Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2018, junij • št. 17



Tradicionalni posvet »Nadzor na delovnem mestu« Ljubljana, 26. september 2018

Policija ostaja eden izmed ključnih državotvornih resorjev

g. Simon Velički, Generalni direktor Policije



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
junij 2018

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

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

Pred nami so poletni dopustniški dnevi, ki pa nikakor ne bodo brezbrižni, kot bi človek pričakoval od tega obdobja. Globalno poslovno in varnostno okolje je izredno dinamično in pred nas venomer postavlja nova tveganja in grožnje za delovanje naših organizacij. Rezultati ravnokar končanih državnozborskih volitev vsekakor obetajo pestro in turbulentno obdobje sestavljanja nove vlade. Vprašajmo se sicer, kaj ima korporativno varnostno okolje s procesom sestavljanja nove vlade. Veliko več, kot bi si seveda želeli. Politične stranke so varnosti v predvolilnem obdobju namenjale sicer večjo pozornost, kot v prejšnjih letih. To pa predvsem zaradi dejstva, da varnostne razmere v mednarodnem prostoru, ki nas obdaja, vsekakor niso vzpodbujajoče. Migrantska problematika, procesi radikalizacije posameznikov, kibernetska tveganja, negativni vplivi narave in nove geostrateške težnje vplivajo tudi na stanje varnosti v Republiki Sloveniji. Glede na dejstvo, da smo v preteklem obdobju, ko se je država reševala iz objema finančne krize, zelo restriktivno posegli v vire za delovanje ključnih nacionalno-varnostnih organov, bi pričakovali od nove vlade hitre in nujne strukturne spremembe, v smeri krepitve teh institucij. Zagotavljanje varnosti v gospodarstvu je zelo močno odvisno od učinkovitega in dobrega delovanja nacionalnih varnostnih organov ter tesnega sodelovanja s predstavniki korporativne varnosti. Če korporativna varnost na drugi strani nima ustreznega sogovornika in partnerja, ki je odziven in razume pomen tesnega sodelovanja pri obvladovanju celega niza tveganj, lahko pride do resnih težav pri zagotavljanju varnosti v teh organizacijah. V tem okviru še posebej izpostavljamo organizacije, ki upravljajo s kritično infrastrukturo. Dobri poslovni rezultati bi morali biti tisti temelj, na katerem bi strateški management teh organizacij, namenil več virov za krepitev varnostnih sistemov v svojih organizacijah, ter le te pripravil na bližajoče nove varnostne izzive, ki sledijo v prihodnosti. V tem okviru so posebej izpostavljena tveganja, ki prihajajo iz kibernetskega okolja.

V zadnjem obdobju smo tudi v Republiki Sloveniji priča nekaterim pomembnim procesom, ki bodo v prihodnje zaznamovali področje, ki je povezano z zagotavljanjem varnosti. V tem okviru posebej izpostavljamo štiri ključna področja, ki so povezana z Zakonom o kritični infrastrukturi, uvajanju evropske uredbe o varstvu osebnih podatkov (GDPR), Zakonu o informacijski varnosti in varnostnim tveganjem, ki jih v naših organizacijah predstavlja človeški potencial.

V tokratni številki prinašamo cel niz aktualnih tem. Posebno pozornost posvečamo izzivom, ki jih prinašajo migracije, dotikamo se pomembnih tem iz korporativno varnostnega okolja, kot so pomen neprekinjenosti delovanja organizacij, radikalizaciji posameznikov v organizacijah kritične infrastrukture in izzivom, ki stojijo pred področjem zasebnega varovanja. 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 prestižni konferenci Dnevi korporativne varnosti in podelitvi odmevnih nagrad Slovenian Grand Security Award, pa prinašamo vpogled v ključne trenutke tega dogodka in nagrajence, ki so letos prejeli nagrade.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
g. Simon Velički, Generalni direktor Policije

POLICIJA OSTAJA EDEN OD KLJUČNIH DRŽAVOTVORNIH RESORJEV

10



NAČRTI NEPREKINJENEGA POSLOVANJA IN KRIZNI NAČRTI V FUNKCIJI OBVLADOVANJA TVEGANJ

Neprekinjenemu poslovanju in kriznemu vodenju se v javnem in zasebnem sektorju daje premalo pozornosti. Seveda je zagotavljanje neprekinjenega poslovanja, s kriznim vodenjem vred, veliko bolj zahtevno v gospodarskih družbah, ki se morajo spopadati s konkurenco ter z vedno novimi izzivi in spremembami.

18



PROTISLOVJA MIGRACIJ IN PRIHODNOST EU

„Ne nasprotujem migracijam, je pa povsem razumljivo, da jih treba omejiti, ljudem pa omogočiti integracijo in se zoperstaviti diskriminaciji“.

/Ayaan Hirsi Ali, aktivistka človekovih pravic/

29



TVEGANJA RADIKALIZACIJE ZAPOSLENIH V ORGANIZACIJAH KRITIČNE INFRASTRUKTURE

Podrobna analiza dejavnikov tveganja, katerim so izpostavljene demokratične družbe v Evropi, zelo hitro prinese ugotovitev, da grožnje niso povezane samo z zunanjimi dejavniki, temveč, da tiste zelo izpostavljene, najdemo ravno znotraj teh družbenih skupnosti.

34



ALI LAHKO NEKAJ, KAR NAS NA PREPROSTEJŠI NAČIN POVEZUJE, PREDSTAVLJA NOVA TVEGANJA?

Danes živimo v dobi, ko nam brezžična omrežja predstavljajo del našega vsakdana, in prav vsa brezžična omrežja so ranljiva in izpostavljena hekerskim napadom.

48

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



KORPORATIVNA VARNOST JE ŠE V ISKANJU USTREZNEGA MESTA V POSLOVNEM OKOLJU

V konkurenčni tekmi so uspešna tista podjetja, ki so se sposobna čim hitreje prilagoditi novim situacijam. Če strateško vodstvo podjetja zanemari obvladovanje varnostnih tveganj, lahko to pomeni izgubo konkurenčnosti, vrednosti delnic podjetja, izgubo delovnih mest, opustitev proizvodnih programov in nenazadnje propad podjetja. Zato morajo lastniki podjetij zahtevati, da se z njihovim premoženjem ustrezno upravlja, da so naložbe varne in nemoteno delujejo ter prinašajo povečanje vrednosti. Uprave so v določenih segmentih odškodninsko, kakor tudi kazensko, odgovorne zaradi neupoštevanja predpisanih varnostnih zahtev. Zaradi navedenega je nujno, da razumemo vlogo in pomen procesa korporativne varnosti, kot orodja v rokah strateškega managementa.

Uvod

Dinamično poslovno okolje, ki je prežeto s celim nizom tveganj in groženj pred poslovne organizacije postavlja zahtevo po ustreznem zavedanju, da je celovitost obvladovanja tveganj in neprekinjenost poslovanja tisti nujni dejavnik uspešnega poslovanja in preživetja na konkurenčnem trgu. Dvigovanju varnostnega zavedanja in pomena korporativne varnosti v slovenskih podjetjih niso prinesli samo tuji lastniki, temveč tudi odpiranje in nastopanje na globalnem trgu ter izkušnje z raznovrstnimi škodnimi in varnostno izpostavljenimi dogodki. Vse to je poslovodstva prisililo k aktivnejšemu urejanju korporativne varnosti v njihovih organizacijskih okoljih.

Pojavljajo se nove oblike varnostnih tveganj, ki imajo zelo močan negativni vpliv na poslovanje in na samo varnost zaposlenih ter premoženje podjetja. Globalizacija je poleg pozitivnih stvari prinesla tudi kar nekaj negativnih. Soočanje z globalnimi varnostnimi izzivi, organiziran kriminal, terorizem, kibernetski napadi, deviantnosti, ki jih izvajajo zaposleni, odtujitve ključnih poslovnih organizacij podjetja in še bi lahko naštevali so sigurno del negativnih procesov glo-

Korporativna varnost je v najširšem pomenu besede dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Kot taka predstavlja eno od osnovnih funkcij za delovanje podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi ostalimi ključnimi funkcijami v podjetju.

*avtor je član Slovenskega združenja korporativne varnosti



balizacije. Realnost je, da je potrebno v podjetjih storiti vse potrebno, da se taka tveganja obvladajo, na nek še sprejemljiv nivo. Korporativna varnost strateškemu vodstvu podjetij zagotavlja učinkoviti mehanizem upravljanja s tveganji.

Definicija korporativne varnosti

Korporativna varnost je v najširšem pomenu besede dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Kot taka predstavlja eno od osnovnih funkcij za delovanje podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi ostalimi ključnimi funkcijami v podjetju. Celovito področje korporativne varnosti, za ustrezno obvladovanje varnostnih tveganj v korporaciji, nujno vključuje področje varnosti, procese neprekinjenega poslovanja, risk managementa, informacijske varnosti, varovanja ključnih informacij podjetja, varnosti zaposlenih in varnosti pri delu. Procesi zagotavljanja korporativne varnosti so nedeljiva celota krovnega modela upravljanja korporacij, ki se izraža skozi korporativno upravljanje in korporativno družbeno odgovornost. Predvsem slednja korporativno varnost, kot proces, postavlja v širši okvir delovanja v razmerju korporacije do družbe kot celote, v okolju, kjer le ta deluje. Korporativna varnost je zaradi svoje kompleksnosti in umeščenosti v širok spekter raznovrstnih procesov delovanja organizacij, še bolj odvisna od uvajanja vedno novih spoznanj.

Podjetja se zaradi vedno bolj izraženih tveganj v okolju poslovanja vedno bolj zavedajo pomena učinkovitega izvajanja korporativne varnosti. Temu procesu smo v zadnjem obdobju priča tudi v Sloveniji.

Celovito področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj v korporaciji nujno vključuje področje fizične, tehnične in informacijske varnosti, procesa neprekinjenega poslovanja, risk managementa, varovanja ključnih informacij podjetja, varovanja zaposlenih in varnosti pri delu.

Tveganja ob neupoštevanju procesa korporativne varnosti

Podjetje, ki zanemarja pomen obvladovanja varnostnih tveganj, je dolgoročno obsojeno na stagnacijo. Tveganja in grožnje poslovnemu procesu, brez njihovega ustreznega obvladovanja, prinesejo povečanje škodnih dogodkov, prekinitve poslovnih aktivnosti, povečanje tveganj povezanih s kadrovskim potencialom in odtekanje ključnih poslovnih informacij. To prinese zmanjšanje konkurenčne sposobnosti v zahtevnem globalnem okolju in izgubo poslovnih partnerjev ter strank. Na področju uveljavljanja korporativne varnosti ekonomska teorija minimalnih vložkov na eni strani in maksimalnih dobičkov na drugi strani, ne zdrži. Pomembno je vzpostaviti zavedanje, da so vložki na področju zagotavljanja korporativne varnosti investicija v obvladljivost in učinkovitost delovanja podjetja in ne nepotreben strošek. Celovito področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj v korporaciji nujno vključuje področje fizične, tehnične in informacijske varnosti, procesa neprekinjenega poslovanja, risk managementa, varovanja ključnih informacij podjetja, varovanja zaposlenih in varnosti pri delu.

Opredelitev sistema korporativne varnosti v podjetju

V podjetju morajo določiti jasno opredeljeno varnostno politiko in pred sprejemanjem ključnih odločitev izvesti temeljit posnetek stanja. Opredeliti in oceniti je treba tveganja in grožnje, predvsem v osnovnem poslovnem procesu in izvesti potrebne ukrepe za celovito obvladovanje varnostnih tveganj na še sprejemljivem nivoju. Nesorazmernost delovanja poslovnega procesa in varnostnih ukrepov ima lahko za podjetje tudi negativne posledice. Omejitev finančnih in drugih virov nas vedno postavljajo pred zahtevo prioritizacije pri izvedbi določenih ukrepov na področju zagotavljanja korporativne varnosti. Vedno obstaja določen odstotek tveganj, ki jih je nemogoče obvladati in bi njihovo obvladovanje povzročilo nesorazmerne finančne vložke. Tako vrsto tveganj v korporativnem okolju obvladujemo preko sistema preprečevanja škod z vzvodi, ki nam jih ponuja zavarovanje posameznih rizikov. Področje korporativne varnosti je v svojem bistvu še posebej občutljivo na nesistemske pristope, ki kljub trenutnemu večkratnemu povečanju sredstev vloženih na to področje sorazmerno ne prinese želenih rezultatov. V tem okviru je še posebej pomembna sistematičnost in kontinuiranost izvajanja procesov na področju zagotavljanja korporativne varnosti.

Digitalizacija in informatizacija družbe

Vsekakor je digitalizacija in informatizacija pomemben dejavnik spremembe poslovnega okolja in procesov. Poleg mnogovrstnih pozitivnih stvari pa je na področju varnosti ta proces prinesel veliko tveganj. Iz analize preteklih izkušenj lahko vidimo, da so tudi slovenska podjetja vedno bolj podvržena varnostnim tveganjem, ki izhajajo iz tega okolja. Vdori v informacijske sisteme, spletne banke in plačilne sisteme podjetij, odtujitev podatkov, širjenje zlonamernih kod in virusov ter ostala informacijska tveganja so v današnjem kibernetskem okolju postala stalnica. Poleg sistemskih pristopov na področju zagotavljanja informacijske varnosti lahko tukaj storimo največ pri osveščanju in usposabljanju naših zaposlenih. Popolne varnosti pa na žalost tudi na tem področju ni mogoče zagotoviti. Zato je pomembno, da ta tveganja zmanjšamo na še sprejemljivo raven, ki nima bistvenega vpliva na učinkovitost našega poslovanja.

Odtekanje ključnih poslovnih informacij in poslovnih tajnosti ter s tem povezani socialni inženiring, malomarnost, nizka organizacijska in varnostna kultura, neizobraženost in namerno izvajanje protizakonitih aktivnosti so tisti dejavniki, ki silijo podjetja h učinkovitejšemu izvajanju ukrepov korporativne varnosti, povezane z nadzorom zaposlenih v njihovih osnovnih delovnih okoljih.

Podjetja morajo na tem področju narediti še zelo veliko, da bo stanje obvladovanja informacijskih tveganj ustrezno urejeno. Še posebej so tukaj izpostavljene organizacije, ki upravljajo s kritično infrastrukturo, katera je nujno potrebna za normalno delovanje širše družbene skupnosti.

Po eni strani nam digitalna tehnologija pomaga vzpostaviti visoko raven varnosti, po drugi strani pa s tem ustvarimo goro novih podatkov, poslovnih in osebnih, ki pa jih je spet treba nekako zavarovati pred nepooblaščenim dostopom. Najpomembnejše je, da se poslovne organizacije zavedajo, da bo potrebno informacijsko varnost čim bolj učinkovito združiti v proces korporativne varnosti. Samo tako se bo lahko zagotovilo ustreznejše in bolj učinkovito obvladovanje tveganj povezanih z informacijsko komunikacijsko tehnologijo. Ustvarjanje parcialnih procesov, ki predstavljajo ločene vrtičke in s tem puščajo ogromno varnostnih praznin, nikakor ni prava pot. Tukaj bodo imela strateška vodstva poslovnih organizacij ključno vlogo, ki se bo odrazila z razumevanjem te potrebe.

Vpliv varnostne kulture na proces korporativne varnosti

V fazi tranzicije so nam vseskozi dopovedovali, da je Slovenija varen otok sredi tveganega sveta. Ta miselnost je dalj časa prevladovala tudi v poslovnem okolju in je izredno škodila ustreznemu varnostnemu zavedanju odgovornih in zaposlenih v organizacijah. Stanje ozaveščenosti se je sicer že začelo izboljševati, a teh procesov ni mogoče vzpostaviti v kratkem časovnem obdobju. V nacionalnih okoljih, predvsem v državah v tranziciji, ki so v okolje tržnega gospodarstva vstopile po družbenih spremembah ob koncu 20. stoletja, je stanje korporativne varnosti še močno v fazi razvoja in iskanja ustreznega mesta v poslovnem okolju. Gre tudi za težave pri razumevanju vloge, poslanstva in nenazadnje odgovornosti strateškega menedžmenta in posledično tudi korporativne varnosti, kot osnovnega orodja za učinkovito obvladovanje tveganj v organizacijah, ki jih vodijo.

Kljub hitremu tehnološkemu razvoju človek ostaja tisti segment, ki ima v procesu obvladovanja varnostnih tveganj ključno vlogo. V večini primerov še vedno predstavlja tisti najšibkejši člen v celovitem sistemskem zagotavljanju varnosti. Odtekanje ključnih poslovnih informacij in poslovnih tajnosti ter s tem povezani socialni inženiring, malomarnost, nizka organizacijska in varnostna kultura, neizobraženost in namerno izvajanje protizakonitih aktivnosti so tisti dejavniki, ki silijo podjetja h učinkovitejšemu izvajanju ukrepov korporativne varnosti, povezane z nadzorom zaposlenih v njihovih osnovnih delovnih okoljih. Naslednji pomemben dejavnik, na katerega moramo biti še posebej pozorni pri zagotavljanju korporativne varnosti, so zunanji izvajalci in pogodbeni partnerji. V zadnjem obdobju se podjetja namreč vedno bolj poslužujejo prenosa določenih procesov na zunanje pogodbene izvajalce. Pri prvi kalkulaciji stroškov se lahko ta oblika zmanjšanja stroškov delovanja podjetja zdi zelo vabljiva, vendar je potrebno na proces oddajanja ključnih funkcij gledati tudi z drugačnega zornega kota, saj za delovanje podjetja lahko prinese zelo velika tveganja, katerih pa se lastniki in menedžment ne zavedajo. S prenosom določenih procesov na zunanje izvajalce podjetje izpostavljamo tveganjem, ki se predvsem izražajo v preveliki odvisnosti od pogodbenih izvajalcev, nevarnost pa

predstavlja tudi dostop nepooblaščenih oseb do ključnih poslovnih informacij, ki predstavljajo konkurenčno prednost na trgu. Ta tveganja lahko nekoliko zmanjšamo tako, da od pogodbenih izvajalcev zahtevamo izpolnjevanje minimalnih standardov, ki jih imamo v podjetju opredeljene v okviru ukrepov za zagotavljanje korporativne varnosti. Zavedati pa se je treba tudi, da popolne varnosti ni in jo je v celoti nemogoče doseči.

Organizacijska umeščenost korporativne varnosti

Znanje varnostnega managerja ni omejeno samo na ozko področje varnosti, temveč se vedno bolj širi tudi na področja informatike, poslovnih ved, prava in ostalih področij. To zahteva, da stroka korporativne varnosti postaja multifunkcionalna in kot taka tudi ustrezno prepoznana v svojem okolju. To za seboj potegne tudi ustrezno umeščenost v organizacijsko-odločevalsko strukturo podjetij. Če korporativno varnostni managerji ne razumejo poslovnega procesa in njegovih posebnosti, nikakor ne morejo učinkovito opravljati svojega dela. Proces korporativne varnosti mora biti povezan neposredno na upravo poslovne organizacije, kar pomeni, da korporativno varnostni manager odgovarja neposredno upravi in predstavlja njeno podaljšano roko. Zelo pomemben je tudi hiter in ustrezen prenos informacij in obveščanje poslovodstva o ključnih dejavnikih tveganja in groženj. Le tako lahko zagotovimo ustrezen odziv na varnostne grožnje dinamičnega poslovnega okolja.

Profil korporativno varnostnega managerja

Korporativno varnostni management predstavlja tisti ustrezen profil, ki v podjetjih skrbi za korporativno varnost, saj ima vsa potrebna znanja, ki so ustrezna za to kompleksno dejavnost. Pomemben korak za dvigovanje ravni znanj in pomena korporativne varnosti predstavlja še magistrski program »Upravljanje s tveganji in korporativna varnost«, ki se že tretje leto izvaja v okviru Fakultete za podjetništvo-GEA College.

Tudi Institut za korporativno varnostne študije in predvsem Slovensko združenje korporativne varnosti imata v tem okviru izredno pomembno vlogo združevanja in tvorjenja sinergij na področju znanja in prenosa dobrih praks na področje korporativne varnosti.



Izzivi profesije korporativno varnostnega managementa

V zadnjem obdobju smo priča dvema temeljnima dejavnikoma, ki pomembno vplivata na razvoj organizacij in njihovo uspešnost. Prva je dinamičnost varnostnega okolja, ki se nenehno spreminja in pred nas postavlja vedno nove oblike varnostnih tveganj. Drugi pomemben dejavnik pa je vsekakor zahtevno ekonomsko okolje in huda konkurenčna tekma med poslovnimi organizacijami. Poslovna filozofija je vedno bolj usmerjena v cilj z manj storiti več in bolj kvalitetno. Vplivu teh procesov se ne more ogniti niti korporativna varnost. Če to pogledamo še skozi prizmo zmanjševanja stroškov in optimizacije ter pritiskov s strani investitorjev lahko vidimo, da so strokovnjaki korporativne varnosti postavljeni pred resne dileme, kako naprej v cilju učinkovitega zagotavljanja varnosti organizacije, njenih poslovnih procesov in zaposlenih.

Boljši časi se obetajo, ko bodo lastniki oziroma vodstvo poslovne organizacije dokončno dojeli nujo po preprečevanju škod in izgub zaradi šibkega celostnega varnostnega stanja podjetja. Obvladovanje varnostnih tveganj lažje zagotavljamo v večjih korporacijah oziroma podjetjih. Večji problem je pri majhnih ali srednje velikih podjetjih, ki si težko privoščijo stalno zaposlenega strateškega korporativno varnostnega managerja. Ena od možnih rešitev je pogodbeno sodelovanje z zunanjim tovrstnim managerjem. Na tem področju v prihodnosti obstaja pomembna zaposlitvena možnost za korporativno-varnostne managerje tako v nacionalnem kakor tudi mednarodnem okolju. Povpraševanje po tovrstnem kadru se izredno povečuje.

Pri tem pa ne smemo omenjene funkcije strateškega varnostnega managementa zamenjevati z dejavnostjo, ki jo ponujajo zasebno-varnostne službe v okviru zavarovanja ljudi in premoženja. Največja nevarnost za nesistemske pristope na področju celovitega obvladovanja varnostnih tveganj v podjetjih predstavlja ravno združevanje teh funkcij v rokah zasebno-varnostnih služb. Te lahko hitro izgubijo skrb za naročnika, vodi pa jih izključno še skrb po lastnem dobičku. Ravno zaradi te nevarnosti mora biti strateški korporativno varnostni manager oseba, ki lastniku nepristransko pomaga pri učinkoviti izbiri najboljšega ponudnika za zagotavljanje posameznih varnostnih storitev ter skrbi za sistemski nadzor nad njenim delovanjem. ■



POSVET

NADZOR NA DELOVNEM MESTU

26. september 2018, Ljubljana

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

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

Institut za korporativne varnostne študije
Cesta Andreja Bitenca 68,
1000 Ljubljana
www.ics-institut.si

ICS
Institut za korporativne varnostne študije

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Simon Velički, Generalni direktor Policije

POLICIJA OSTAJA EDEN OD KLJUČNIH DRŽAVOTVORNIH RESORJEV

Dinamično varnostno okolje pred Republiko Slovenijo postavlja nove izzive in tveganja. O priložnostih in tudi varnostnih izzivih razvoja Policije smo izkoristili priložnost in se pogovorili z novim Generalnim direktorjem Policije g. Simonom Veličkim.

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

V Policiji svoje delovanje stalno prilagajamo varnostnim razmeram in razpoložljivim sredstvom. To je izziv, ki nam ne bo izostal tudi v prihodnje, saj bo treba tudi v bodoče sproti spreminjati organizacijo dela glede na aktualno varnostno situacijo in predvsem glede na kadrovske zmožnosti, še posebej na policijskih postajah. Že sedaj pa pripravljamo različne projekte, ki neposredno ali posredno vplivajo na način našega delovanja, npr. zmanjšanje administrativnih bremen, e-policist, Infopol.

Slovenska policija je bila v obdobju po osamosvojitveni vojni deležna pogostih organizacijskih sprememb. Razlogi so bili različni, od spremenjenih družbenih razmer, novih operativnih okoliščin, sprejemanja novih nalog zaradi nacionalnih in mednarodnih obveznosti, do racionalizacije stroškov poslovanja zaradi neugodnih javnofinančnih razmer v Sloveniji. Različne organizacijske spremembe so močno posegle v delo zaposlenih in enot, v zadnjih letih pa je bilo na področju organiziranosti delovanja policije največ težav prav zaradi kadrovskega primanjkljaja.

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

Državljani od policije v času, ko se pojavljajo številčne in nove oblike varnostnih groženj, pričakujejo hitro in učinkovito odzivanje. Organiziranost policije, njene metode in tehnike dela morajo slediti dinamiki varnostnih dogajanj. Nove oblike operativnega dela potrebujejo nova razvojna vlaganja ter znatne logistične, materialne in finančne vire. Za uspešno in varno izvajanje policijskega dela na vseh nivojih je treba zagotoviti osebno in zaščitno opremo policistov, ustrezno tehnično in oborožitveno opremo ter usposobljenost. Stalen pritok sredstev je tako potreben za najrazličnejše stroške in investicije.

Policija je imela velike težave s pomanjkanjem sredstev predvsem v letih, ko je bila t.i. finančna kriza na vrhuncu. Večletno varčevanje je že doseglo optimalne učinke, hkrati pa na določenih delih delovanja policije tudi negativen vpliv, tako na redno delo, kot na materialno-tehnične pogoje dela. V zadnjih treh letih pa smo prejeli dodatna finančna sredstva, 121,5 mio. evrov, in preprečili negativne trende, kar je zasluga trenutnega vodstva notranjega ministrstva.

Razvoju tehnologije se prilagajajo tudi storilci, zato je za potrebe odkrivanja, preiskovanja in preprečevanja tovrstnih kaznivih dejanj ključnega pomena sodelovanje policije s pristojnimi organi in s privatnim sektorjem pri nas in v tujini.

*avtor je član Slovenskega združenja korporativne varnosti

Za delo policistov pa je najpomembneje, da nabavljamo novo opremo, ki je namenjena njihovi varnosti in tudi, da skrbimo za novo informacijsko-telekomunikacijsko tehnologijo. Na koncu lahko omenim še, da smo s pridobljenimi sredstvi prenovili tudi policijsko uniformo.

Kibernetska tveganja so v informacijski družbi vedno bolj izražena. Kje so še rezerve medsebojnega sodelovanja med policijo in korporativno varnostjo za zagotavljanje višje varnosti v slovenskih poslovnih organizacijah?

Razvoju tehnologije se prilagajajo tudi storilci, zato je za potrebe odkrivanja, preiskovanja in preprečevanja tovrstnih kaznivih dejanj ključnega pomena sodelovanje policije s pristojnimi organi in s privatnim sektorjem pri nas in v tujini.

Opažamo pa, da še vedno ostaja veliko kaznivih dejanj neprijavljenih in zaradi take neobveščenosti se potem težje odzivamo in ukrepamo na področju informacijske varnosti. To vpliva tudi na morebitno izvajanje preventivnih ukrepov, npr. prek medijev. Zato je na mestu poziv k večji odgovornosti in prijavljanju takih dogodkov policiji ter h krepitvi omenjenega sodelovanja.

Nasilno izražanje nezadovoljstva na ulicah večjih slovenskih mest je pokazalo, da Policija ob množičnih izgredih na različnih koncih Slovenije stežka zagotavlja dovolj sil, ki bi poskrbele za javni red in mir. Kako izboljšati komunikacijo med Policijo in odgovornimi v organizacijah za korporativno varnost pri usklajenih aktivnostih zavarovanja premoženja in varnosti na površinah, ki so v neposredni bližini varnostno rizičnih dogodkov?

Javni shodi in javne prireditve so ustavno zagotovljena pravica, ki jo lahko omeji le zakon. Zakon o javnih zbiranjih določa aktivnosti in odgovornosti organizatorjev, ki morajo na shodih in prireditvah poskrbeti za varnost ljudi. Organizator z rediteljsko službo ali varnostno službo izvaja vse ukrepe, policija pa v varovanje vstopi, ko je treba vzpostaviti red oziroma, ko je ta huje ali množično kršen.

Za izvajanje tovrstnih nalog imamo dovolj usposobljenih policistov, ki bi tudi v primeru večjega števila izgredov na različnih delih Slovenije lahko izvajali svoje naloge in zagotavljali varnost. V vseh varnostno zahtevnih situacijah namreč vrednotimo razpoložljive informacije in na tej podlagi prilagajamo svoje aktivnosti, kar bi se zgodilo tudi v primeru razpršenih izgredov.



Seveda pa na tem področju obstajajo tudi priložnosti. Vzajemno sodelovanje med različnimi deležniki, ki imajo skupen cilj zagotavljati varnost v najširšem smislu, je izziv sodobne družbe. Vsi pa moramo razumeti svojo vlogo v družbi in se odgovorno obnašati.

Družbeno stanje na področju dojemanja varnosti v Sloveniji ni na ustreznem nivoju. Kako to varnostno kulturo in zavedanje tako pri posameznikih kakor tudi pri vodilnih strukturah organizacij javnega in zasebnega okolja dvigniti na višji ustreznejši nivo?

Policija je ena od vodilnih na tem področju, saj na različne načine vzpodbuja državljane in druge subjekte v lokalnem okolju k samozaščitnemu ravnanju in s tem krepi varnostno zavest. To dokazuje vedno večje število preventivnih akcij in projektov, ki jih sami ali pa skupaj z državljani in drugimi organizacijami izvajamo na različnih ravneh. Letno opravimo okoli 13.000 dejavnosti, ki vzpodbujajo razvoj varnostne kulture, povečujemo pa tudi finančna sredstva za te aktivnosti. Imamo poseben sistem evidentiranja policijskega dela v skupnosti, s pomočjo katerega ugotavljamo, koliko takšnih aktivnosti izvedemo in kakšni so učinki v lokalnem okolju. Rezultati kažejo, da letno v povprečju opravimo 6.000 svetovanj, v katera je vključenih 12.000 različnih lokalnih subjektov.

Združevanje različnih družbenih skupin je ključnega pomena za obvladovanje trenutne varnostne situacije. Zavedamo se, da lahko samo skupaj s partnerji soodgovorno ustvarjamo čim boljše varnostne razmere.

Pri policijskem delu v lokalnem okolju se srečujemo z različnimi posamezniki, običajnimi državljani, kot tudi z vodilnimi v subjektih javnega in zasebnega okolja. Aktivnosti izvajamo na vseh področjih varnosti, tako na področju kaznivih dejanj, javnega reda in miru ter prometa.

So po vašem mnenju procesi centralizacije državne uprave in s tem tudi policijske organizacije pravi korak v smeri zagotavljanja javne varnosti?

Policijska organizacija je enovita in centralizirana na treh nivojih. Izkušnje iz preteklosti kažejo, da smo bili zaradi majhnosti države in predvsem enovite organizacije sposobni hitro in učinkovito reagirati v različnih situacijah, npr. v primeru migrantske krize. V primeru popolnoma decentraliziranih enot bi se vsekakor povečali nekateri postopki glede kadrovske pomoči, enotnega izvajanja dela, financ.

Centralizacija organizacije pa ne pomeni, da enote, ki so na drugem ali tretjem nivoju, niso pri svojem delu samostojne. Nasprotno. V policiji ves čas dajemo velik poudarek samostojnosti pri vodenju in izvajanju nalog – nenazadnje imamo veliko projektov, npr. delo v lokalni skupnosti in drugi, katere so posamezne enote začele izvajati in s tistimi, ki so bili uspešni, smo seznanili druge enote, da so jih lahko začeli izvajati tudi oni.

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

V policiji si, poleg stalnega izobraževanja, različnih oblik usposabljanj in izpopolnjevanj, prizadevamo tudi k vzpostavitvi stimulativnega kariernega sistema. Lani je posebna delovna skupina pripravila predlog izhodišč za prenovo kariernega sistema, letos pa smo začeli razvijati model upravljanja s potenciali za vodenje in izbirnih postopkov policijskih vodij.

Do sredine leta moramo presistemizirati delovna mesta policistov v V. tarifnem razredu, za katera se zahteva poklic policista, v ustrezna delovna mesta v VI. tarifnem razredu. To je posledica uveljavitve določb 110. člena Zakona o organiziranosti in delu v policiji, ki prinaša ustrezno umestitev delovnih mest glede na zahtevnost nalog in dvig poklicnega standarda.

Menite, da bi bilo potrebno v proces izobraževanja vključiti tudi strokovnjake s področja korporativne varnosti?

Prizadevamo si, da v programih izobraževanja in usposabljanja gostimo različne strokovnjake, ki pomagajo s svojim znanjem in širino zapolniti posamezne vrzeli ter obogatiti znanje policistov. Že več let aktivno sodelujemo z različnimi strokovnjaki iz drugih ministrstev, vrhovnega državnega tožilstva, varuha človekovih pravic, informacijske pooblaščenke, nenazadnje tudi s predstavniki različnih nevladnih organizacij.



Vsekakor mednje sodijo tudi strokovnjaki korporativne varnosti, žal pa smo omejeni s finančnimi sredstvi in za sodelovanja ne moremo sklepati avtorskih pogodb.

Kako med mladimi zagotoviti ustrezno zanimanje za poklic policista?

Zaradi dviga poklicnega standarda se je izobraževanje za poklic policista v 2012 preoblikovalo v višje strokovno izobraževanje po prenovljenem študijskem programu Policist. Študij na tem programu je izrazito praktično naravnan in, poleg pridobivanja strokovnega znanja, omogoča razvoj socialnih in osebnostnih kompetenc. Teoretični del študija se prepleta z učenjem na delovnem mestu. Zelo pomembno je, da bodoči policisti povezujejo teorijo in poznavanje zakonodaje z vsakdanjimi življenjskimi okoliščinami, v katerih morajo strokovno ukrepati.

Glede na dvig zahtevnosti policijskih nalog pa si na več načinov prizadevamo, da bi pridobili nov, kakovosten kader. V zadnjih letih aktivno spodbujamo zaposlovanje in od leta 2015 vsako leto objavljamo razpis za zaposlitev kandidatov za policiste in napotitev na višješolski študijski program za poklic Policist. Naš cilj je 100 do 150 novih zaposlitev, žal pa dosegamo manjši obseg zaposlitev od načrtovanega. Za izpolnjevanje zavez schengenskega sporazuma večkrat letno objavimo tudi razpis za zaposlitev kandidatov za policiste za varovanje schengenske meje. Od načrtovanih 100 delovnih mest nam jih je v lanskem letu uspelo popolniti okoli 50.

Zaradi upada interesa po zaposlovanju v policiji želimo z aktivnejšo promocijo o zaposlitvenih možnostih doseči večje zanimanje za zaposlitev v policiji, vendar pa se število prijav na zaposlitvene oglase zmanjšuje. Menimo, da na to vpliva tudi trenutna pozitivna gospodarska rast, na podlagi katere se povečujejo zaposlitvene možnosti v drugih organizacijah.

Menite, da je združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti lahko odgovor na obvladovanje zahtevne varnostne situacije in ali so lahko taka združenja ustrezen partner Policiji pri zagotavljanju njenega osnovnega poslanstva?

Združevanje različnih družbenih skupin je ključnega pomena za obvladovanje



trenutne varnostne situacije. Zavedamo se, da lahko samo skupaj s partnerji soodgovorno ustvarjamo čim boljše varnostne razmere. Seznanjanje policije o varnostnih problemih in prizadevanje po skupnem reševanju teh problemov je pomembno. Zato smo pred leti dali pobudo, da se po občinah ustanovijo varnostni sosveti, ki združujejo različne subjekte. Takih sosvetov je trenutno ustanovljenih 163.

V varnostni sosvet se lahko vključi vsak, ki je zainteresiran za tovrstno delovanje. Sodelovanje med varnostnimi sosveti in policijo vključuje obravnavo varnostne problematike, hkrati pa se prek izmenjave mnenj in pobud rešuje konkretne varnostne probleme. Sodelovanje med varnostnimi sosveti in policijo je dobro, želimo pa si še več različnih subjektov, ki bi pri tem sodelovali, tudi Združenje korporativne varnosti. Različna združenja so Policiji lahko ustrezen partner pri zagotavljanju našega osnovnega poslanstva, seveda v okviru obstoječih pristojnosti in zakonodaje.

Institut za korporativne varnostne študije in Slovensko združenje vsako leto podeljujejo prestižno nagrado Slovenian Grand Secrity Award, med drugim tudi v kategoriji najbolj varno mesto in najbolj varna občina. Menite, da tukaj obstajajo stične točke sodelovanja s Policijo predvsem na področju v lokalno skupnost usmerjeno policijsko delo?

Pred petimi leti je slovenska policija sprejela novo strategijo policijskega dela v skupnosti, ki spreminja vlogo policije v družbi ter način policijskega dela, ki je usmerjen k uporabnikom varnostnih storitev policije. Nova vloga temelji na partnerskem sodelovanju in medsebojnem zaupanju. Policija in javnost morata namreč skupaj ugotavljati varnostne probleme in jih skupaj reševati, da se izboljša kakovost življenja. Ko govorimo o varnosti v nekem okolju, je namreč zelo pomembno dojemanje in zaznavanje varnostnih pojavov oziroma občutek varnosti ljudi, ki v tem okolju živijo in delajo. Zato je pomembno tesno sodelovanje z lokalno skupnostjo.

Slovenian Grand Security Award v omenjenih kategorijah je primerljiva s prometno varnostno oceno policije, ki pa žal temelji le na statističnih podatkih. Stične točke nedvomno so. Utemeljitev ocene in izbira pri vaši nagradi je nedvomno kazalnik policiji, katera so tista področja, kjer lahko svoje delo še izboljšamo. ■

Opomba: fotografije so iz arhiva Policije

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. · TES Termoelektrarna Šoštanj · LUKA KOPER Port of Koper · lek član skupine Sandoz · REISSWOLF secret. service. · BTC · A1 · Občina Slovenska Bistrica · MARIBORSKI VODOVOD · 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!

Pošta Slovenije
INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O. INFORMATIKA
triglav
KONTROLA ZRAČNEGA PROMETA SLOVENIJE
Telekom Slovenije
AKRAPOVIČ
interblock LUXURY GAMING PRODUCTS
spica
ELEKTRO LJUBLJANA
Ford SUMMIT AVTO
SIEMENS
DARS
CINKARNA
Elita i.b. d.o.o.
Nova KBM PRIPRAVLJENI NA JUTRI
LON
ZARJA ELEKTRONIKA
UNISTAR PRO
Slovenske železnice
energetika ljubljana

www.ics-institut.si

Avtor: Boštjan Videmšek / DELO



KOLUMNA

EVROPSKI ZLOČIN PROTI ČLOVEČNOSTI

Dve leti in dva meseca po zaprtju balkanske begunske poti in sprejetju evropsko-turškega begunskega dogovora, s katerim je Bruselj za šest milijard evrov usodo sto tisočih ljudi na begu na velikem bazarju človeške tragedije prodal Ankari, je – v domači javnosti – vprašanje begunstva in migracij zopet v središču pozornosti. A žal iz povsem napačnih razlogov.

Migracije, ena najbolj temeljnih značilnosti civilizacij, so se namreč znašle v srčiki populizma, cenenega političnega marketinga, ustvarjanja vzdušja strahu, širjenja lažnih novic in razkroja temeljnih humanističnih vrednost Evrope.

Nekaj takega kot »ponovitev« balkanske begunske poti se ne more več zgoditi. Obdobje med poletjem 2015 in pomladjo 2016 je bilo namreč unikatno. Vrsta držav je (dogovorno) odprla svoje meje. Ustvaril se je humanitarni koridor, po katerem je več sto tisoč ljudi vstopilo v Evropsko unijo. Na balkanski begunski poti se je združilo več migracijskih poti – tudi iz Srednje Azije (preko Irana in Turčije) ter iz osrednjega Sredozemlja, preko katerega je pred in po zaprtju balkanske poti v Evropo vstopalo največ beguncev in migrantov.

Toda sprejetje evropsko-turškega dogovora, s katerim je turški predsednik Recep Tayyip Erdogan dobesedno preko noči zaustavil od zgoraj navzdol organizirano tihotapljenje ljudi na grške egejske otoke in s tem dokazal neposredno sodelovanje turške države v množičnih migracijah proti EU, je močno spremenilo stanje stvari. Meje v nekdanjem balkanskem koridorju so se zaprle. Na madžarsko-srbski, madžarsko-hrvaški, makedonsko-grški in slovensko-hrvaški meji so zrasli zidovi, bodeče žice in stražni stolpi – militaristična infrastruktura iz nekih drugih časov. Evropska unija je na grških vzhodnih egejskih otokih (Hios, Samos, Lezbos, Kos) postavila tako imenovane vroče točke (hot-spots), dejansko pa koncentracijska taborišča našega časa, kjer je po zaprtju balkanske poti začela zaustavljati in kopičiti begunce in migrante, ki so kljub zavedanju o agresivnem koncu evropske dobrodošlice še vedno – v sicer bistveno manjšem številu – prihajali na grške otoke.

To je povzročilo novo poglavje velike begunske tragedije, ki je močno načela etično – in humanistično – jedro Evrope. Trenutno je v taboriščih na grških otokih, kamor se redno vračam, ujetih okoli 13.000 ljudi. Životarijo – ne živijo – v nemogočih razmerah. Hrana je slaba, varnost neobstoječa. Policijsko nasilje je skupaj z rasizmom, ksenofobijo in celostnim poniževanjem in razgrajevanjem dostojanstva, del vsakdanjika. Vse skupaj negativno vpliva tudi na lokalne skupnosti, ki so marsikje v Grčiji pokazale ogromno sočutja, a to ima omejen rok trajanja. Ker ne država ne Evropska unija nista pristopili na pomoč, so se jezni in razočarani ljudje, kako naravno je to, obrnili proti najšibkejšim in najbolj ranljivim. Proti beguncem in migrantom. Zaradi globokih frustracij, vseprisotnega sindroma posttravmatskega stresa, popolne nemoči in brezupa – ujetost – so se začeli krhati tudi odnosi med različnimi begunskimi in migrantskimi skupinami. Kompleksnih razmerij in razmer evropski birokrati pač niso bili sposobni nagovoriti, vse skupaj pa se je še dodatno zaostrilo po lanskem avgustu, ko so nevladne organizacije v begunskih taboriščih, po dekretu grške vlade, kateri je tako ukazal Bruselj, zamenjali predstavniki grških oblasti. Udarila je tudi birokracija, tiha banalnost zla. Spoštovanje človekovih pravic je postalo slaba šala, kršenje ključnih mednaro-

dnih konvencij prav tako – tu se je s spremenjeno azilno zakonodajo »izkazala« tudi Slovenija, ki s svojo natančno sistematizirano odvračilno azilno politiko že ves čas kriči ob bolečini drugega.

Evropa je s svojo (proti) migrantsko in (proti) begunsko politiko v zadnjih letih zakrivila velik zločin proti človeštvu – samo na tako imenovani osrednji sredozemski begunski poti je od leta 2000 naprej umrlo okoli 40.000 ljudi. Nikoli jih ne bodo pokopali. Mnogi so ostali tudi brez imen in priimkov – brezimne žrtve, ki so umrle na begu pred vojnami, mučenjem, totalitarnimi režimi, revščino in brutalnimi posledicami klimatskih sprememb, ki bodo že v bližnji prihodnosti glavno gonilo globalnih migracij. Mimogrede: begunske krize v Evropski uniji, razen v Grčiji, in pogojno v Italiji, ni bilo. V času odprte balkanske begunske poti je v Evropo prišlo manj beguncev, kot jih je iz vojne v Siriji, najbolj krvavega konflikta našega časa, ki je vstopil v osmo leto, prebežalo v sosednji Libanon. Demografsko, politično, socialno in varnostno izjemno vplivna sredozemska državica, ki še ni zacelila ran lastne državljanske vojne (1975-1990), trenutno gosti poldrugi milijon sirskih beguncev. Skoraj tretjino celotnega prebivalstva, in več kot celotna Evropska unija, v kateri živi pol milijarde ljudi. Podobno je mogoče reči za Jordanijo in tudi Turčijo, kjer še vedno živi skoraj tri milijone sirskih beguncev.

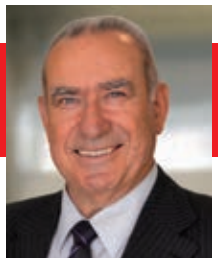
Ravno osrednja sredozemska pot – iz Libije do italijanskih otokov – bo še vrsto let glavna migracijska pot proti Evropski uniji. Sahel je eno najbolj suhih in vročih področij sveta, kjer se pospešeno sušijo vodni izviri, Sahara pa se vsako leto premakne od pet do sedem kilometrov proti jugu, bo iz leta v leto manj stabilen. Že sedaj – v popolnem brezvladju – je središče organiziranega kriminalna (tihotapljenje z ljudmi, drogo, cigaretami, alkoholom, orožjem, ...) in skrajnih islamističnih skupin (od »lokalne« podružnice Al Kaide do nigerijskega skrajnega gibanja Boko Haram). Le še huje bo – suša – in pritisk na obale Severne Afrike se bo stopnjeval.

A namesto, da bi se Evropska unija, ki bo brez dvoma glavni cilj migracij, ukvarjala z razlogi, se ne zna soočiti niti s posledicami. Evropski birokrati so se pred meseci celo odločili, da bodo za zaustavljanje ljudi na poti proti jugu stare celine »uporabili« libijske milice, ki istočasno vodijo libijsko obalno stražo, sužnjelastniška taborišča in paravojaške posadke, obenem pa so na vrhu piramide organiziranega kriminala v regiji. Z velikimi »podkupninami« poskuša Evropa reševati svojo politično zagato – pospešen vzpon skrajne desnice – tudi v Nigru in Maroku; kmalu tudi v Maliju in Mavretaniji.

To niti slučajno ni rešitev. Nasprotno. ■



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





NAČRTI NEPREKINJENEGA POSLOVANJA IN KRIZNI NAČRTI V FUNKCIJI OBVLADOVANJA TVEGANJ

Neprekinjenemu poslovanju in kriznemu vodenju se v javnem in zasebnem sektorju daje premalo pozornosti. Seveda je zagotavljanje neprekinjenega poslovanja, s kriznim vodenjem vred, veliko bolj zahtevno v gospodarskih družbah, ki se morajo spopadati s konkurenco ter z vedno novimi izzivi in spremembami. Tako so zagotavljanje neprekinjenega poslovanja (Business Continuity), obvladovanje nevarnosti, ogroženosti in tveganj (Risk Management) ter obvladovanje kriznega vodenja (Crisis Management) v vsaki uspešni gospodarski družbi nujne sestavine korporativnega upravljanja.

Oris obravnavane teme

Iz ekonomskih, poslovnih in organizacijskih ved je namreč znano, da je podjetje podvrženo rasti, razvoju, stagnaciji, včasih pa tudi propadu. V trenutnih globalnih in regionalnih kriznih gospodarskih, finančnih, socialnih in varnostnih okoliščinah je treba biti previden in predvideti vse potrebno za obvladovaje obstoječega in prihodnjega stanja poslovanja.

Kot je uvodoma rečeno ima načrt neprekinjenega poslovanja najprej preventivni namen, to je, da nastopa zoper nastanek izrednih dogodkov in represivni (kurativni) namen, ko gre za razreševanje izrednega dogodka in za razreševanje krizne situacije (krizno vodenje).

Preudarni lastniki, upravljalci, menedžment, strokovnjaki in nadzorniki že v času ugodnih poslovnih rezultatov nenehno mislijo tudi na slabe poslovne čase, na neizkoriščene poslovne priložnosti in na morebitne krizne okoliščine, ki v nekem preseku časa doletijo vsako gospodarsko družbo. Gre potemtakem za odziv na sedanje razmere in na negotovo prihodnost, ob domnevi, da bo tudi v prihodnje prihajalo do izrednih dogodkov, ki bodo zmotili, ali ovirali, ali celo prekinili normalno poslovanje. Iz splošne ocene ranljivosti in ogroženosti gospodarstva izhaja, da je v prvi vrsti treba polagati pozornost na ranljivost, izpostavljenost in ogroženost informacij in komunikacij, tehnično-tehnološko ogroženost, požarno ogroženost, ogroženost od konkurentov, nekatere segmente kriminalne ogroženosti, na ogroženost neposrednega okolja (vandalizem, stavke, nesreče) in na ogroženost, ki prihaja iz naravnih sil. V zadnjem času vse bolj v ospredje prihajajo nove vrste izpostavljenosti in ogroženosti gospodarskih družb povezane z vse večjo kadrovsko problematiko, kulturno raznolikostjo, socialno izpostavljenostjo in neustreznim naborom zunanjih pogodbenih izvajalcev (outsourcing). V skrajnem primeru je torej treba računati tudi na izpad poslovanja na osnovni lokaciji in na začasni prehod poslovanja na rezervni lokaciji, kjer mora biti vzpostavljena redundantna strojna, programska in druga oprema, ki omogoča delovanje

*avtorja sta člana Slovenskega združenja korporativne varnosti



ključnih (kritičnih) poslovnih funkcij in procesov. Le na ta način je možno zagotavljati nujne informacije, komunikacije in druge storitve tudi v kriznih razmerah. Gre torej za **načrten pristop k upravljanju neprekinjenega poslovanja,** ki ima svojo preventivno funkcijo (preprečevanje izrednih dogodkov, škod in izgub) in represivno (kurativno) funkcijo s katero je treba razreševati nastali izredni dogodek in morebitno krizno stanje - vzpostavitev kriznega vodenja z namenom minimiziranja nastale škode in čimprejšnje vzpostavitve normalnega poslovanja po kriznem stanju. S tega vidika lahko načrte neprekinjenega poslovanja s kriznimi načrti označimo kot **glavno poslovno orodje obvladovanja tveganj.** To zlasti velja za obvladovanje tveganj v multinacionalkah in v sektorjih kritične infrastrukture, ki so dolžni zagotoviti delovanje tudi v kriznem stanju. Za temeljit pristop k obvladovanju tveganj, ki ga lahko označimo z nazivom **integrirano obvladovanje tveganj** pa je treba uporabiti določene standarde kot so ISO 31000:2018 (obvladovanje tveganj), ISO/IEC 27000:2018 (obvladovanje informacijskih tveganj), SIST EN ISO 22301:2014 (neprekinjeno poslovanje), ISO 9001:2015 (vodenje sistema kakovosti), uporabiti obvezne in certifikacijske varnostne standarde ter **izvirno (**ali bolje rečeno za naše potrebe uporabno) **metodologijo** ocenjevanja ranljivosti, ogroženosti in tveganj. Do izvirne metodologije pa je kar zahtevna pot, kajti iz široke palete metod za ocenjevanje ranljivosti in ogroženosti tveganj ter modelov upravljanja s tveganji, je treba proučiti tiste segmente, ki so uporabni v našem gospodarstvu zlasti v multinacionalkah in v kritični infrastrukturi. Priprava takega modela obvladovanja tveganj, ki bo za uporabnike preprost in razumljiv ter hkrati učinkovit, so potrebna široka znanja o upravljanju groženj, tveganj, neprekinjenem poslovanju in kriznem vodenju, poleg tega pa tudi dobro poznavanje gospodarskih dejavnosti, ki jih je smiselno pregledati in proučiti tudi z operativnimi metodami raziskovanja.

Načrtno zagotavljanje neprekinjenega poslovanja gospodarskih družb

Načrti neprekinjenega poslovanja so učinkovito sredstvo (poslovno orodje) zagotavljanja poslovanja in delovanja gospodarske družbe tudi v okoliščinah izrednih dogodkov in kriznih stanj. Zagotavljajo torej korporativno vodenje, varnost, skladnost in poslovno uspešnost na dolgi rok ter ščitijo konkurenčno prednost, zanesljivost, zaupanje, ugled, sloves in dobro ime gospodarske družbe. Kajti v gospodarski (pa tudi v kakšni drugi) družbi se lahko v nekem preseku časa pripetijo naslednji **izredni dogodki**: potres, poplava, velik požar, eksplozija, grožnja z bombo, najdeno eksplozivno sredstvo, sabotaža, izpad informacijskega sistema, vdor v informacijski sistem, izpad (elektronskih) komunikacij, izpad energijske podpore, izlitje nevarnih snovi, iznos zaupnih dokumentov, zloraba osebnih in tajnih podatkov, odmevna afera, velika tehnično-tehnološka okvara na opremi in drugi izredni dogodki. Ključni namen neprekinjenega poslovanja je po standardu **ISO 22301** sposobnost organizacije, da po izrednem dogodku čim prej nadaljuje s proizvodnjo, z dobavo proizvodov in/ali storitev na sprejemljivi vnaprej določe-

Načrti neprekinjenega poslovanja so učinkovito sredstvo (poslovno orodje) zagotavljanja poslovanja in delovanja gospodarske družbe tudi v okoliščinah izrednih dogodkov in kriznih stanj.

ni način, to je z načrtom. V tem kontekstu je upravljanje neprekinjenega poslovanja definirano kot holističen pristop, ki identificira potencialne grožnje in tveganja organizacije ter njihov vpliv na vse poslovne procese. Hkrati proces upravljanja neprekinjenega poslovanja predstavlja osnovni okvir za vzpostavitev sistema **poslovne odpornosti na vsa tveganja** v katerikoli organizaciji. Sicer pa mora ocena ranljivosti in ogroženosti pokazati kateri od zgoraj navedenih izrednih dogodkov so bolj in kateri manj verjetni, da se bodo tudi dejansko zgodili. Za vse tiste izredne dogodke, ki so bolj verjetni za nastanek je treba pripraviti scenarije in po njih testirati načrt neprekinjenega poslovanja. Iz tega izhaja kaj naj načrt neprekinjenega poslovanja vsebuje, upoštevajoč standard in dobro prakso.

Potrebni vsebinski sklopi načrta neprekinjenega poslovanja so tako naslednji:

- ključni podatki o gospodarski družbi (dejavnosti, trgi, poslovna uspešnost, strategija, idr.),
- namen in koristnost zagotavljanja neprekinjenega poslovanja,
- ključne (kritične, najpomembnejše) poslovne funkcije, ki morajo delovati tudi v kriznih stanjih,
- ključni kadri,
- ključni zunanji pogodbeni izvajalci,
- SWOT analiza,
- ugotovljene vrzeli (pomanjkljivosti) v poslovnih procesih,
- izvleček iz ocene ranljivosti,
- izvleček iz ocene ogroženosti,
- celovita ocena tveganj z registrom tveganj in ukrepi obvladovanja tveganj – gre zlasti za oceno poslovnih (razvojnih, projektnih, finančnih), proizvodnih, tržnih in dobaviteljskih tveganj, informacijskih, komunikacijskih in logističnih tveganj, varnostnih tveganj, tveganj človeških virov ter tveganj poslovnih partnerjev in pogodbenih izvajalcev,
- **krizni načrt** za obvladovanje kriznega vodenja.

Kot je uvodoma rečeno ima načrt neprekinjenega poslovanja najprej preventivni namen, to je, da nastopa zoper nastanek izrednih dogodkov in represivni (kurativni) namen, ko gre za razreševanje izrednega dogodka in za razreševanje krizne situacije (krizno vodenje).

Vzpostavljanje kriznega vodenja v sklopu neprekinjenega poslovanja

Razreševanje nastalega izrednega dogodka, ki je povzročil znatno materialno in finančno škodo – lahko pa tudi človeško, moralno pa še kakšno drugo škodo – se praviloma razrešuje z metodo kriznega vodenja.

Za potrebe kriznega vodenja je treba izdelati **krizni načrt,** ki naj vsebuje (osnovni metodološki okvir):

- sestav kriznega štaba z dokumenti o imenovanju vodje štaba in članov štaba,



- kompetence, naloge in ukrepi kriznega štaba,
- povezovanje z internim štabom civilne zaščite,
- potencialna krizna stanja, ki jih lahko povzročijo verjetni izredni dogodki iz ocene ranljivosti, ogroženosti in tveganj,
- scenariji za posamezna krizna stanja oziroma posamezne izredne dogodke,
- testiranje scenarijev z vajami (vsakoletno načrtovanje določene vaje),
- interni alarmni sistem in sistem odzivanja na alarme,
- poimenska določitev dosegljivosti odgovornih oseb (24 ur na dan),
- obveščanje operativno komunikacijskega centra policijske uprave (OKC PU), zaradi ukrepanja policije,
- delovanje internega varnostno nadzornega centra (IVNC) in/ali pogodbenega VNC, ki opravi obveščanje in organizira varovanje z varnostniki,
- uporaba načrta evakuacije, če je to zaradi nevarnosti za ljudi in živali potrebno,
- preveritev intervencijskih poti na območju krizne situacije,
- z vidika družbene odgovornosti in seznanjanja javnosti krizni štab organizira tiskovno konferenco med in/ali po razreševanju izrednega dogodka oziroma krizne situacije,
- ureditev zbirke dokumentov o razreševanju krizne situacije.

Za saniranje posledic in konkretne škode izrednega dogodka, ki je povzročil krizno situacijo krizni štab izdela poseben **operativni opomnik**, kot pripomoček za izvajanje potrebnih aktivnosti v procesu sanacije. Smiselne in uporabne sestavine opomnika so lahko naslednje:

- fotografiranje in video snemanje nastale škode na zgradbah, prostorih in opremi,
- interno raziskovanje izrednega dogodka – ugotovitev vzroka in posledic,
- raziskovanje, ki je v pristojnosti uniformirane in kriminalistične policije, ustrezne inšpekcije in gasilstva,
- način in čas fizičnega varovanja lokacije in prostorov – zunanji izvajalec fizičnega varovanja – pogodba,
- ocena škode – opisno in v evrih,
- način saniranja poškodb na zgradbi, prostorih, instalacijah, strojni in programski opremi ter dokumentaciji, arhivih in drugem,
- izbor izvajalcev za saniranje poškodb – sklepanje pogodb,
- terminski plan saniranja poškodb,
- spremljanje in nadziranje saniranja poškodb,
- testiranje obnovljenih prostorov, strojne in programske opreme ter ostalih sistemov,
- ponovni zagon poslovanja na osnovni lokaciji,
- pregled zavarovalnih pogodb (polic) in seznanitev zavarovalnice o nastalem izrednem dogodku in potencialni škodi,
- oblikovanje zbirke dokumentov o sanaciji.

Navedeno mora biti elektronsko dokumentirano in uporabno v postopku, ko bo oškodovana gospodarska družba od zavarovalnice terjala povrnitev škode.

Obvladovanje tveganj z zavarovalnim portfeljem

Eden od (zlasti s finančnega vidika) zelo pomembnih ukrepov obvladovanja tveganj je tudi zavarovanje premoženja, procesov, ljudi in odgovornosti. Tveganja (rizike), ki izhajajo iz naravnih sil, požarne rizike, rizike kriminalne narave, tehnično-tehnološke rizike in rizike odgovornosti je treba zavarovati pri izbranih zavarovalnicah. Ustvariti si je treba takšen **zavarovalni portfelj** (komplet, nabor, zbirko zavarovanj), ki za primerno ceno zavarovalnih storitev omogoča optimalni finančni vložek in optimalni finančni učinek po nastali škodi. Ali povedano drugače: Za povrnitev škode na bazi zavarovalnih polic je treba vložiti poseben zahtevek zavarovalnici in se pri tem pogajati tako, da se doseže povrnitve škode v višini, ki jo določa zavarovalna pogodba. Zaradi tega je nujno, da se nastala škoda in vsa dogajanja, ki so v poslovne procese vnesla hudo motnjo dokumentirajo, upoštevajoč tudi rezultate preiskovalnih dejanj policije in inšpekcije. Posebej je treba opozoriti, da se pri zavarovalnih poslih ne splača igrati z zavarovalniškimi prevarami in goljufijami. Vsi zavarovalniški posli morajo potekati na podlagi strokovnih ocen ranljivosti, ogroženosti in tveganj, na podlagi dejanskih podatkov o nastalem izrednem dogodku oziroma škodi ter v skladu z zakonodajo in dobro prakso.

Integrirano obvladovanje tveganj

Ko se temeljito lotevamo obvladovanja poslovnih, varnostnih in drugih tveganj se soočamo z vsaj naslednjimi izrazi: varnost (safety, security), nevarnost (danger), varnostni izzivi (security challenges), varnostna tveganja (security risks), varnostne grožnje (security threats), negotovost (uncertainty), izpostavljenost (exposure), preprečevanje škod in izgub (loss prevention), cost/benefit – obvladovanje stroškov, itd. Temeljito lotevanje obvladovanja tveganj lahko poimenujemo integrirano obvladovanje tveganj (IOT), ki v prvi vrsti pomeni interdisciplinarni, sistemski, celovit, profesionalni in odgovorni pristop k problemu. Drugi vidik IOT se vidi v tem, da se tveganjem posveča pozornost v vseh poslovnih procesih na vseh organizacijskih ravneh in na vsakem delovnem mestu. Tretji vidik IOT je **načrt neprekinje-**



Temeljito obvladovanje tveganj je tek na dolge proge, ki zahteva interdisciplinaren pristop, poglobljeno oceno in analizo ranljivosti in ogroženosti, stalno ažurnost in uvajanje stalnih izboljšav v procese upravljanja s tveganji.

Za razmislek

Verjetno ni treba nikogar posebej prepričevati, da temeljito obvladovanje tveganj ni preprosta zadeva in enkraten projekt. Temeljito obvladovanje tveganj je tek na dolge proge, ki zahteva interdisciplinaren pristop, poglobljeno oceno in analizo ranljivosti in ogroženosti, stalno ažurnost in uvajanje stalnih izboljšav v procese upravljanja s tveganji. Morda je prav zato tveganjem v gospodarstvu namenjeno občutno premalo pozornosti. Morda pa tudi zato, ker ima Slovenija še vedno status varne države, v kateri ni prav velikih varnostnih in drugih groženj, morda tudi zato, ker je v gospodarstvu vse več lastninskih in kadrovskih zmešnjav, ali tudi zato, ker je že kar preveč raznih metod in modelov, ki jih nekatere gospodarske družbe neposredno uporabijo. Denimo Silver Bullet Risk, orodje za celovito upravljanje tveganj uporabljajo nekatere gospodarske družbe – tudi v kritični infrastrukturi. Kakorkoli, Ernest in Young v svojih publikacijah trdita, da organizacije, ki se celovito lotevajo obvladovanja tveganj dosegajo do trikrat večje dobičke in hkrati utrjujejo konkurenčno prednost in poslovno odpornost. Verjemimo, da to drži. Potemtakem bi se splačalo izdelati model, vzorec ali celo pravo metodologijo obvladovanja tveganj, ki bi bila širše uporabna in pripravljena v obliki programskega orodja – aplikacije. Kdo bo tisti, ki se bo lotil tega izziva? ■



nega poslovanja s kriznim načrtom, na bazi standarda ISO 22301:2014 in standarda ISO/IEC 27000:2018. Četrti vidik IOT je **uvedba standarda upravljanja tveganj ISO 31000:2018, ki že v osnovi nakazuje, da gre za integrirano upravljanje s tveganji v katerikoli organizaciji**. Peti vidik IOT je uvedba varnostnih standardov v poslovanje, zlasti OHSAS 18001, ISO 14001, HACCP/IFS/ISO 22000, GDPR – varstvo osebnih podatkov, standardov fizičnega in tehničnega varovanja (pristopna kontrola, videonadzor, protivlomna zaščita, VNC), varstva pred požari in drugih. Tu je še šesti vidik IOT, ki z uporabo nekaterih poslovnih orodij kot so HRM - upravljanje človeških virov), CRM – upravljanje strank, BSC – model uravnoteženih poslovnih kazalnikov, SA 8000/ISO GSR 26000 – družbena odgovornost, KAIZEN – stalne izboljšave, 20 ključev – čiščenje organizacije, idr. In jasno, uporaba zavarovalnih storitev je sklepno dejanje temeljitega obvladovanja tveganj.

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: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Tone Stanovnik, direktor Špice International d.o.o.*

RAZVOJNI INOVATIVNI PRISTOPI KLJUČ ZA USPEŠNO POSLOVANJE PODJETJA

Podjetje Špica International je dobitnik prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj inovativna varnostna rešitev« za leto 2017. Prizadevanja za učinkovit razvojni in inovativni pristop se kažejo v dobrih rezultatih poslovanja, novih izzivih in poslovnih priložnosti. O ključnih razvojnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z g. Tonetom Stanovnikom.

Koncern ŠPICA INTERNATIONAL predstavlja vodilno regijsko skupino podjetij na področju rešitev Registracije delovnega časa in Kontrole pristopa. Nam lahko prosim podrobneje pojasnete katera so glavna težišča vaših rešitev, ki na trg varnostnih rešitev prinašajo dodano vrednost?

Na področju rešitev tehničnega varovanja je IDentifikacija oseb in pripadajoče opreme neke vrste rdeča nit, ki je vtkana takorekoč v vsa področja našega življenja. Ko smo pred 30 leti, kot eno prvih računalniških podjetij v Sloveniji, začeli svojo prodorno pot, smo imeli podaljšano ime podjetja Špica International, Sistemi za avtomatsko IDentifikacijo. Dotično tehnološko področje pa je v zadnjem obdobju doživelo popoln preporod, saj se je skozi IoT – Interneta stvari, prebilo takorekoč v prvo vrsto tehnologij prihodnosti. Od tehnologije same, pa se seveda ne da živeti, saj jo je potrebno vgraditi v sistemske rešitve, ki uporabnikom rešujejo ključne vsakodnevne probleme. Tako smo na samem začetku zastavili sistem za Kontrolo Pristopa v prostore. Skozi 30 letno obdobje, pa se je okoli te centralne aplikacije nanizala ogrlica spremljajočih modulov, ki rešujejo ključne probleme kot so: Registracija delovnega časa z elektronsko najavo odsotnosti in potnimi nalogi, IDentifikacija vozil na parkirišču podjetja, IDentifikacija obiskovalcev v recepciji, IDentifikacija in kontrola logičnega dostopa do informacijske infrastrukture (centralno tiskanje, avtorizacija na osebnem računalniku).

Ključne informacije podjetja je seveda potrebno in možno zaščititi z najboljšimi možnimi tehnološkimi sredstvi, vendar je vedno potrebno vzporedno graditi tudi kulturo in moralne vrednote podjetja, ki preventivno zmanjšujejo potencialne grožnje.

Vse te rešitve smo povezali v Time&--Space platformo okoli univerzalne identifikacijske kartice, ki pa je že danes lahko kar vaš mobilni telefon. Hkrati smo v sodelovanju s sestrskimi Špica podjetji v vseh državah bivše Jugoslavije, mnogim slovenskim velikim podjetjem omogočili centralno nadzorovan varnostni sistem, ki občutno zmanjšuje tveganja in olajša vodenje podjetij v viharnem balkanskem kotlu.

Ravno čez slab mesec, pa bomo na največjem svetovnem sejmu IFSEC 2018 pokazali našo novo inovacijo - sistem za kontrolo dostopa brez čitalcev, ki smo ga poimeovali DoorCloud. Gre za IoT rešitev, ki smo jo namestili v računalniški oblak Azzure.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

S svojim poslovanjem ste močno prisotni v mednarodnem okolju, posebej v regiji JV Evrope, kjer so varnostna tveganja še posebej specifična. Ali svoje odločitve o širitvi poslovanja na določene trge temeljite tudi na strateških analizah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Ko smo začenjali pred 30 leti smo bili seveda »mladi« in smo si brezkompromisno v ime podjetja dodali besedo »International« - celemu svetu smo namreč želeli sporočiti, da želimo svoje informacijske rešitve izvažati. To ni bila le želja, ampak smo svoje ambicije podkrepili z večkratno prisotnostjo na največjem računalniškem sejmu v Evropi - CeBit Hannover. Naša rešitev je bila v tistih časih seveda za reguliran nemški trg še prešibka, so nas pa zato toliko bolj opazili regijski kupci, ki so v tistih časih v velikem številu obiskovali ta sejemski dogodek in se zvečer veselili jugoslovanskega »meeting pointa« na Špica razstavnem prostoru. Tudi mnogi obiskovalci iz Bližnjega vzhoda so se v tistih časih z veseljem oglasili pri nas in tako smo vzpostavili svoje prodajne bazne tabore v vseh mestih bivše Jugoslavije in glavnih mestih Bližnjega vzhoda, kjer smo zgradili močna partnerska podjetja. Danes smatramo Adriatic regijo za svoj domači trg in šteje za nas, kot »ustrezen«, le izvoz zunaj regije, kamor se intenzivno usmerjamo. Internetna tehnologija nam pri tem precej pomaga, saj je sedaj tudi vzhodni trg izpostavljen udaru novih, revolucionarnih mobilnih in oblačnih rešitev,ki bodo popolnoma premešale karte na trgu.

Ste podjetje, ki veliko sredstev vlagate v lasten razvoj novih tehnoloških rešitev. Nam lahko zaupate svojo vizijo na tem področju za prihodnje obdobje?

Vsekakor se zavedamo, da smo v središču prebojnih, revolucionarnih sprememb, ki jih morda zaradi 30 letne zgodovine niti ne bi opazili. Ocenjujem, da ohranjamo stik z napredkom tudi zaradi tesnega sodelovanja z mlajšo generacijo, ki danes prihaja iz fakultet. Tudi z njihovo pomočjo, s svežimi, inovativnimi očali, sodelujemo pri razvoju in celo tvorimo napredek. Vstopili smo v kapitalsko povezavo in mentorski program s tremi start-up podjetji, ki delujejo v naši smeri in si tako omogočili inoviranje na robu naše osnovne dejavnosti, ki prinaša seveda trenutno glavno dodano vrednost. Smeri, v katere menimo, da se bo naša branža razvijala, bodo zelo verjetno povezane z:

- vstopom IDentifikacijske kartice v mobilni telefon,
- vzpostavitvijo družine tesno prepletenih Time&Space aplikacij,
- prebojem uporabniško prijaznih vmesnikov na tehnologiji Vision, Voice in Biometrija.



Kako so po vašem mnenju pomembne ključne informacije podjetja v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali varovanju teh informacij v Špici International namenjate veliko pozornost?

Ključne informacije podjetja je seveda potrebno in možno zaščititi z najboljšimi možnimi tehnološkimi sredstvi,

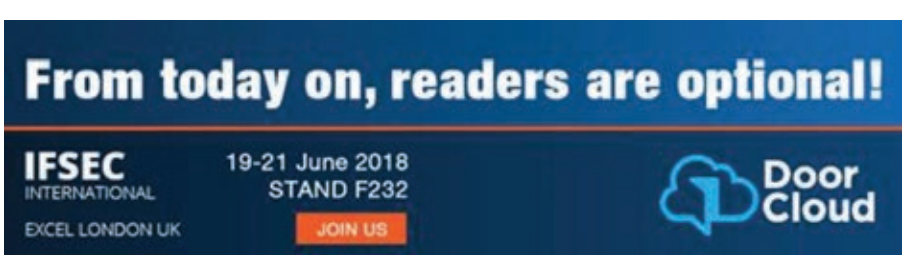
vendar je vedno potrebno vzporedno graditi tudi kulturo in moralne vrednote podjetja, ki preventivno zmanjšujejo potencialne grožnje. V Špici smo kot eno prvih računalniških podjetij svoje poslovanje uredili po ISO9001 standardih, ki smo jih zadnja leta nadgradili na ISO27001. Slednji posebno skrb namenja sistematičnemu upravljanju in varovanju informacij. Zato vsako leto izvedemo interno in še uradno presojo, ki pokažeta na potrebna področja izboljšav. Le te potem z ukrepi, ki jih sprejemamo na kvartalnem nivoju, tudi nadzorovano izvedemo. Hkrati pa naš trud na kadrovskem področju vzdržuje visoko lojalnost zaposlenih do podjetja in tako zgrajeno znanje ostaja v podjetju. Na ta način gradimo pomembno dodano vrednost, ki jo usmerimo v nove razvojne cikle. Nenazadnje pa so lojalni zaposleni pomemben, če ne ključen vir varnosti podjetja. Kot veste, nobena tehnološka rešitev ni dovolj varna, da bi zaustavila posameznika, ki lahko povzroči škodo, nenamerno ali z namenom.



Ocenjujem, da ohranjamo stik z napredkom tudi zaradi tesnega sodelovanja z mlajšo generacijo, ki danes prihaja iz fakultet. Tudi z njihovo pomočjo, s svežimi, inovativnimi očali, sodelujemo pri razvoju in celo tvorimo napredek.

Ste letošnji prejemniki prestižne nagrade Slovenian Grand Security Award v kategoriji »Najbolj inovativna varnostna rešitev«. Nam lahko zaupate kaj vam pomeni prejem take nagrade?

Nagrade smo seveda zelo veseli in nas obvezuje, da visoke standarde inovativnosti na področju tehničnega varovanja vzdržujemo tudi v prihodnje. Varovanje in inovativnost na prvi pogled delujeta kot nasprotna si pola - preveč varnosti lahko zavira inovativnost in poslovne procese. Naša glavna prednost je, da znamo s pravo mero usklajenosti obe področji razvijati tako, da je »volk sit in koza cela«. Če aktivno ne zaznavamo sprememb, ki se dogajajo v naši okolici, nas te lahko presenetijo nepripravljene. Zato ves čas prežimo za novimi poslovnimi modeli in inovacijami, ki nas držijo korak ali dva pred konkurenti. Trenutno je na primer bančni sektor zelo na udaru digitalne transformacije. In prav v bančnem sektorju imamo izgrajene svoje najmočnejše kompetence - prvih devet od desetih slovenskih bank po velikosti namreč uporablja naš sistem Time&Space. Tako, kot so banke in komintetni že nekaj časa v procesu prehoda izplačevanja s plastičnimi karticami na mobilni telefon, je ta inovativna sprememba tudi del naše trenutne, intenzivne razvojno-raziskovalne osredotočenosti. Z našo inovativno storitvijo www.doorcloud.com bomo letos nastopili na dveh največjih Evropskih sejmih IFSEC LONDON in SECURITY ESSEN.



Kje v prihodnosti lahko pričakujemo največje spremembe vezane na uvajanje novih tehnologij na področju obvladovanja varnostnih tveganj? Rešitve t.i. pametnih mest so postale realnost.

Pametna mesta so seveda zgrajena na pametnih zgradbah in to sta dva stebra slovenske »pametne specializacije«, kjer je Špica intenzivno prisotna. V pametnih zgradbah z našim znanjem in inovacijami gradimo tako imenovano »Inteligentno vstopno točko« - gre za pametna vrata, ki vas na vstopu v prostor prepoznajo podobno, kot vas v virtualnem svetu prepozna spletno mesto in vam dinamično prilagodi vsebino, glede na vaše predhodne interakcije in atribute. Na ta način s svojimi pametnimi rešitvami občutno izboljšamo uporabniško izkušnjo, ki je ključnega pomena za razširitev uporabe storitve. Na področju pametnih mest pa gradimo »Inteligentno parkirno točko« - gre za senzorje, ki so nameščeni na parkirnih prostorih v mestu in obiskovalca preko mobilne aplikacije vodijo do najbližjega prostega parkirnega mesta. Na ta način se občutno zmanjšuje nepotrebna poraba goriva, ko krožimo po mestu in iščemo parkirišče. Rešitev omogoča ponudnikom, da ceno prilagodijo povpraševanju, podobno kot letalski prevozniki prilagodijo ceno letov. Nenazadnje pa bomo zoznikom na ta način prihranili nekaj nervoze in napetosti – torej rešitev blagodejno vpliva na počutje.

Vaše rešitve presegajo samo področje obvladovanja varnostnih tveganj. V katerih segmentih vezano na optimizacijo poslovnih procesov lahko najdemo vaše rešitve?

Poleg uspehov, ki jih trenutno nizamo na projektih kritične infrastrukture kjer smo v zadnjem obdobju dosegli zavidljive rezultate bi rad izpostavil področje kjer hkrati z zmanjševanjem varnostnih tveganj dvigujemo tudi učinkovitost in produktivnost. To so projekti povezani z logistiko skozi proizvodnjo, skladiščenjem in transportom do trgovin in končnih kupcev. Učinkovito obvladovanje teh logističnih poti omogoča podjetjem pomembno konkurenčno prednost. V zadnjem obdobju pa se na tem področju dogajajo tudi velike spremembe poslovnih modelov. Tudi tehnološki velikani kot so Amazon, Google se osredotočajo na ta področja. Kjer se dogaja »revolucija« je pomembno, da ste poleg z odprtimi očmi, da izkoristite priložnost in pridobite spet korak prednosti.

Glede na to, da ste visoko tehnološko podjetje, ste vi in posredno vaše stranke v svoji dejavnosti zelo izpostavljene kibernetskim tveganjem. Kakšne ukrepe v podjetju izvajate na področju zagotavljanja informacijske varnosti?

Naša interna krovna varnostna politika pokriva 25 področij, kjer obstajajo potencialne nevarnosti. Ta področja smo natančno analizirali in vzpostavili ukrepe, ki zmanjšujejo tveganja do sprejemljive višine. Vedno namreč velja oceniti, do katere mere je investicija v varovanje še racionalna. Teh 25 področij vsako leto ponovno pretehtamo in glede na napredek tehnologije in potencialnih groženj, ponovno prilagodimo. Celoten sistem obvladovanja ukrepov imamo podprt z računalniškim programom, ki vodstvu omogoča krovni pregled na realizacijo. Tako lahko zagotavljamo, da imamo s sistemom upravljanja in varovanja informacij zagotovljena tri ključna področja:

- zaupnost, saj do informacij lahko pridejo le tisti, ki so za to pooblaščeni,
- celovitost, saj varujemo popolnost informacij ter metod za njihovo obdelavo,
- razpoložljivost, saj imajo pooblaščeni uporabniki dostop do informacij in pripadajočih virov takrat, ko jih potrebujejo.

Kako uspete v podjetju zagotavljati uravnoteženost med na eni strani zelo restriktivnimi varnostnimi zahtevami varovanja ključnih informacij organizacije in na drugi raziskovalni iniciativnosti, ki je včasih zelo občutljiva na prevelike omejitve delovnega okolja?

Osebno ocenjujem, da je ravno to največja prebojna moč inoviranja, ko uspete na dveh diametralno nasprotnih področjih hkrati doseči napredek, in to ne eden, na račun drugega. Lep primer je japonski prodor na ameriški avtomobilski trg. Ko so poskušali samo z nizko ceno je šlo počasi in s težavo. Ko pa so nizki ceni dodali še visoko kakovost so postali skoraj nepremagljivi. Zanimiv primer iz gospodarstva so severnoevropske države, ki jih krasi visoka stopnja socialne pravičnosti, hkrati pa so na vrhu svetovnih lestvic učinkovitosti in konkurenčnosti. Na prvi pogled gre za nezdružljivo simbiozo, za nesprejemljivo nasprotje, a ravno inovativni pristopi so tisti, ki skandinavcem omogočajo, da delajo bolje in ne nujno več. Slovenija z zgodovinsko močnim socialnim čutom lahko črpa te inovativne pristope iz različnih koncev sveta, ter jih sestavi v mozaik, ki nas bo konkurenčno razmejil od ostalega sveta in nam omogočil globalno prebojnost.



Naša interna krovna varnostna politika pokriva 25 področij, kjer obstajajo potencialne nevarnosti. Ta področja smo natančno analizirali in vzpostavili ukrepe, ki zmanjšujejo tveganja do sprejemljive višine.

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

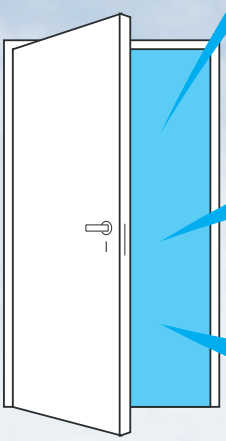
Za poslanstvo pravijo, da je ključnega pomena pri vsakem združenju, saj vsebuje nek skupni visoki cilj, ki ga posameznik zaradi svoje majhnosti, nikoli ne more doseči. To je eden od glavnih treh motivatorjev človeka, da deluje v skupnosti. Drugi je superiornost, ki je spet pogojena s črpanjem najboljših praks iz okolja in Dobre prakse so najbolj učinkovite za predstavnike istih sektorskih združenj. Nenazadnje je pomembno, da kljub različnosti in avtonomiji, ki je tretji motivator, uspeš te inovacije in pristope inovativno uskladiti s partnerji. Slovensko združenje korporativne varnosti omogoča ravno vse te tri elemente in z odličnim sodelovanjem s sorodnimi združenji v Adriatic regiji, je za Špico in mene osebno, odlična platforma za odriv v nove skupne poslovne uspehe in preboje. ■

Opomba: fotografije so iz arhiva Spica International d.o.o.

Kontrola pristopa tudi brez čitalcev

Door Cloud je inovativna rešitev na področju kontrole pristopa. Sloni na napredni mobilni aplikaciji in novi generaciji pametnih krmilnikov.

Door Cloud



Mobilna aplikacija Door Cloud

Z Door Cloud mobilno aplikacijo čitalcev ne potrebujete. S pomočjo aplikacije izberete vrata, ki jih želite odpreti. Vašo zahtevo aplikacija Door Cloud nato preko oblaka sporoči krmilniku, ki odklene ključavnico – seveda le, če imate za to ustrezne pravice.

Je Door Cloud varen?

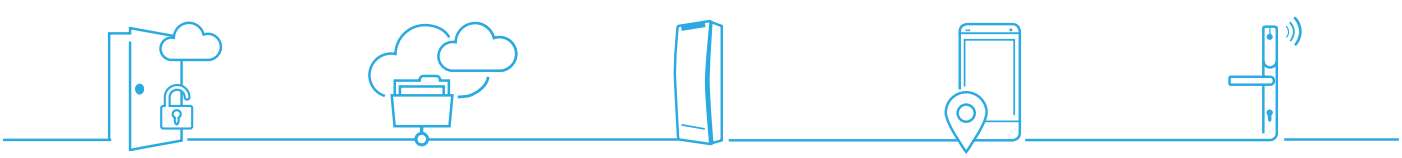
Door Cloud temelji na Microsoftovi oblačni platformi Azure in s krmilniki komunicira preko kriptiranega IoT protokola.

Zakaj Door Cloud?

- Enostavna namestitev brez čitalcev in strežnikov.
- Preprosto dodajanje novih pristopnih točk in lokacij.
- Mesečna naročnina namesto visoke začetne investicije.
- Primerno tudi za manjša podjetja.
- Podpora za HID čitalce in Aperio ključavnice.
- Napredna mobilna aplikacija, ki nadomesti kartice in čitalce.

WWW.DOORCLOUD.COM

Obiščite nas na **IFSEC 2018**
19. - 21. junij, stojnica F232



Kontrola pristopa | Storitev v oblaku | HID čitalci in Špica krmilniki | Pristop brez čitalca | Brezžične ključavnice Aperio

Špica international d.o.o., Pot k sejmišču 33, 1000 Ljubljana, www.spica.si, info@spica.si, 01 568 08 00

Avtor: Vojko Volk / veleposlanik



PROTISLOVJA MIGRACIJ IN PRIHODNOST EU

„Ne nasprotujem migracijam, je pa povsem razumljivo, da jih treba omejiti, ljudem pa omogočiti integracijo in se zoperstaviti diskriminaciji“.

/Ayaan Hirsi Ali, aktivistka človekovih pravic/

Uvodni citat ameriške aktivistke somalskega rodu Ayaan Hirsi Ali odraža vso preprostost odgovora na ključna vprašanja o tem, kako pristopati k problematiki priseljevanja. Odraža dejstvo, da je vsako priseljevanje, ki je zgodovinski fenomen že od začetkov človeštva, še posebej priseljevanje beguncev, hkrati humanitarno a tudi varnostno vprašanje. Od tod tri ključne besede;

- **omejevanje migracij** kot legitimen odgovor na preveliko priseljevanje, varnost in stabilnost držav;
- **integracija priseljencev** kot dolžnost držav, ki sprejema priseljence;
- **nediskriminacija priseljencev** zaradi rasnih, kulturnih ali verskih različnosti.

Ayaan Hirsi Ali ni po naključju zadela tudi zaporedje svojih besed; najprej omejevanje, tudi kot omejevanje z ukrepi za izboljšanje razmer tam, od koder pribežniki prihajajo, potem integracija in nazadnje nediskriminacija. In vendar je priseljevanje v zadnjih treh letih postalo ključni problem, ki močno deli politične duhove po Evropi. Zakaj že?

I.

Kar je za ZDA že desetletja povsem običajen pojav je Evropo leta 2015 skoraj spravilo na kolena in privedlo EU na rob obstoja. Priseljenski val, ki je zaradi steka različnih okoliščin, predvsem pa vojne v Siriji in razmer v Libiji, nenadoma zajel južno in srednjo Evropo, je v Evropo v kratkem času prinesel dober milijon ljudi, spočetka večinoma pribežnike, kasneje pa vse bolj predvsem ekonomske priseljence, ki iščejo boljše življenje. O tem priča tudi struktura držav, od koder zadnji priseljenci prihajajo in v katerih ni vojnega stanja, niti posebej nevzdržnih varnostnih razmer (Pakistan, Bangladeš, Indija, Tunis, Alžirija), so pa v njih težavne gospodarske in socialne razmere. Medtem ZDA že pol stoletja, vsako leto, sprejmejo v povprečju skoraj milijon legalnih priseljencev. Z milijonoma in pol prispelih v letih 2016 in 2017 je skupno število stalnih priseljencev v ZDA od leta 1970 naraslo na 45 milijonov in predstavljajo 13.5 odstotka celotnega prebivalstva ZDA (326 mio prebivalcev leta 2017). ZDA nenehno potrebujejo novo delovno silo ob tem, da imajo še iz druge polovice 19. stoletja eno najbolj učinkovitih organizacij, ko gre za obravnavo in sprejem priseljencev. Sprejem priseljencev je bil v zadnjih letih še povečan, zlasti zaradi ugodnih gospodarskih razmer v ZDA in nizke brezposelnosti, ki letošnjo pomlad že pada pod 4 odstotke. Sklep je skratka preprost; medtem ko je v ZDA priseljenstvo zgodovinski temelj države in še vedno aktualna demografska oz. gospodarska nuja, je za EU priseljenstvo nerešljiv problem, ki jo politično ogroža in ustvarja vsaj ta hip nerešljive spore med državami. Kako je mogoče, da je za 326 milijonsko Ameriko milijon in pol priseljencev na leto korist, za 510 milijonsko EU pa je dober milijon priseljencev v treh letih problem in varnostna grožnja?

To protislovje, ki je videti zares krepko, ima seveda svojo preprosto razlago, ki je hkrati razlaga vseh težav EU. Gre za to, da za razliko od ZDA, EU ni država in mora za vse ključne politične odločitve pridobiti soglasje vseh držav, katere jo tvorijo. Ko je EU končno prišla do odločitev o tem, kako obravnavati migracijski val, prenoviti šengenska pravila, prilagoditi azilno politiko in določiti priseljenske kvote državam, se je kvotam uprlo nekaj vzhodnoevropskih držav in vse je obstalo. Še več, prišlo je do reakcije zahodnih članic EU, ki so blokado vzhodnih ocenile za licemerno in nesolidarno, ter celo

Povsem jasno je torej, da EU še nekaj časa ne bo sposobna imeti enotne politike do priseljencev, posledice pa utegnejo biti zelo resne, še posebej v primeru, da bi se tudi na tej podlagi utemeljila politika EU dveh hitrosti.

napovedale finančne ukrepe tem državam v aktualni razpravi o prihodnjem proračunu. Povsem jasno je torej, da EU še nekaj časa ne bo sposobna imeti enotne politike do priseljencev, posledice pa utegnejo biti zelo resne, še posebej v primeru, da bi se tudi na tej podlagi utemeljila politika EU dveh hitrosti. V takem primeru bi brez dvoma krajši konec potegnile revnejše vzhodne članice EU, ki so vse po vrsti gospodarsko odvisne od zahodnih članic, razvojno pa tudi od evropskih sredstev, ki se bodo pomembno znižala že zgolj zaradi izstopa Velike Britanije iz EU.

Ob začetku 20. stoletja je prebivalstvo današnje EU predstavljalo kar 35 odstotkov svetovnega prebivalstva, v letu 2016 pa le še dobrih 6 odstotkov. Ob sedanjih trendih bo do leta 2060 padlo na vsega 4 odstotke svetovnega prebivalstva. Navkljub tehnološkemu napredku ti podatki kažejo, da ima EU velik demografski problem, staranje in zmanjševanje prebivalstva, med vodilnimi članicami pa ima največji problem prav Nemčija, kjer število prebivalstva zadnje desetletje stagnira. In v tem kontekstu lažje razumemo izjavo kanclerke Merklove ob začetku priseljenskega vala, ko je želela verjeti, da se lahko pojav obrne v prid Nemčije in pozabljajoč, da gre za nevaren precedens zato, ker je šlo za nelegalno in povsem nenadzorovano priseljevanje, ki z načrtno priseljensko politiko nima resne povezave. O demografskih zadregah Nemčije pa priča tudi izjava Merklove o odnosih med Nemčijo in Indijo; „Indija potrebuje delovna mesta, Nemčija pa potrebuje ljudi, zato je sodelovanje nujno za urejanje demografskih potreb obeh držav“. Kljub temu je bilo zadnje desetletje, navkljub krizi iz leta 2008, po gospodarskih dosežkih najuspešnejše v zgodovini EU. Res je, da EU (22 odstotkov svetovnega BDP) po moči še ni dosegla ZDA (24 odstotkov), a je res tudi, da je celoten evropski trg že dolgo močnejši od ZDA. Sledi seveda Kitajska, ki je bliskovito dosegla kar 15 odstotkov svetovnega BDP-ja se njena rast zadnja leta umirja. Podatki skratka zelo jasno govorijo o tem, da ZDA svojo demografsko stabilnost ohranjajo s skrbno načrtovanim priseljevanjem, Kitajci tega problema nimajo, EU pa se ga loteva z velikimi težavami in političnimi zapleti.

Podatki skratka zelo jasno govorijo o tem, da ZDA svojo demografsko stabilnost ohranjajo s skrbno načrtovanim priseljevanjem, Kitajci tega problema nimajo, EU pa se ga loteva z velikimi težavami in političnimi zapleti.



II.

V Evropi se kot posledica priseljenskega vala iz leta 2015 oblikujeta dva osnovna politična pristopa do priseljevanja. Prvi, recimo mu **varnostni,** se je utemeljil na priseljevanju kot grožnji, ne samo kot vprašanje fizične varnosti ampak tudi kot grožnji zahodni oziroma v tem primeru evropski civilizaciji a tudi kulturi in identiteti narodov. In drugi pristop, recimo mu **humanitarni,** ki nastane kot odraz povsem človeškega razumevanja za težaven položaj pribežnikov, ki so bežali pred vojno in vojnimi razmerami. Prvi pristop k priseljevanju, kot varnostnemu vprašanju, zelo kmalu postane domena velike večine desnih političnih opcij, kjer simbolično vodilno vlogo prevzameta Madžarska in njen voditelj Orban, sledijo pa mu še nekatere države vzhodne in srednje Evrope in med njimi deloma tudi Slovenija, z namestitvijo rezilne žice na južni meji. Drugi pristop k priseljevanju pa se oblikuje v okviru levih političnih opcij in v starih članicah EU, posebej tistih, ki so se s priseljenskim vprašanjem same že dolgo ubadale, zlasti Italija pa tudi Francija in Grčija. Preprosto dejstvo pa seveda je, da je vsak priseljenski val, še posebej, če je plod posebnih razmer ter posledično ilegalen in nenadzorovan, hkrati humanitarno in varnostno vprašanje. In tu znova nastane protislovje; je demografski problem EU kot pomanjkanje delovne sile in ljudi tudi varnostno vprašanje ali ne?

V Nemčiji se pomanjkanje delovne sile že postavlja tudi kot varnostno vprašanje. Razlika med Nemčijo na eni ter Italijo, Španijo in tudi Francijo na drugi strani je namreč v tem, da ima Nemčija neprimerno strožje predpise in nadzor, ko gre za sivi trg delovne sile. Ali z drugimi besedami; medtem ko so Velika Britanija, Francija in deloma tudi Italija v zadnjih letih povečevale število prebivalstva s povečanim priseljevanjem, se v Nemčiji to ni zgodilo in število prebivalcev stagnira. Druga skrajnost je Italija, kjer v njenih južnih deželah že vrsto let prihaja do suženjskega izkoriščanja ilegalnih sezonskih delavcev na poljih, ki prihajajo iz Afrike a tudi iz južne Evrope in v razmerah, nevrednih človeka, delajo za 2 do 3 evre na uro. Italijanski mediji že nekaj let poročajo o fenomenu „para-

dižnikovega pravokotnika“ med mesti Foggia, Taranto, Lecce in Brindisi, kjer v sezoni dela tudi več kot 20 tisoč ilegalnih obiralcev. Podobno je tudi v sosednjih deželah, od Neaplja do Sicilije. K temu je treba prišteti še nepregledno število „pomočnic v gospodinjstvu“, ki v pollegalnih razmerah skrbijo za otroke ali ostarele ter ogromen gradbeni sektor, v katerem namesto redno zaposlenih deluje na tisoče ilegalcev. Italija je država, ki ima eno od najvišjih stopenj nezaposlenosti v EU tudi zaradi teh, znova protislovnih razmer; podjetjem se ne izplača redno zaposlovati, dokler deluje sivi trg, delavcem pa se zaradi mizerno plačanih prekarnih del ne izplača tvegati izgubo socialnih nadomestil. Zaenkrat so bolj kot gospodarske vidne politične posledice vse bolj protislovnih demografskih razmer v državah EU. Razen v Nemčiji, kjer se je stopnja nezaposlenosti marca 2018 spustila na vsega 3.4 odstotka, kar meji na praktično polno zaposlenost vseh za delo sposobnih, so gospodarstva držav EU še vedno v varnih okvirih stopenj nezaposlenosti predvsem pa še bolj zgovornih razmerij med številom zaposlenih in nezaposlenih. Slednji podatek je namreč pomemben zato, ker se v mnogih vzhodno in srednjeevropskih državah nezaposlenost znižuje tudi zaradi visoke stopnje izseljevanja za delo sposobnih, kjer je posebej negativen zgled zlasti sosednja Hrvaška.

Preprosto dejstvo pa seveda je, da je vsak priseljenski val, še posebej, če je plod posebnih razmer ter posledično ilegalen in nenadzorovan, hkrati humanitarno in varnostno vprašanje. In tu znova nastane protislovje; je demografski problem EU kot pomanjkanje delovne sile in ljudi tudi varnostno vprašanje ali ne?



III.

Bolj kot gospodarski, se problem pomanjkanja delovne sile in vse večje nuje po priseljencih kaže kot politični problem. Zlasti v državah z velikim številom priseljencev oziroma ti. prosilcev za azil, kjer birokracija potrebuje dalj časa za „triažo“ priseljencev, nastaja problem s tistimi, ki v pogosto težkih razmerah čakajo, iščejo priložnostna dela ali pa se lotijo ilegalnih dejavnosti. Posledica je, da priseljencem izrazito nenaklonjene politične sile, praviloma desne, te razmere posplošujejo in ustvarjajo ozračje nevarnosti, pa čeravno statistike držav ne potrjujejo teze, da priseljenci po delinkventnosti kakorkoli odstopajo. Ob Nemčiji in Avstriji je predvsem Italija izrazit primer države, kjer se je problem pribežnikov v letih 2016 in 2017 postavil kot prvorazredno varnostno vprašanje, zlasti v tistih okoljih, kjer so nastali začasni zbirni centri in s tem napetosti med pribežniki in lokalnim prebivalstvom. Sredi leta 2017 je v italijanski vladi prišlo do ocene da, če priseljenski val ne bo nekako ustavljen, bodo „prihodnje volitve povsem enostranske, edina tema bodo pribežniki, rezultat pa vnaprej odločen“. Notranji minister Marco Minniti

je s podporo EU dosegel sporazum z libijskimi oblastmi, ki je močno spremenil razmere. Italija je z dodatnimi ladjami, čolni in tehnično opremo opremilo libijsko obalno stražo, v zameno pa je Libija ozemlje nadzora razširila na dvakratno oddaljenost svojih teritorialnih voda od obale. Dotlej so namreč ladje humanitarnih organizacij in civilnih združenj pribežnike reševale iz morja bližje libijskim vodam, odtlej pa jim to ni bilo več mogoče početi. Na ta način je bila učinkovito razbita naveza med kriminalnimi združbami, ki je organizirala ilegalne prevoze po morju in njihovimi vrinjenci v organizacije civilne družbe, ki so pomagali pri načrtovanih „pomorskih nesrečah in reševanjih“. Število pribežnikov v Italijo je bilo v jeseni 2017 praktično čez noč prepolovljeno in prej ključno varnostno vprašanje je do konca leta izginilo iz ospredij medijske pozornosti. Minister Minniti, član levosredinske vlade in levosredinske Demokratske stranke, je bil sicer deležen ostrih kritik humanitarnih organizacij in civilne družbe a je dejstvo, da so prav po njegovi zaslugi italijanske volitve marca 2018 sploh imele pravi smisel in normalno vsebino. Rezultat je bil kljub temu odločno na strani desne sredine in populističnega Gibanja 5 zvezd, leva sredina pa je doživela zgodovinski poraz.

Italijanski primer razkriva nedoslednost in mestoma skrajnost tistih političnih opcij, praviloma levih, ki vztrajajo pri stereotipu o „krivdi belega človeka» oziroma krivdi zahoda za razmere v nerazvitem svetu. Kar deloma seveda drži, a dejstvo je, da pribežniki ne prihajajo samo iz vojnih območij in držav, ki jih je napadel NATO, ampak od povsod tam, kjer so nevzdržne gospodarske in družbene razmere, kjer so visoke stopnje kriminala in kjer je veliko rasne, verske in druge nestrpnosti. Ljudje odhajajo iz teh razmer v boljše življenje, tako kot ljudje iz vzhodne Evrope odhajajo po boljše življenje na zahod, ljudje iz južne Evrope odhajajo v vzhodno Evropo. Ogromna večina priseljencev v ZDA so Mehičani, v Mehiki pa ni vojne niti je ni napadel NATO ...

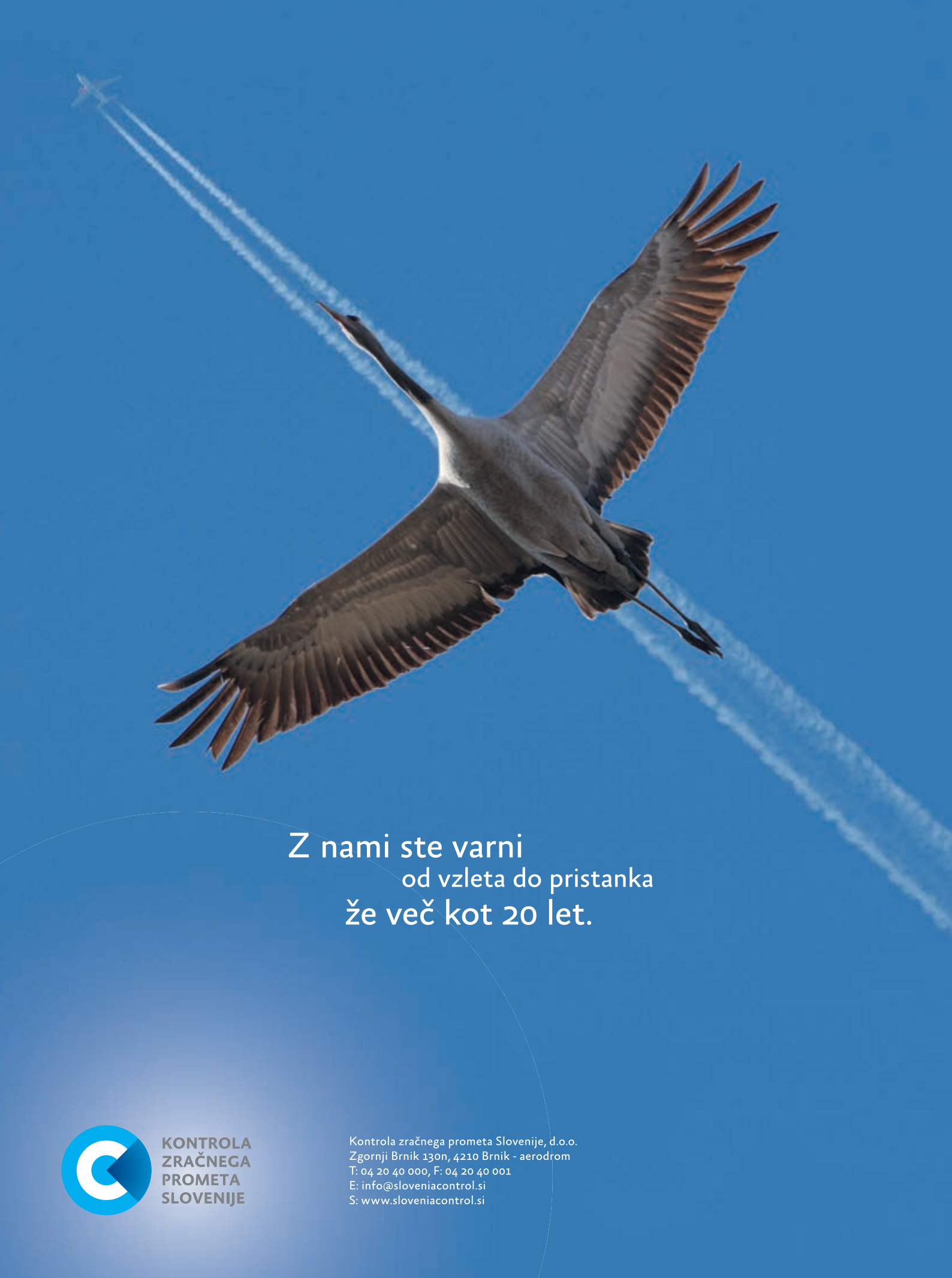
Druga nedoslednost in tudi skrajnost pa je odnos tistih desnih političnih opcij, ki priseljenstvo zavračajo v celoti, k čemur se je v zadnjem obdobju povsem približal tudi madžarski predsednik Orban. Z vidika demografskih razmer v Evropi pa je takšna politika težko vzdržna, še manj pa z vidika nuje, da se EU glede osnovnih potez priseljenske politike poenoti, prenovi šengenska pravila in azilno politiko. Še najmanj so pri tem pomembne «priseljenske kvote», ki so jih vzhodne članice EU kategorično zavrnile, Slovenija pa sprejela in s tem izkazala redko lastnost med novimi članicami EU; sposobnost sprejeti kompromis in ravnati solidarno.

Namesto zaključka

Prav s sprejetjem svoje kvote priseljencev se je Slovenija politično in tudi „moralno“ kvalificirala za nastajajočo EU prve hitrosti, še bolj kot s svojimi gospodarskimi in drugimi kazalci družbenega razvoja. Če je EU nastala kot zveza utemeljena na skupnih vrednotah in gospodarskih potrebah, se bo notranja delitev EU, če bo kdaj do nje prišlo, utemeljila na dveh zelo pragmatičnih kriterijih.

Prvi bo kriterij sposobnosti, zlasti sposobnosti učinkovitega delovanja v okvirih novih naprednih sodelovanj, od enotnejših financ in davkov, pa tja do prispevka k skupni in seveda večji varnosti šengenskih meja. **Drugi pa bo kriterij volje**, torej politične pripravljenosti in nenazadnje tudi družbene zrelosti držav, da sodelujejo v krogu najboljših. Če želimo biti z najboljšimi moramo tako tudi delovati. Če kdo vidi Slovenijo v „drugi ligi“ EU, skupaj z vzhodnimi članicami, pa naj to jasno pove in utemelji. V Sloveniji imamo za zdaj oboje, sposobnost in voljo. In pri tem naj tudi ostane. ■





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*



TVEGANJA RADIKALIZACIJE ZAPOSLENIH V ORGANIZACIJAH KRITIČNE INFRASTRUKTURE

Podrobna analiza dejavnikov tveganja, katerim so izpostavljene demokratične družbe v Evropi, zelo hitro prinese ugotovitev, da grožnje niso povezane samo z zunanjimi dejavniki, temveč, da tiste zelo izpostavljene, najdemo ravno znotraj teh družbenih skupnosti.

Uvod

Že bežna analiza terorističnih dejanj storjenih v zadnjih 15 letih v Evropi kaže, da so bila v večini storjena s strani državljanov posameznih evropskih držav, ki so se na podlagi njihovih političnih, verskih in drugih stališč radikalizirali do te mere, da so bili pripravljeni svoja stališča uveljavljati s storitvijo terorističnih dejanj. Poleg žrtev, ki so vsekakor tragičen produkt teh procesov, je zahodne demokratične družbe predvsem pretreslo spoznanje, da so sociološko te družbe ostale brez ustreznih odgovorov, kako je možno, da se posamezniki v teh okoljih radikalizirajo do te mere, da so pripravljeni za ceno lastnih življenj uveljavljati ta prepričanja na škodo sodržavljanov. Sociološki procesi v demokratičnih družbah, ki se vedno bolj odražajo skozi marginalizacijo določenih družbenih skupin, vedno močnejše razslojevanje, v nekaterih primerih tudi segregacijo, potrošništvo, kot vrednoto, ki je izpodrinila vse ostale vrednote in odtujila posameznike te skupnosti, so samo nekateri negativni dejavniki, kateri imajo neposreden vpliv na ugodno okolje za radikalizacijo. Ko v okvir razprav dodamo še procese informatizacije in digitalizacije družbe, lahko z gotovostjo trdimo, da je delovanje družbe poleg ostalih problemov postalo močno odvisno od novih tehnoloških rešitev. Le te na eni strani omogočajo virtualnost medčloveških odnosov, ki poteka na podlagi interneta in vseh delujočih socialnih omrežij. To pa so ene od tistih poti, ki omogočajo izvajanje procesov radikalizacije skupin in tudi posameznikov.

Trendi, ki smo jim priča v zapletenem varnostnem okolju, kažejo na to, da zaposleni v organizacijah postajajo eden od ključnih dejavnikov za uspešnost organizacij, pa naj si gre to za javno ali zasebno gospodarsko okolje. Na drugi strani pa zaposleni postajajo tudi pomemben dejavnik tveganja.

Vloga zaposlenih v organizaciji

Trendi, ki smo jim priča v zapletenem varnostnem okolju, kažejo na to, da zaposleni v organizacijah postajajo eden od ključnih dejavnikov za uspešnost organizacij, pa naj si gre to za javno ali zasebno gospodarsko okolje. Na drugi strani pa zaposleni postajajo tudi pomemben dejavnik tveganja. Ta ugotovitev je še posebej pomembna, ko govorimo o zaposlenih, ki delujejo na pomembnih segmentih znotraj organizacij, katere upravljajo kritično infrastrukturo. Radikalizacija takih posameznikov, ki bi bili pripravljeni za dosego svojih ciljev izvesti teroristični napad in s tem onemogočiti delovanje kritične infrastrukture, bi imelo za določen del družbene skupnosti lahko katastrofalne posledice. Te posledice pa se ne bi odražale samo v obliki človeških žrtev, temveč bi imele vpliv

*avtor je član Slovenskega združenja korporativne varnosti

tudi na različne procese v družbi, ki bi bile zaradi nedelovanja dotične kritično infrastrukturne zmogljivosti prekinjene. Psihološki moment takega dejanja bi bil še močneje izražen.

Sistemski ukrepi obvladovanja tveganj

Ravno pri strateškem managementu se varnostno zavedanje o pomenu korporativne varnosti in varnosti nasploh, počasi dviguje in prihaja v ospredje. Vendar se vse prevečkrat dogaja, da strokovno znanje in sposobnost korporativno varnostnega managementa v organizacijah, ni na ustreznem nivoju, da bi izkoristil ta »zvezdniški trenutek« in se v določenih situacijah izkazal kot učinkovit mehanizem za ustrezno obvladovanje tveganj. Ta lažna zazibanost in samozadovoljnost je v svetu takih dinamičnih sprememb, kakršne se vsakodnevno dogajajo, praktično obsojena na takojšen neuspeh. Zaradi navedenega je potrebno, bolj kot kadarkoli do zdaj, vlagati v stalno izobraževanje in dograjevanje svojih znanj ter veščin.

Seveda v okviru procesov korporativne varnosti, ki jih izvaja organizacija, lahko opredelimo naslednje splošne aktivnosti za preprečevanje tveganj, ki zmanjšujejo možnost groženj v organizaciji:

- Sprejemanje in uveljavljanje varnostnih politik in nadzornih mehanizmov;
- Zagotavljanje, da so ključne informacije, procesi in sredstva ustrezno zavarovana;
- Stalno spremljanje informacijskega omrežja in spremljanje sumljivih aktivnosti, ki odstopajo od normalnih procesov;
- Zagotavljanje, da ima korporativna varnost na voljo ustrezna sredstva in vire, ki omogočajo ustrezno izvajanje varnostnih procesov (vključno s procesi informacijske varnosti);
- Usklajevanje s pravnimi strokovnjaki in zagotavljanje skladnega delovanja vseh ključnih procesov v organizaciji.

V organizacijah, ki upravljajo kritično infrastrukturo pa lahko dodatno opredelimo še procese, ki so vezani na zaposlene:

- Izvajanje ustreznih postopkov preverjanja ob novih zaposlitvah oseb na ključnih delovnih mestih;
- Usposabljanje zaposlenih za izvajanje aktivnosti predpisane v varnostnih protokolih za različne deviantne situacije;
- Vzpodbujanje zaposlenih, da po določenih poteh prijavljajo nezaželena in odklonska ravnanja v organizacijskem okolju, kjer delujejo;
- Ustrezni organi, vključno s predstavniki korporativne varnosti, morajo imeti znanje o indikatorjih, ki nakazujejo vedenja, katera pri posameznikih kažejo na radikalistično oz. odklonsko vedenje;
- Dokumentiranje in ocenjevanje vseh incidentov v organizaciji, ki so povezani z nenavadnim ali nasilnim obnašanjem, ki kaže indikatorje nevarnosti radikalizacije;
- Stalno usklajevanje s pravnimi strokovnjaki in strokovnjaki na področju zagotavljanja javne varnosti, da se zagotavlja skladnost delovanja s potrebnimi zakonskimi predpisi.

Seveda je v modernem dinamičnem poslovnem okolju v organizacijah, pri zaposlenih, izredno težko zagotoviti ponotranjenje varnostnih vrednot posameznega organizacijskega okolja. Varnostna kultura je proces, ki se ustvarja na daljši rok in ga ni možno zagotoviti s trenutnimi in kratkoročnimi ukrepi. Danes je predvsem višina dohodkov tista vrednota, ki pri mladih prevladuje pred stalnostjo zaposlitve oz. varnostjo delovnega okolja. Če v to dodamo še procese, ki jih Evropa uveljavlja skozi procese prostega pretoka blaga, storitev, financ in delovne sile, potem lahko vidimo, da je zagotavljanje varnostnih procesov v organizacijah zelo kompleksno in zahtevno delo. Ravno radikalizacija posameznikov je tisti proces,





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.

ki zahteva izredno temeljito poznavanje posameznikov, zaposlenih v organizaciji, na ključnih delovnih mestih, ki so sami po sebi kritični zaradi vpliva, ki ga ima tak zaposleni na neprekinjenost delovanja kritične infrastrukture. Ob tem spremljanju zaposlenih je potrebno seveda paziti, da ukrepi ne posegajo v človekovo zasebnost in ustavno zagotovljene pravice in v ta del posegajo samo v tistih delih, ki so zakonsko dopustni in upravičeni zaradi potreb, ki jih ima delovno mesto na katerem deluje taka oseba.

Na drugi strani se je potrebno zavedati, da se proces radikalizacije posameznikov skrajšuje, kar pomeni še dodatno nevarnost oz. težavo pri pravočasnem zaznavanju tega deviantnega procesa. Na to dinamiko vplivajo različni dejavniki od interneta, samoradikalizacije, močnejšega nadzora obveščevalnih in varnostnih služb nad posameznimi centri, kjer se vrši domnevna radikalizacija in ostali procesi v družbi, kjer so pripadniki vedno bolj odtujeni eden od drugega.

Čeprav je radikalizaciji v zadnjem obdobju namenjene precej pozornosti, je le ta usmerjena bolj na radikalizirane posameznike, ki se vračajo iz bojišč v tujini nazaj v Evropo, radikalizaciji v šolah, zaporih, verskih skupnostih, manj pa je ta radikalizacija proučevana znotraj delovnih okolij, še posebej tistih v katerih upravljajo kritično infrastrukturo.

Za učinkovitost procesov zagotavljanja varnosti pa ni dovolj samo učinkovitost delovanja korporativne varnosti znotraj teh organizacij. Nujno je dobro sodelovanje z javnimi institucijami, ki skrbijo za javno varnost, kot so policija ali druge obveščevalno-varnostne službe. Ta proces je eden izmed ključnih dejavnikov učinkovitega in dobro delujočega javno-zasebnega partnerstva pri zaščiti kritične infrastrukture. Ta dejavnik je še posebej izpostavljen zaradi dejstva, da velika večina organizacij, ki upravlja določeno kritično infrastrukturo, prehaja v upravljanje zasebnega kapitala.

Naslednji pomemben dejavnik, ki je tudi bistven pri upoštevanju obvladovanja tveganj, pa je outsorcing, ki ga organizacije, katere obvladujejo kritično infrastrukturo, najemajo na trgu. Glede na dejstvo, da se organizacije vedno bolj poslužujejo zunanjih izvajalcev, pri zagotavljanju tistih procesov v organizacijah, ki imajo lahko določeno mero kritičnosti, se je potrebno zavedati problema, ki ga lahko prinese ta proces v razmerju do nevarnosti radikalizacije.

Vendar, če ocenimo možnost, da se neposredno spremlja aktivnosti zaposlenih na ključnih delovnih mestih v kritični infrastrukturi, ko so enkrat zaposleni in bi lahko bili podvrženi procesu radikalizacije, hitro ugotovimo, da ni ustreznih sistemskih in zakonskih okvirov, kateri bi dajali jasne podlage za izvajanje določenih aktivnosti. Tudi evropska platforma Radicalization Awareness Network (RAN NET) v svojem okviru trenutno ne predvideva skupine, ki bi se konkretno ukvarjala s procesi radikalizacije zaposlenih v organizacijskih okoljih, še posebej tistih, kjer upravljajo s kritično infrastrukturo.[1] Aktivnosti so prepuščene subjektom korporativne varnosti v organizacijah, ki lahko izvajajo preventivne ukrepe spremljanja in ozaveščanja zaposlenih v teh organizacijah. Verjetno se je za strinjati z ugotovitvijo, da so sami zaposleni v organizaciji najboljši senzorji za spremljanje in pojavljanje deviantnih pojavov s strani posameznikov v teh organizacijah. Vendar se je potrebno zavedati, da je za vzpostavitev takega stanja varnostne kulture v teh kolektivih potrebno izvajati načrtne ukrepe in, da je to stanje, ki ga je možno doseči na daljši časovni rok.

Ravno na področju radikalizacije je nujno dobro sodelovanje med predstavniki korporativne varnosti in predstavniki nacionalnih varnostnih institucij. Kot primer dobre prakse velja v Republiki Sloveniji izpostaviti Slovensko združenje korporativne varnosti, ki deluje v okviru Instituta za korporativne varnostne študije[2]. Omenjeno združenje vključuje večino organizacij, ki v Republiki Sloveniji upravljajo kritično infrastrukturo. Znotraj omenjenega združenja, pa so zelo aktivne tudi določene javne institucije, kot na primer SI-CERT, Urad informacijskega pooblaščenca, Urad za varovanje tajnih podatkov in Gasilska zveza Slovenije. Zelo tesno z združenjem sodeluje tudi Policija in Ministrstvo za obrambo. Ta platforma združevanja in izmenjave dobrih praks in izkušenj se je v neposredni izvedbi določenih aktivnosti na področju dvigovanja kvalitete zaščite kritične infrastrukture pokazala, kot izredno učinkovita.

Zaključek

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. Če v ta okvir dodamo še nevarnosti, ki jih prinašajo procesi radikalizacije, potem lahko ugotovimo, da bo tem ukrepom v prihodnje potrebno nameniti večjo pozornost.

[1] Več o RAN NET dostopno na https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran_en.

[2] Več o Slovenskem združenju za korporativno varnost dostopno na http://www.ics-institut.com/members/corporative-security-association. ■





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 ISO 9001:2000

www.dahuasecurity.com

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

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



IZZIVI SLOVENSKEGA ZASEBNEGA VAROVANJA

Do sedaj je veljalo prepričanje, da je sprememba edina stalnica. V vse hitreje razvijajoči se družbi, ki postaja vse bolj digitalizirana in robotizirana, pa lahko že razvijamo novo prepričanje, ki gre v smeri, da postaja naša stalnica predvidevanje in razumevanje prihajajočih sprememb. Če bomo torej želeli biti v toku dogajanj in biti del sprememb, bomo morali biti sposobni zaznavati prihajajoče potrebe in razvojne usmeritve družbe tako na lokalnem, še bolj pa globalnem nivoju in jih biti sposobni tudi razumeti.

Za zasebno varovanje je tovrstno delovanje in zavedanje še toliko bolj pomembno, saj je učinkovitost ukrepov varovanja usodno odvisna od pravočasnosti in pravilnosti zaznav o prihajajočih spremembah v okolju, ki imajo lahko za posledico tudi spremenjene varnostne okoliščine in s tem povezane potrebe. Učinkovitost zasebnega varovanja torej temelji na predvidevanju, napovedovanju in zaznavanju bodočih razmer in potreb ter prilagajanju in ustreznemu ukrepanju glede na nastale spremembe v družbi in v okolju. Gre torej za specifično dejavnost, kjer sta vizionarstvo in sposobnost zaznavanja sprememb v prihodnosti ključnega pomena za uspešnost delovanja in razvoja dejavnosti. Kljub vse večji digitalizaciji in robotizaciji pa v dejavnosti zasebnega varovanja človek s svojimi individualnimi potrebami, čustvi in sposobnostmi še vedno predstavlja enega ključnih dejavnikov. Pa naj si bo to človek v funkciji varnostnika, interventa, prevoznika denarja, varnostnega tehnika ali pa načrtovalca varnostnih sistemov in rešitev.

Na področju zaposlovanja bi bilo med drugim potrebno omogočiti izvajanje storitev z varnostnim osebjem, ki ob izpolnjevanju vseh zakonskih zahtev, ni nujno v rednem delovnem razmerju pri imetniku licence, ampak lahko izvaja naloge varovanja tudi na kakšni drugi pogodbeni podlagi (pogodba o delu, študentska napotnica ipd.).

V kateri točki se nahaja zasebno varovanje

Zasebno varovanje je do pred kratkim bolj ali manj uspešno sledilo spreminjajočim se družbenim razmeram in potrebam ter družbenemu in tehnološkemu razvoju. V zadnjem času pa opažam, da je razkorak med potrebami in razvojem na eni strani in sposobnostjo prilagajanja zasebnega varovanja le-tem na drugi strani, vse večji. Kaže se na različnih področjih, med katerimi predvsem prevladuje prepočasi se razvijajoče zakonodajno področje (zasebno varovanje, javna zbiranja, delovna zakonodaja ipd.), ki v nekaterih segmentih celo zavira razvoj stroke in uvajanje sodobnih tehnoloških, organizacijskih in drugih rešitev, kadrovsko področje, ki v obdobju konjunkture predstavlja še posebej velik problem, področje plač, ki zaradi neustreznega vrednotenja učinkov zasebnega varovanja ne zagotavlja ustreznega plačila in nagrajevanja varnostnega osebja, področje standardizacije, ki bi lahko bolj sistemsko uredilo razmere na trgu ter področje javnega naročanja, ki žal še vedno favorizira ceno pred ostalimi (ekonomskimi, kakovostnimi, razvojnimi ipd.) merili za izbor ponudnikov. Slovenija se je z vključevanjem in aktivnim delovanjem v evropskih in svetovnih integracijah resno lotila celostne prenove in posodobitve na vseh področjih. Naj še posebej izpostavim področje varnosti osebnih podatkov in zaščite kritične infrastrukture, kot trenutno najbolj aktualnih področij, ki so neločljivo povezana

*avtor je član Slovenskega združenja korporativne varnosti

tudi z zasebnim varovanjem. Dejstvo je, da vse našteto postavlja zasebno varovanje pred veliko preizkušnjo, ki zahteva hitro ukrepanje in vizionarsko naravnanost pri uvajanju nujnih sprememb.

Kateri so ključni izzivi

Zakonodajno področje
Nujna je posodobitev obstoječe zakonodaje na področju zasebnega varovanja, ki bo omogočala večjo fleksibilnost in uvajanje novih tehnologij v procese varovanja. Na področju zaposlovanja bi bilo med drugim potrebno omogočiti izvajanje storitev z varnostnim osebjem, ki ob izpolnjevanju vseh zakonskih zahtev, ni nujno v rednem delovnem razmerju pri imetniku licence, ampak lahko izvaja naloge varovanja tudi na kakšni drugi pogodbeni podlagi (pogodba o delu, študentska napotnica ipd.). V zasebnem varovanju precejšen delež v strukturi naročil predstavljajo izredna naročila in sezonska povečanja naročil, ki bi jih podjetja ob uvedbi omenjenih sprememb lažje in učinkoviteje obvladovala. Še posebej bi bile koristi vidne v času konjunkture, ko je odliv kadra iz dejavnosti še posebej velik. Na področju varovanja javnih zbiranj bi bilo smiselno razmisliti o novi vlogi in pooblastilih rediteljev, ki bi ob vzpostavitvi ustreznega sistema izobraževanja (morebiti tudi uvedbi novega NPK za reditelja) in registriranja lahko bistveno pripomogli k lažji izvedbi varovanja javnih zbiranj, še posebej tistih z nižjimi stopnjami tveganj. Na področju prevozov denarja še vedno obstaja veliko sivih polj. Ne eni strani oboroženi varnostniki v varnostnih vsebnikih prenašajo po nekaj sto evrov, na drugi strani pa trgovke, prevozniki hitre pošte ali kakšni drugi izvajalci za tretje osebe prenašajo večje vsote gotovine in pri tem ne upoštevajo niti najmanjših varnostnih ukrepov. Pomembno besedo pri iskanju rešitev bi lahko imele tudi zavarovalnice, ki bi z zaostritvijo zavarovalnih pogojev lahko bistveno pripomogle k zmanjšanju omenjenih razlik. Še posebej okostenela se mi zdi ureditev področja upravljanja z varnostno nadzornimi centri. Nove rešitve na področju informacijskih tehnologij omogočajo bistveno bolj učinkovito upravljanje z alarmnimi in drugimi stanji. Posebej pomembna pri tem je hitrost prenosa podatkov ter ustreznost alarmiranja in obveščanja pristojnih služb. S sodobnejšimi rešitvami, ki bi bile zakonsko dovoljene, bi se lahko v procesu alarmiranja in obveščanja prihranilo tudi do nekaj minut, kar je lahko ključnega pomena pri obvladovanju izrednih dogodkov in zmanjševanju posledic le-teh.

Vrednotenje dela
Namenoma sem napisal vrednotenje dela. Ne gre le za vzpostavitev plačnega sistema, ki bi omogočal višja plačila in nagrajevanje dela varnostnega osebja tudi po učinku. Gre za celoten proces prenove vrednotenja dejavnosti kot take, ki z ustreznostjo ponujenih rešitev in proaktivno vlogo dokazano podjetjem zmanjšuje tveganja in verjetnost nastanka škodnih dogodkov, s tem pa podjetjem povečuje dobiček. Del le-tega bi lahko podjetja namenila nagrajevanju dela varnostnega osebja po sistemu, večja učinkovitost - višje nagrajevanje dela. Vsekakor dejavnost, v kateri nagrajevanje dela temelji na minimalni plači, na dolgi rok ne more biti privlačna za visoko motivirane in najboljše kadre in je obsojena na životarjenje in stagniranje.

Javna naročila
V zadnjem času se veliko naporov namenja iskanju novih rešitev na področju javnega naročanja storitev zasebnega varovanja. Nujno je potrebno presekati stanje, v katerem je cena še vedno najpomembnejši faktor nakupnega odločanja zavezancev za javna naročila. Vsekakor obstaja veliko drugih meril, s katerimi lahko naročnik vzpostavi uspešen model ocenjevanja ponudb, ki omogoča izbor ponudnikov na podlagi ekonomsko najboljše in ne cenovno najugodnejše ponudbe. Pri tovrstnem modelu ocenjevanja ponudb se pojavljajo določena tveganja povezana z nejasnostjo določenih meril (v praksi je kar nekaj takih primerov), ki ne omogočajo jasne primerljivosti ponudnikov in transparentnosti ponudb, zato je pri določanju meril torej nujno potrebno slediti temeljnim načelom javnega naročanja, ki zagotavljajo konkurenčnost in enakopravnost ponudnikov. Zakonodajo o javnem naročanju je nujno potrebno spremeniti tudi v delu, ki določa usklajevanje cen z rastjo cen življenjskih potrebščin, še posebej pa v primerih sprememb izplačila plač in dviga minimalne plače. V teh primerih je potrebno vzpostaviti instrument avtomatske uskladitve cen takoj





po nastanku spremembe, v nasprotnem primeru je lahko že ob minimalnih spremembah ogroženo poslovanje zasebnih varnostnih podjetij, posledično pa so ogrožena tudi delovna mesta.

Kritična infrastruktura

Pred kratkim je bil sprejet Zakon o kritični infrastrukturi, katerega namen je sistemsko urediti zagotavljanje neprekinjenega delovanja kritične infrastrukture Republike Slovenije. V tem procesu ima zasebno varovanje pomembno vlogo, saj s svojimi rešitvami upravljavcem kritične infrastrukture pomaga pri obvladovanju varnostnih tveganj praktično na vseh področjih varovanja in nivojih upravljanja. Iz tega vidika bi bilo smiselno določiti posebne pogoje, ki jih morajo izpolnjevati izvajalci zasebnega varovanja, ki so angažirani v procesih varovanja kritične infrastrukture, s tem pa jim omogočiti poseben status, ki jim omogoča neprekinjeno in učinkovito izvajanje nalog varovanja tudi ob izrednih dogodkih in v morebitni krizi. Tu predvsem mislim na ustrezno umestitev službe varovanja v proces varovanja upravljavca kritične infrastrukture in zagotovitev ustreznega financiranja službe varovanja.

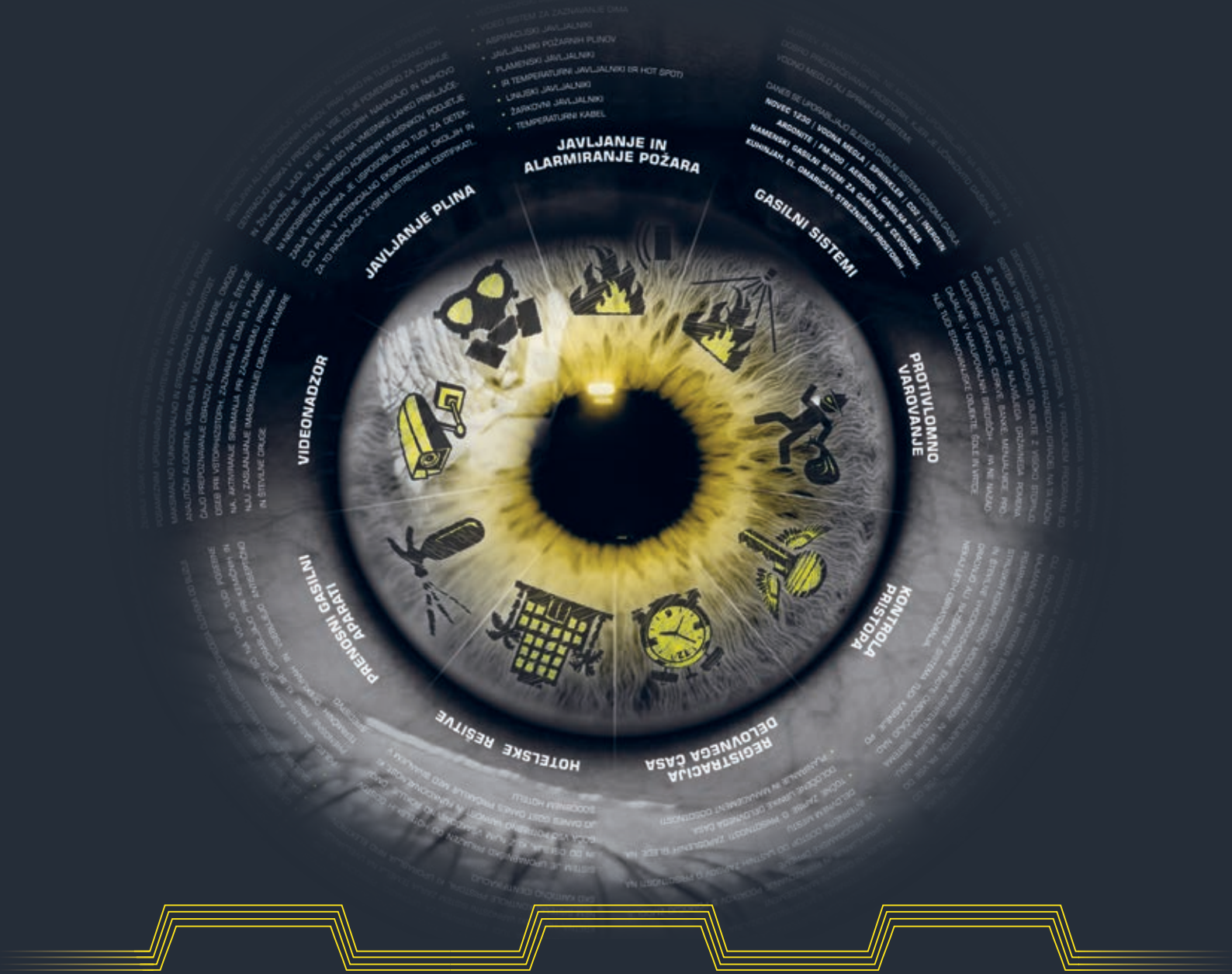
S sodobnejšimi rešitvami, ki bi bile zakonsko dovoljene, bi se lahko v procesu alarmiranja in obveščanja prihranilo tudi do nekaj minut, kar je lahko ključnega pomena pri obvladovanju izrednih dogodkov in zmanjševanju posledic le-teh.

Pristojnosti nad zasebnim varovanjem

V zadnjem času so vse glasnejši pomisleki o ustreznosti umestitve zasebnega varovanja. Glede na to, da gre po eni strani za zagotavljanje javnega reda in reda na varovanem območju, po drugi strani pa za pridobitno gospodarsko dejavnost, se upravičeno zastavlja vprašanje ustreznosti umestitve zasebnega varovanja v nacionalno varnostni sistem države. Je ustrezna obstoječa zakonska rešitev, ki Ministrstvo za notranje zadeve določa za izvajanje vseh upravnih nalog na področju zasebnega varovanja? Naj navedem primer področja požarnega, kjer je določeno, da to področje spada pod pristojnost Ministrstva za obrambo. Morebiti bi bilo smiselno razmisliti tudi o tem, da upravne naloge iz gospodarskega področja prevzame kako drugo ministrstvo.

Zaključna misel

Upam, da sem s svojimi razmišljanji uspel v vas prebuditi razmišljanje o potrebnosti sprememb v zasebnem varovanju. Verjamem, da dejavnost premore dovolj strokovnega znanja in pozitivne energije za uvajanje nujnih sprememb, ki bodo vsem deležnikom zagotovile boljšo in varnejšo prihodnost in lepši jutri. ■



Varno v nov dan

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

www.zarja.com

ZARJA ELEKTRONIKA



Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



REPORTAŽA:
Mednarodna konferenca »Dnevi korporativne varnosti 2018«

PODELITEV NAGRAD »SLOVENIAN GRAND SECURITY AWARD 2018«

9. mednarodna konferenca »Dnevi korporativne varnosti 2018« je privabila več kot 250 udeležencev iz celotne regije JV Evrope. V okviru otvoritvene slovesnosti je potekala podelitev nagrad »Slovenian Grand Security Award 2018« za dosežke na področju varnosti v preteklem letu.

Institut za korporativne varnostne študije (ICS) je ob so-organizaciji Slovenskega združenja korporativne varnosti in SE European Corporate Security Association (SECSA) v mesecu marcu organiziral tradicionalno mednarodno konferenco z nazivom »**Dnevi korporativne varnosti**«. Dogodek je utrdil sloves najpomembnejšega dogodka s področja korporativne varnosti v celotni regiji, ki je združil vidne predstavnike gospodarstva, politike in stroke. To dokazuje več dejavnikov, od pomembnih gostov gospodarskega in javnega življenja na sami otvoritveni slovesnosti, število zadovoljnih udeležencev, ki je letos preseglo številko 250, cel niz odmevnih tem, ki so nam jih predstavili vrhunski predavatelji iz Slovenije in tujine in nenazadnje prikaz celega niza najnovejših tehnoloških rešitev, katere so na konferenci predstavljali različni razstavljavci.

Konferenco so s svojimi svečanimi nagovori odprli izr. prof. **dr. Denis Čaleta**, predsednik organizacijskega odbora, **g. Alojz Kovšca**, predsednik Državnega sveta Republike Slovenije, **mag. Miloš Bizjak**, državni sekretar ministrstva za obrambo, **mag. Sonja Šmuc**, generalna direktorica GZS







*avtor je član Slovenskega združenja korporativne varnosti







in **g. Boštjan Šefic**, državni sekretar Ministrstva za notranje zadeve. Vsi so v svojih nagovorih poudarili zahtevnost varnostnega okolja, ki nas obdaja in pred naše organizacije postavlja kompleksne zahteve za obvladovanje tveganj, katerim smo izpostavljeni. Varnost je postala dobrina, katera je v trenutnih razmerah izredno izpostavljena. Posebej je bilo poudarjeno, da korporativna varnost postaja pomemben **proces na čelu novega razvoja slovenskega gospodarstva**. Omenjeni dogodek pa predstavlja odlično priložnost za izmenjavo izkušenj, dobrih praks in predvsem najnovejših spoznanj kako učinkovito obvladovati tveganja, katerim so izpostavljene naše organizacijske sredine. Institut za korporativne varnostne študije s svojim aktivnim delovanjem predstavlja tisti prostor, kjer zelo aktivno sodelujejo organizacije in podjetja gospodarskega in javnega okolja ter s tem krepijo učinkovitost svojega delovanja na področju obvladovanja tveganj.

Na otvoritvi mednarodne konference je potekala tudi podelitev »**Slovenian Grand Security Award 2018**« za dosežke na področju varnosti v preteklem letu. Slovenska velika nagrada varnosti je prestižna nagrada s področja varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje Institut za korporativne varnostne študije, ICS-Ljubljana, v sodelovanju s Slovenskim združenjem korporativne varnosti.

Nagrada je namenjena procesom dvigovanja splošnega zavedanja in varnostne kulture v širši družbeni skupnosti, ki vsebuje poslovna in druga okolja. V šestih kategorijah neodvisna komisija izbira tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev.

Nagrado za »**Najboljšega korporativno varnostnega managerja**« je letos prejel **g. Stanislav Veniger** iz podjetja Zavarovalnica Triglav d.d., ki mu jo je podelil dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti. Nagrado za **»Najbolj varno podjetje«** je tokrat prejelo podjetje **CETIS d.d.** Predsednik upravnega odbora g. Marko Mohar je prejel priznanje iz rok mag. Sonje Šmuc, generalne direktorice GZS.

Nagrado za **»Najbolj varno mesto«** je prejela **Mestna občina Nova Gorica**. Župan g. Matej Arčon je prejel nagrado s strani g. Alojza Kovšce, predsednika Državnega sveta Republike Slovenije. Gospod Boštjan Šefic je predal nagrado mag. Jasni Gabrič, Županji **Občine Trbovlje** v kategoriji **»Najbolj varna občina«**.













Tokrat je nagrado za **»Najbolj inovativno varnostno rešitev«** prejelo podjetje **Špica International d.o.o**. Nagrado je prevzel direktor podjetja g. Tone Stanovnik, ki mu jo je predal g. Andrej Slapar, predsednik uprave Zavarovalnice Triglav. Nagrada v kategoriji **»Najboljša knjiga s področja varnosti«** je bila letos podeljena **g. Boštjanu Videmšku**. Zaradi njegove odsotnosti je nagrado prevzel odgovorni urednik zunanje politične redakcije g. Veso Stojanov, ki mu jo je predal mag. Miloš Bizjak, državni sekretar ministrstva za obrambo. **Časnik DELO** je letos prepričal neodvisno komisijo in prejel nagrado v kategoriji **»Najbolj inovativna medijska podpora«**. Nagrado je prevzel g. Miha Jenko, eden od prvih peres omenjenega časnika, ki mu jo je predal mag. Aleksander Mervar, direktor podjetja ELES. Poleg podelitve nagrad v omenjenih kategorijah, pa je bila letos podeljena tudi posebna **nagrada za življenjsko delo** na področju korporativne varnosti, ki jo je iz rok mag. Mirana Vršca, soustanovitelja Instituta za korporativne varnostne študije, prejel **g. Dušan Dular** iz podjetja Krka d.d..

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

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

Po slovesnem delu je otvoritveno predavanje tokrat izvedel prof. dr. Ernest Petrič, svetovalec predsednika Republike in bivši predsednik Ustavnega sodišča Republike Slovenije in je bilo namenjeno predstavitvi »Pogled na izzive bodočega mednarodnega varnostnega okolja«. Konferenca se je nadaljevala s predavanji odličnih mednarodnih strokovnjakov. Naj omenimo nekatere - g. Aleksandar Rajčević (Risk & Compliance Manager South East Europe - IKEA South East Europe), g. Andrej Podvršič (Generalni Direktor korporativne varnosti v korporaciji Chemours Company, G. Faiz Djellouli, (Head of CITI Cybersecurity,ENGIE, France), g. Luigi REBUFFI (Secretary General, European Cyber Security Organisation - ECSO), g. Stefano Bracco (Security Officer at ACER - Agency fort the Cooperation of Energy Regulators)... Za tem se je zvrstilo še vrsto zanimivih predstavitev praktičnih izkušenj









in novih tehnoloških rešitev na področju korporativne in informacijske varnosti.

Posebej velja izpostaviti še dve okrogli mizi, ki sta obravnavali zadnjo aktualno tematiko povezano z uveljavljanjem nove zakonodaje na področju zaščite kritične infrastrukture in seveda Evropske uredbe o varstvu osebnih podatkov (GDPR). Naslov prve okrogle mize je bil »Zaščita kritične infrastrukture-razkorak med realnostjo varnostnega okolja in novimi zakonskimi rešitvami v Republiki Sloveniji«. Druga pa je bila poimenovana in posvečena »Izkušnjam in izzivom pooblaščene osebe za varstvo osebnih podatkov pred uvedbo GDPR – Kako izbrati pravega DPO (Data Protection Officer-ja)?« Že sama aktivna razprava je pokazala, da so bile teme izredno aktualne. V razpravo so se poleg vabljenih gostov na okroglih mizah izredno aktivno vključili tudi udeleženci konference, kar daje dogodku še posebno vsebinsko težo. Izmenjava dobrih praks in izkušenj je namreč tisto, kar vsebinsko bogati ta dogodek. Skozi razpravo med strokovnjaki je bilo tudi zaznati posamezne nove trende na področju celovitega zagotavljanja korporativne varnosti.

Izziv, ki je bil postavljen na sami konferenci »Korporativna varnost na čelu gospodarskega razvoja« je bil skozi odlične razprave in okrogle mize povsem opravičen. Postavljeni so bili trdni strokovni temelji, ki jih bodo strokovnjaki s tega področja uveljavljali v neposrednih poslovnih okoljih. Skozi razpravo med strokovnjaki je bilo zaznati posamezne nove trende na področju celovitega zagotavljanja korporativne varnosti. Kako pomemben postaja proces obvladovanja tveganj kaže tudi podatek o udeleženosti predstavnikov strateškega managementa skozi celoten program konference Dnevi korporativne varnosti 2018.

Cel niz dogodkov, skozi dvodnevni program, je tudi tokrat omogočil tkanje novih strokovnih poznanstev, izmenjavo novih izkušenj in seveda strokovne afirmacije posameznih strokovnjakov ter ponudnikov varnostnih rešitev. Letošnja rdeča nit je bila vsekakor povezana z informacijsko varnostjo, risk managementom, kibernetsko varnostjo, zaščito kritične infrastrukture, uveljavitvijo GDPR in številnimi aktualnimi temami.

Za konec velja še vabilo vsem, ki ste pripravljeni vlagati v svoje znanje in potrebujete rešitve za celovito obvladovanje varnostnih tveganj na jubilejne 10. Dneve korporativne varnosti, ki bodo v ustaljenem terminu v marcu 2019. ■

10. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 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 INŠTITUTA WWW.ICS-INSTITUT.SI!

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



ALI LAHKO NEKAJ, KAR NAS NA PREPROSTEJŠI NAČIN POVEZUJE, PREDSTAVLJA NOVA TVEGANJA?

Danes živimo v dobi, ko nam brezžična omrežja predstavljajo del našega vsakdana, in prav vsa brezžična omrežja so ranljiva in izpostavljena hekerskim napadom.

Brezžična omrežja nas obdajajo na vsakem koraku, a še vedno ostajajo ena največjih skrbi, kar se tiče varnosti organizacije pri postavljanju takega omrežja.

Problemi omrežja se delijo na tri kategorije: **dostopnost, zaupnost in integriteta**.

Dostopnost predstavlja ali je omrežje dostopno uporabnikom, kadar mora biti. Z uporabo motilcev signala bi lahko nekdo motil prenose podatkov znotraj omrežja, kar bi rezultiralo nedostopnost omrežja. Zadnja leta so vedno bolj popularni napadi s konstantnim pošiljanjem signalov napravi, le ti so energijsko potratni, kar privede do hitrejše spraznitve baterije in onemogočanja dostopnosti naprave.

Zaupnost je, ko so informacije poslane skozi mrežo na način, da ga lahko berejo samo ciljani prejemniki. To se najlažje doseže s šifriranjem samih podatkov med prenosom.

Integriteta pomeni, da podatki prispejo do prejemnika nedotaknjeni ali modificirani, ker gre prenos podatkov po zraku, so lahko le ti prestreženi in modificirani na precej preprost način. To pomeni, da so brezžična omrežja, kar se tiče integritete samih podatkov med prenosom bolj ranljiva kot žična omrežja.

V sklopu vsake organizacije se pojavljajo varnostna vprašanja povezana s temi dejavniki. Kje so določena tveganja dopustna ter s kakšnim namenom. Velikokrat se išče kompromis med varnostjo in finančnim vložkom, vendar gre pri tovrstni zaščiti bolj za ozaveščenost in zmožnost pravilnega in varnega konfiguriranja.

Nekatere dostopne točke celo, kot privzeto, uporabljajo nezavarovano dostopno točko, kar pomeni, da ima vsakdo lahko dostop do podatkov, ki se nezaščiteno prosto pretakajo po zraku. Predstavljajte si, kot, da bi morali živeti v hiši, sredi nevarne soseske, kjer so vrata stalno odklenjena in vsa okna odprta.

Brezžična omrežja predstavljajo vez med svetom in uporabniki ne glede na njihove omejitve, kar se tiče razdalje in pokritosti. Pojavljajo se povsod in vsi so nanj povezani. Seveda se tukaj pojavi težava, ko se ves promet steka skozi en usmernik, kar lahko izpostavi ranljivostim vse naprave, ki so povezane na dotično omrežje.

Prisotnih je več razlogov zaradi katerih so brezžična omrežja izpostavljena takšnim grožnjam. Eden izmed njih je, ker izmenjava podatkov poteka med dostopno točko in napravo preko zračnih radijskih valov, kateri so izpostavljeni vsakomur in prav tako izpostavlja naprave, katere delujejo v nekem omrežju in so ranljive za napade. Brezžična omrežja so ranljiva na več načinov in sicer preko neavtorizirane dostopne točke (ang. Rogue access point), slabo nastavljenimi varnostnimi parametri, z napadom, ki povzroči storitev nedostopno (ang. DoS – Denial of Service) in še mnogimi drugimi.

Neavtorizirana dostopna točka je lahko definirana kot odprto omrežje za nekoga, ki dejansko ne bi smel imeti dostopa

*avtor je član Slovenskega združenja korporativne varnosti



do njega. Je dostopna točka, katera je bila nameščena v omrežje brez eksplicitne avtorizacije lastnika oz. administratorja omrežja. Ustvarjena je lahko z namenom dobronamernega povezovanja ostalih brezžičnih naprav v to omrežje (npr. mobilni telefoni ali tablice) lahko pa tudi z namenom kasnejših hekerskih napadov. Tudi, če ta točka ni bila ustvarjena za zle namene, je lahko zlorabljena s strani tretje osebe v bližini ali s strani izkušenega hekerja. V praksi se lahko zgodi, da podjetje, ki nima brezžičnega omrežja, dobi svoje neavtorizirano brezžično omrežje, katero je ustvaril zaposleni preko ethernet povezave znotraj podjetja ali obiskovalec podjetja. Ne glede na namen, se zopet pojavi nova nenadzorovana dostopna točka, ki nudi novo potencialno povezavo v notranje omrežje praktično komurkoli. Najlažje se zavarujemo pred tovrstnimi napadi s postavitvijo ustreznih sistemov in spremljanjem določenih parametrov ter z ustrezno varnostno politiko.

Denial of Service ali napad za zavrnitev storitve je grožnja s katero se spopadajo tudi brezžična omrežja. Je kibernetični napad, kateri prekine gladek prenos podatkov poslanih preko omrežja s tako imenovanim poplavljanjem omrežja, katerega se doseže s pošiljanjem velike količine prometa, z namenom upočasnitve, ali celo prekinitve sistema samega. Tarče so lahko katerakoli podjetja, ki to občutijo z nedelovanjem brezžičnih storitev. Poznamo tudi distribuirane tovrstne napade, kateri se lahko preko zlonamerne programske kode izvedejo iz več desetih ali tisočih IP naslovov, tako da je nemogoče blokirati in zaustaviti tak napad. Ampak to je že stvar interneta.

Postavljanje t.i. dostopnih točk na lahko dostopna mesta, kar lahko pripelje do tega, da nekdo s slabimi nameni ali pa zaposleni, ki mu je vseeno za varnost podjetja, zlahka prestavi, zamenja ali tovarniško ponastavi, kar lahko zopet pripelje do velike izpostavljenosti ranljivostim. Pomembno je tudi stalno spremljanje same konfiguracije dostopne točke, saj sama pravilna postavitev le te ni zadosti, pomembno je konstantno spremljanje, kajti ostati mora pravilno konfigurirana.

Zunanji varnostni pregledi doprinesejo nov pogled s strani izkušene osebe, na podlagi katerega je nato izdelano poročilo s smernicami v smislu izboljšanja brezžične varnosti.

V praksi napadalci največkrat ciljajo na »lahke tarče«. Dobro se je izogibati izpostavljanju prisotnosti brezžičnega omrežja, saj lažje ko ga je najti, večja je verjetnost da bo napaden. Obvezno je potrebno spremeniti SSID (Serivce Set Identifier) iz tovarniško dodeljenega na poljubno izbranega. Primer dobre prakse je izogibanje izbiranja imena, kateri je lahko povezljiv z lastnikom omrežja, kot recimo ime podjetja, priimek, dejavnost s katero se ukvarjate itd., saj s tem napadalcu, v primeru da ste ciljani, v trenutku omogočite, da to napravo poveže z vami in mu tako olajšate delo. Izjema bi morda bila dostopna točka za goste, katera pa mora biti obvezno popolnoma ločena od notranjega in službenega omrežja. Če je izvedljivo, je dobro prilagoditi antene in jakost signala tako, da signal doseže samo nujno dostopne točke.

Slabo konfigurirane dostopne točke so lahko tudi nekonfigurirane dostopne točke, kar pomeni, da so nastavljene na privzete nastavitve. Če se poslužujemo privzetih nastavitev, smo zlahka tarča nekoga, ki zna poiskati tovarniške nastavitve določenega modela naprave in si s tem pridobiti neavtoriziran dostop do omrežja. Nekatere dostopne točke celo, kot privzeto, uporabljajo nezavarovano dostopno točko, kar pomeni, da ima vsakdo lahko dostop do podatkov, ki se nezaščiteno prosto pretakajo po zraku. Predstavljajte si, kot, da bi morali živeti v hiši, sredi nevarne soseske, kjer so vrata stalno odklenjena in vsa okna odprta.

Zaradi povečanja odvisnosti od brezžičnih omrežij, so organizacije primorane uvesti celovito zaščito pred takšnimi napadi, katera vključuje tudi varnostna testiranja. Zunanji varnostni pregledi doprinesejo nov pogled s strani izkušene osebe, na podlagi katerega je nato izdelano poročilo s smernicami v smislu izboljšanja brezžične varnosti. Sama informacijska varnost je tesno povezana z varnostno kulturo podjetja in ozaveščenosti zaposlenih, saj je največkrat zgolj malomarnost tista, katera doprinese ranljivost. Tukaj torej ne gre za neko posebno in drago opremo, katera bi nas naredila bolj varne, temveč zgolj za pravilno upravljanje in nadzorovanje konfiguracij, ter zaščitenim prenosom in šifriranjem podatkov. ■

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



VARNOSTNO KOPIRANJE PODATKOV OZ. BACKUP

Imate pripravljen rezervni plan, če vaš disk odpove? In v primeru, če vam nekdo ukrade pametni telefon, z vsemi fotografijami in kontakti vred? Kaj pa, če »staknete« okužbo z izsiljevalskim virusom, ki vam zaklene vse dokumente in zahteva za povrnitev le-teh odkupnino?

Varnostno kopiranje podatkov ni ravno najbolj priljubljeno opravilo, vendar pravo vednost podatkov spoznamo šele takrat, ko v najbolj neprimernem času ostanemo brez zelo pomembnih podatkov. Živimo v digitalnem svetu in podatkov na različnih elektronskih nosilcih le-teh imamo vsak dan več. Pomislite, če ostanete brez že skoraj dokončane diplomske naloge, dostopa do spletne banke, fotografij pomembnejših življenjskih dogodkov, kontaktov v telefonu ali pa v poslovnem svetu brez arhiva elektronske pošte, poslovnih dokumentov in baz podatkov... Mišljenje, da se meni/nam to ne more zgoditi, je žal napačno, zato je prvi in najpomembnejši korak spoznanje, da morate poskrbeti za varnostno kopiranje podatkov tako v zasebnem kot tudi v poslovnem svetu, kjer pa si v današnjem času sploh ne bi smeli več dovoliti tveganja, da ni sistemsko urejenega varnostnega kopiranja podatkov.

Zagotovo imate na svojih elektronskih napravah podatke, kot so dokumenti, fotografije, videoposnetki, ki so preveč pomembni in dragoceni, da bi jih izgubili. Zato je redna izdelava varnostne kopije teh podatkov zelo pomembna. V različnih sistemih lahko varnostne kopije izdelujete na različne, a vendar precej enostavne načine.

Kako ustvarimo varnostne kopije podatkov?

Načinov je seveda več, vsekakor pa varnostno kopiranje ne zahteva posebnega računalniškega znanja in je v nekaterih primerih tudi brez dodatnih stroškov. Veljata pa pravili, da ni dovolj le enkrat letno poskrbeti za kopije in da poskušamo podatke shranjevati na dve ločeni lokaciji.

1. Zunanji trdi disk
Backup podatkov na zunanji disk je gotovo najhitrejši in najenostavnejši način. Zunanji diski, tudi tisti z večjimi kapacitetami, so cenovno zelo dostopni, kupimo jih lahko že v skoraj vsaki računalniški trgovini, tudi spletni. Podatke lahko ročno skopirate na zunanji disk ali pa naložite programsko opremo, ki bo ta proces avtomatizirala. Izbira tovrstnih programov je velika, na voljo so tudi brezplačne različice. Uporabite lahko tudi omrežne diske ali diskovna polja, na katera lahko kopiramo z vseh računalnikov na omrežju, vendar je ta možnost dražja in zahteva nekaj več tehničnega znanja.

2. Shranjevanje v oblak
Z razmahom oblačnega računalništva smo dobili še eno možnost varnostnega kopiranja – sinhronizacijo v oblak. Ta ne zahteva nakupa dodatne strojne opreme in omogoča dvosmerno sinhronizacijo med oblakom in več računalniki, zgolj z namestitvijo posebnega programa. Podjetij, ki nudijo shranjevanje v oblak je več, razlikujejo pa se najbolj po tem koliko prostora nudijo uporabniku brezplačno ter kako skrbijo za varnost podatkov. Shranjevanje varnostnih kopij v oblak je vsekakor enostavna, hitra in cenovno dokaj ugodna rešitev. Vendar pa pri shranjevanju varnostnih

kopij v oblak upoštevajte tudi dejstvo, da varnostne kopije shranjujete pri samem ponudniku storitve (primer Google, Apple ...), zato se v tem primeru tudi strinjate z njegovo politiko in pogoji uporabe. Le-te predhodno tudi dobro preberite.

V primeru, da pride do kakršnekoli izgube podatkov, je v takšnem primeru varnostna kopija tista edina, ki vas lahko »reši«, zato pravočasno poskrbite za vaše podatke preden bo prepozno.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

3. CD/DVD/Blu-ray
Podatke skopirajte na CD, DVD ali Blu-ray diske, ki jih nato shranite na varno mesto, kjer se ne bodo poškodovali. Če nimate ustrezne programske opreme za ustvarjanje podatkovnih diskov, lahko uporabite kakšen brezplačen program (primer CDBurnerXP). Zadnja leta se uporaba teh podatkovnih nosilcev zmanjšuje, predvsem ker ne omogočajo tolikšne fleksibilnosti, kot zunanji trdi diski ali oblačno kopiranje.



Na spletnem portalu Varni na internetu (https://www.varninainternetu.si/2018/kje-pa-vi-hranite-najlepse-spomine/) so na voljo različna gradiva, kjer najdete tudi navodila kako na različnih napravah narediti varnostno kopijo. Vaš znanje o varnostnem kopiranju pa lahko preverite tudi v kvizu (https://mitaliresnica.si/).

Tri zlata pravila varnostnega kopiranja

Ker je podatkov, ki jih shranjujete na svoje elektronske naprave vedno več, s tem eksponentno rastejo tudi možnosti, da jih izgubite. Poleg osnovne človeške previdnosti je edina rešitev redno varnostno kopiranje. A velja si zapomniti, da vsako varnostno kopiranje ni pravilno in s tem ni nujno zagotovljen nemoten dostop do vaših podatkov.

Če ste za shranjevanje kopij izbrali zunanji disk, z njim ravnajte previdno. Pomembno je tudi, da je čim bolj kakovosten. Pred izbiro ponudnika storitev shranjevanja podatkov v oblaku preverite njegove reference, po spletu pobrskajte za izkušnjami z njegovimi storitvami in preberite drobni tisk. Cena storitev naj bo drugotnega pomena. Vselej preverite tudi, ali ima ponudnik storitve v oblaku možnost dvostopenjske avtentikacije, da do podatkov ne bi morebiti dostopale nepooblaščene osebe.

Posebej je pomembno, da varnostne kopije naredite za vse elektronske naprave, ki jih uporabljate, pa tudi, da to delate čim bolj redno. Še preden se lotite varnostnega kopiranja, si zapomnite pravilo 3-2-1.

3 - Vedno imejte tri kopije vseh pomembnih datotek. Primer: originalna datoteka naj bo na vašem računalniku, kopiji pa spravite na zunanji disk in v oblak.

2 - Vselej uporabljajte dva različna tipa medijev. Primer: varnostno kopirajte na USB-ključek in optični medij, na primer DVD, ali v oblak.

1 - Eno varnostno kopijo vedno hranite ločeno od drugih. Primer: če vam v stanovanju zagori ali ga poplavi, obstaja možnost, da bodo uničeni tako računalnik kot oba nosilca z varnostnima kopijama (npr. USB-ključ in DVD). Zato eno kopijo spravite na varno v oblak.

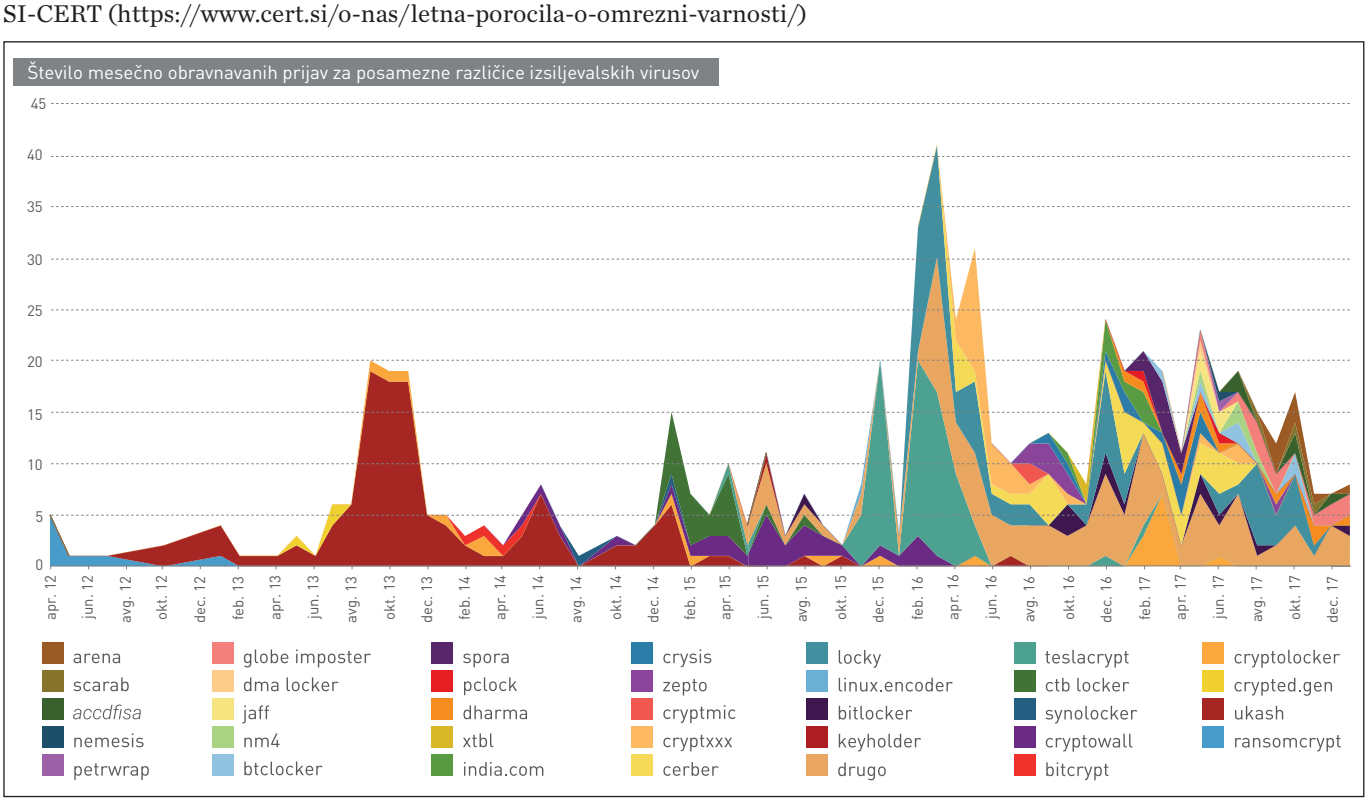




Varnostne kopije pa vam bodo prišle prav tudi v primeru, če pride do okužbe z izsiljevalskimi virusi, ki zaklenejo vse dokumente na računalniku in nato zahtevajo plačilo odkupnine. V zadnjih letih so namreč postali resna težava na področju računalniške varnosti. Žrtev izsiljevalskih virusov lahko postane vsak spletni uporabnik in vsako podjetje. Računalniški kriminalci ne izbirajo in pogosto skušajo doseči čim več žrtev ter si zagotoviti čim večji dobiček. Podjetja in organizacije bodo zelo verjetno plačale odkupnino, saj nujno potrebujejo podatke za svoje poslovanje.

V primeru, da pride do kakršnekoli izgube podatkov, je v takšnem primeru varnostna kopija tista edina, ki vas lahko »reši«, zato pravočasno poskrbite za vaše podatke preden bo prepozno. ■

Število mesečno obravnavanih prijav za posamezne različice izsiljevalskih virusov. Še več informacij najdete v letnem poročilu SI-CERT (https://www.cert.si/o-nas/letna-porocila-o-omrezni-varnosti/)





Lahko noč, skrbi.

Triglav komplet

Združite zavarovanja cele družine in prihranite do 50 %.

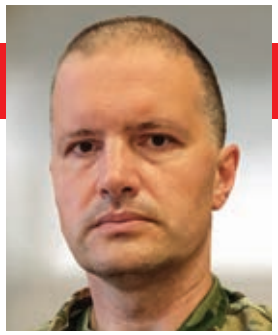
O svojih zavarovanjih ne razmišljate pogosto, a z občutkom varnosti, ki vam ga dajo, živite vsak dan.

Vse bo v redu.

triglav

www.triglav.si

Avtor: VVU XIII. r. dr. Gregor Potočnik / Slovenska vojska - katedra vojaških ved



OPERACIONALIZACIJA SKUPIN ZA ODZIVANJE NA RAČUNALNIŠKE GROŽNJE

Operacionalizacija Skupin za odzivanje na računalniške grožnje – CERT[1] oziroma Pristojnih organov za odzivanje na incidente na področju računalniške varnosti - CSIRT[2]

»Non progredi est regredi.«

Uvod

Direktiva (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L št. 194 z dne 19. 7. 2016, str. 1), (v nadaljnjem besedilu: Direktiva 2016/1148/ES), ni prvi pravni akt, je pa eden prvih pravnih aktov, ki dejansko določa, da imajo »Omrežja in informacijski sistemi ter storitve ključno vlogo v družbi« in na ta način ne samo *de iure*, ampak *de facto* operacionalizira zanesljivost in varnost, kot bistveni, za gospodarske in družbene dejavnosti ter zlasti za delovanje notranjega trga Evropske unije.

Operacionalizacija odzivov na incidente

Skupine za odzivanje na računalniške grožnje – CERT, oziroma Pristojni organi ali skupine za odzivanje na incidente na področju računalniške varnosti – CSIRT, (v nadaljevanju besedila bomo uporabili za oba termina kratico CSIRT) so povezane z nastankom programa, ameriškega ministrstva za obrambo, *Software Technology for Adaptable, Reliable Systems* (STARS) leta 1982 (Druffel 1983). Na podlagi navedenega programa so bili strokovnjaki z ameriškega ministrstva za obrambo in strokovnjaki iz gospodarstva povezani v skupno delovanje, saj so na ameriškem ministrstvu za obrambo ugotovili, da predstavlja programska oprema izziv za delovanja na področju kritične infrastrukture, ali celo, da je programska oprema vzrok za zamude in nevšečnosti pri delovanju kritične infrastrukture (Druffel 2017). Eden izmed rezultatov STARS programa in prizadevanj ameriškega ministrstva za obrambo, profesorjev fakultet ter gospodarstva je bila ustanovitev SEI »Software Engineering Institut« (Eastman 1983). Inštitut je imel štiri glavna vodila delovanj: prenos tehnologije, raziskovanje, direktna podpora in izobraževanje (Druffel 2017). V tistem času ni bilo univerz ali fakultet, ki bi imele podobne programe izobraževanj in je bil organizacijski izziv umestitve SEI v izobraževalni sistem. Leta 1984 so na Carnegie Mellon University (CMU), njihovem oddelku za znanstveno računalniško raziskovanje pričeli s sodelovanjem s SEI (Barbacci 1985).

CMU in SEI sta ključna pri nastanku prvega CERT-a. Drugega novembra 1982 je, takrat še študent g. Morris, izdelal enega prvih »črvov« in spravil na »kolena« svetovni internet. Črv je bil poimenovan po njegovem izumitelju, kot »Morrisov črv«. V 72. urah, po zaznavi črva, sta programerja ameriške državne agencije *Defense Advanced Research Projects Agency* (DARPA) ugotovila, kako črv deluje in pričela s podajanji nasvetov, kako črva omejiti oziroma odstraniti iz sistemov. Komunikacija je bila otežena in veliko subjektov se je tudi izključilo iz Arpaneta (eden izmed predhodnikov interneta). Strokovnjaki iz DARPA so ugotovili, da če bi bil avtor črva bolj zloben, bi nastala mnogo večja škoda, kot dejansko je. DARPA je takrat s SEI sklenila, da bo SEI ustanovila skupino za odzivanje na računalniške grožnje »computer emergency response team – CERT«, z operativnim konceptom da (Druffel 2017): »*bo to nevladna organizacija, nevtralen posrednik, brezoblasten organ;bo imela dostop do ključnih strokovnjakov;bo slonela na prejšnjih zaupanja vrednih odnosih;bo sodelovala z dobavitelji zaradi ublažitve ranljivosti; bo nadgradila DARPA položaj v družbi ob sodelovanju SEI in CMU;bo imela sporazum o »obvodu«*

birokracije;bo ustvarila povezavo skupin za odzivanje na računalniške grožnje po zgledu CERT.« Šestega decembra 1988 je pričel delovati CERT, delo je obsegalo: »zagotavljanje zanesljive in zaupanja vredne, 24 urne, *enotočkovne točke za nujne primere; omogočanje komunikacije med strokovnjaki v zvezi reševanja varnostnih problemov; služenje, kot osrednja točka prepoznavanja in odpravljanja ranljivosti računalniških sistemov; ohranjanje tesnih vezi z raziskovalnimi dejavnostmi in izvajanje raziskav za izboljšanje varnosti obstoječih sistemov; izvajanje proaktivnih ukrepov za izvajanje ozaveščenosti in razumevanja informacijske varnosti in računalniške varnosti v celotni skupnosti uporabnikov informacijskih sistemov in ponudnikov storitev; služiti kot model drugim skupinam za odzivanje na računalniške grožnje«* (Druffel 2017).



Od leta 1988 do danes

CERT-i oziroma CSIRT-i so doživeli strokovno prelomnico z ustanovitvijo Foruma skupin za odzivanje na računalniške grožnje »Forum of Incident Response and Security Teams (FIRST)«, povod za nastanek FIRST je bil »črv Wank«[3] eden prvih »črvov« hektavistične narave (Schell 2002) leta 1989. Takrat se je pokazala ne dovolj učinkovita komunikacija med strokovnjaki in organizacijami in med možnimi rešitvami nastale težave. Ena izmed rešitev je bila ustanovitev FIRST, ki se je pokazala, kot učinkovita in deluje še danes.

Začetni incidenti in kibernetski napadi so bili mnogo manj učinkoviti in družbeno ali celo globalno neogrožajoči v primerjavi z incidenti in kibernetskimi napadi, ki so se pričeli dogajati po letu 2000 in še posebej po letu 2001. Ameriški odziv je predstavljal poleg drugih ukrepov, še vzpostavitev nacionalnega CERT-a (US-CERT), ki je bil del državne uprave (GSA)[4] že od ustanovitve





leta 2000. Podrobnejši časovni razvid je viden v prilogi. Odziv informacijsko naprednejših držav (vsaj nivoja držav skupin G8 ali G20) je bil prav tako, da so nacionalne CERT-e ustanovili, kot državne organe oz. kot del državne uprave.

Primerjava CERT-ov oziroma CSIRT-ov

Direktiva 2016/1148/ES je pomenila z normativnega vidika prelomnico v slovenski zakonodaji na področju informacijske varnosti. Samo zaznavanje kibernetskega prostora slovenski zakonodajni veji ni predstavljalo nekaj novega.[5] Pa vendar je predstavljala navedena direktiva močan impulz izvršni veji oblasti, da je pričela s pripravo zakona, ki bo implementiral Direktivo 2016/1148/ES. Tudi zato je Državni zbor 17. aprila 2018 sprejel Zakon o informacijski varnosti (ZInfV)[6] in v njegovem členu 28 določil, da je »Nacionalni CSIRT odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij SI-CERT pri javnem zavodu Akademska in raziskovalna mreža Slovenije.« Navedena določba predstavlja *satis alio*.[7] Takšna ureditev bo z vidika nacionalnovarnostnega sistema Republike Slovenije predstavljala še velik izziv. Ne samo zaradi dejstva, da nobena od držav članic G8[8] ali G20,[9] ne informacijsko bolj razvita država od Slovenije ter hkratna članica EU in NATA, nima nacionalnega CSIRT-a v sklopu javnega zavoda,[10] kar ARNES (Akademska in raziskovalna mreža Slovenije) je, temveč tudi zaradi dejstva, da so vse naštete države v začetni fazi imele nacionalne CERT-e v sklopu univerz, fakultet ali raziskovalnih inštitutov, vendar so se v kasnejši fazi zavedle, da informacijsko okolje prepomebneje vpliva na vsakdanje življenje ljudi in delovanje države. Zatorej so v večini primerov naštete države pustile »začetne« CERT-e na univerzah, fakultetah ali inštitutih in ustanovile nacionalne CSIRT-e kot državne organe ali kot dele državne uprave. Slovenija še ni zmogla tega koraka, kljub temu, da je že dr. Grizold leta 1999[11] napisal, da je nacionalnovarnostni sistem organiziran tako, da »njegovi posamezni deli delujejo v vzajemni povezanosti in odvisnosti ter so urejeni tako, da zagotavljajo varnost družbi v širšem smislu« ter, da so »Varnostni sistem, varnostni mehanizem in varnostni instrument tri ravni, ki jih mora upoštevati politika države.« Slovenija z določbami ZInfV, ne o določitvi (Arnes-a), ampak predvsem zaradi sistemske umeščenosti Nacionalnega CSIRT-a ni upoštevala ugotovitev glede nacionalnovarnostnega sistema dr. Grizolda, ne izkušenj in dobrih praks informacijsko bolj razvitih držav od Slovenije.

Predvidevam lahko, na podlagi izkušenj informacijsko bolj razvitih držav, da bo Slovenija imela zaradi tega, ker je njen Nacionalni CSIRT javni zavod, težave najmanj pri operacionalizaciji kibernetskega kriminala (kvaliteta sodelovanja javni zavod – državni organi pregona), stopnji zaupanja (med izvajalci bistvenih storitev, ponudniki digitalnih storitev in organi državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti in med javnim zavodom ali drugače, ali bodo res vsi našteti poročali javnemu zavodu o »svojih« incidentih oz. nepravilnostih. Izkušnje kažejo da ne, in da rešujejo (»svoje težave« v »tihem«) in nazadnje, morda

celo najpomembnejše, javni zavod ne more koristiti dodane vrednosti »etičnih hekerjev« oz. »white hat«, kaj šele »black hat« delovanja, kljub temu, da je bilo napisanih že mnogo znanstvenih del, ki zagovarjajo razne oblike »hekanja« v korist države in družbe. Dodano vrednost »etičnih hekerjev« oz. »white hat« in tudi »black hat« lahko operacionalizira samo državni organ v povezavi z državnimi organi pregona in nikakor ne javni zavod.

Rešitev bi bila, da bi se oddelek SI-CERT (del Arnes-a) preoblikoval ali vsaj sistemsko formalno premestil v »del« državne uprave ali državnega organa.

Slovenija ima primarno organizacijski problem in ne gmotni oz. finančno materialni. Organizacijsko smo še vedno v letu 1989, ko so bili CERT-i del univerz, fakultet in inštitutov, saj, na podlagi člena 28. ZInfV, ne dojemamo vloge in poslanstva nacionalnih CSIRT-ov in nacionalnovarnostnega sistema.

Literatura

- ACM. 1989. Communications of the ACM 32, 6 (June 1989): Entire issue devoted to the subject of the Morris Worm. Example article: Eugene H. Spafford, "The Internet Worm: Crisis and Aftermath:" 678-687.
- Barbacci, M. R.; Habermann, A. N.; & Shaw, M. 1985. The Software Engineering Institute: Bridging Practice and Potential. IEEE Software 2, 6 (November 1985): 4-21 (ISSN:0740-7459).
- Direktiva (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L št. 194 z dne 19. 7. 2016, str. 1).
- Druffel, Larry; Redwine, Samuel, Jr.; & Riddle, William. 1983. The DoD STARS Program. IEEE Computer (November 1983): 21-30.
- Druffel, Larry. 2017. A Technical History of the SEI. Carnegie Mellon University.
- Resolucija o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 56/01).
- Eastman, Neil. S. 1983. Study Report on the DoD Software Engineering Institute. Institute for Defense Analysis.
- Grizold. Anton. 1999. Obrambni sistem Republike Slovenije. Visoko policijsko-varnostna šola. Ljubljana.
- Schell, B.H., Dodge, J.L., with S.S. Moutsatsos. 2002. The Hacking of America: Who's Doing It, Why, and How. Westport, CT: Quorum Books.
- Zakon o informacijski varnosti (Uradni list RS, št. 30/18).
- Zakon o zavodih (Uradni list RS, št. 12/91, 8/96, 36/00 – ZPDZC in 127/06 – ZJZP).

[1] Terminologija povzeta po Direktivi (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L št. 194 z dne 19. 7. 2016, str. 1), (v nadaljnjem besedilu: Direktiva 2016/1148/ES).

[2] Ibidem.

[3] Ko se je delavec ameriškega zračnega in vesoljska državnega organa v Marylandu prijavil v sistem, se mu je na ekranu izpisal napis: "WORMS AGAINST NUCLEAR KILLERS; YOUR SYSTEM HAS BEEN OFFICIALLY WANKed."

[4] Ameriški »General Services Administration.«

[5] Leta 2001 je Državni zbor sprejel Resolucijo o strategiji nacionalne varnosti Republike Slovenije (Uradni list RS, št. 56/01), kjer je v točki 3.3 že bilo navedeno, da je »informacijska oziroma kibernetična blokada« vir ogrožanja nacionalne varnosti Republike Slovenije. Resolucija je političen akt, pa vendar imamo eno prvih uradnih navedb v zvezi kibernetskega delovanja. Naslednica Resolucije, iz leta 2010, zadevo še podkrepi.

[6] Zakon o informacijski varnosti (Uradni list RS, št. 30/18).

[7] Popolnoma nekaj drugega in posebnega, kot imajo države, ki so bolj informacijsko razvite, bolj izkušene in imajo daljšo tradicijo delovanja na informacijske področju.

[8] Države: Francija, Italija, Japonska, Kanada, Nemčija, Rusija, VB in ZDA.

[9] Države: Argentina Avstralija, Brazilija, Francija, Indija, Indonezija, Italija, Japonska, Južna Afrika, Južna Koreja, Kanada, Kitajska, Mehika, Nemčija, Rusija Saudska Arabija, Turčija, VB in ZDA.

[10] Države: Argentina Avstralija, Brazilija, Francija, Indija, Indonezija, Italija, Japonska, Južna Afrika, Južna Koreja, Kanada, Kitajska, Mehika, Nemčija, Rusija Saudska Arabija, Turčija, VB in ZDA.

[11] Zakon o zavodih (Uradni list RS, št. 12/91, 8/96, 36/00 – ZPDZC in 127/06 – ZJZP) določa v členu 1: »Zavodi so organizacije, ki se ustanovijo za opravljanje dejavnosti vzgoje in izobraževanja, znanosti, kulture, športa, zdravstva, socialnega varstva, otroškega varstva, invalidskega varstva, socialnega zavarovanja ali drugih dejavnosti, če cilj opravljanja dejavnosti ni pridobivanje dobička.« Delo in poslanstvo nacionalnega CSIRT-a je mnogo več, kot to. ■



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

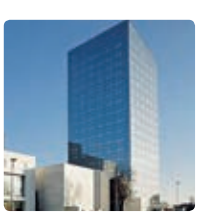
FAKULTETA ZA PODJETNIŠTVO

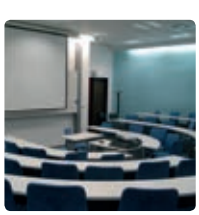
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

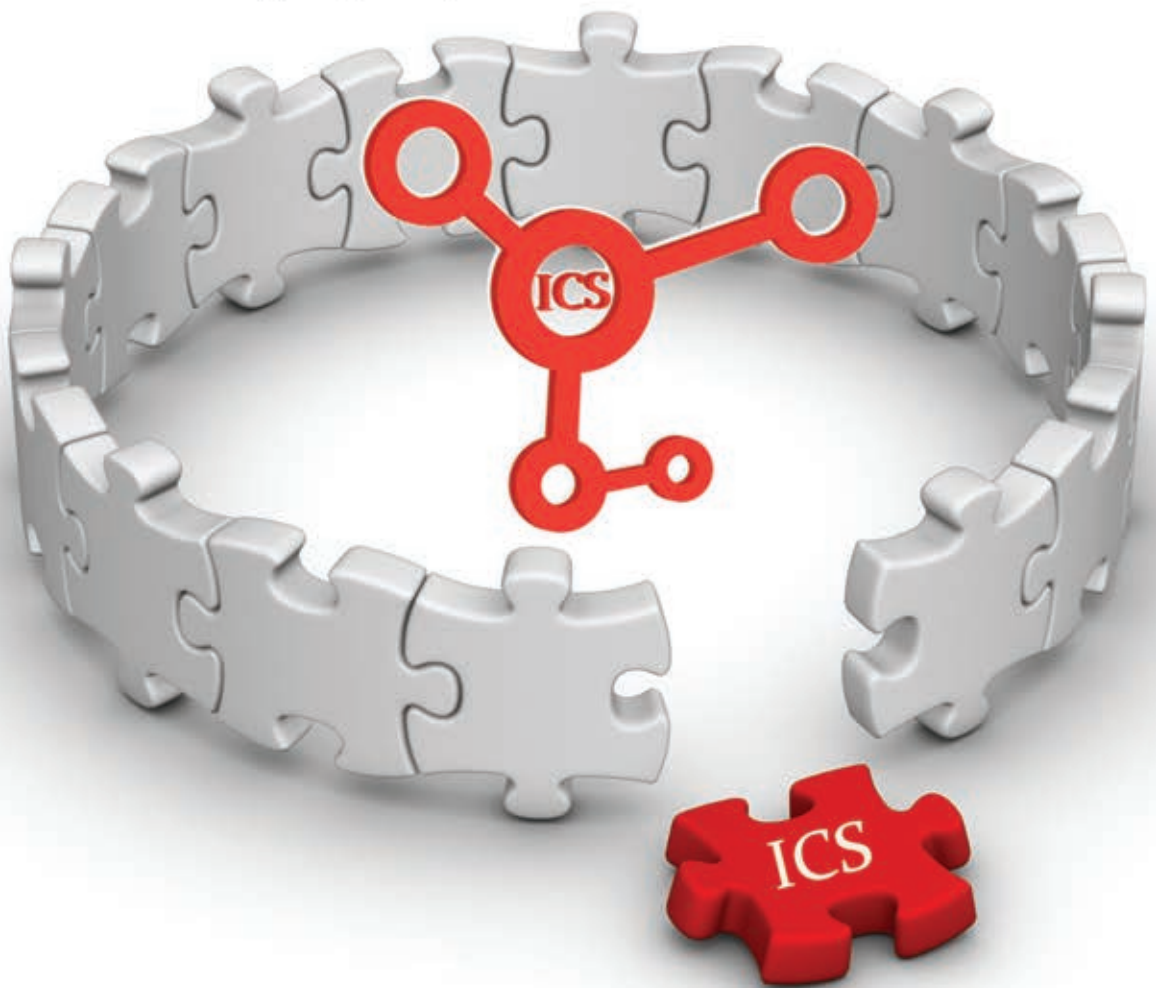
10. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 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