Profesionalni storilci lahko pridobijo ustrezno strokovno znanje za premagovanje predvidljivih varnostnih ukrepov. Glede na razmerje z organizacijo lahko storilce ločimo še na notranje in zunanje.

Pri načrtovanju in izvajanju varnostnih ukrepov v oskrbovalnih verigah je tako poleg navedenih elementov kriminalnih dejanj potrebno upoštevati tudi značilnosti morebitnih storilcev.

Sistem upravljanja varnosti oskrbovalnih verig

Z večanjem varnostnih groženj, povečevanjem števila predpisov in potrebo po hitrem izmenjavanju informacij o prevozu blaga od začetne do končne točke prodaje se je okrepila tudi potreba organizacij po celovitem in sistematičnem upravljanju varnosti oskrbovalnih verig.

Sistem upravljanja varnosti oskrbovalnih verig opredeljuje družina ISO standardov 28000 (28000, 28001, 28003 in 28004). Standard ISO 28000 je upravljavski standard, ki določa zahteve za upravljanje sistema varnosti oskrbovalnih verig ter povezuje upravljanje varnosti z drugimi vidiki poslovnega upravljanja. Ti vidiki vključujejo dejavnosti, ki jih izvajajo druge organizacije oziroma s svojim

delovanjem te na njih vplivajo. Uporablja pragmatičen pristop, pri katerem so opredeljene stopnje tveganja posameznih operacij znotraj oskrbovalne verige, kar omogoča organizaciji oceno tveganja s podporo orodij za upravljanje, kot so kontrole, ključni kazalci uspešnosti, notranje revizije in usposabljanje. ISO 28000 je tako primeren za vse organizacije, ki bi rade implementirale varnostni sistem oskrbovalnih verig in ga vključile v obstoječi sistem upravljanja (npr. sistem upravljanja kakovosti ISO 9001), ne glede na to ali gre za velike korporacije ali manjša podjetja, ki se ukvarjajo s proizvodnjo, servisiranjem, skladiščenjem ali transportom.

Mednarodna organizacija za standardizacijo (International Standards Organization) je izdala družino standardov 28000 leta 2007 z namenom opredelitve zahtev in smernic za organizacije, ki želijo nadgraditi varnost oskrbovalnih verig, ter za certifikacijske organe, ki izvajajo revizije in podeljujejo certifikate za sisteme upravljanja varnosti oskrbovalnih verig. Družina standardov 28000 sestoji iz naslednjih standardov:

- ISO 28000:2007 – *Specifikacije za sisteme upravljanja varnosti oskrbovalnih verig.*
- ISO 28001:2007 – *Najboljše prakse za implementacijo varnosti oskrbovalnih verig, ocen in načrtov – Zahteve in smernice.*
- ISO 28003:2007 – *Zahteve za revizijske in certifikacijske organe sistemov upravljanja varnosti oskrbovalnih verig.*
- ISO 28000:2007 – *Smernice za implementacijo standarda ISO 2800.*

Pravilno implementiran in delujoč sistem za upravljanje varnosti oskrbovalnih verig, skladen s standardom ISO 28000, poleg večje varnosti in zanesljivosti organizacijam prinaša tudi naslednje prednosti:

- Upravljanje varnosti postane proces, katerega učinkovitost je merljiva in izboljšljiva.
- Omogoča osredotočenje virov in prizadevanj na področja visokega tveganja, identificirana s pomočjo ocene tveganja.
- Omogoča primerjavo upravljanja obstoječega varnostnega sistema z drugimi mednarodnimi standardi.
- Dokazuje zainteresiranim stranem zavezanost k izvrševanju sistematično upravljane varnosti.

Ustrezno stopnjo varnosti je mogoče doseči le s sistematičnim in strokovnim pristopom, upoštevanjem globalnih varnostnih standardov in priznanih industrijskih praks ter z nenehnim izobraževanjem, medsebojnim sodelovanjem in proaktivnim prepoznavanjem kriminalnih trendov.



Zaključek

Zagotavljanje varnosti oskrbovalnih verig predstavlja enega izmed največjih izzivov za proizvajalce blaga visoke vrednosti ter za ponudnike logističnih storitev. Porast zahtev za zagotavljanje varnosti namreč določajo trije dejavniki: globalizacija svetovne trgovine, ki je bila ustvarjena in je odvisna od prostega pretoka ljudi, blaga in informacij, podjetja zahtevajo vedno bolj učinkovite logistične operacije, vse večje pa je tudi tveganje terorističnih napadov.

Poleg tega grožnjo ne predstavljajo več samo oportunistični kriminalci. Danes organizirani kriminalni obroči delujejo globalno in uporabljajo vedno bolj sofisticirane napade na vozila, prostore in osebje, da bi dosegli svoje cilje. Ustrezno stopnjo varnosti je mogoče doseči le s sistematičnim in strokovnim pristopom, upoštevanjem globalnih varnostnih standardov in priznanih industrijskih praks ter z nenehnim izobraževanjem, medsebojnim sodelovanjem in proaktivnim prepoznavanjem kriminalnih trendov.

Viri

- Ekwall, D., Lantz, B. (2015). *Modi operandi for cargo theft in EMEA – A seasonality analysis.* Springer Science+Business Media, New York 2015.
- Ekwall, D., Lantz, B. (2017). *Cargo theft risk and security:product and location.* Nofoma, Lund, Sweden 2017.
- Facility security requirements. Transported Asset Protection Association, FSR 2017.
- International standard ISO 28001 (2007). *Security management systems for supply chain – Best practices for implementing supply chain security, assessments and plans - Requirements and guidance.*
- JBW Group International (2009). *Supply Chain Security and ISO 28000.* ■

Avtor: Žiga Podgoršek / Certificirani Etični heker, Institut za korporativne varnostne študije*



VARNOST OBLAKA PREDSTAVLJA VARNOST NAŠIH APLIKACIJ IN PODATKOV

Varnost oblaka predstavlja varnost podatkov, aplikacij in infrastrukture vključene v oblak. Veliko varnostnih vidikov je vključenih v okolje oblaka, prav tako je veliko vidikov varnosti oblaka bodisi privatne, javne ali hibridne narave enakih, kot v lokalni prostorski IT arhitekturi.

Varnost v oblaku vključuje ekosistem ljudi, politik in tehnologije, ki ščitijo podatke in aplikacije, ki delujejo v oblaku. Profesionalne ocene varnosti v oblaku in penetracijski testi so ključnega pomena pri zagotavljanju, da ponudniki storitev v oblaku izpolnijo vladne predpise in da odgovorno, na kar se da visokem nivoju, zaščitijo dragocene podatke.

Veliko je visokih varnostnih vprašanj povezanih z oblakom. Med njih spadajo neavtorizirana dostopanja do podatkov, šibke pristopne kontrole, občutljivost na napade in nedostopnost do podatkov v primeru prekinitve povezave (kar vpliva tako na tradicionalne IT sisteme, kot na oblak). Prav tako, kot vsako računalniško okolje, z vidika varnosti, potrebuje vzdrževane primerne preventivne varnostne mehanizme, je enako tudi pri oblaku. Potrebno se je zavedati, ali so podatki in sistemi varni, ali poznamo trenutno stanje varnostnih sistemov, ali smo obveščeni v trenutku, ko se nekaj nenavadnega dogodi in ali lahko sledimo anomalijam in se nanje primerno odzovemo.

Čeprav mnogo ljudi razume prednosti okolja v oblaku, se mnogi vzdržijo posluževanja te tehnologije, zaradi strahu pred varnostnimi grožnjami, ki jih ta predstavlja. Glede na to, da gre za dinamično okolje se stvari stalno spreminjajo prav tako kot varnostne grožnje. Stvar je v tem, da je v večini pogledov varnost oblaka, pravzaprav varnost IT. Ko razumemo te specifične razlike med okoljema, pod besedo oblak ni več prva asociacija nevarnost ali grožnja.

Med najpomembnejša varnostna vprašanja spada dostop do oblaka. Tradicionalna IT okolja največkrat kontrolirajo dostop s perimetričnim varnostnim modelom. Okolja v oblaku so visoko povezana, kar povzroči, da promet lažje obide tradicionalne perimetrične zaščite. Nezanesljivi aplikacijski programski vmesniki (ang. API), šibek identitetni in poverilni management, hekanje uporabnikov in zlonamerni notranji sodelavec lahko predstavljajo grožnje sistemu in podatkom, ki jih vsebuje. Preprečevanje neavtoriziranih dostopov v oblaku dosežemo s podatkovno osredotočenim šifriranjem, to pomeni s šifriranjem prav vseh podatkov. Prav tako je potrebno utrditi avtorizacijski proces, kateri potrebuje močna gesla in 2 nivojsko avtentikacijo. Priporočljiva je vgradnja varnostnih mehanizmov na vsak nivo.

Oblak se nanaša na gostovane resurse, dostopne uporabniku preko programa. Infrastruktura oblaka, vključno z vsemi podatki, ki jih procesira, je dinamična, prilagodljiva in prenosljiva. Varnostne kontrole oblaka se morajo odzvati na okoljske spremenljivke in spremljati delovne obremenitve podatkov, kadar so v tranzitu in kadar počivajo na disku, bodisi kot neločljiv del delovne obremenitve (npr. Šifriranje), bodisi dinamično, preko sistema za upravljanje z oblaki in API-jev. To pripomore k zaščiti okolja v oblaku pred poškodovanjem sistema in izgubo podatkov.

Profesionalne ocene varnosti v oblaku in penetracijski testi so ključnega pomena pri zagotavljanju, da ponudniki storitev v oblaku izpolnijo vladne predpise in da odgovorno, na kar se da visokem nivoju, zaščitijo dragocene podatke.

*avtor je član Slovenskega združenja korporativne varnosti

Sofisticirane grožnje so vse, kar negativno vpliva na sodobno računalništvo, kar seveda vključuje tudi oblak. Vedno bolj sofisticirana zlonamerna programska oprema in drugi napadi, kot so napredni že prisotni napadi (ang. Advanced persistent threats) so dizajnirani, da se ognejo omrežnim obrambam s ciljanjem na ranljivosti v računalniškem skladu (ang. Computing stack). Odgovornost vsakega posameznika je, da ostane v koraku s časom, na področju varnostnih praks v oblaku, katere se razvijajo, da bi sledile vedno novim nastajajočim nevarnostim.



Varnost v oblaku v več korakih:

- Varnost se začne graditi pri samem začetku dizajniranja oblaka. Načrtovati je potrebno tokove dela, ki uporabljajo skupne in odgovorne procese po skupinah dela z namenom definiranja in implementiranja varnosti v življenjski cikel IT okolja. V primeru uporabe tehnologije, ki ima visoko povezana okolja, kot npr. v oblaku, se je potrebno zavedati, da je nekaj varnostnih kontrol morda v rokah ponudnika oblačnih storitev, kar pomeni v rokah tretje osebe. Potrebno se je dogovoriti, kateri varnostni procesi in kontrole so potrebni za dotično okolje? Na katerem nivoji, bo potekalo sodelovanje s ponudnikom oblačnih storitev? Kako bo potekala komunikacija pomembnih varnostnih odločitev med skupinami?
- Avtomatizirana uporaba varnostnih procesov za izvajanje kontinuirane povratne zanke v vseh življenjskih fazah cikla aplikacije. Avtomatizacija varnostnih pregledov in procesov ima več prednosti; preprečuje podvajanje in zmanjšuje človeške napake, zagotavlja centralizirano nadzorno ploščo za sprejemanje odločitev in postopke hitrega iskanja in odzivanja na grožnje. Avtomatizacijo lahko uporabite tudi za izgradnjo varnostnih vrat, ki v primeru neuspešnosti varnostnega pregleda prepreči izvedbo. Kljub vsemu se lahko pojavljajo lažni alarmi in notranje grožnje. Avtomatizacijo je potrebno upravljati tako, da deluje dobro s specifičnimi potrebami ekipe, ki dela na njem. Pri vgradnji varnosti se je potrebno stalno spraševati ali so na mestu kontrole, da preprečijo neavtorizirane dostope in spremembe. Uporabljati je potrebno šifriranje, kjer je to mogoče.
- Tradicionalni modeli varnosti, ki se opirajo na ročne procese, niso združljivi z varnostnimi potrebami novih distribuiranih tehnologij, kot je oblak. Te tehnologije in orodja ter procesi, ki jih podpirajo, se močno zanašajo na avtomatizacijo. Ne glede na to, ali uporabljate fizični, virtualni, zasebni ali javni oblak, se je potrebno prepričati, da ima infrastruktura vgrajene zaščitne, varnostno opremljene platforme, katere so običajne v vseh vaših okoljih.
- Ne smemo pozabiti investirati v upravljalna orodja, ki obravnavajo avtomatizirane varnostne procese pri spremembah konfiguracij, revizijskih sledi in sanacij. Dodelitev vlog v zgodnji fazi in skladno s specifičnimi varnostnimi potrebami pomagajo ohraniti trdno varnostno okolje. Zagotoviti je potrebno, da so privilegiji dodeljeni le tistim, ki jih potrebujejo za opravljanje svojega dela. Po navadi se ta proces zgodi, ko se novi ljudje pridružijo podjetju, vendar je treba redno posodabljati uporabniške podatke, še posebej, ko ljudje odhajajo iz podjetja. V mislih je potrebno imeti; Ali imamo na voljo orodja za analizo in ublažitev incidenta? Kako se bo avtomatiziralo samodejno izvajanje, revizijo in regulacijo varnostnih pravilnikov skladno z delovno obremenitvijo?
- Varnostno okolje se hitro spreminja. Načrtovati je potrebno redno revizijo v skladu z vzporednimi spremembami v zahtevah glede upravljanja in revizije. Potrebno je vedeti, kje iskati informacije o varnostnih opozorilih ter nasvetih in seveda uporabiti te informacije za ustrezno prilagoditev. Kljub najboljšim varnostnim načrtom, se odkrivajo vedno novi vektorji napadov. Uvedba hitrega odziva na varnostne grožnje je ena najpomembnejših stvari, ki jih lahko storite za zaščito vašega podjetja. Imeti partnerja, ki vas vodi skozi popravke, rešitve in obnovitve, je ključnega pomena za to, da je vaše podjetje na pravi poti.

Ne glede na to, kakšno vrsto oblaka uporabljate, ste odgovorni za zavarovanje lastnega prostora znotraj tega oblaka. Uporaba oblaka, ki ga vzdržuje nekdo drug, ne pomeni, da lahko sedite križem rok. Pomanjkanje skrbnega pregleda je glavni razlog za varnostne napake. Varnost v oblaku je odgovornost vsakogar in vključuje:

- Uporabo zanesljive programske opreme. Kar je v vašem oblaku, je ključnega pomena. Kot pri vsaki kodi, ki jo

Med najpomembnejša varnostna vprašanja spada dostop do oblaka. Tradicionalna IT okolja največkrat kontrolirajo dostop s perimetričnim varnostnim modelom. Okolja v oblaku so visoko povezana, kar povzroči, da promet lažje obide tradicionalne perimetrične zaščite.



Skratka, če povzamem je oblak lahko varna in smiselna rešitev, ki pa vseeno predstavlja nova tveganja, zaradi katerih moramo redno preverjati svoje sisteme v oblaku ter slediti varnostnim smernicam in tako zagotavljati varnost naših sistemov in aplikacij ter podatkov na najvišjem možnem nivoju.

prenesete iz zunanjega vira, se je potrebno zavedati, od kje prvotno izvirajo določeni paketi, kdo jih je zgradil in ali je znotraj njih kašna zlonamerna koda. Pridobite programsko opremo iz znanih in zaupanja vrednih virov ter zagotovite, da so vzpostavljeni mehanizmi za pravočasno zagotavljanje in nameščanje posodobitev.

- Skladnost s predpisi. Osebni, finančni in drugi občutljivi podatki so predmet strogih predpisov o skladnosti. Zakonodaja se razlikuje glede na to, kje in s kom poslujete. Pred izbiro oblaka je potrebno preveriti zahteve glede skladnosti.
- Prenosljivost. Ali lahko svoje delovne obremenitve preprosto premaknemo v drug oblak? Dogovori o nivojih storitev (ang. Service level agreement) morajo biti jasno določeni, kdaj in kako ponudnik oblačnih storitev vrne podatke in aplikacije stranke, tudi če to ni predvideno v bližnji prihodnosti, je vseeno pričakovan scenarij. Prepreči-te prihodnje težave z onemogočanjem lahkega prenosa, tako da imate v mislih prenosljivost.
- Zaposlovati in sodelovati s kvalificiranimi in zanesljivimi ljudmi, ki razumejo kompleksnost varnosti v oblaku. Včasih je infrastruktura javnega oblaka lahko bolj varna kot zasebni oblak posamezne organizacije, saj ima ponudnik javnih oblakov po navadi bolj obveščeno in opremljeno varnostno ekipo.

Skratka, če povzamem je oblak lahko varna in smiselna rešitev, ki pa vseeno predstavlja nova tveganja, zaradi katerih moramo redno preverjati svoje sisteme v oblaku ter slediti varnostnim smernicam in tako zagotavljati varnost naših sistemov in aplikacij ter podatkov na najvišjem možnem nivoju. ■

VEDNO IZPOLNIJO PRAVO ŽELJO

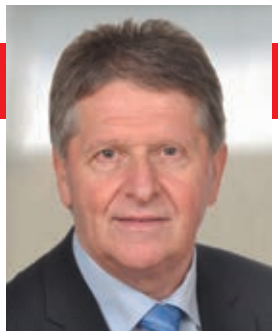


Nakup na www.btc-city.com/darilniboni
in na Info točki v Dvorani A.

TRGOVINE V BTC CITY LJUBLJANA SO V DECEMBRU
ODPRTE TUDI OB NEDELJAH OD 9.00 DO 15.00

BTC CITY

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



STRELSKI NAPAD: PREŽIVI S TREMI »S« (STECI, SKRIJ SE, SPOPADI SE!)

Statistika kaže, da so strelski napadi v skokovitem porastu, niso izključeni tudi v Sloveniji. Korporativni varnostni managerji se srečujemo s številnimi izzivi pri načrtovanju za navedeni primer, zlasti na področju kritične infrastrukture, v smislu upravljanja aktivnosti, vzpostavitvi operativnega okolja in varovanja zaposlenih. Pri tem je osnovno vprašanje: »Ali poznamo svoje zmožnosti predvidevanja in upravljanja tveganj ter sposobnosti za odgovor na strelski napad v podjetju?«

Uvod

To ni domišljija: »Gospa Koma prihaja!«. Navedeni izraz je koda za AMOK (nazaj prebrano: koma) situacijo. V današnjem varnostno spreminjajočem in negotovem okolju nobeno podjetje ali organizacija ni imuna na možni strelski napad. Gre za globalen in zelo kompleksen problem, saj se skoraj tedensko krvavo dogaja na vseh koncih sveta (ne glede na politične, gospodarske, socialno – ekonomske, religiozne ali kakšne druge značilnosti države), storilci so iz vseh družbenih slojev (zaposleni, tako bogati kot revni, drugi »prizadeti« ipd.), dejanja pa izvajajo proti različnim skupinam posameznikov in na različnih krajih (delovna mesta podjetij, šole, bolnišnice, koncertne dvorane, trgovski centri, kinodvorane, verski objekti ipd.).

Strelski napad

Strelski napad je nenormalna situacija v naselju, ko eden ali več storilcev v besu narcističnega maščevanja, sovraštvu, norosti, obupu, brezciljno ali sistematično, z orožjem ali drugimi nevarnimi predmeti umorijo ali poškodujejo enega ali več posameznikov. Gre za brutalno aktivne, zelo dinamične situacije, v katerih storilec ravna na skrajno zločinsko destruktiven način in ima namen v čim krajšem času umoriti ali poškodovati čim več nedolžnih posameznikov. Zaradi tega morajo biti zaposleni in drugi (stranke, pogodbeni izvajalci ipd.) pripravljeni sodelovati v preventivnih aktivnostih na delovnem mestu za zaščito svojega življenja, še pred prihodom policije.

Razumljivo je, da je obravnavana tema občutljiva, saj v preteklosti ni nihče razmišljal ali pričakoval, da se bo moral na delovnem mestu boriti za lastno fizično preživetje. Ne obstaja samo en enoznačen odgovor, kaj storiti v navedenem primeru, ampak razmišljanje o možnem dogodku, sprejeti preventivni ukrepi in postopki, lahko povečajo verjetnost reševanja življenja zaposlenih in preprečujejo materialno škodo. Čeprav ne obstaja širši okvirni profil napadalca, je več možnih kazalnikov, ki lahko nakazujejo na možnost potencialnega napadalca.

Strelski napad se ne zgodi kar naenkrat (obstaja manjša verjetnost, da se lahko pojavi tudi spontano), ampak je v večini primerov končna faza daljšega pripravljalnega procesa (Füllgrabe, 2010). Vse aktivnosti napada so vnaprej načrtovane. Motiv storilca večinoma ni znan ter ni nikakršne povezave med storilcem in žrtvami.

Füllgrabe (2010) pravi, da ima posameznik, ki je nagnjen k strelnem napadu, narcistično osebnost in dostikrat vidi vse negativno. Njegov pogled na svet zajema prepričanje, da:

> Glavni namen odziva na strelski napad je preprečiti, zmanjšati ali omejiti dostop do potencialne žrtve, zmanjšati možnosti izgube življenj in zmanjšati materialno škodo.

*avtor je član Slovenskega združenja korporativne varnosti



- se z njim ravna nepošteno,
- ima pravico ustvariti pravičnost v svetu,
- bo z nasiljem in orožjem dosegel cilj, da ustvari boljši svet.

Največji problem predstavlja narcistično maščevanje, saj veliko posameznikov hoče biti družbeno priznanih. Storilec si hoče z ubijanjem zagotoviti, da ne bo nikoli pozabljen, pokazati, da obstaja v družbi.

Psiholoških dejavnikov, ki vplivajo na nastanek amok dogodkov je veliko, strokovnjaki za to področje pa so si enotni, da so poglavitni vsaj trije dejavniki:

- psihopatološko stanje zatemnitve zaznavanja stvarnosti, do česar lahko pride zaradi različnih psihičnih obolenj in motenj, zlorab zdravil, prepovedanih drog, alkohola in podobnih substanc – v takšnem stanju se storilec deloma ne zaveda jasno in zunanji svet zaznava v delcih, kot nevarnost zase ter zato izvede napad,
- psihopatološko stanje maničnega besa, pri čemer storilec usmerja nasilje proti povzročitelju stresa (cilju napada) – tega se hoče razbremeniti s streljanjem, gibanjem, razbijanjem, pogosto tudi s slačenjem, in fizično napade vsakega, ki ga želi pri tem ustaviti ali omejevati,
- narcistično maščevanje, do česar navadno pride, ko storilec čuti, da »umira« oziroma da ne pripada več tej družbi. Lahko se zgodi, da storilec predhodno »kliče« na pomoč, vendar se družba na ta poziv ne odzove. Za svoje »umiranje« krivi družbo, zato se odloči, da ji bo pokazal svoj »jaz« in da ga družba ne bo nikoli pozabila. Zato se odloči, da se bo maščeval »zlobnemu zunanjemu svetu«, za katerega meni, da je kriv za njegovo »umiranje«. Pri načrtovanju obstaja t. i. »pot planiranega nasilja«, pri čemer so analize pokazale, da obstajajo določene stopnje in znaki, ki jih je mogoče prepoznati, še preden se zgodi napad.

Po začetnem pojavu strelskih napadov v Evropi, je dolgo časa veljalo prepričanje, da se storilci nenadoma in nenačrtovano odločijo za izvršitev tovrstnih kaznivih dejanj. Novejša spoznanja pa kažejo, da se takšna skrajnje nasilna dejanja ne zgodijo nenadoma, temveč so storilci to nasilje načrtovali in ga razvijal po naslednjih fazah:

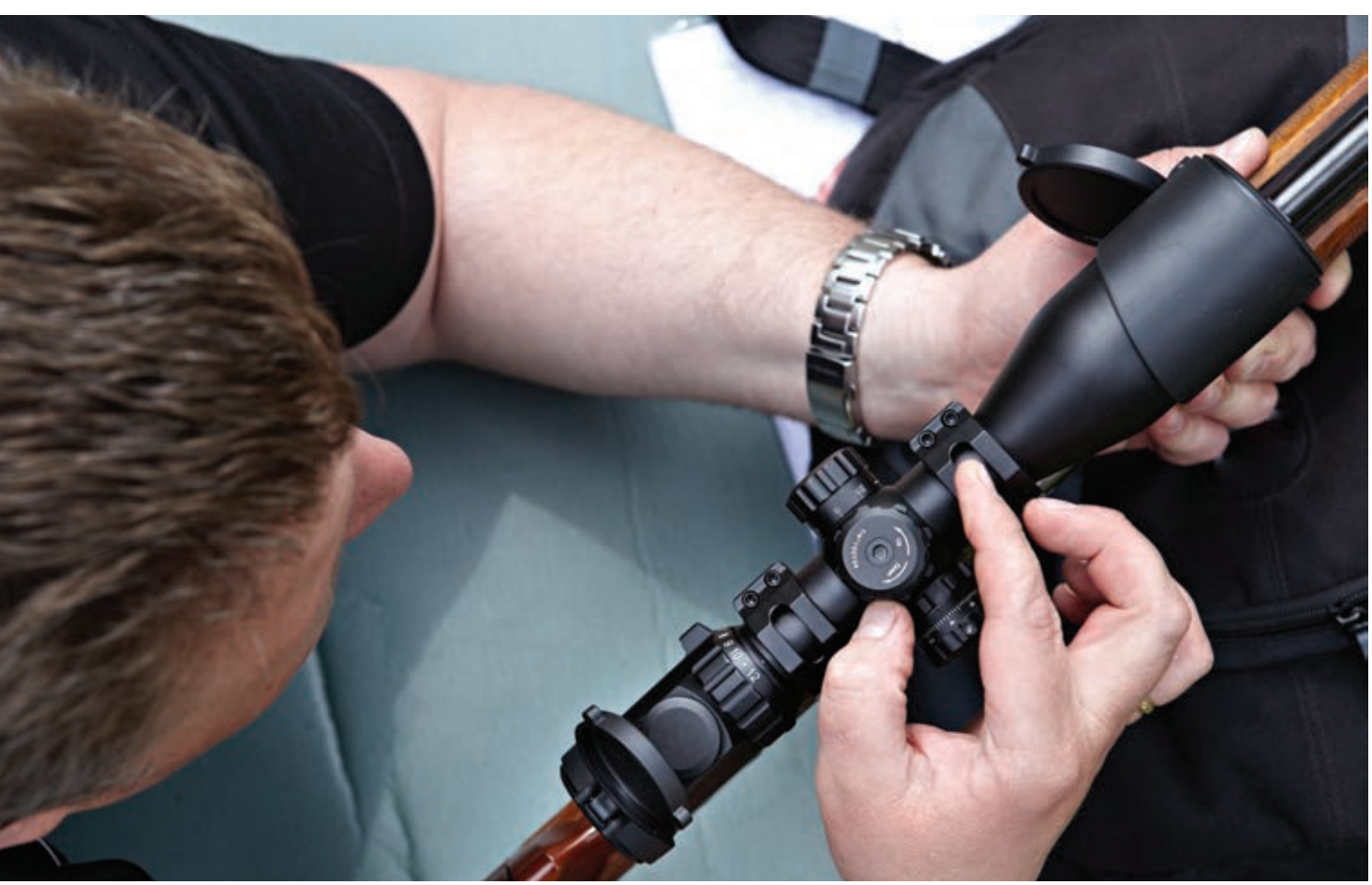
- razlog za pritoževanje – do tega pride zaradi občutka nepravičnosti, izgube, usode ipd., kar pri storilcu spodbudi željo po maščevanju, prepoznavnosti in slavi,
- zamisel – pri tej fazi gre za pogovarjanje storilca z drugimi o tovrstnih, že storjenih dogodkih, poosebljenje z drugimi storilci, navdušenje nad močjo orožja, fiksacijo na obletnice tovrstnih dogodkov iz preteklosti ipd.,
- raziskovanje in planiranje dejanja – za to fazo je značilno sumljivo ogledovanje in raziskovanje cilja napada, pridobivanje informacij, preizkušanje varnostnega sistema, izdelava načrtov ipd.,
- priprava pred napadom – pri tem storilec pridobiva in pripravlja orožje, strelivo, bombe, osebno zaščitno opremo, prevoz, išče in določa datume s posebnim pomenom, se usposablja in izvaja končne priprave,
- preizkušanje – konkretni preizkusi varnostnega sistema cilja napada, nasilen in večkrat ponovljen pristop, (ločeni) poskusi različnih aktivnosti, končni ogledi in priprave,
- izvedba strelskega napada. Ni nujno, da so v vseh primerih priprave na nasilje »prehodile enako pot«.

Upravljanje tveganj, situacijska preventiva, poznavanje svojih sodelavcev in budnost so pomembni za varnost zaposlenih na delovnih mestih.

Opozorilni znaki

Dejavnikov, ki vplivajo na to, da se bo posameznik odločil za izvedbo strelskega napada je veliko, zato je tudi veliko različnih značilnosti storilcev teh dejanj. Opozorilni znaki sprememb vedenja napadalca se lahko pojavijo, preden ta identificira cilj napada. Opozorilni znaki, poleg že zgoraj navedenih, pogosto vključujejo:

- vsako vedenje, ki je del raziskave, načrtovanja, priprave ali izvedbe napada,
- maščevanje – trpinčeni posameznik, ki meni, da ima pravico, ker ga napačno obravnavajo, hoče vplivati na skupnost s strahom, zato uporablja grožnje in silo, eksplozivne izbruhe jeze ali besa brez provokacije,
- izkušnje s pomembno ali resnično osebno izgubo v tednih in/ali mesecih pred napadom, kot so smrt bližnjih, zlom, razveza ali izguba službe,
- diskriminacija – osamljenost, odrinjenost v službi in socialni okolici, nima prijateljev, težave z učenjem, stare travme, zagrenjenost, nezmožnost navezovanja normalnih stikov z drugim spolom, težnja k samomoru,
- opozorilno vedenje, ki kaže na vse bolj patološko preokupacijo napadalca z mentalnimi težavami (povečanje agresivnosti proti drugemu ali drugi vzroki, vedno bolj napadalna mnenja, vedno večja negativna karakterizacija objekta fiksacije, vpliv družine ali drugih na objekt fiksacije, besni ali jezni posameznik – običajno ga spremlja socialno ali poklicno poslabšanje statusa, povečana močna nihanja razpoloženja ipd.),
- vsako vedenje, ki kaže na psihološko željo po oblasti ali na »vojaško miselnost«, ki je tesno povezana z orožjem ali drugim vojaškim ali varnostnim pripomočkom, se identificira s prejšnjimi napadalci ali morilci, za negativno napredovanje mnenja do določenega vzroka ali prepričanja, opazno nestabilni, čustveni odzivi,
- opozorilno vedenje agresije, ki se zdi nepovezano z nasiljem na poti in je bilo prvič storjeno. Tako vedenje se lahko uporabi za preizkušanje sposobnosti napadalca, da dejansko izvede nasilno dejanje, je lahko merilo za odziv na napad, motivacija za ukrepanje v okolju ali vedenjsko preizkušanje,
- povečanje pogostosti ali raznolikosti vseh navedenih aktivnosti, povezane s ciljem napada, tudi če so te relativno neškodljive, običajno v dnevih ali tednih pred napadom. Napadalec lahko objavi opozorilno sporočilo tretjim osebam o nameri napada (z e – pošto, na družbenem omrežju, pisno ipd.),
- obvestilo o nasilju dokazuje nasilen »akcijski imperativ«, ki se povečuje iz obupa ali stiske. Napadalec meni, da ni druge možnosti, razen nasilja in posledice nasilja so za njega utemeljene,



- neposredno sporočena opozorila o napadu. Grožnja je pisna ali ustna komunikacija, ki izrecno navaja željo ali namen škode, poškodbe ali ubijanja posameznikov, ki so simbolično ali dejansko povezani s ciljem napada.

Načrt odziva

Glavni namen odziva na strelski napad je preprečiti, zmanjšati ali omejiti dostop do potencialne žrtve, zmanjšati možnosti izgube življenj in zmanjšati materialno škodo. Možnosti za razmislek na osebni ravni o odzivanju na napad so povezani s tremi »s« (steci, skrij se, spopadi se) (Houston, 2012, FBI, FEMA), v nadaljevanju je predstavljenih nekaj konkretnih navodil za reagiranje:

- steci: takoj se odstranite iz nevarnega območja,
- skrij se: poiščite varen kraj, kjer se lahko skrijete in/ali zavrnete dostop napadalca,
- spopadi se: kjer je ogroženo vaše življenje ali življenje drugih, se lahko odločite osebno fizično napasti in oslabiti napadalca.

Tek
Če je prehodna pot za izhod v sili, se umaknite iz prostora. Evakuirajte se ne glede na to, ali se drugi strinjajo s tem; pustite svoje osebne stvari za seboj; pomagajte drugim pobegniti; če je to mogoče, preprečite drugim vstop na območje napada; ne premikajte ranjenih; ko ste na varnem pokličite policijo. Javite naslednje podatke: koliko je strelcev, kje je/so strelci, ali je/so zapustili prizorišče, kaj nosijo (vključno z neprebojnim jopičem), v kateri smeri se premikajo, katere vrste orožja imajo, koliko je bilo strelov, kdaj ste nazadnje slišali strel, kje se nahajate, koliko zaposlenih je z vami, koliko zaposlenih je ranjenih, ali so talci ipd.

Skrij se
Če umik ni varen, se skrijte na čim bolj varnem mestu. Zaklenite vrata, če so na voljo ključavnice; vrata založite s težkim pohištvom; zaprite okna in žaluzije; izklopite luči; utišajte vse elektronske naprave; skrijte se za omaro ali mizo; če je mogoče, pokličite policijo; če ne morete govoriti, pustite odprto telefonsko linijo.

Spopadi se
Kot zadnje sredstvo in le, če je vaše življenje v neposredni nevarnosti, poskušajte prekiniti in/ali onesposobiti napadalca tako, da čim bolj agresivno delujete proti njemu; mečete predmete (gasilni aparat, stol, prenosni računalnik, fascikel ipd.); kričite; sprejmite posledice svojega dejanja (silobran).

Zaključek

Upravljanje tveganj, situacijska preventiva, poznavanje svojih sodelavcev in budnost so pomembni za varnost zaposlenih na delovnih mestih. zkušnje držav, kjer je prihajalo do strelskih napadov, kažejo, da se morajo vsi deležniki varnosti v družbi skupno soočati s tem pojavom. Medinstitucionalni pristop je ključnega pomena za učinkovito in uspešno preprečevanje tovrstnih dogodkov, saj samostojno ukrepanje posameznih subjektov ne daje pravega učinka. Začeti je treba že pri ustrezni vzgoji otrok v družini in izgrajevanju strpne družbe z ničelno toleranco do nasilja, centri za socialno delo, zdravstvene ustanove, kadrovske službe podjetij, policija in drugi organi pa se morajo bolj aktivno povezovati ter si izmenjevati podatke, ki lahko pripomorejo k temu, da se pravočasno odpravijo dejavniki, ki lahko privedejo do strelskega napada.

Posameznikov miselni konstrukt realnosti se nanaša na »objektivno« oceno stvarnosti v doživljanju okolja. Večina redko, če kdajkoli, doživi nenormalno situacijo zaradi naravne nesreče ali nevarnega dogodka, ki ga povzroči posameznik. Rezultat tega je, da večina ne zazna tveganja, zavajajoče izkušnje pa lahko posameznika vodijo tudi v prepričanje, da je imun pred možnimi nenormalnimi situacijami, da se »to njemu ne more pripetiti«. Namesto tega večina misli, da so varni pred naravo in drugim posameznikom (na tisto, česar ne vidijo, tudi ne pomislijo). Raziskave o zaznavanju tveganja sklepajo, da večina posameznikov misli, da se nenormalne situacije v bližnji prihodnosti ne bodo zgodile, in če se bodo zgodile, se bodo zgodile drugim in ne z njim. To predstavlja problem za tiste, ki opozarjajo na možen strelski napad. Opozorila morajo premagati naravno prepričanje, ko posameznik misli, da je varen, in ga nato usmerjati, da sprejme zaščitne ukrepe in postopke, ki niso povsem v skladu z njegovim dojemanjem varnosti na delovnem mestu. Dejansko je ocena nevarnosti strelskega napada zelo zapleten proces, zasnovan bolj na teoretičnih analizah, simulacijah raznih scenarijev kot na neposredni izkušnji.



Opozorila morajo premagati naravno prepričanje, ko posameznik misli, da je varen, in ga nato usmerjati, da sprejme zaščitne ukrepe in postopke, ki niso povsem v skladu z njegovim dojemanjem varnosti na delovnem mestu.



Pripravljenost na strelski napad vključuje: preprečevanje, zaščito, ublažitev, odzivanje in okrevanje. Ta področja se nanašajo na tri časovne okvire, ki so povezani z dogodkom: pred napadom, med napadom in aktivnostim po strelskem napadu.

Načrtovanje in odzivanje na strelski napad se nanaša na pet faz upravljanja (Emergency Operations Plans, 2014):

- preprečevanje, pomeni aktivnosti in zmožnosti, potrebne za preprečitev, zaustavljanje ali zaustavitev neposredne grožnje napada. Preprečevanje se nanaša na ukrepe in aktivnosti za ohranitev varnosti na delovnem mestu,
- zaščita pomeni zmožnost zavarovanja zaposlenih pred strelnim napadom. Zaščita se osredotoča na upravljanje tveganj, varnostno organizacijo, fizično, tehnično, mehansko varovanje, stalne in občasne ukrepe ter postopke, ki ščitijo zaposlene pred ogrožanjem na delovnem mestu,
- omilitev pomeni zmožnosti, potrebne za odpravo ali zmanjšanje posledic izgube življenja zaposlenega in premoženjske škode podjetja z zmanjšanjem vpliva posledic napada. To tudi pomeni zmanjšanje verjetnosti, da se bo napad dejansko zgodil,
- odziv pomeni zmogljivosti, potrebne za stabilizacijo nenormalne situacije, ki se je že zgodila. Nanaša se na obnovo in vzpostavitev varnega delovnega okolja, zavarovanje življenja zaposlenih, preprečevanje uničenja premoženja podjetja in olajšanje prehoda na okrevanje,
- obnova pomeni zmogljivosti, potrebne za pomoč podjetju, ki je doživelo strelski napad, pri čimprejšnjem obnavljanju poslovne dejavnosti in zmanjšanju ter odpravi posledic napada.
- Ne glede na vse navedeno, se strelskega napada ne da popolnoma preprečiti, lahko pa se z ustreznim skupnim pristopom zmanjša tveganje za njegov nastanek. Posebna pozornost naj bo namenjena usposabljanju zaposlenih za navedeni primer. To bo priložnost, da se zagotovi pripravljenost na možni strelski napad in tako se bo zmanjšal tudi strah na delovnem mestu.

Literatura:

1. FBI Active Shooter Resources. https://www.fbi.gov/about/partnerships/office-of-partnerengagement/active-shooter-resources. 8.10.2018.
2. FEMA Active Shooter online training course - IS-907: Active Shooter: What You Can Do? https://training.fema.gov/is/courseoverview.aspx?code=IS-907. 12.10.2018.
3. Füllgrabe, U. (2010). Amok: Gesellschaftliche und kulturelle Hintergrundfaktoren. Kriminalistik, 64(5), 288-294.
4. Houston, R. (2012). Regional Disaster Preparedness: Run > Hide > Fight Surviving an Active Shooter. http://www.readyhoustontx.gov/videos.html. 4.10.2018.
5. Incorporating Active Shooter Incident Planning into Healthcare Facility Emergency Operations Plans (2014). HHS, ASPR, DHS, FEMA, U.S. Dept. of Justice and FBI. ■

Avtor: mag. Matjaž Drev / Urad Informacijskega pooblaščenca RS*



BODO OSEBNI PODATKI ZARADI GDPR BOLJE VAROVANI?

V prvi polovici leta 2018 se je v javnosti ustvaril vtis, da so osebni podatki dejansko postali nova valuta, kratica »GDPR« pa se je v kolektivno zavest zakoreninila kot simbol nove evropske zakonodaje, ki bo v temeljih spremenila področje varstva osebnih podatkov, če ne drugače, z večmilijonskimi kaznimi. Zato ne preseneča, da se je vprašanje ali gre za revolucijo na področju regulacije varstva osebnih podatkov pogosto zastavljalo celo v ožjih strokovnih krogih. Odgovori so bili pogosto odvisni od interesov in pričakovanj posameznih deležnikov, kar je še dodatno zapletlo razumevanje kaj GDPR sploh je in kaj pomeni za upravljavce osebnih podatkov v Evropski uniji.

Uvodoma velja pojasniti, da je **GDPR** angleška kratica za Splošno uredbo o varstvu podatkov (ang. **G**eneral **D**ata **P**rotection **R**egulation). Ta predstavlja nov zakonodajni okvir, ki ureja področje varstva osebnih podatkov na območju Evropske unije in nadomešča Direktivo 95/46/ES iz leta 1995, ki je do 25.5.2018, ko se je začelo neposredno uporabljati določbe GDPR, določala pravila igre na področju varstva osebnih podatkov. Države članice EU so na podlagi prej omenjene direktive sprejele nacionalne zakone in na podlagi teh izvajale inšpekcijski nadzor v zvezi z (ne)zakonito obdelavo osebnih podatkov. V Sloveniji je to nalogo prevzel Informacijski pooblaščenec. Nacionalni zakon, ki je stopil v veljavo 1.1.2005 in predstavlja prenos zahtev omenjene direktive v slovenski pravni red, pa se imenuje Zakon o varstvu osebnih podatkov (ZVOP-1).

Zapisano drugače: Varstvo osebnih podatkov se v EU ni začelo sistematično urejati šele 25.5.2018, ko se je začela neposredno uporabljati GDPR, pač pa že leta 1995, ko je bila sprejeta Direktiva 95/46/ES. Iz primerjalnega branja Direktive 95/46/ES, ZVOP-1 in GDPR je razvidno, da so bili temelji varstva osebnih podatkov postavljeni že leta 1995 in da GDPR zato ne prinaša radikalnih sprememb, pač pa nujno potrebne posodobitve. Nov zakonodajni okvir tako ne predstavlja revolucije, pač pa evolucijo varstva osebnih podatkov v EU.

Ob tem se velja vprašati, zakaj sploh prenova celotnega zakonodajnega okvirja. Razlogov je več. Temelj je sicer res bil postavljen že leta 1995, vendar so posamezne države članice EU v različnih časovnih intervalih in na različne načine implementirale določbe Direktive 95/46/ES v svoje nacionalne zakone, zaradi česar varstvo osebnih podatkov v EU vsaj na operativni ravni ni bilo poenoteno. Dodatno težavo je povzročalo ne dovolj učinkovito mednarodno sodelovanje. Vse večji delež obdelave osebnih podatkov so prevzemale mednarodne korporacije, ki jih je bilo zaradi geografske razpršenosti in izrazite finančne (pre)moči težko, včasih celo nemogoče, ustrezno regulirati. Ob tem je težnjo po posodobitvi zakonodajnega okvirja dodatno spodbudil hiter razvoj informacijske tehnologije v povezavi z množično obdelavo osebnih podatkov v kontekstu »računalniških oblakov«, »interneta stvari« in »pametnih mest«. Kot na drugih področjih varnosti, se je tudi tu izrazila potreba po vključevanju različnih deležnikov javnega in zasebnega sektorja (t.i. javno zasebno partnerstvo) v izgradnjo celovitega sistema varstva osebnih podatkov. Izkazalo se je, da zgolj represivni pristop ne bo zadoščal, ampak bo potrebno vzpostaviti preventivno razsežnost, zato je GDPR vpeljal koncepte, kot so »vgrajena zasebnost«, »ocene učinkov tveganj na zasebnost« in »samoprijave kršitev varstva osebnih podatkov«.

Vendar pa osnovi ni koncepti, sem sodijo kategorije »pojmov«, »načel«, »pravne podlage za obdelavo osebnih podatkov«, »pogodbene obdelave«, »iznosa osebnih podatkov v tretje države« in »zavarovanja osebnih podatkov«, ostajajo podobni. Zato upravljavce, ki so imeli že pred 25.5.2018 zgledno urejeno varstvo osebnih podatkov, spremembe ki jih prinaša GDPR, ne bi smele pretirano skrbeti.

Med temi spremembami je tudi nekaj opaznih novosti, ki utegnejo pomembno vplivati na operativno izvedbo varstva osebnih podatkov in s tem posredno tudi na dvig splošne ravni varnosti.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Obseg prispevka ne dopušča celovitega pregleda vseh novosti, zato bodo na tem mestu omenjene nekatere bolj zanimive. Dve takšni sta upoštevanje konceptov »vgrajene« in »privzete« zasebnosti, ter izdelava »ocen učinkov tveganj na zasebnost«. Gre za to, da naj bi se v primerih, kjer se bo izvajala množična obdelava osebnih podatkov z informacijskimi sredstvi, in kjer je tveganje za varstvo osebnih podatkov še posebej veliko, že v začetni fazi priprave projekta razmislilo in dokumentiralo, kako celoten proces obdelave izpeljati na način, ki bo predstavljal kar najmanjši poseg v zasebnost posameznikov glede na zasledovani cilj, hkrati pa se bo predvidelo ključna tveganja in vgradilo varovalke, ki bodo tveganja zmanjšale oziroma zmanjšale škodljive posledice.

Opazna novost je tudi oblikovanje novega poklica oziroma vloge »pooblaščenih oseb za varstvo podatkov«. Nekatere organizacije (javni sektor, upravljavci, kjer obdelava osebnih podatkov predstavlja temeljno dejavnost, upravljavci, ki obsežno obdelujejo občutljive osebne podatke) bodo morale imenovati pooblaščene osebe za varstvo podatkov, ki bodo opravljale vlogo svetovalcev in koordinatorjev, in ki naj bi s svojim aktivnim pristopom prispevale k izgraditvi bolj varnih procesov obdelave osebnih podatkov.

Dodatna ključna novost je vzpostavitev sistema »samoprijav«. Pred 25.5.2018 upravljavci in pogodbeni obdelovalci, če so zaznali kršitev varstva osebnih podatkov, te niso bili dolžni prijaviti nadzornemu organu. Zdaj je drugače. V primerih hujših kršitev varstva osebnih podatkov je treba obvestiti nadzorni organ, v primerih najhujših kršitev pa celo prizadete posameznike.

Omembe vredna novost je tudi možnost sprejetja posebnih kodeksov in pridobitev certifikatov s področja varstva osebnih podatkov. Osnovna ideja sledi že uveljavljenim praksam certificiranja organizacij, vendar velja opozoriti, da uradnih certifikatov (GDPR jih imenuje »mehanizmi potrjevanja«) zaenkrat še ni mogoče pridobiti, se pa na trgu pojavljajo druge oblike certificiranja, zaradi česar prihaja do nejasnosti in napačnega razumevanja.

Namen prispevka ni izčrpno prikazati GDPR in sprememb, ki jih ta prinaša, pač pa v osnovnih obrisih pojasniti kaj GDPR sploh je, kakšne bodo nekatere najbolj opazne novosti, hkrati pa opozoriti, da področje varstva osebnih podatkov ni nekaj novega, ampak se v EU sistematično ureja že od leta 1995. GDPR v tem kontekstu prinaša pomembne in nujne posodobitve, vendar gre, kot že zapisano, za evolucijo in ne za revolucijo na področju varstva osebnih podatkov v EU. Seveda pa bo zgolj čas pokazal ali bodo zaradi GDPR in sprememb, ki jih ta prinaša, osebni podatki v »virtualnem svetu« bolje zavarovani ali ne.

Viri:

- Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.
- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
- Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07-UPB1). ■

10. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

13. – 14. MAREC 2019



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 INSTITUTA WWW.ICS-INSTITUT.SI!

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*



REPORTAŽA

ZAKLJUČKI NACIONALNEGA POSVETA S PODROČJA KIBERNETSKE VARNOSTI

V četrtek 15.11.2018 se je v Državnem svetu Republike Slovenije odvijal odmeven posvet z naslovom »Kibernetska varnost Republike Slovenije v luči vedno pogostojših hekerskih vdorov – kako učinkovito implementirati rešitve Zakona o informacijski varnosti?«. Posvet je potekal v okviru soorganizacije Informacijskega pooblaščenca, Urada za varovanje tajnih podatkov, SI-CERT in Instituta za korporativne varnostne študije.

Popolnoma polna dvorana je vsekakor dober pokazatelj, kako pereča je obravnavana tema, povezana s tveganji v kibernetskem okolju in kako pomembna je javna razprava za dvigovanje razumevanja in za strateške odločitve na tem kompleksnem področju.

Posvet sta s svojimi nagovori odprla mag. Sandi Čurin, državni sekretar na MNZ in ga. Mojca Prelesnik, Informacijska pooblaščenka. V nadaljevanju je dr. Denis Čaleta, predsednik Slovenskega združenja za korporativno varnost, svečano sprejel nove korporativne člane v Slovensko združenje korporativne varnosti. V združenje so bili uradno sprejeti naslednji korporativni člani dr. Marta Svoljšak Jerman, Petrol d.d., g. David Marjanović, Petrol d.d., g. Božidar Dajčman, NKBM d.d., ga. Irena Španinger, NKBM d.d. in g. Bojan Peršl, UKC Ljubljana.

V nadaljevanju je potekala zanimiva razprava v okviru okrogle mize, na kateri so sodelovali mag. Matej Tonin, poslanec DZ RS, mag.Nataša Dolenc, v.d. direktorja UVTP, mag. Tanja Muha, direktorica AKOS, g. Gorazd Božič, SI-CERT in g. Marjan Kavčič, Direktorat za informacijsko družbo, Ministrstvo za javno upravo. Razpravo je moderiral dr. Denis Čaleta, ICS-Ljubljana.

Glavne poudarke razprave lahko združimo v naslednja težišča:

- Država in pooblaščene institucije že zamujajo z izdelavo podzakonskih predpisov, ki so ključni za nadaljevanje implementacije Zakona o informacijski varnosti;
- Razumevanje strateške politike je ključno za nadaljevanje sistemske ureditve in implementacijo določil Zakona o informacijski varnosti v realno življenje. S tem, da se svetovalec predsednika vlade za nacionalno varnost, brez jasno opredeljenega razloga, ni želel udeležiti pomembne razprave, nas ne navdaja z optimizmom glede razumevanja in prioritizacije kibernetske varnosti v Republiki Sloveniji;
- Državni zbor s svojimi komisijami, kakor tudi Vlada RS, imata v okviru dvigovanja varnostnega zavedanja v celotni družbi izredno pomembno vlogo;
- Pomanjkanje kadrovskih virov je bilo izpostavljeno kot resen problem, ki se ga bo potrebno lotevati zelo načrtno in v okviru javno-zasebnega sodelovanja;
- Ravno tako bo potrebno javno-zasebnemu partnerstvu v prihodnje nameniti veliko več pozornosti, kot smo ji bili priča do sedaj. Omenjeni Zakon o informacijski varnosti za to predvideva zelo jasne podlage. Bistveno pa je razumevanje pri najbolj odgovornih akterjih v nacionalno-varnostnem okolju. Nacionalne institucije morajo biti na čelu razvoja tega partnerstva, ne pa kot v večini sedanjih primerov, glavna ovira in zaviralci;

*avtor je član Slovenskega združenja korporativne varnosti

- Ključni organi, ki imajo trenutno največ pristojnosti in tudi odgovornosti, kot na primer UVTP, nujno potrebujejo dodatne kadrovske vire, za uspešno izvedbo zastavljenih nalog, izhajajočih iz zgoraj navedenega zakona;
- Pri pripravi podzakonskih aktov se je potrebno izogniti podvajanju in predvsem drugačnim metodološkim izhodiščem, ki jih v realno okolje že prinašajo Zakon o kritični infrastrukturi in drugi pomembni zakoni. Nikakor ne smemo dovoliti, da se neposredni upravljavci bistvenih storitev, še dodatno obremenijo z birokratskimi zavezami, temveč je potrebno skozi sodelovanje iskati sinergije za skupno delovanje na področju preprečevanja kibernetskih tveganj. V razpravi so bili izpostavljeni tudi primeri dobre prakse sodelovanja bančnega sektorja z SI-CERT in seveda aktivnosti, ki se odvijajo v okviru Slovenskega združenja korporativne varnosti;



- Kibernetska tveganja informacijskega okolja so dejstvo, zato nas to spoznanje sili v aktivnejši pristop do reševanja izzivov, ki se pojavljajo na tem kompleksnem področju;
- Vsi razpravljalci so si želeli, da bi bila kibernetska varnost na prioritetni listi vsakokratne vladajoče politike, višje. Pričakovanja od trenutne vlade so visoka. Dokazati pa jih bo potrebno s povečanjem vložkov, predvsem finančnih in kadrovskih, na to zahtevno področje. Podani so bili tudi predlogi, da bi bilo potrebno določiti odstotek od BDP, ki bi se namenil temu zelo pomembnemu področju;
- V prihodnosti se tudi v evropskem okolju pričakuje spremembe določenih usmeritev in direktiv, kar bi lahko prineslo poenostavitev oz. poenotenje določenih procesov, ki so sedaj razpršeni oz. se v določenih delih podvajajo;
- SI-CERT vsekakor ostaja najpomembnejši operativni organ na področju kibernetske varnosti, ki ga nikakor ne smemo podirati, temveč na njegovem delovanju iskati druge bolj primerne oblike organiziranosti in delovanja;
- Pojavlja se pomanjkanje koordinacije med vsemi pristojnimi organi, kar bo v prihodnjem obdobju ena od najbolj prioritetnih nalog;
- Z uvajanjem novih storitev 5G se bo močno razširil krog subjektov, ki se bodo pojavljali v okviru digitalnih procesov in informacijskih storitev. To AKOS postavlja v še pomembnejšo vlogo pri koordinaciji in nadzoru tega pomembnega področja;
- Nujno bo potrebno sprejeti akcijski načrt za implementacijo določil Strategije o kibernetski varnosti, samega Zakona o informacijski varnosti, kakor tudi priprave nove strategije o informacijski varnosti. Velik del razpravljavcev je posebej izrazil pričakovanje, da mora področje kibernetske varnosti imeti pomembnejšo mesto v okviru nove Zasnove o strategiji nacionalne varnosti RS.
- V razpravi je bilo posebej izpostavljeno obžalovanje, da trenutni Zakon o informacijski varnosti ni uzakonil odgovornega poročanja o varnostnih ranljivostih. Udeleženci posveta so bili soglasni, da je skrajni čas, da se tudi v Sloveniji naredi korak naprej tako na ravni pravne regulacije oz. postavitve pravnega okvira odgovornega razkrivanja varnostnih ranljivosti, kot tudi v smeri dviga ozaveščenosti odgovornih o nujnosti hitrega ukrepanja ob razkritju. Obstoječo definicijo kaznivega dejanja napada na informacijski sistem bi namreč dejansko lahko razumeli kot absolutno kriminalizacijo vsakršnega, tudi odgovornega prepoznavanja varnostnih ranljivosti informacijskih sistemov, ki pušča zelo majhne (tako rekoč nične) možnosti za izključitev protipravnosti v primeru naročenih testov ranljivosti ali obstoja skrajne sile. Pravnega instituta, ki bi posebej v teh primerih izključeval protipravnost, namreč ni. Zgolj na posameznem državnem tožilcu tako leži odgovornost za presojo ali obstajajo v posameznem primeru okoliščine, ki upravičujejo odločitev, da se kljub obstoju vseh znakov kaznivega dejanja, bodisi kazenski pregon odloži, bodisi se kazenskega pregona ne začne ali se od pregona odstopi. To pa ne zagotavlja nobenih varovalk za zaščito posameznikov, ki so varnostne ranljivosti razkrili.

V zaključku posveta se je v razpravo vključila tudi zainteresirana publika tako, da smo imeli priložnost slišati tudi kaj se dogaja s procesi vzpostavitve CSIRTA državnih organov, kako se Slovenska vojska sooča z izzivi na področju kibernetske obrambe, ali sploh razumemo pravi pomen in vlogo kibernetske varnosti ter mnenje o zlorabah medijske zakonodaje, kot delom kibernetsko propagandnih tveganj.

Za konec še enkrat povzamimo misel, ki jo je na uvodu izrekel moderator posveta dr. Denis Čaleta in sicer »čas za iluzije je minil. Pred nami je čas, ki od nas zahteva smelost, operativno učinkovitost in preseganje parcialnih interesov posameznih organizacij v smeri zagotavljanja ustrezne kibernetske varnosti Republike Slovenije.«

Vsekakor je bila splošno podprta ideja o nadaljevanju podobnih javnih razprav, ki na eni strani dvigujejo varnostno zavedanje, ter na drugi strani strateškim odločevalcem prinašajo ustrezne strokovne predloge, s strani zainteresirane strokovne javnosti. Za zaključek je bilo slišati, da bodo organizatorji tega posveta vsekakor nadaljevali po tej poti. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj Upravljanje s tveganji in korporativna varnost?

- **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

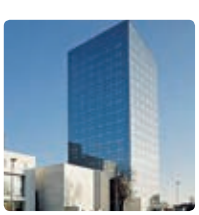
FAKULTETA ZA PODJETNIŠTVO

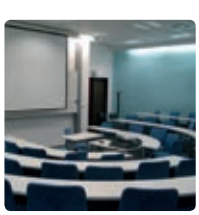
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

10. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

»RISK MANAGEMENT IN CYBERSPACE«

INTEGRACIJA FIZIČNIH IN INFORMACIJSKIH PROCESOV

NUJNOST KIBERNETSKEGA OKOLJA



13.—14. marec 2019

DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI