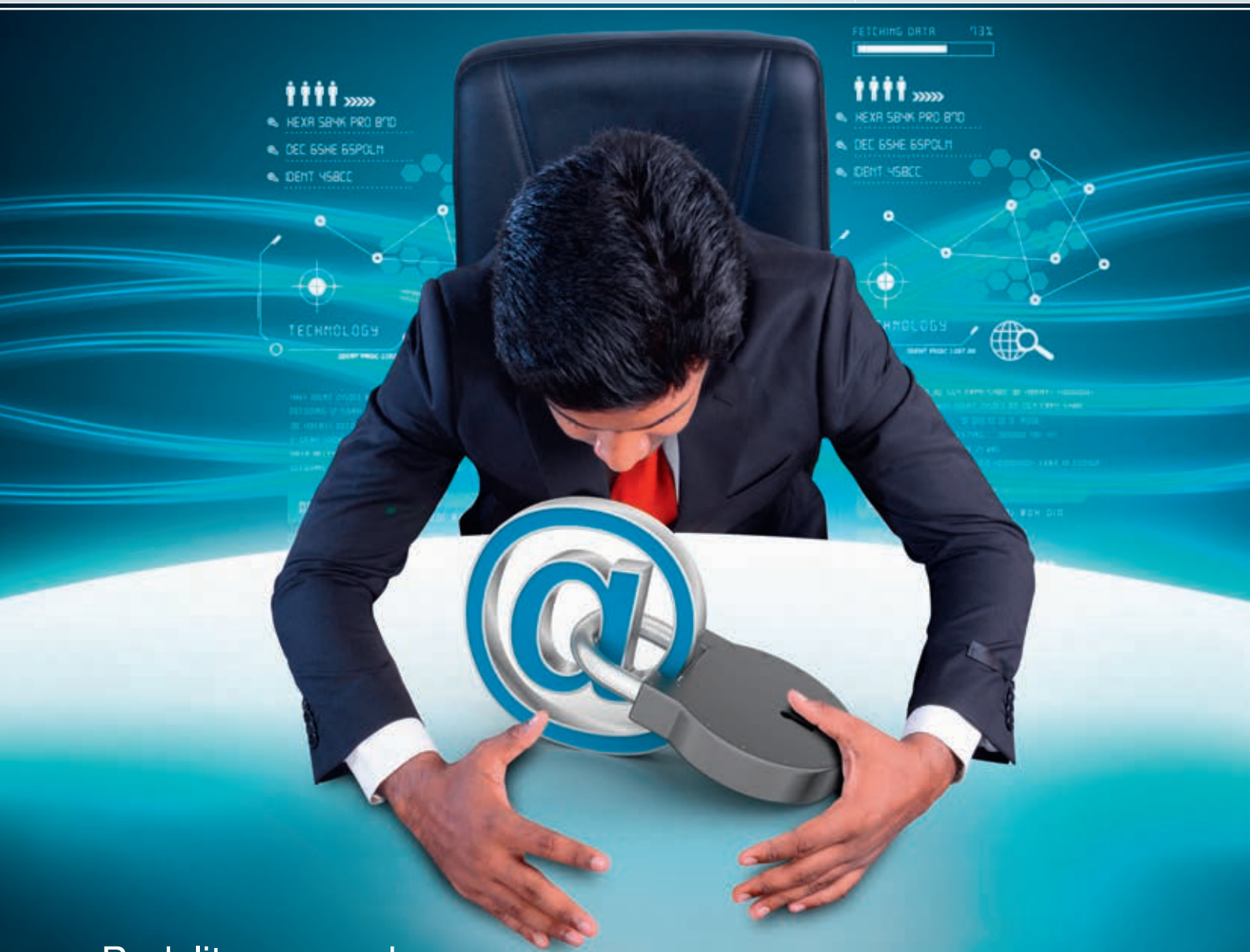
Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2016, oktober • št. 12



Podelitev nagrad »Slovenian Grand Security Award 2016«

Za uspešno delo Računskega sodišča je ključno ocenjevanje tveganj

Tomaž Vesel, predsednik Računskega sodišča Republike Slovenije

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

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

IZVIRNA MISEL

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

PRAVA IZBIRA

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

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

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

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

Integralni varnostni sistemi (celovito varovanje)

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

Varovanje oseb in premoženja

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

Kakovost in varnost

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

Krizno vodenje (krizni menedžment)

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

IZOBRAŽEVANJE

Varnostni menedžment

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





Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
ICS-Ljubljana

Tisk:
Evrografis d.o.o.

Datum izida
oktober 2016

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.

Okolje, ki nas obdaja, nas dnevno postavlja pred pomembne izzive na področju zagotavljanja varnosti. Na žalost so vsi varnostno izpostavljeni dogodki iz naših glav prepodili še zadnje iluzije, da živimo v popolnoma varnem okolju, kjer se nam nič ne more zgoditi. Dnevno smo soočeni s tveganji in grožnjami, ki se pojavljajo na različnih področjih. Od tragičnih dogodkov v zdravstvenih institucijah, informacijskimi tveganji spletnih prevar in vdorov v računalniške sisteme podjetij, kraje osebnih in drugih pomembnih podatkov, kaznivih dejanj, ki so bila uperjena tudi proti poslovnim organizacijam in seveda nevarnosti širšega mednarodnega okolja, kjer poleg mednarodnega terorizma še vedno prevladuje močno izražen strah pred ponovnim valom beguncev in migrantov, ki bi pljusknili na naše meje. Ob vseh teh varnostno izpostavljenih dogodkih se počasi, vendar vztrajno, krepi občutek in zavedanje, da je varnost postala dobrina, katera ni več samo po sebi umevno dejstvo, temveč, da se je potrebno obvladovanja tveganj lotiti sistemsko. To še posebej velja za podjetja in druge organizacije, ki delujejo v tem zahtevnem globalnem okolju.

Seveda nas na drugi strani pozitivni trend, ki ga zaznavamo na področju zavedanja o pomenu varnosti, lahko navdaja z zmernim optimizmom. Slovensko združenje za korporativno varnost se kot najmočnejša civilno strokovna asociacija vsak mesec krepi z vstopom novih članov. Seveda ima za dvig tega zavedanja izredno pomembno vlogo in mesto ravno pričujoča revija Korporativna varnost, ki s svojimi prispevki aktualizira različna varnostna področja in bralcem ponuja uvid v dobre prakse in izkušnje posameznih strokovnjakov.

V tokratni številki smo posebej namenili prostor kar trem intervjujem ter tako poskušali narediti programsko shemo revije še bolj zanimivo in aktualno. V intervjujih se dotikamo področja nadzora nad javnimi financami, vloge korporativne varnosti v slovenski globalni korporaciji in seveda prihodnosti na področju uveljavljanja profesije korporativne varnosti. V prispevkih nikakor nismo mogli mimo informacijske varnosti, ki jo prinašajo prispevki iz različnih vsebin tega aktualnega področja. Osvetlili pa smo tudi vlogo analize in ocenjevanja ranljivosti, groženj in tveganj, kot osnovne podstati za učinkovit in celovit pristop do obvladovanja varnostnih tveganj. V prispevkih odpiramo tudi vidike povezane z zaščito kritične infrastrukture, kot enega izmed ključnih segmentov za normalno funkcioniranje sodobne družbe. V kolumni pa nastavljamo zrcalo pristojnim institucijam, ki so pristojne za nadzor nad nelegalnim izvajanjem nalog na področju korporativne varnosti. Neustrezen nadzor na trgu omogoča delovanje različnim »strokovnjakom«, ki s svojim nestrokovnim in predvsem nesistemskim delovanjem naročnikom povzročajo dodatne stroške in v ničemer ne prispevajo k ureditvi varnostnih razmer v družbi. Za konec smo vam ponudili še celovito reportažo z Dnevov korporativne varnosti 2016 in s svečanosti ob podelitvi prestižnih varnostnih nagrad »Slovenian Grand Security Award«, ki predstavlja vrhunski dogodek v širšem regijskem prostoru.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
mag. Karol Turk,
svetovalec predsednika uprave za korporativno varnost

KORPORATIVNA VARNOST POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

12



RANLJIVOST, VARNOSTNE GROŽNJE IN VARNOSTNA TVEGANJA SI PODAJAJO ROKE

Namen tega prispevka je povedati nekaj o pristopu k obvladovanju varnostnih sprememb, varnostnih groženj, varnostnih tveganj in ranljivosti organizacij, pri čemer je poudarek na njihovi medsebojni povezanosti in soodvisnosti. Gre namreč za pomemben segment v ocenjevanju stanja varnosti na ravni države, subjektov kritične infrastrukture, gospodarstva in civilne družbe.

15



ORGANIZIRANOST VARNOSTNIH SLUŽB V RAZMERAH TERORISTIČNIH ALI AMOK NAPADOV

Sedanja komercializacija v dejavnosti zasebnega varovanja, podrejenost te dejavnosti finančnim dobičkom je zaskrbljujoča in v nasprotju s pomenom te panoge.

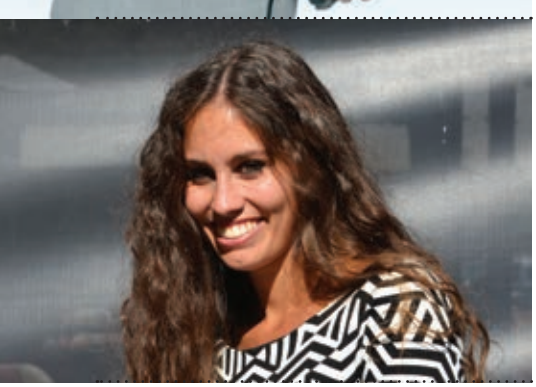
32



HEKERJI VDIRAJO V ELEKTRONSKO POŠTO SLOVENSKIH PODJETIJ

Geslo za elektronsko pošto je najpomembnejše med vsemi. Pogosta izjava "Pa kaj, če mi vdrejo v moj mail, saj nimam ničesar za skrivati", se v večini primerov izkaže za še kako zgrešeno.

37



INTERVJU
Elena Blaževič, absolventka magistrskega študija »Management korporativne varnosti«

MANAGEMENT KORPORATIVNE VARNOSTI POMEMBEN POKLICNI PROFIL PRIHODNOSTI

55

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
Tomaž Vesel, predsednik Računskega sodišča Republike Slovenije

ZA USPEŠNO DELO RAČUNSKEGA SODIŠČA JE KLJUČNO OCENJEVANJE TVEGANJ

Pogovarjali smo se s predsednikom računskega sodišča Tomažem Veselom. Je pravnik, strokovnjak za javno naročanje in nadzor nad (u)porabo javnih sredstev, ki je poleg Računskega sodišča Republike Slovenije (računsko sodišče), kjer je pred tem delal kot revizor, vrhovni državni revizor in namestnik predsednika, svoje izkušnje pridobival tudi kot član Državne revizijske komisije, ki nadzira pravilnost postopkov javnih naročil. Njegov ugled sega tudi čez meje in presega zgolj revizijsko področje (sodelovanje v mednarodnih organizacijah vrhovnih revizijskih institucij, kot so INTOSAI, EUROSAI ...), saj je julija letos kot nogometni navdušenec postal tudi predsednik komisije za revizijo in skladnost pri Mednarodni nogometni zvezi (FIFA).

Računsko sodišče je v zadnjem obdobju pod vašim vodstvom izredno aktivno. Nam lahko prosim pojasnite težišča delovanja tega vašega mandata.

Računsko sodišče je vrhovna državna revizijska institucija, kar pomeni, da bdi nad celotno porabo javnih sredstev v Republiki Sloveniji. To je naš moto in tudi razlog, zaradi katerega institucija obstaja – da upravljavcem javnih sredstev nastavimo ogledalo, v katerem vidijo, kako ravnajo s premoženjem davkoplačevalcev, ter o ugotovitvah obveščamo tudi najširšo javnost.
Pri svojem delu skušamo uravnoteženo skrbeti, tako za konkretna sistemsko pomembna področja, kjer ocenjujemo povečana tveganja za nastanek nepravilnosti ali nesmotrnosti (tako smo na primer že pred časom glasno opozarjali na naraščajoč javni dolg), kot tudi za odzivnost institucije na aktualna javnofinančna vprašanja. Med težišči našega dela naj izpostavim na primer: povečevanja zmožnosti črpanja sredstev EU, razdeljevanje javnih sredstev, kjer ni določenih meril in kriterijev in se zato ne zasleduje največji učinek glede na vložena sredstva, primeri, ko država ali občina za opravljanje javnih nalog ustanovi zasebni subjekt, za katerega ne veljajo pravila javnega sektorja, prehod sredstev iz javnega v zasebni sektor, kot so javna naročila, koncesije, javno-zasebna partnerstva in podobno.

> Davkoplačevalci si zaslužimo izvedeti, kako se upravlja z našim premoženjem, da lahko zahtevamo ustrezne spremembe na bolje!

*avtor je član Slovenskega združenja korporativne varnosti



Glede na to, da delamo na zelo različnih področjih (uprava, šolstvo, zdravstvo, sociala ...) in pri zelo različnih revidirancih (država, občine, javni zavodi, javne agencije, podjetja v večinski državni lasti ...) je naše delo precej pestro ter hkrati zahteva zelo široka znanja revizorjev in ostalih zaposlenih.
Glavna ovira pri izvajanju naših pristojnosti so naši zelo omejeni viri (v času krize med letoma 2008 in 2015 se je proračun računskega sodišča zmanjšal za skoraj četrtino) ter vedno nove pristojnosti oziroma obvezne revizije, ki nam jih nalaga zakonodajalec. Vse to povečuje vrzel med pričakovanji javnosti o našem delu in hkratni prisotnosti na zelo različnih področjih ter tem, kaj je računsko sodišče objektivno sposobno nadzirati.

V Republiki Sloveniji smo bili v preteklosti priča izredno malomarnemu upravljanju z javnimi financami v različnih delih javnega sektorja. Kakšno vlogo oz. pristojnosti sploh ima računsko sodišče, ko govorimo o preprečevanju teh anomalij?

Zakonodajalec bi Računskemu sodišču Republike Slovenije lahko pomagal do ostrejših zob – na podlagi njihovih ugotovitev bi se lahko pričel tudi postopek za ugotavljanje, ali bi odgovorni osebi uporabnika javnih sredstev za neko obdobje prepovedali razpolagati z javnimi sredstvi.

Cilj vsake revizije je izrek mnenja o poslovanju revidiranca, v našem primeru torej enega ali več uporabnikov javnih sredstev. Glavno orodje oziroma pristojnost, če želite, je neoviran dostop do podatkov o poslovanju, kar nam omogoči, da ocenimo pravilnost in tudi smotrnost (u)porabe javnih sredstev. Ko podrobno spoznamo poslovanje revidiranca, ga opozorimo na nepravilnosti ali nesmotrnosti v njegovem poslovanju ter mu podamo priporočila za izboljšanje poslovanja. Pri tem lahko izdamo tudi zahtevo za izvedbo popravljalnih ukrepov, ki se lahko nanašajo na odpravo ugotovljenih preteklih nepravilnosti/nesmotrnosti ali na sprejem ukrepov za zmanjšanje tveganj za prihodnje nepravilno/nesmotrno poslovanje.
Na ta način zagotovimo specialno prevencijo (izboljšanje poslovanja pri konkretnem revidirancu), z javno objavo revizijskih poročil pa tudi generalno prevencijo, saj so z ugotovitvami in presojo računskega sodišča seznanjeni tudi drugi podobni subjekti.

Kaj odgovarjate kritikom delovanja računskega sodišča, ki tej instituciji očitajo, da je »brezzobi tiger«?

Ne vem. Morda nepoznavanje prava. Računsko sodišče je državni organ in

za vse dele države velja, da imajo samo tiste pristojnosti, ki so nanje prenesene z zakoni. Vsako preseganje z zakonom določene pristojnosti bi pomenilo grobo kršenje temeljnih pravnih načel, predvsem načela zakonitosti in načela delovanja pravne države. Računsko sodišče po zdajšnjem zakonu nima kaznovalnih pristojnosti in si jih samo tudi ne more in ne sme vzeti. Računsko sodišče je neodvisno strokovno telo, ki lahko opravi pregled poslovanja – preiskavo, če želite – in o tem poroča pristojnim organom, da ukrepajo vsak v skladu s svojimi pristojnostmi. Ustrezno ukrepanje je hkrati tudi njihova odgovornost.

Primerjalno gledano je v Evropi in Svetu več različnih modelov ureditve vrhovne revizijske institucije, na grobo jih lahko delimo na tiste s sodno pristojnostjo in tiste brez nje. Naša institucija spada med slednje, saj naša poročila nimajo narave sodne odločbe. Vseeno pa moramo priznati, da imamo med institucijami brez sodne pristojnosti eno najširših revizijskih pristojnosti, vsaj če pogledamo med državami članicami EU. Pri tem imam v mislih predvsem nabor potencialnih revidirancev.

Če bi zakonodajalec želel, bi našemu »tigru« lahko pomagal do ostrejših zob. V mislih imam morebitno spremembo zakonodaje, ki bi omogočila, da bi se na podlagi naših ugotovitev lahko pričel postopek za ugotavljanje, ali bi odgovorni osebi uporabnika javnih sredstev za neko obdobje prepovedali razpolagati z javnimi sredstvi. Ocenjujemo, da bi to lahko izboljšalo pripravljenost odgovornih za odpravo ugotovljenih nepravilnosti oziroma nesmotrnosti in s tem bistveno povečalo učinek našega dela. Prepričan sem, da je to ideja, ki je vredna dodatnega razmisleka, seveda pa je pomembno vprašanje ali bo politika zbrala dovolj interesa, da bi nam zaupala orožje, ki bi se v prihodnje lahko obrnilo tudi proti njej.

Nam lahko navedete nekaj podatkov o obsegu in statistiki obravnave najbolj perečih primerov v zadnjem obdobju?

V lanskem letu smo skupaj izdali 65 revizijskih in 21 porevizijskih poročil v katerih smo našteli 441 izvedenih ukrepov za izboljšanje poslovanja in uporabnikom javnih sredstev podali še dodatnih 250 priporočil ter pripravili 138 pisnih odgovorov na njihova vprašanja. Pomemben je tudi podatek, da smo prejeli tudi 455 pobud za izvedbo revizij, saj to kaže na visoko raven zaupanja v delo računskega sodišča. Poleg tega s svojimi opozorili in priporočili sodelujemo tudi v postopkih priprave več zakonov in drugih predpisov.

Zelo nehvaležno je izmed vseh opravljenih revizij v posameznem letu izpostaviti le nekatere, saj vsi revizorji računskega sodišča vestno in zavzeto opravljajo svoje delo, pa naj gre za revizijo poslovanja nekega manjšega vrtca ali pa morda upravljanja z javnim dolgom, ki bo bremenil še prihodnje generacije. Se pa težko izognem nekaterim revizijam, ki so bile v javnosti zelo pričakovane in katerih ugotovitve so tudi najbolj odmevale, kot so na primer revizija poslovanja Holdinga slovenskih elektrarn pri investiciji v 6. blok Termoelektrarne Šoštanj (TEŠ 6), ustanovitev in poslovanje Družbe za upravljanje terjatev bank (DUTB oziroma »slaba banka«), pa tudi še trajajoča revizija poslovanja Nove ljubljanske banke pri upravljanju s slabimi terjatvami in najemanju zunanjih storitev.



Seveda se vprašanju o bančnih luknjah ne moremo izogniti. Kje so bile zamujene priložnosti na strani nadzornih institucij, ki bi lahko preprečile ta negativni proces? Kakšno vlogo bi po vašem morala imeti v tej zgodbi institucija, ki jo sedaj vodite?

Vrednostnih sodb o delu nadzornih organov seveda ne morem podati, dokler ne opravimo revizije njihovega poslovanja. Tu pa prihaja do težav, saj že skoraj dve leti usklajujemo ali in pod kakšnimi pogoji ter s kakšnim ciljem lahko računsko sodišče sploh revidira poslovanje centralne banke. Zavedamo se, da je to zaradi vpetosti bančnega nadzornika v širšo evropsko monetarno politiko občutljivo vprašanje, s katerim se ne sooča le Slovenija, ampak tudi druge države članice EU.

Brez dvoma pa na računskem sodišču budno spremljamo omenjeno področje, pri katerem zaznavamo specifična tveganja, ki zahtevajo ustrezno obravnavo. Ne nazadnje je v kapitalu državnih bank vezanih veliko sredstev davkoplačevalcev in posledično je zato velik javni interes po učinkovitem nadzoru nad bančnim sistemom. Vsaj za v prihodnje .

Kakšno je vaše sodelovanje s Komisijo za preprečevanje korupcije? Zdi se, da omenjena komisija izgublja svoje pomembno mesto v družbi. Kako ocenjujete te dejavnike glede

na to, da je veliko oškodovanj javnega premoženja in nesmotrne porabe javnih sredstev neposredno povezano s korupcijskimi dejanji?

Računsko sodišče konstruktivno sodeluje z večino državnih organov. Za delo nadzornih organov je zelo pomembno zaupanje javnosti v nepolitičnost in strokovnost njihovega dela. Brez tega se še tako pomembne ugotovitve razvodenijo in (pre)pogosto potihnejo brez ustreznih sankcij.
Pri korupcijskih kaznivih dejanjih večkrat pozabljamo, da so zanje v prvi vrsti pristojni organi odkrivanja in pregona kaznivih dejanj, se pravi policija in tožilstvo. Izpostavim lahko predvsem policijo, s katero v zadnjem času aktivno sodelujemo. Bi si pa včasih želeli še več aktivnosti z njihove strani. Tudi pri kazenskih ovadbah, ki jih na podlagi ugotovitev iz revizij vlaga računsko sodišče.

Kako ocenjujete vašo vlogo pri nadzoru nad podjetji, ki so v večinski državni lasti oz. ima država kontrolni delež pri upravljanju. Kakšne so vaše pristojnosti in predvsem kako ste uspešni pri pridobivanju ustreznih informacij, ki vam omogočijo učinkovito analizo porabe javnih sredstev?

Za upravljanje in posledično nadzor nad podjetji v državni lasti je odgovoren Slovenski državni holding (SDH), ki so mu zaupane milijarde evrov državnega premoženja. Nadzor nad njim izvaja – in s tem tudi prevzema del odgovornosti – Vlada Republike Slovenije, kot skupščina SDH. Po zakonu o SDH iz leta 2014 sme računsko sodišče izvesti revizije pravilnosti in smotrnosti poslovanja SDH in v gospodarskih družbah, v katerih ima SDH neposredno ali posredno prevladujoč delež glasovalnih pravic.
Ravno pri državnih podjetjih, ki poslujejo po pravilih, ki veljajo tudi za zasebne gospodarske družbe, se v praksi najpogosteje srečujemo z zapleti pri pridobivanju dokumentacije, ki bi nam omogočila celovit vpogled v njihovo poslovanje. Morda še večjo težavo pa imamo pri poročanju o njihovem poslovanju, saj pogosto skladno z zakonom o gospodarskih družbah ogromno dokumentacije označijo kot poslovno skrivnost. Rezultat tega so javno objavljena »počrnjena« poročila, za katere si želimo, da bi jih bilo v prihodnje vedno manj, saj si davkoplačevalci zaslužimo izvedeti, kako se upravlja z našim premoženjem, da lahko zahtevamo ustrezne spremembe na bolje.

»Položaj pri Mednarodni nogometni zvezi sem prevzel, ker predstavlja izjemen izziv sodelovati pri vzpostavitvi novega načina dela v organizaciji, ki brez dvoma sodi med najvplivnejše na področju športa na svetu.«

Določena javna podjetja upravljajo s kritično infrastrukturo, ki je nujno potrebna za delovanje širše družbene skupnosti. Ste v takih organizacijah še posebej pozorni na zlorabe in neustrezno poslovanje, ki bi imelo lahko za posledico tudi omejeno delovanje kritične infrastrukture?

Pozorni smo na celoten spekter delovanja pri vseh uporabnikih javnih sredstev, ki so po zakonu o računskem sodišču lahko naši revidiranci. Seveda pri ocenjevanju tveganj v poslovanju poleg verjetnosti nastanka neželenega dogodka upoštevamo tudi težo posledic, ki bi jih neželeni dogodek povzročil. Ta je v primeru ključne infrastrukture, o kateri sprašujete, še posebej velika.
Ocena tveganj in ocena predvidenih učinkov naše revizije sta dva ključna vidika, ki jih upoštevamo pri pripravi našega načrta dela, to je pri odločitvi, koga bomo kdaj revidirali in na katere dele poslovanja bomo še posebej pozorni. Realnost pa je takšna, da lahko zaradi omejenih virov v posameznem letu vedno revidiramo precej manj, kot bi si želeli.

Slovensko združenje za korporativno varnost predstavlja eminentno združbo organizacij in posameznikov s področja korporativne varnosti. Izmenjava dobrih praks in informacij na področju obvladovanja tveganj, kjer so vključena tudi finančna tveganja, bi vsekakor lahko koristila delovanju vaše institucije. Menite, da bi lahko računsko sodišče s svojo priključitvijo tej asociaciji postavilo dober primer sodelovanja v javno-zasebnem okviru?

Na računskem sodišču pozdravljamo vsako pobudo, ki bi lahko prispevala k izboljšanju upravljanja z javnimi sredstvi. Odprti smo za različne oblike sodelovanja, ki omogočajo prenos znanj in izkušenj, seveda ob upoštevanju specifičnih pristojnosti in pooblastil, ki jih imamo/imajo vpleteni. Računsko sodišče že zdaj skuša na različne načine svoje pridobljene izkušnje deliti z drugimi in na ta način še dodatno dvigniti stopnjo zavedanja o pomembnosti dobrega poslovanja z javnimi sredstvi.
Ugotavljamo, da se poslovodstva pogosto ne zavedajo dovolj pomena pravočasnega ocenjevanja tveganj in sprejemanja ustreznih ukrepov za zmanjšanje verjetnosti neželenih dogodkov ali vsaj za zmanjševanje škode ob njihovem pojavu. Če bi se, bi bilo naše delo lahko precej lažje in hitrejše, pa tudi ugotovitve bi bile pogosto manj boleče.

Pred kratkim ste prevzeli eno od ključnih funkcij v okviru Mednarodne nogometne zveze in sicer postali ste vodja komisije za revizijo in skladnost. Če to pogledamo skozi prizmo nedavnih finančnih in korupcijskih škandalov, ki so pretresala to organizacijo je ta vaša vloga še pomembnejša. Kakšni motivi so vas vodili k temu angažmaju?

Angažma definitivno izvira iz veselja do nogometa, vendar so bili prvi kontakti vzpostavljeni prek mednarodnega sodelovanja na revizijskem področju. Ta odgovoren in zahteven položaj sem prevzel, ker predstavlja izjemen izziv sodelovati ne le pri razkrivanju nepravilnosti, ki so se dogajale, temveč tudi pri vzpostavitvi novega načina dela v organizaciji, ki brez dvoma sodi med najvplivnejše na področju športa na svetu. Skupaj z najožjim vodstvom FIFA prenavljamo vse ključne procese in vzpostavljamo sistem zavor in ravnovesij. Vse z namenom, da čim več denarja usmerimo v nogometne programe po celem svetu. Prepričan sem, da nam bo to uspelo, čeprav je pred nami še dolga pot. Pri tem delu s pridom izkoriščam izkušnje pridobljene z dosedanjim delom na področju nadzora porabe (javnih) sredstev. ■

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.



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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

SKUPAJ SMO MOČNEJŠI!

lek član skupine Sandoz

PHILIP MORRIS LJUBLJANA D.O.O.

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

ZARJA ELEKTRONIKA

Elita i.b. d.o.o.

CINKARNA

Slovenske železnice

MARIBORSKI VODOVOD

simobil.si

OBČINA SLOVENSKA BISTRICA

triglav

ELES

NZS NOGOMETNA ZVEZA SLOVENIJE

energetika ljubljana

hse Holding Slovenske elektrarne d.o.o.

TES TERMOELEKTRARNA ŠOŠTANJ

LUKA KOPER Port of Koper

luka d.d.

Republika Slovenija

REISSWOLF secret. service.

Zanesljivo vsepovsod POŠTA SLOVENIJE

interblock LUXURY GAMING PRODUCTS

SIEMENS

TelekomSlovenije

DARS

Nova KBM PRIPRAVLJENI NA JUTRI

univerzitetni klinični center ljubljana

gorenjegroup

si·cert

INFORMACIJSKI POOBLAŠČENEC

www.ics-institut.si

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



KOLUMNA
miran.vrsec@ics-institut.si

O ČEVLJIH SODI NAJ ČEVLJAR

Stari Rimljani so govorili, da naj o čevljih sodi le čevljar. Podobno je želel povedati France Prešeren v svojem sonetu Apel in čevljar, ko je v zadnjem stavku zapisal: »Le čevlje sodi naj Kopitar«. Markus Tullius Cicero, rimski teoretik in filozof pa je zapisal: »Quam Quisque norit artem, in hac se exerceat«, kar v prevodu pomeni: »Vsakdo naj opravlja le tisto kar zna« in s tem nekako povedal bistvo omenjenih misli.

Skupno vsem tem mislim je, da naj delo opravljajo le za to kvalificirane osebe, še posebej menim, da to velja za ljudi, ki ocenjujejo in sodijo o delu drugih. Svoja razmišljanja v tej smeri bom razvil na primeru vožnje motornega vozila kategorije B.

Večina od nas se je v svojem življenju tako ali drugače naučila voziti motorno vozilo kategorije B. In večina od nas je prepričana, da to dejansko tudi zna. Pa vendar to ni zadostni pogoj, da z motornim vozilom kategorije B tudi dejansko lahko upravlja v cestnem prometu. Ta mandat nam je podeljen šele, ko pridobimo veljavno vozniško dovoljenje za vožnjo motornega vozila kategorije B. Pri tem bi želel posebej poudariti, da imamo mandat samo za vožnjo motornih vozil kategorije B in ne tudi za vožnjo motornih vozil drugih kategorij, čeprav tudi to morda celo znamo. Ko vozniško dovoljenje za vožnjo motornih vozil kategorije B iz različnih razlogov ni več veljavno, nam vožnja teh vozil, s trenutkom prenehanja veljavnosti vozniškega dovoljenja, ni več dovoljena, pa čeprav vozilo še vedno znamo voziti. To jasno določa veljavni Zakon o voznikih. In to dejstvo nam je vsem povsem jasno, ga popolnoma razumemo in praviloma tudi spoštujemo. Za to ne potrebujemo posebnih razlag ali prepričevanj, da je temu tako.

Ravno zaradi navedenega dejstva še toliko manj razumem, zakaj temu ni tako tudi na področju zasebnega varovanja, predvsem v delu, ki se nanaša na svetovalne storitve in storitve nadzora kot npr. izdelava ocen ogroženosti, ranljivosti in varnostnih tveganj, optimiziranje varnostnih rešitev v organizacijah, izdelava internih in drugih aktov, ki v organizacijah urejajo področje upravljanja z varnostnimi tveganji, načrtovanje varovanja z izdelavo načrtov in pravil varovanja, organiziranje področja upravljanja z varnostnimi tveganji in na koncu tudi nadziranje izvajanja uvedenih rešitev v praksi. Zakonodaja, ki ureja področja zasebnega varovanja, je prav tako kot zakonodaja, ki ureja področje vožnje motornih in drugih vozil, povsem jasna tudi v delu, ki določa pogoje, ki jih mora izpolnjevati posameznik in tudi pravna oseba, ki se želi ukvarjati z eno od oblik zasebnega varovanja med katere spadajo: varovanje ljudi in premoženja, varovanje oseb, prevoz in varovanje gotovine ter drugih vrednostnih pošiljk, varovanje javnih zbiranj, varovanje prireditev v gostinskih lokalih, upravljanje z varnostno-nadzornim centrom, načrtovanje sistemov tehničnega varovanja in izvajanje sistemov tehničnega varovanja. Ja, za-

Pri tem se mi zastavlja vprašanje materialne in kazenske odgovornosti posameznikov, ki na tak nezakonit način izvajajo nadzor in podajajo svoja »strokovna« mnenja. Verjetno bi bilo to vprašanje zanimivo tudi za zavarovalnice, ki včasih izplačujejo vrtoglave odškodnine za škodne dogodke, do katerih oškodovanci, tudi zaradi nezakonito izvedenih pregledov, morebiti sploh niso upravičeni.

*avtor je član Slovenskega združenja korporativne varnosti

konodaja je jasna, v praksi pa je situacija žal povsem drugačna. Če nam je na eni strani povsem jasno, da vožnja motornih vozil kategorije B brez veljavnega vozniškega dovoljenja, kljub našemu zadostnemu znanju o vožnji teh vozil, ni dovoljena, pa na področju zasebnega varovanja temu ni tako. Imamo kar nekaj strokovnjakov, ki se, ali pa so se v svoji poklicni karieri bolj ali manj neposredno ali celo samo posredno ukvarjali s problematiko varnosti v gospodarskih in drugih družbah, sedaj pa kot samostojni strokovnjaki ali pa skriti pod okrilje pravnih oseb ponujajo storitve svetovanja, projektiranja, načrtovanja in nadziranja posameznih varnostnih področij. Če se večina vpraša, ali to znajo, pa se praviloma le redki vprašajo, ali to počnejo zakonito, odgovorno in na primerni strokovni ravni.

Za lažje razmišljanje bom izpostavil dve od sicer širokega nabora področij, kjer je tovrstna problematika še izjemno aktualna. Prvo se nanaša na sicer že preklicani sklep Sveta Banke Slovenije o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, ki je med drugim določal pogoje za izvajanje nadzora varovanja v bankah. Večina preglednikov ni izpolnjevala pogojev za izvajanje tovrstnih pregledov, ne glede na dejstvo, da so s strani Zbornice RS za razvoj slovenskega zasebnega varovanja prejeli pooblastilo za izvajanje omenjenih pregledov. Ker niso posedovali veljavne službene izkaznice za varnostnega menedžerja, niso imeli zakonske podlage za izvajanje tovrstnih pregledov. Takšni pregledi, in teh je bila velika večina, so bili torej izvedeni nezakonito in kot taki niso imeli nobene formalne veljave. Tudi po preklicu omenjenega sklepa Sveta Banke Slovenije sem prepričan, da se omenjeni pregledi v nekaterih bankah še izvajajo na podoben način. Pri tem se mi zastavlja vprašanje materialne in kazenske odgovornosti posameznikov, ki na tak nezakonit način izvajajo nadzor in podajajo svoja »strokovna« mnenja. Verjetno bi bilo to vprašanje zanimivo tudi za zavarovalnice, ki včasih izplačujejo vrtoglave odškodnine za škodne dogodke, do katerih oškodovanci, tudi zaradi nezakonito izvedenih pregledov, morebiti sploh niso upravičeni. To pomeni, da bi se tudi zavarovalnice morale zavedati tovrstnih varnostnih in odškodninskih tveganj.

Drug primer, ki je v praksi splošno razvit in se ga vsaj po mojem vedenju do sedaj še nihče ni lotil reševati, je nadzor nad načrtovanjem in izvajanjem sistemov tehničnega varovanja. Gre za dve ločeni, a medsebojno povezani področji zasebnega varovanja, nad katerimi praviloma v času gradnje objektov ali adaptacij objektov izvajajo nadzor gradbeni nadzorniki. Iz vidika zakonodaje, ki ureja področje gradnje objektov, to ni sporno, je pa še kako sporno z vidika zakonodaje, ki ureja področje zasebnega varovanja. Tudi v tem primeru podjetja, ki izvajajo tovrstni nadzor ne posedujejo potrebnih licenc, posamezniki pa ne potrebnih službenih izkaznic. Tudi za tovrstne nadzore bi lahko rekli, da so nezakoniti in kot taki neveljavni. O tem problemu bi moral razmišljati menedžment zasebnega varovanja in nadzorniki kompetentni za področje zasebnega varovanja.

Lahko bi še in še našteval podobne primere, vendar povedano zadostuje za potrebe tokratne kolumne. Z mojimi razmišljanji želim le opozoriti na neurejenost področja svetovanja in nadziranja ter nerazumevanje oziroma nezmožnost razumevanja nekaterih ključnih vpletenih v to problematiko. Za omenjeni problem so v veliki meri krivi tudi državni nadzorni mehanizmi, predvsem Inšpektorat RS za notranje zadeve, ki svoje aktivnosti usmerja predvsem v nadzorovanje podjetij z licencami, ki se ukvarjajo z varovanjem ljudi in premoženja, varovanjem javnih zbiranj in varovanjem gostinskih lokalov, kar je verjetno enostavneje, kot loviti na terenu tiste posameznike in podjetja, ki nimajo dovoljenj za opravljanje svetovalnih in nadzornih storitev, pa to zelo na veliko in za visoke pogodbene vrednosti kljub temu opravljajo.

Za omenjeni problem so v veliki meri krivi tudi državni nadzorni mehanizmi, predvsem Inšpektorat RS za notranje zadeve, ki svoje aktivnosti usmerja predvsem v nadzorovanje podjetij z licencami, ki se ukvarjajo z varovanjem ljudi in premoženja, varovanjem javnih zbiranj in varovanjem gostinskih lokalov, kar je verjetno enostavneje, kot loviti na terenu tiste posameznike in podjetja, ki nimajo dovoljenj za opravljanje svetovalnih in nadzornih storitev, pa to zelo na veliko in za visoke pogodbene vrednosti kljub temu opravljajo.

Moja razmišljanja bom zaključil z mislijo, ki ima izhodišče v uvodno napisanih mislih Rimljanov, Prešerna in Cicera: »Naj se z varnostjo ukvarjajo za to kompetentni in licencirani strokovnjaki, saj bo v nasprotnem primeru varnost postala nevarnost«. Ali drugače povedano: Če ne bomo obvladovali varnostnih tveganj se lahko kaj hitro zgodi kaj nepredvidenega, šokantnega in škodljivega za ljudi, premoženje in vrednote. Zato je že čas, da damo besedo izobraženim ter z znanjem, izkušnjami in dobro prakso pripravljenim strokovnjakom, ki vedo kaj počnejo. Le na ta način bodo naročniki varnostnih storitev pridobivali dodano vrednost v procesih upravljanja korporativne varnosti. To še posebno velja za posodabljanje varnostnih sistemov v kritični infrastrukturi državnega pomena. ■



Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
mag. Karol Turk, svetovalec predsednika uprave za korporativno varnost

KORPORATIVNA VARNOST POSTAJA POMEMBEN DEL MEDNARODNIH KORPORACIJ

Gorenje d.d. postaja s svojim širjenjem poslovanja globalna korporacija, ki je izpostavljena celemu nizu tveganj katerega pred njo postavlja dinamično varnostno okolje. Korporativna varnost s tem postaja pomembno orodje v rokah strateškega managementa, ki mu omogoča učinkovitejše obvladovanje varnostnih in drugih s tem povezanih tveganj.

Korporativna varnost je zelo pomembna nit vaše poslovne kariere. Nam lahko poveste katera so ključna področja pristojnosti korporativne varnosti v vaši organizaciji?

Z vidika varnosti so pristojnosti razpršene na različne segmente korporativne varnosti. Ključni element so seveda pooblastila, ki jih ima določena oseba za izvajanje nalog. V smislu varnosti družbe je primarna naloga fizično in tehnično varovanje matične družbe in družb v tujini. S strateškega vidika pa je pomembna vključenost v vse sfere varnostne politike družbe, ki je določena s krovno varnostno politiko. Aktivnosti se izvajajo tako v smislu preventivnega kot kurativnega vidika na področju informacijske varnosti, ocene tveganj, notranje preiskave, skratka spremljanje in analiziranje vseh varnostnih pojavov, ki bi lahko negativno vplivali na delovanje družbe.

Gorenje d.d. predstavlja globalno korporacijo, ki ima sedež v Republiki Sloveniji. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Vsak poslovni sistem je izpostavljen različnim tveganjem. Družba Gorenje ima vzpostavljen oddelek za upravljanje s tveganji, ki ima vzpostavljena ustrezna orodja za upravljanje s tveganji. Politika upravljanja s tveganji je vzpostavljena v vseh poslovnih procesih Skupine Gorenje z namenom doseganja strateških in operativnih ciljev. Tveganja, kot tudi skladnost tveganj se neprestano meri, spremlja in dopolnjuje na podlagi parametrov tveganj določenih v katalogu tveganj. Ključna so seveda finančna tveganja, tržna tveganja, tveganja delovanja ter tveganja ugleda in dobrega imena. Organizacijsko je oddelek umeščen na področje, ki ga pokriva član uprave za ekonomiko in finance.



Politika upravljanja s tveganji je vzpostavljena v vseh poslovnih procesih Skupine Gorenje z namenom doseganja strateških in operativnih ciljev.

*avtor je član Slovenskega združenja korporativne varnosti



V Sloveniji se osebe, ki so zadolžene za strateško načrtovanje in izvajanje procesa korporativne varnosti zelo redko nahajajo na prvem nivoju odločanja oz. v njegovi bližini. Primerljiva praksa v mednarodnem okolju pa kaže ravno v smeri te potrebe, saj je zaradi dinamičnosti varnostnega okolja, vedno težje zagotavljati ustrezen celovit pristop do obvladovanja tveganj za organizacijo. Menite, da bo to počasi postala praksa tudi v slovenskem prostoru?

Že ustaljene dobre prakse v tujini se z določenim časovnim zamikom uvajajo tudi v Sloveniji, čeprav je Slovenija imela že v preteklosti izgrajen kakovosten varnostni sistem, ki je bil vzročni model za tujino. Celovit in sistematičen koncept varnosti je v teh turbulentnih časih nujno potreben in menim, da se tega počasi zavedajo vsi tisti, ki se zavedajo svoje družbene odgovornosti. Tako v resnih in uspešnih družbah varnost ni več sekundarnega pomena temveč postaja ključni del poslovnega procesa družbe.

Celovit in sistematičen koncept varnosti je v teh turbulentnih časih nujno potreben in menim, da se tega počasi zavedajo vsi tisti, ki se zavedajo svoje družbene odgovornosti. Tako v resnih in uspešnih družbah varnost ni več sekundarnega pomena temveč postaja ključni del poslovnega procesa družbe.

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

V kolikor se strateški management zaveda svoje odgovornost in obstaja jasna vizija razvoja družbe ter je projekt kakovostno pripravljen, z vsemi pozitivnimi in negativnimi vidiki potem finančna sredstva ne morejo biti ovira za izvedbo projekta. V Gorenju poteka kar nekaj projektov in moram poudariti, da ima predsednik in uprava družbe izreden posluh za realizacijo pripravljenih projektov.

V zadnjem obdobju so se v vašem podjetju najavile pomembne spremembe v lastniški strukturi. Nam lahko zaupate kako pomemben je v takih primerih učinkovit sistem varovanja ključnih poslovnih informacij.

Lastniška struktura družbe Gorenje zaenkrat ostaja nespremenjena, kako bo v prihodnje pa so lahko samo špekulacije. Dejstvo je, da je uhajanje zaupnih informacij iz različnih družb in institucij vseslovenski problem oz. slovenski šport.
Družba Gorenje ima izgrajen standardiziran poslovno informacijski sistem, vendar tako kot v vsakem sistemu je tudi v tem kakšna vrzel.



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

Pogosto poudarjam, da brez varnosti ni razvoja individuma, še manj pa družbe v takšni ali drugačni obliki. Vsak vložek v varnost sicer predstavlja strošek, ki je lahko za nekoga nepotreben, dejansko pa se ob nepredvidenem negativnem dogodku lahko obrestuje na kvadrat. Različna kazniva dejanja storjena v škodo družbe, neupoštevanje ocene tveganj v poslovnih procesih lahko povzročijo stečaj družbe, kar je bilo za Slovenijo značilno v preteklosti. Osebno menim, da se vsi deležniki v poslovnih procesih bolj ali manj zavedajo svoje družbene odgovornosti in da upoštevajo tveganja pri poslovanju. Ne smemo pa zanemariti, da je v poslovnem svetu tveganje spremljajoč pojav vsakega posla in da je od ocene tveganja odvisna odločitev o izvedbi posla. Skratka upravljanje tveganj je ključna funkcija s katero se mora ukvarjati strateški management.

Kako so po vašem mnenju pomembne ključne informacije korporacije v konkurenčni tekmi za uspešno poslovanje na globalnem tržišču. Ali temu področju v Gorenju namenjate veliko pozornost?

Informacija je ključni element pri vseh odločitvah in v tem kontekstu ni izvzeta tudi konkurenčna prednost. Vsaka tehnološka izboljšava produkta ali nov produkt, ki se pojavi na trgu pred konkurenco ima boljšo prodajno izhodišče, seveda ob podpori dobrega marketinga. Z vidika konkurenčnosti je tako ključni element za vsako razvojno družbo varovanje intelektualne lastnine in v Gorenju temu segmentu dajemo velik poudarek že v procesu izobraževanja zaposlenih. Samo osvečeni zaposleni lahko gradijo visoko varnostno kulturo in s tem posledično vplivajo na nižjo stopnjo kraje intelektualne lastnine. Skratka, vrednote podjetja, inovativnost in vizija je tisto, kar ločuje uspešna podjetja od manj uspešnih.

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

Izobraževanje in usposabljanje je vse življenjski proces in vsak vložek v izobraževanje se podvoji. Ob hitrih spremembah na vseh področjih pa je vsak vložek v posameznika še toliko bolj pomemben.

Pred dvema letoma se je začel izvajati podiplomski magistrski program »management korporativne varnosti«, ki ga v soorganizaciji pripravljata Institut za korporativne varnostne študije – ICS in GEA College - Fakulteta za podjetništvo. Menite, da je to prava pot za uveljavljanje stroke in predvsem za izobraževanje strokovnjakov s področja korporativne varnosti v Republiki Sloveniji?

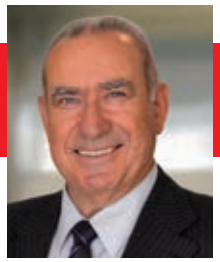
Dejstvo je, da različne fakultete ponujajo različne študijske programe in s tem producirajo različne profile varnostnih menedžerjev. V kolikor želimo interdisciplinaren profil z vidika korporativne varnosti potem je vsekakor potrebno iskati strokovnjake te smeri izobraževanja. Poudariti pa želim, da je pridobljena izobrazba samo vstopnica za določen klub, zatem pa je potrebno delo.

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

Izmenjava mnenj, dobre prakse, strokovna združenja imajo lahko samo pozitivne učinke, saj lahko tako ustvarjamo neko dodano vrednost za družbo, ki ji pripadamo in za lasten razvoj. ■

Ne smemo pa zanemariti, da je v poslovnem svetu tveganje spremljajoč pojav vsakega posla in da je od ocene tveganja odvisna odločitev o izvedbi posla. Skratka upravljanje tveganj je ključna funkcija s katero se mora ukvarjati strateški management.

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





RANLJIVOST, VARNOSTNE GROŽNJE IN VARNOSTNA TVEGANJA SI PODAJAJO ROKE

Namen tega prispevka je povedati nekaj o pristopu k obvladovanju varnostnih sprememb, varnostnih groženj, varnostnih tveganj in ranljivosti organizacij, pri čemer je poudarek na njihovi medsebojni povezanosti in soodvisnosti. Gre namreč za pomemben segment v ocenjevanju stanja varnosti na ravni države, subjektov kritične infrastrukture, gospodarstva in civilne družbe.

Če želimo oceniti realno stanje nacionalne varnosti, varnosti subjektov kritične infrastrukture, varnosti gospodarskih in drugih družb in varnosti državljanov, pač ne gre drugače, kot da se poglobimo v vse dejavnike, ki vplivajo na stanje varnosti. Ti dejavniki pa so: **varnostna ranljivost** državnih institucij, subjektov kritične infrastrukture, gospodarstva in civilnih institucij, **varnostne spremembe** v realnem času, prikrite, potencialne in realne **varnostne grožnje** kot mehanizem ustrahovanja in negotovosti ter **varnostna tveganja**, ki jih vodstva, upravljavci in nadzorniki v procesih odločanja vse prevečkrat postavljajo na stranski tir. Varnostni strokovnjaki se dobro zavedajo, da je to **varnostna napaka** tistih, ki bi morali že na strateški ravni skrbeti za čim boljšo varnost premoženja, procesov in človeških virov. V tem kontekstu bi se moral vsaj menedžment korporativne varnosti v organizacijah zavedati in imeti znanje o celovitem obvladovanju varnostnih tveganj, ki se prične pri ugotavljanju ranljivosti, nadaljuje v prepoznavanju varnostnih sprememb in varnostnih groženj in naposled v upravljanju varnostnih tveganj. Prav tako je pomembno zavedanje varnostnega menedžmenta organizacije, da je potrebno z upravljavskega vidika z varnostjo upravljati tako na strateški, kot tudi operativni ravni, z geopolitičnega vidika pa tako v makro, kot tudi mikro okolju. Gre torej za varnostno verigo v kateri so zgoraj navedeni segmenti varnosti v tesni povezavi in v medsebojni odvisnosti. Potrebno je samo malo miselnega preskoka, da se to spoznanje uporabi v procesih ocenjevanja stanja varnosti na ravni države, subjektov kritične infrastrukture, gospodarstva in civilne družbe.

Varnostna ranljivost kot opozorilni sistem za varnostne in druge izboljšave

Vsaka organizacija je v določeni meri ekonomsko, poslovno, socialno in varno-

> Varnostno ranljive so tiste organizacije, ki ne upoštevajo zakonskih določil, nimajo profesionalno izdelanih varnostnih ocen in varnostnih politik, ki ne uvajajo varnostnih standardov, ki nimajo izdelanih načrtov fizičnega in tehničnega varovanja, varnostnih navodil, ki se resno ne lotijo urejanja notranjega pravnega reda (pravilniki), potrebnega za upravljanje korporativne varnosti, ki nimajo vzpostavljenih notranjih in zunanjih nadzornih mehanizmov in ki nimajo vzpostavljenega sistema uvajanja stalnih izboljšav v varnostnih procesih.

*avtorja sta člana Slovenskega združenja korporativne varnosti



stno ranljiva. Ugotavljanje ekonomske in poslovne ranljivosti je možno z metodiko SWOT (prednosti, slabosti, priložnosti, nevarnosti poslovanja), BSC (uravnoteženi finančni in drugi kazalniki poslovanja), sistemom 20 ključev (analiza 20 področij poslovanja) in drugimi podobnimi poslovnimi orodji. Ugotovljene slabosti in nevarnosti v poslovanju (slaba organiziranost, nagnjenja h korupciji in kriminalu, odsotnost varnostne kulture in poslovne etike, itd.) so pokazatelj ranljivosti poslovnih procesov, s tem pa tudi eden od virov podatkov za ugotavljanje varnostne ranljivosti. V tem kontekstu je torej za našo razpravo pomembna **varnostna ranljivost,** ki se izraža v tem, da imajo varnostni sistemi organizacij varnostne luknje oziroma **varnostne vrzeli**, ki na lahek način omogočajo kraje, vlome, vdore in druga škodljiva ravnanja. Ranljivost kot pomemben segment pri ocenjevanju varnosti lahko opredelimo v obrazcu R= f (C, V, T), ki pove, da je varnostno tveganje odvisno od groženj (Threat), ranljivosti (Vulnerability) in posledic (Consequence) (Chertoff, 2009). Varnostno ranljive so tiste organizacije, ki ne upoštevajo zakonskih določil, nimajo profesionalno izdelanih varnostnih ocen in varnostnih politik, ki ne uvajajo varnostnih standardov, ki nimajo izdelanih načrtov fizičnega in tehničnega varovanja, varnostnih navodil, ki se resno ne lotijo urejanja notranjega pravnega reda (pravilniki), potrebnega za upravljanje korporativne varnosti, ki nimajo vzpostavljenih notranjih in zunanjih nadzornih mehanizmov in ki nimajo vzpostavljenega sistema uvajanja stalnih izboljšav v varnostnih procesih. Takšno stanje v določeni gospodarski družbi ali v drugi organizaciji pomeni alarm za vodstvo in za menedžment korporativne varnosti, da se z varnostnimi, organizacijskimi, kadrovskimi in drugimi izboljšavami loti reorganizacije varnostnega sistema.

Varnostne spremembe z izrednimi dogodki

Področje varnosti je izredno dinamično. Vsakodnevno se dogajajo varnostne spremembe, ki se izražajo s t.i. izrednimi dogodki. Odmevni so izredni dogodki večjega obsega, ki vnesejo v vsakodnevno relativno mirno delo, obratovanje, poslovanje in življenje nemir, preplah, strah, negotovost, tveganje, ali celo šok, paniko, grozo in obup. Situacija je toliko hujša, če določene državne institucije, subjekti kritične infrastrukture, gospodarske družbe in civilne (nevladne) organizacije niso na kaj takega pripravljene. Med izredne dogodke velikih razsežnosti in posledic uvrščamo: potrese, povodnji, orkane, tornade, ciklone, viharje, obilne padavine, letalske, rudniške, železniške in cestnoprometne nesreče, večje vlome in roparske napade, teroristična dejanja, »električne mrke«, razlitja ogromnih količin nevarnih snovi v morje, vodovje ali v zemljo (ogrožanje podtalnice), velike gozdne požare in požare ter eksplozije na industrijskih objektih in objektih z velikim številom ljudi (poslovne zgradbe, kinodvorane, gostinski lokali, hoteli, gledališča, športna igrišča, vlaki, avtobusi), itd. Posledice vsakega izrednega dogodka so praviloma neugodne, ker se izražajo v materialni, finančni, poslovni, človeški in moralni škodi in hkrati izgubi. Če so materialne, finančne, poslovne, obratovalne (proizvodne) in človeške posledice šokantne, opredelimo tak dogodek kot havarijo oziroma katastrofo. Vsak izredni dogodek velikega obsega je treba razreševati po načrtu odzivanja na katastrofe. V manjšem ali večjem obsegu je v prihodnje treba računati na varnostne spremembe pri naslednjih izrednih dogodkih:



- naravne nesreče (potresi, poplave, viharji, plazovi, obilne padavine, idr.),
- industrijske nesreče (eksplozije, kemična izlitja, požari, tehnološke okvare, delovne nesreče, okoljske nesreče),
- bombne grožnje, sabotaže, izgredi, stavke,
- teroristični napadi na kritično infrastrukturo in na druge tarče (bombne grožnje, eksplozije, strelski napadi idr.),
- kriminalna dejanja (vlomi, ropi, goljufije, korupcija, zlorabe, poneverbe, gospodarsko vohunstvo, kraje, ugrabitve, utaje),
- interesni konflikti (zlorabe informacij, poslovne goljufije, motnje v sistemih plač, socialne bombe, idr.),
- družbena deviantnost posameznikov ali manjših skupin,
- nuklearne nesreče.

Na nekatere navedene varnostne spremembe je možno preventivno vplivati vsaj v toliki meri, da ne pride do izrednih dogodkov nepredstavljivih (apokaliptičnih) razsežnosti. V tej smeri bi morale biti pripravljene državne interventne institucije (policija, zaščita in reševanje, gasilstvo, vojska), interne varnostne službe in zasebno varovanje, ki trži varnostne storitve. Posebno varnostno pozornost bi morali nameniti kritični infrastrukturi državnega pomena.

Varnostne grožnje kot mehanizem ustrahovanja

Vsaka varnostna grožnja je resen ustrahovalni dogodek, ki terja razumen odziv tistega, ki grožnjo sprejme in od vseh, ki so vpleteni v razreševanje grožnje. Podatki preteklih let povedo, da so grožnje raznim podjetjem državnim institucijam (denimo sodiščem) in posameznikom na dnevnem redu. Problem pa je v tem, da ni prave metodologije, ki bi zagotavljala transparenten pregled števila, strukture in moči groženj. Na tem mestu se bomo zadovoljili z osnovnim pristopom k sprejemanju grožnje in odzivom nanje. Postopek upravljanja z varnostno grožnjo-potrebni podatki, je po našem predlogu naslednji:

- **ugotovitev tipa grožnje** – grozi neznana oseba ali neznana organizacija
- **kdo sporoča grožnjo (kdo grozi, ogroža)** - anonimna oseba, anonimna organizacija, znana oseba, znana organizacija
- **komu je namenjena grožnja** – splošna grožnja, grožnja znani osebi, ali znani skupini ali znani organizaciji
- **namen grožnje** – uboj, umor, telesna poškodba (fizični napad), grožnja družinskim članom (napad, ugrabitev), grožnja z eksplozivom (eksplozija), grožnja z nesrečo v prometu, grožnja izgube delovnega mesta, grožnja kraje oziroma tatvine nekega sredstva, grožnja s požarom, idr.
- **način grožnje** – neposredno osebno, po klasičnem telefonu, po mobilniku, elektronska pošta, pismo, grožnja posredno po drugi osebi
- število groženj – enkrat, dvakrat, večkrat
- **datum in ura grožnje** – podnevi, ponoči
- **lokacija grožnje** (povsem znana, domnevno znana, neznana)
- **odziv osebe, ki je sprejela grožnjo** - izpolni določen obrazec, ali kako drugače zapiše ali si zapomni sporočilo o grožnji, takojšnje obveščanje VNC in glavnega managerja korporativne varnost, takoj preštudira navodilo za

Posledice vsakega izrednega dogodka so praviloma neugodne, ker se izražajo v materialni, finančni, poslovni, človeški in moralni škodi in hkrati izgubi.



primer grožnje, takoj obvesti osebe, ali oddelek ali organizacijo na katero se grožnja nanaša (če to ne stori VNC)
- **odziv managementa korporativne varnosti**-odziv mora biti takojšen
- **odziv policije** -zabeleži se čas odziva in ukrepanje ter rezultati ukrepanja
- **uresničena grožnja** eksplozija, napad, ugrabitev, idr.– čas, kraj, kdo je domnevno uresničil grožnjo, policijski in kriminalistični ogled, posledice, ukrepanje zaščite in reševanja ter gasilcev (če je potrebno), zdravstvena in socialna oskrba, idr.

Po vsaki grožnji sledijo previdnostni ukrepi ogrožene osebe ali ogrožene organizacije, tako v bivalnem okolju, delovnem in poslovnem okolju ter v okolju gibanja. Tako se lahko zgodi, da se bo – poleg previdnostnih ukrepov zaradi grožnje - okrepilo tudi fizično in tehnično varovanje ogrožene osebe ali ogrožene organizacije.

Celovito obvladovanje varnostnih tveganj

Kaj sploh je varnostno tveganje? Enostavna definicija je naslednja: Varnostno tveganje pomeni, da se bo lahko zgodilo nekaj škodljivega, če v varnostni sistem ne uvedemo potrebne varnostne ukrepe in varnostne standarde, hkrati pa tudi pomeni, da smo varnostno ranljivi. Najprej poglejmo s katerimi vrstami varnostnih tveganj se je treba spopadati v gospodarskih in drugih družbah. Najbolj prisotna so naslednja varnostna tveganja: tveganja naravnih, okoljskih in drugih nesreč, tveganja delovnih nesreč, požarna tveganja, informacijska tveganja, kriminalna tveganja, teroristična tveganja, vohunska tveganja (Carnivore, Echelon), tveganja iznosa in izdaje zaupnih podatkov in dokumentov in druga varnostna tveganja. V zadnjem času so vse bolj v ospredju tudi socialna tveganja, ki se izkazujejo tudi v raznih pojavnih oblikah družbene deviantnosti, kot posledici vse večjih družbenih in socialnih neenakosti (napadi na državne uradnike, policiste, zdravnike, uspešne posameznike, uživanje nedovoljenih substanc in alkohola ipd.). Gre torej za široko paleto varnostnih tveganj, ki zares terjajo profesionalen pristop k njihovemu obvladovanju. Morda je tudi to razlog, da se v gospodarskih in drugih družbah otepajo varnostnih tveganj, ker pač ni znanja, dobre prakse in ustrezne metodologije obvladovanja tveganj. Uporabiti pa je potrebno vsaj nekaj osnovnih pristopov k analizi, kontroli in izravnavanju varnostnih tveganj, kar je prikazano v spodnji sliki (Vršec, 2008). Posebej je treba opozoriti, da je celovito obvladovanje varnostnih tveganj možno le, če nekatera varnostna tveganja (denimo požarna) zavarujemo pri zavarovalnicah za določeno zavarovalno premijo. To pomeni, da si je treba ustvariti ustrezen zavarovalni portfelj, ki bo skupaj z varnostnim sistemom tvoril učinkovito upravljanje korporativne varnosti. Pri tem je potrebno poudariti, da je pri izgradnji varnostnih sistemov in uvajanju varnostnih rešitev v poslovne procese organizacije upoštevamo zavarovalne pogoje, saj v nasprotnem primeru ob nastanku škode izgubimo vse zavarovalne pravice.

Znana in v praksi uporabljena pa je še vrsta drugih metod obvladovanja tveganj kot so denimo: PRA Rapid Risk Assessment (Metoda za hitro oceno tveganj), PHA Preliminary Hazard Analysis (Metoda za predhodno analizo tveganj), MOSAR Method for a Systemic of Risk (Metoda za sistemsko analizo tveganj), Business Impact Analysis (BIA analiza - ISO 27001) in druge. Za potrebe obvladovanja varnostnih tveganj v gospodarskih in drugih družbah pa je izdelana (izvirna) podrobnejša metodologija, ki jo bosta avtorja tega prispevka morda obelodanila kdaj pozneje.

Varnostna prihodnost

Ko premišljujemo o nekajletni varnostni preteklosti in varnostni sedanjosti nam misli uhajajo v varnostno prihodnost, ki najbrž ni postlana z rožicami. Vedno več je naravnih in ekoloških nesreč, terorizem se je intenzivneje začel razraščati tudi v Evropo, migrantski tokovi v Evropske dežele bodo (po napovedih) potekali v milijonih, nič pa tudi ne kaže, da bi suvereno obvladovali kriminal in korupcijska tveganja. Obeta se torej klavrna podoba prihodnje varnosti, v kateri se v vsakdanje življenje, delo in poslovanje vrašča **aktualna varnostna paradigma,** ki pravi: na vsakem koraku živeti z mislijo na (ne)varnost. Morda to ne velja povsod. Slovenija je namreč neogrožena in varna država. Vsaj tako nenehno oznanjajo uradne izjave. Upamo in si tudi želimo, da bi ta varnostna ocena vzdržala čim dlje.

Viri

- Chertof, M., Hamilton, L.M. (2009). Homeland Security. University of Pennsylvania Press.
- Vršec, M. (2008). Redefiniranje ranljivosti in ogroženosti podjetij z izvirnim metodološkim pristopom (Redefining the vulnerability and threat to companies with an authentic methodological approach). V: Rajkovič Vladislav (ur.). 27. mednarodna znanstvena konferenca o razvoju organizacijskih znanosti. Znanje za trajnostni razvoj. Portorož, 19.-21. marec 2008. Zbornik. Kranj. Moderna organizacija, str. 3061-3074. ■



Elesovi ambasadorji vrednot so: Jakov Fak, kolesarke ekipe BTC City, Miha Podgornik, Atletska zveza Slovenije, Benjamin Savšek in Marin Medak.

PRENAŠAMO ENERGIJO. PRENAŠAMO VREDNOTE.

Energija teče, skupaj z nami. Ker 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 sogradimo 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.

www.eles.si

ELES

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



KRITIČNA INFRASTRUKTURA IN TVEGANJA STEČAJNIH POSTOPKOV

V zadnjem obdobju ugotavljamo, da je varnostno okolje vse bolj kompleksno in nepredvidljivo. Tudi Republika Slovenija ni imuna na vse vplive, ki jih prinašajo grožnje in tveganja. Stečajni postopki z neurejenimi procesi lahko zelo hitro pripeljejo do porasta tveganj za nemoteno delovanje kritične infrastrukture.

Dnevno poslušamo novice, ki nas v zvezi z delovanjem nacionalno-varnostnega sistema presenečajo, če ne kar šokirajo. Ob načrtnemu varčevanju in zatiskanju pasu v tistih vitalnih subjektih nacionalno-varnostnega sistema je danes pravzaprav tragikomično, da poslušamo strateško politično vodstvo, ki trdi, da je stanje normalno in obvladljivo. Žalostno je namreč dejstvo, da se politika ne zaveda pomena temelja, ki ga za obstoj in delovanje te države predstavlja nacionalna varnost ter institucije, ki zagotavljajo našo varnost in ozemeljsko celovitost.

Ob tragičnih novicah, ki jih v zadnjem obdobju pred nas postavlja življenje je nekako neopazno in brez velikega odziva v začetku leta odjeknila novica o stečaju gospodarske družbe, katera naj bi upravljala pomembno informacijsko infrastrukturo. Na to novico pa se razen strokovne javnosti ni odzval praktično nihče. Še posebno se ni zdramila in zganila Vlada republike Slovenije z vsem mehanizmom, ki bi moral skrbeti za nemoteno delovanje kritične infrastrukture. Preden si odgovorimo na vprašanje ali je res možno, da se v stečaju znajde organizacija, ki upravlja kritično infrastrukturo in predvsem, da del stečajne mase postane kritična infrastruktura, pojasnimo nekaj ključnih dejavnikov.

Kritična infrastruktura je nujna za zagotavljanje nemotenega delovanja širše družbene skupnosti. Poleg terorističnega ogrožanja, kibernetskih, kriminalnih in drugih tveganj so kritični infrastrukturi predstavljale pomembno tveganje tudi naravne nesreče, katerim se nismo izognili niti v Sloveniji. Spomnimo se samo žleda in poplav, ki sta nas v tistem trenutku resno opomnila kako pomebna je kritična infrastruktura za normalno funkcioniranje družbe. Država ima nalogo, da uredi ustrezno normativno okolje s katerim se opredeli kateri deli nacionalne infrastrukture sodijo v kritični del. Del te infrastrukture ima zaradi svoje soodvisnosti in vpetosti tudi mednarodne učinke na sosednje države. Pomembno je poudariti še, da določene države kritično infrastrukturo razdelijo v posamezne podsektorje, ki so procesno, vsebinsko in tehnološko zaključene celote. V tem okviru je potrebno posebej izpostaviti podsektorja proizvodnje in prenosa električne energije in komunikacijsko-informacijske tehnologije. Si danes sploh lahko zamišljamo normalno funkcioniranje družbe brez električne energije in delovanja informacijske tehnologije? Iz primera nesreče z žledom, kjer sta bila zelo onemogočena ravno ta dva sektorja in je bil pomemben del države brez električne energije, posledično pa tudi brez ustrezno delujoče informacijske in komunikacijske tehnologije, lahko hitro ugotovimo, da je stvar veliko bolj resna, kot si jo predstavljajo politiki in za to zadolženi uradniki po posameznih ministrstvih. V tem delu lahko z vso strokovno gotovostjo zatrdimo, da Vlada Republike Slovenije in njene za to pooblaščene strukture niso opravile svoje domače naloge. Tudi v tem primeru se kaže birokratski pristop nerazumevanja realnih problemov in neodzivanje na potrebe realnega okolja. Vzpostavljanje celovitega in dobro delujočega nacionalnega sistema kritične infrastrukture in zagotavljanje neprekinjenosti njenega delovanja je stihijsko, nesistemsko in absolutno prepočasno. S tem pa seveda ne ogrožamo samo Republike Slovenije temveč se tudi v tem primeru pojavljamo kot nezanesljiv dejavnik mednarodnega okolja, ki ne izvaja ustreznih ukrepov za celovito obvladovanje tveganj.

Za pravilno razumevanje tega problema pa je potrebno izpostaviti še javno zasebno-partnerstvo, ki je v primeru delovanja kritične infrastrukture ključ-

*avtor je član Slovenskega združenja korporativne varnosti

ni dejavnik. Privatizacijski procesi in prehajanje lastnine v zasebno poslovno upravljanje je pomembno povečalo del zasebnih lastnikov, ki upravljajo s kritično infrastrukturo. Seveda smo na žalost tudi do vzpostavitve trdnega javno-zasebnega partnerstva pristopili samo z birokratskim pristopom, kjer nikakor niso vzpostavljene ustrezno delujoče sinergije. Obema partnerjema v tem procesu mora biti v interesu neprekinjeno delovanje kritične infrastrukture. Državi zaradi neprekinjenosti delovanja in zagotavljanja nemotenega delovanja družbe, zasebnemu lastniku pa ta neprekinjenost in varnost delovanja prinaša ustrezen dobiček in zagotavljanje osnovnega poslovnega poslanstva organizacije. Seveda je v tej interakciji še vrsta dejavnikov, ki so s stališča države zelo pomembni in imajo lahko v posameznih primerih resen vpliv na zagotavljanje nacionalne varnosti. Lastništvo v organizacijah, ki upravlja s kritično infrastrukturo, bi moralo s tega vidika še kako zanimati državo, predvsem s stališča nacionalne varnosti in zagotavljanja neprekinjenosti delovanja ključnih procesov. V tem okviru je informacijsko komunikacijska tehnologija še posebej izpostavljen podsektor kritične infrastrukture. Kriteriji za določitev kritične infrastrukture so pripravljeni zelo pavšalno in niso bili predhodno simulirani in analizirani. Ta argumentacija kaže tudi na dejstvo, da ravno s tega stališča ni mogoče z gotovostjo oceniti ali so trenutno določena kritična infrastruktura in organizacije, ki z njo upravljajo, sploh realno opredeljene. Na nacionalnem posvetu v Državnem Svetu Republike Slovenije, ki je potekal v mesecu maju 2016, je bilo ugotovljeno, da Republika Slovenija zamuja z implementacijo in pripravo ustreznih zakonskih in sistemskih rešitev na področju zaščite kritične infrastrukture. Vsekakor bo potrebno narediti dodatne napore pri jasni opredelitvi kateri infrastrukturni deli, procesi in storitve so tista nujna kritična infrastruktura, ki je potrebna za nemoteno delovanje širše družbene skupnosti. Jasni in metodološko preverjeni kriteriji za določitev kritičnosti posamezne infrastrukture so tisti, ki bodo zmanjševali dvom o tem kaj sploh je kritična infrastruktura. Seveda pa je potrebno jasno zavedanje, da normativnim ukrepom in samemu procesu določevanja kritične infrastrukture nujno sledi tudi zagotavljanje ustreznih virov za izvedbo celovitega sistema zaščite le te. Vsekakor bodo take razprave bistveno pripomogle pripravljavcem zakonskih rešitev na področju zaščite kritične infrastrukture, da bodo taka stanja, ki povzročajo tveganja, ustrezno predvideli in zakonsko normirali.

Jasni in metodološko preverjeni kriteriji za določitev kritičnosti posamezne infrastrukture so tisti, ki bodo zmanjševali dvom o tem kaj sploh je kritična infrastruktura.

Sedaj pa konkretneje poglejmo primer telekomunikacijske družbe T-2 d.o.o., ki se je v začetku leta znašla v stečajnih postopkih. Skozi razpravo in argumentacijo na zgoraj omenjenem nacionalnem posvetu je kot primer nastopal stečajni postopek, ki se je vodil v primeru podjetja T-2 in kateri je skozi celoten proces pokazal na cel niz nedorečenosti. Omenjeni proces ponovno kaže na ozek parcialni pogled posameznih struktur, brez, da bi bili v državi sposobni pogledati na celovit spekter vplivnih dejavnikov in posledic. V vsakem primeru gre pri vsakem stečaju za poskus urejanja odnosov med lastnikom pravne osebe in upniki v okviru zakona. Seveda pa se nam v tem primeru takoj postavi primarno vprašanje, kako zagotoviti ustrezno izvedbo stečaja pravne osebe, ki upravlja s kritično infrastrukturo, da ne pride do nepopravljivih tveganj za delovanje te kritične infrastrukture in seveda posledično za nacionalno varnost. Zavedati se je potrebno, da stečajna masa družbe predstavlja njeno dejavnost in infrastrukturo, ki sta lastniško, logistično in organizacijsko nerazdeljeni. V primeru zahtev upnikov po delitvi stečajne mase oz. prodaje premoženja po delih, lahko pride pri taki infrastrukturi, med katero lahko sodi tudi kritična infrastruktura, do nepopravljivih posledic za nacionalne interese in nacionalno varnost. Informacijska družba v delu svojega delovanja zagotavlja podporo neprekinjenemu informacijskemu de-





Ob popolni odsotnosti zavedanja odgovornih v Sloveniji in birokratskega odzivanja ustreznih služb, nam lahko sploh kdo zagotovi, da so naše komunikacije varne pred nepooblaščenimi prisluhi.

lovanju posameznih institucij slovenske države. Dejstvo je, da imamo v tem povezanem mednarodno varnostnem okolju tudi svojo odgovornost do mednarodnih organizacij in zavezništev kamor smo vključeni. Kaj bi se hipotetično zgodilo, če bi omenjeno družbo skupaj s temi deli kritične infrastrukture kupil kitajski ali ruski kapital, ki tesno sodeluje s svojimi državnimi in obveščevalnimi strukturami. Ob popolni odsotnosti zavedanja odgovornih v Sloveniji in birokratskega odzivanja ustreznih služb, nam lahko sploh kdo zagotovi, da so naše komunikacije varne pred nepooblaščenimi prisluhi. Kot del zavezništva, ki moramo na svojem ozemlju zagotavljati del tako imenovanega »host nation support«, tudi za zavezništvo lahko predstavljamo določeno stopnjo tveganja. Če tako podjetje podpira del državne informacijske infrastrukture, pa je to dejstvo še bolj zaskrbljujoče. Trenutno namreč odgovorne institucije nimajo pravega interesa, znanja in zadostnih zakonskih mehanizmov za učinkovitejše uveljavljanje nacionalnih interesov v takih konkretnih primerih. Članstvo v navedenih organizacijah predstavlja pomembno odgovornost, še posebej ko govorimo o informacijskih tveganjih, ki so s pojavom kibernetskih groženj še dodatno izpostavljene in jih je potrebno ustrezno obravnavati. Velikokrat se dogaja, da se pooblaščene institucije preveč ozko usmerjajo v zagotavljanje tehnične informacijske infrastrukture manj pa na neprekinjenost storitev, ki so v celoti zelo pomembne kadar govorimo o neprekinjenem delovanju informacijske in komunikacijske kritične infrastrukture. V tem okviru moramo izpostaviti tveganje za izvajanje prisluhov komunikacij s strani državnih in zasebnih-korporativnih subjektov. Ta nevarnost je v dobi grobe gospodarske konkurenčne tekme izredno izpostavljena. Stečajni postopki z neurejenimi procesi lahko zelo hitro pripeljejo do porasta tveganj in možnosti za izvedbo prisluškovanja in prestrezanja komunikacijskih in informacijskih poti.

Republika Slovenija mora vsem svojim državljanom neprestano zagotavljati komunikacijsko zasebnost, kot ustavno opredeljeno kategorijo. V primeru nesistemskih rešitev in stihijskih prodajnih procesov si težko zamislimo, da bo to ustavno določilo ustrezno zagotovljeno. V navezavi na prejšnji odstavek in na pomen informacijske infrastrukture pa je potrebno jasno izpostaviti to dolžnost države do zagotavljanja ustavno določenih pravic, ki jih opredeljujeta 37. člen Ustave RS in sicer o varnosti pisem in drugih občil in seveda 38. člen, ki obravnava varstvo osebnih podatkov. Ti dve pomembni ustavni področji postavljata zakonodajalca, še posebej pa državne institucije, v položaj povečane skrbi, kadar govorimo o stečajnih postopkih informacijskih podjetij. Taki primeri nam na omenjenem področju



odpirajo nekaj zelo pomembnih dilem, ki jih bo potrebno v prihodnje posebej upoštevati in se na take primere ustrezno pripraviti ter v nadaljevanju učinkoviteje odzivati.

Vsekakor je omenjeni primer lahko vzorčni primer nedefiniranega stečaja, ko nekatere stvari niso ustrezno opredeljene in zaradi tega lahko prinesejo pomembna varnostna tveganja, ki se lahko odrazijo v nedelovanju določenega dela informacijske infrastrukture, obveščevalnega delovanja tujih služb in nepooblaščen prisluh informacij, nezagotavljanje komunikacijske zasebnosti in drugih tveganj. Če pri takih primerih, kot je stečaj družbe T-2 d.o.o., gledamo samo ozki interes urejanja ekonomsko-finančnih odnosov lahko pri zagotavljanju nacionalne varnosti nastanejo pomembna tveganja. Še večji problem pa nastane, če se teh tveganj in kompleksnosti tega procesa sploh ne zavedamo.

Za konec moramo odpreti še sposobnost sodne veje oblasti, da se ustrezno spoprime s tako kompleksnimi primeri obravnave. Splošno ugotovitev lahko strnemo v smeri, da imajo stečajni upravitelji premalo informacij in znanja, da bi lahko ustrezno obvladovali tako kompleksne stečajne postopke, ki vsebujejo poslovni subjekt, kateri je upravljavec kritične infrastrukture. Stečajni postopek se ne sme uporabljati kot orodje zagotavljanja parcialnih interesov in omejevanja konkurence. To je še posebej pomembno kadar govorimo o poslovnih subjektih, ki upravljajo s kritično infrastrukturo.

Splošno ugotovitev lahko strnemo v smeri, da imajo stečajni upravitelji premalo informacij in znanja, da bi lahko ustrezno obvladovali tako kompleksne stečajne postopke, ki vsebujejo poslovni subjekt, kateri je upravljavec kritične infrastrukture.

V zaključku želim podati nekaj predlogov za rešitev nastale praznine, ki morajo iti v smeri dopolnitve normativne podlage, katera ureja stečajne postopke in v njo vnesti ustrezne procese, kadar gre za stečaj organizacije, ki je v ključnem nacionalnem interesu oz. je del kritične infrastrukture. Posebno pozornost bo pri pripravi teh rešitev potrebno posvetiti informacijski kritični infrastrukturi saj je njena neustrezna obravnava povezana tudi z nevarnostjo poseganja v ustavno varovane pravice, ki jih opredeljuje 37. in 38. člen Ustave Republike Slovenije. Vlada Republike Slovenije in njene institucije pa morajo pospešiti dokončno urejanje sistema zaščite kritične infrastrukture in v celoti postaviti temelje za učinkovito sodelovanje na področju javno-zasebnega partnerstva, ko gre za vprašanje upravljanja kritične infrastrukture, katera je ključna za normalno funkcioniranje širše družbene skupnosti. ■

Avtor: Boštjan Vrečko / koordinator SUNP-a v Telekomu Slovenije*



TELEKOM SLOVENIJE JE PRVI V SLOVENIJI PREJEL MEDNARODNI CERTIFIKAT ISO 22301 ZA SISTEM UPRAVLJANJA NEPREKINJENEGA POSLOVANJA

V Telekomu Slovenije kot nacionalnem telekomunikacijskem operaterju ter ponudniku celovitih IKT-storitev upravljamo z omrežno infrastrukturo z največjo razpršenostjo, velikostjo in pokritostjo v državi. Skupaj s svojimi odvisnimi družbami smo prepoznani kot vodilni pri uvajanju in povezovanju novih generacij mobilnih in fiksnih komunikacij, sistemske integracije in storitev v oblaku ter multimedijskih vsebin. Kot vodilni nacionalni operater v Sloveniji ter v razvoj in prihodnost usmerjeno podjetje, ki svoje dosežke presoja z zadovoljstvom uporabnikov, se zaveda tudi svoje družbene odgovornosti.

V Telekomu Slovenije se zavedamo pomena varnosti ter zagotavljanja nemotenega delovanja omrežja in razpoložljivosti storitev tako v običajnih pogojih delovanja kot ob izrednih razmerah. V primeru večjih izpadov tako zagotavljamo čim hitrejšo povrnitev delovanja omrežja in storitev v normalno delovanje. Zato smo v družbi poleg sistema vodenja varovanja informacij pristopili tudi k vzpostavitvi sistema upravljanja neprekinjenega poslovanja (SUNP). V letu 2016 smo kot prvi v Sloveniji za vzpostavljen sistem pridobili tudi mednarodni certifikat ISO 22301:2012, s čimer smo potrdili, da je vzpostavljen sistem v skladu z najvišjimi zahtevami, ki jih določa standard, in da se zavedamo pomena varnosti in zagotavljanja delovanja omrežja ter informacijsko komunikacijskih storitev kot podpore delovanju ostali kritični infrastrukturi na ravni države.

Kaj je sistem upravljanja neprekinjenega poslovanja (SUNP)?

Gre za vzpostavljen proces vodenja oz. upravljanja, ki zagotavlja ogrodje za identificiranje ključnih storitev in poslovnih procesov družbe ter njihov vpliv na poslovanje. Na tej osnovi nato opredelimo potencialne grožnje in njihove posledice v primeru, da bi prišlo do vpliva na varnost in izvajanje poslovanja družbe. V nadaljevanju pa se pripravijo ukrepi in aktivnosti za povečanje varnosti in odpornosti družbe na eni ter hitrejše okrevanje ob izrednih dogodkih na drugi strani. Slednje z ustrezno organizacijsko strukturo, ki omogoča koordiniranje in izvajanje potrebnih aktivnosti tako ob izrednih dogodkih kot pri načrtovanju, upravljanju in razvoju sistema.

Tako kot za vse sisteme vodenja, je tudi za SUNP značilno, da gre za cikličen in nenehen proces izboljševanja, ki poteka v več fazah. Prva je faza vzpostavitve, v okviru katere se opredelijo obseg, cilji, kontrole, procesi in postopki, ki so pomembni za izboljšanje procesa neprekinjenega poslovanja z namenom doseganja zastavljenih rezultatov, ki morajo biti usklajeni z vzpostavljenimi politikami in cilji družbe. Sledi faza izvedbe in upravljanja, v kateri se izvajajo in upravljajo zastavljeni cilji, opredeljeni v delu procesa vzpostavitve. V tej fazi se izvaja tudi nadzor procesov in postopkov poslovanja. V naslednji fazi spremljanja in vrednotenja izvajanja se spremlja, testira in pregleduje uspešnost samega vzpostavljenega sistema ter zastavljenih ciljev, v okviru ugotovitev pomanjkljivosti pa se opredeli ukrepe za njihovo sanacijo in izboljšanje (ukrepe je potrebno predhodno uskladiti z vodstvom). V fazi

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

vzdrževanja in izboljševanja se vzdržuje in izboljšuje sistem s korektivnim ukrepanjem, ki temelji na rezultatih vodstvenega pregleda in ponovne ocene samega sistema neprekinjenega poslovanja, njegovih ciljev in širjenja njegovega obsega.

SUNP v Telekomu Slovenije

V Telekomu Slovenije smo se pri vpeljavi SUNP-a kot ponudnik informacijskih in komunikacijskih storitev osredotočili na izvajanje storitev, zagotavljanje varnosti ter izvajanje s tem povezanih poslovnih procesov. Za Telekom Slovenije je bil storitveno usmerjen pristop najprimernejši in najbolj učinkovit tudi s stališča okrevanja oz. zagotavljanja varnosti omrežja in storitev, kar nam narekuje zakonodaja.

Glavno vodilo pri določitvi ključnih storitev in poslovnih procesov je bilo zagotavljanje varnosti in varovanje interesov uporabnikov oz. naročnikov naših storitev, zaposlenih, nenazadnje pa tudi ustvarjanje vrednosti za lastnike. Pri tem smo se v zadnjem obdobju srečali tudi z zahtevami po vpeljavi postopkov neprekinjenega poslovanja s strani naših večjih poslovnih uporabnikov in poslovnih partnerjev. Z vpeljanim sistemom tako zmanjšujemo potencialni izpad prihodkov v primeru prekinitve izvajanja ključnih storitev in poslovnih procesov družbe, ob tem pa smo pri vpeljavi sistema sledili tudi zahtevam Zakona o elektronskih komunikacijah (ZEKom-1) in Splošnega akta o varnosti omrežja in storitev. Navedena akta smo sicer dolžni spoštovati in zagotavljati vsi telekomunikacijski operaterji v Republiki Sloveniji.

Da v Telekomu Slovenije zagotavljamo varnost in zanesljivo delovanje ključnih storitev, ki jih uporabnikom nudimo na trgu informacijsko-komunikacijskih tehnologij, je ključno to, da ima družba, v izogib hujšim motnjam poslovanja, vzpostavljen celovit, strukturiran, vzdrževan, nadzorovan in optimiziran SUNP. Njegov najpomembnejši namen je zagotavljanje varnosti in delovanja ključnih storitev in poslovnih procesov tako v normalnem delovanju kot tudi v primeru izjemnih stanj. Zato imamo za zagotavljanje delovanja ključnih storitev in poslovnih procesov vzpostavljeno organizacijsko strukturo z jasno opredeljenimi vlogami v vseh pogojih poslovanja. Poleg organizacijske strukture smo opredelili tudi ukrepe za zmanjševanje



tveganj in preprečevanje vpliva možnih groženj na delovanje ključnih storitev in poslovnih procesov ter vzpostavili načrte okrevanja na več ravneh. Tako smo vzpostavili krovni načrt odziva za okrevanje poslovanja, ki se ga uporabi v primeru izrednega dogodka in je namenjen skupini za okrevanje poslovanja, ki jo sestavljajo ključni predstavniki poslovodstva. Njegov namen je zagotoviti jasen in transparenten postopek ravnanja v primeru izrednih dogodkov, z jasno opredeljenimi odgovornostmi posameznikov in vseh delavcev družbe. Cilj krovnega načrta je v največji možni meri preprečiti morebitne nadaljnje poškodbe ali celo žrtve na strani delavcev, preprečiti poškodbe sredstev družbe, omogočiti hitro evakuacijo delavcev, zagotoviti jasno in organizirano komunikacijo z notranjimi in zunanjimi javnostmi, zmanjšati posledice izrednega dogodka, vzpostaviti začasne postopke poslovanja družbe ter omogočiti čim hitrejši pričetek odprave napak na prizadetih sredstvih in posledično ključnih storitvah ali poslovnih procesih. Poleg tega smo pripravili tudi načrte okrevanja na ravni ključnih storitev in poslovnih procesov, ki so namenjeni tehničnim skrbnikom. Njihov namen je zagotoviti, da se prizadeta ključna storitev oz. poslovni proces čim hitreje povrneta v normalno delovanje ter priprava načrtov okrevanja na ravni posameznega sredstva oz. vira, ki je ključen za delovanje posamezne storitve oz. poslovnega procesa ter v pomoč posameznim skrbnikom virov pri vzpostavljanju oz. povrnitvi njegovega ponovnega delovanja.

Predvsem pa je pomembno, da se z analizo vpliva na poslovanje določi in s strani poslovodstva potrdi ključne storitve in poslovne procese družbe. S pomočjo analize se določi in pripravi tudi ustrezne strategije, ki vključujejo ukrepe in postopke za čim večjo varnost in razpoložljivost delovanja v normalnih razmerah ter njihovo čim hitrejše okrevanje v primeru izrednega dogodka.

Ključno pri tem je, da so vzpostavljeni postopki in načrti okrevanja ažurni, zato jih je potrebno periodično pregledovati in testirati. Vsa testiranja se ovrednotijo, na tej osnovi pa se po potrebi načrte dopolni in ustrezno prilagodi. Periodično

Glavno vodilo pri določitvi ključnih storitev in poslovnih procesov je bilo zagotavljanje varnosti in varovanje interesov uporabnikov oz. naročnikov naših storitev, zaposlenih, nenazadnje pa tudi ustvarjanje vrednosti za lastnike. Pri tem smo se v zadnjem obdobju srečali tudi z zahtevami po vpeljavi postopkov neprekinjenega poslovanja s strani naših večjih poslovnih uporabnikov in poslovnih partnerjev.

Cilj krovnega načrta je v največji možni meri preprečiti morebitne nadaljnje poškodbe ali celo žrtve na strani delavcev, preprečiti poškodbe sredstev družbe, omogočiti hitro evakuacijo delavcev, zagotoviti jasno in organizirano komunikacijo z notranjimi in zunanjimi javnostmi, zmanjšati posledice izrednega dogodka, vzpostaviti začasne postopke poslovanja družbe ter omogočiti čim hitrejši pričetek odprave napak na prizadetih sredstvih in posledično ključnih storitvah ali poslovnih procesih.

izvajamo tudi ocenjevanje tveganj za posamezne ključne vire, storitve in poslovne procese, na podlagi analize tveganj pa izvedemo predlagane ukrepe za njihovo zmanjšanje na sprejemljivo raven.

Zelo pomembno je tudi, da se učimo iz samih izrednih dogodkov. Zato se po njihovi sanaciji izvede analiza, kjer se ocenjuje oz. vrednoti tako razlog nastanka in potek okrevanja oz. ponovne vzpostavitve delovanja, ki nam je v veliko pomoč pri postavljanju in izboljševanju zaščitnih ukrepov, postopkov in načrtov okrevanja ter zagotavljanja neprekinjenega poslovanja.



Sistem se na letni ravni vrednoti z notranjimi presojami, ki predstavljajo osnovo za izvedbo pregleda, ki ga opravi poslovodstvo (vodstveni pregled). Ob zaključku ciklusa se skladnost SUNP-a s standardom presoja tudi z zunanjimi presojami neodvisnih inštitucij.

Rezultat nenehnih izboljšav je ustrezno vzpostavljen in vzdrževan SUNP, s katerim torej zagotavljamo varnost delavcev in drugih oseb v poslovnih prostorih družbe, zagotavljamo varnost omrežja, ključnih storitev in poslovnih procesov, pa tudi njihovo okrevanje in povrnitev delovanja v najkrajšem možnem času.

V Telekomu Slovenije smo sistem vzpostavljali in razvijali od leta 2006. Po združitvi družb Mobitel in Telekom Slovenije v letu 2011 smo oba vzpostavljena sistema poenotili, v letu 2014 pa vzpostavili enovit sistem. Pri vpeljavi smo že v osnovi sledili zahtevam in usmeritvam standarda ISO 22301:2012.

Da gre za vzpostavitev kompleksnega sistema, je dovolj že podatek, da imamo v Telekomu Slovenije v SUNP trenutno vključenih 16 ključnih storitev in poslovnih procesov s preko 100 povezanimi ključnimi viri oz. sredstvi, njihovo število pa skladno z načrtom vsako leto narašča. Za obstoječe ključne storitve in poslovne procese je trenutno izdelanih preko 360 dokumentov na različnih ravneh, v sam proces pa je vključenih okoli 350 zaposlenih.

Pri vzpostavitvi sistema je bila pomembna tudi njegova povezanost z obstoječimi sistemi, predvsem s sistemom varnosti ter nadzora omrežja in storitev, ki v samem SUNP-u igrata odločilno vlogo. Obstoječe dežurne službe so ključne pri zaznavanju nevarnosti in groženj ter čim hitrejšem ukrepanju. Ob izrednem dogodku je sicer zelo pomembno tudi obveščanje zunanjih javnosti - poleg uporabnikov naših storitev predvsem ključnih institucij.

Prioriteta je zagotavljanje delovanja omrežja in storitev ter številk za klic v sili, predvsem 112 in 113. Zato zagotavljamo tako podporo in obveščanje nosilcev varnostnega in obrambnega sistema ter sistema zaščite in reševanja kot tudi podporo ostalim sektorjem kritične infrastrukture ter prednostnim uporabnikom. Glede iz tega izhajajoč pomen samega informacijsko-telekomunikacijskega sektorja in Telekoma Slovenije ter medsebojne soodvisnosti z ostalimi sektorji kritične infrastrukture je potrebno operativno sodelovanje med njimi in v prihodnje tudi jasno definiranje ukrepov tako z nosilci varnostnega in obrambnega sistema ter sistema zaščite in reševanja kot z ostalimi sektorji kritične infrastrukture na ravni države.

Premiki v tej smeri so v zadnjem času že nakazani, hkrati pa se usklajujejo, vzdržujejo in preverjajo tudi postopki in ukrepi z AKOS-om kot regulatorjem, nevladnimi institucijami, kot npr. Slovenian Computer Emergency Response Team (SI-CERT), in tudi z evropskimi organizacijami, kot so European Union Agency for Network and Information Security (ENISA).

Vzpostavitev učinkovitega SUNP-a in njegova certifikacija je za organizacijo, kakršna je Telekom Slovenije, zelo pomembna, in sicer tako z vidika varnosti in zagotavljanja delovanja omrežja (ter z njim povezanimi storitvami in poslovnimi procesi) kot z vidika zmanjševanja izgube prihodkov. Nenazadnje pa je naš skupni cilj zagotavljanje zadovoljstva uporabnikov naših storitev.

Verjamem, da nam bodo sledile tudi druge organizacije, ki se prav tako zavedajo pomena varnosti in kritičnosti delovanja sistemov tako na področju informacijskih in komunikacijskih storitev kot na ostalih področjih, ki so pomembna za zagotavljanje varnosti in delovanja kritične infrastrukture na ravni države. ■

8. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 15.—16. marec 2017



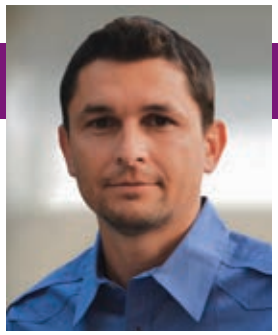
PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

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

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

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

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



REPORTAŽA:
Mednarodna konferenca »Dnevi korporativne varnosti 2016«

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD 2016

Ob slovesnem dogodku je potekala tudi 7. mednarodna konferenca »Dnevi korporativne varnosti 2016«, ki je tokrat v svojem okviru združila 20 predstavitev in dve odmevni okrogli mizi.

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«. Udeležba več kot 180 udeležencev in visokih gostov iz širšega regijskega prostora je ponovno dokazala, da dogodek nedvomno ostaja najkvalitetnejši regijski dogodek na področju korporativne varnosti.

Odlična konferenca je v organizaciji Instituta za korporativno varnostne študije ponovno dokazala, da je vsebinsko ena od najpomembnejših v širšem regijskem prostoru. Skozi odlična predavanja in dve odmevni okrogli mizi so udeleženci lahko tudi sami razpravljali o dobrih praksah in najnovejših spoznanjih na področju korporativne varnosti.

Konferenco so s svojimi svečanimi nagovori odprli izr. prof. **dr. Denis Čaleta**, predsednik organizacijskega odbora, **mag. Mitja Bervar**, predsednik Državnega sveta Republike Slovenije, **g. Boštjan Šefic**, državni sekretar Ministrstva za notranje zadeve, **ga. Mojca Prelesnik**, Informacijska pooblaščenka in **g. Aleš Polajnko**, iz podjetja Tend d.o.o., ki je bil letošnji generalni sponzor dogodka. 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. Omenjeni dogodek pa predstavlja odlično priložnost za izmenjavo izkušenj, dobrih praks in







*avtor je član Slovenskega združenja korporativne varnosti







predvsem najnovejših spoznanj na področju korporativne varnosti.

Na otvoritvi mednarodne konference je potekala tudi podelitev »**Slovenian Grand Security Award 2016**« za dosežke na področju varnosti v letu 2015. Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje Institut za korporativne varnostne študije, ICS-Ljubljana, v sodelovanju s Slovenskim združenjem korporativne varnosti.

Nagrada je namenjena procesom dvigovanja splošnega zavedanja in varnostne kulture v širši družbeni skupnosti, ki vsebuje poslovna in druga okolja. V šestih kategorijah neodvisna komisija izbira tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev. To kvaliteto nagrajujemo z uglednim priznanjem, ki so bili tokrat podeljena za dosežke na področju varnosti v letu 2015.

Nagrado v kategoriji »Najboljši korporativno varnostni manager« je prejel **mag. Boris Kankaraš** iz podjetja Luka Koper, ki mu jo je podelil dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti. Nagrado »Najbolj varno podjetje« je tokrat prejelo podjetje **Zavarovalnica Triglav**. Predsednik uprave g. Andrej Slapar je prejel priznanje iz rok mag. Mirana Vršca, soustanovitelja ICS-Ljubljana. Nagrado za »Najbolj varno mesto« je prejela **Mestna občina Ljubljana**. Podžupan g. Dejan Crnek je prejel nagrado s strani mag. Mitje Bervarja, predsednika Državnega sveta Republike Slovenije. Gospod Boštjan Šefic, državni sekretar MNZ je predal nagrado g. Stanislavu Mlakarju, podžupanu **Občine Slovenska Bistrica** v kategoriji »Najbolj varna občina«.

Tokrat je nagrado »Najbolj inovativna varnostna rešitev« prejelo podjetje **Biokoda d.o.o.** Nagrado je prevzel g. Gregor Spagnolo, ki mu jo je predal mag. Aleksander Mervar, direktor ELES. V kategoriji »Najboljša knjiga s področja varnosti« je bila letos nagrada podeljena **prof. dr. Iztoku**

Posebej je potrebno izpostaviti, da so na letošnji konferenci poleg strokovnjakov s področja korporativne varnosti, svoj velik delež k vsebinskem delu konference dodali tudi strateški managerji iz različnih podjetij. To dokazuje, da je korporativna varnost vedno bolj prepoznana kot učinkovito orodje v rokah strateških vodstev v podjetjih za bolj učinkovito obvladovanje varnostnih tveganj.













Podbregarju, ki mu jo je predala mag. Katja Kraškovic, dekanja Fakultete za podjetništvo-GEA College. Informativna oddaja **Planet Danes** je prepričala neodvisno komisijo in prejela nagrado v kategoriji »Najbolj inovativna medijska podpora«. Nagrado je prevzel g. Mirko Majer, voditelj oddaje in sicer mu jo je predal mag. Miran Vršec. Na koncu pa je bila podeljena še posebna nagrada, ki jo je za življenjski prispevek na področju varnosti prejel **g. Zdenko Hriberšek** iz podjetja Gorenje d.d.. Nagrado mu je predal dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti.

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.

Naj v zaključku omenimo, da je 7. mednarodna konferenca »Dnevi korporativne varnosti 2016«, v svojem obsegu zajela 20 predstavitev in dve okrogli mizi. Letos je znotraj glavne konference z osrednjo temo »Korporativna varnost kot orodje v rokah strateškega managementa« potekala tudi konferenca z nazivom »Informacijska varnost - danes in jutri«, ki je udeležencem ponudila zelo aktualne in praktično uporabne informacije s področja obvladovanja informacijske varnosti in kibernetskih tveganj.

Odlični predavatelji so se v okviru dveh temeljnih konferenčnih področjih, ki sta obsegali sekciji povezani s korporativno in informacijsko varnostjo, vsebinsko dotaknili najbolj perečih in aktualnih tem. Skozi predavanja so bila izpostavljena zadnja spoznanja in najnovejše prakse ter izmenjane izkušnje pri obvladovanju tveganj v organizacijskih sredinah. Posebej je potrebno izpostaviti, da so na letošnji konferenci poleg strokovnjakov s področja korporativne varnosti, svoj velik delež k vsebinskem delu konference dodali tudi strateški managerji iz različnih podjetij. To dokazuje, da je korporativna varnost vedno bolj prepoznana kot učinkovito orodje v rokah strateških vodstev v podjetjih za bolj učinkovito obvladovanje varnostnih tveganj. Naj omenim samo nekatere **ga. Ksenija Butenko Černe**, članica uprave Lek d.d., **mag. Danilo Burnač**, direktor Mariborskega vodovoda, **mag. Boris Mohar**, direktor Urada RS za varovanje tajnih podatkov, **g. Aleš Polajnko**, Direktor podjetja TEND d.o.o. in **g. Rok Novak**, direktor podjetja Reisswolf Slovenija in še vrsto drugih odmevnih strateških voditeljev. Že na uvodni slovesnosti pa sta **g. Andrej Slapar**, predsednik uprave Zavarovalnice Triglav in **mag. Aleksander Mervar**, direktor ELES nakazala pomembnost korporativne varnosti in samega dogodka Dnevi korporativne varnosti.

Za konec velja še vabilo na 8. Dneve korporativne varnosti, ki bodo v ustaljenem terminu v marcu 2017. ■








ICS
ICS
DAYS OF CORPORATE SECURITY
tend


ICS
ICS

ICS


ICS




ICS






ICS
ICS









Avtor: Ingo Falk Pasch Wallersberg / Slovensko združenje korporativne varnosti*



ORGANIZIRANOST VARNOSTNIH SLUŽB V RAZMERAH TERORISTIČNIH ALI AMOK[1] NAPADOV

Sedanja komercializacija v dejavnosti zasebnega varovanja, podrejenost te dejavnosti finančnim dobičkom je zaskrbljujoča in v nasprotju s pomenom te panoge.

V sedanjih razmerah postaja in utegne postati še bistveno bolj očitno, da je dosedanji razvoj v tej panogi zgrešen – kakovost je skoraj v celoti podrejena finančnim dobičkom. Usposobljenost varnostnega osebja je na nesorazmerno nizki ravni in tudi za obvladovanje rizika – ko se še nismo srečevali s sedanjo nevarnostjo terorističnih napadov - nezadovoljiva. Te ugotovitve veljajo za prav vse države – članice EU, čeprav so med njimi sicer glede pravnega in dejanskega pomena te dejavnosti in kakovosti usposabljanja varnostnega osebja tudi pomembne razlike. Res je sicer, da Slovenija kot majhna država, katere politični in gospodarski pomen v širši mednarodni skupnosti ni vpliven, z veliko verjetnostjo ni v ospredju interesov mednarodnih akterjev in terorističnih organizacij in zato za njih tudi ne zanimiva tarča. Vse bolj pa utegne biti glede na njen geopolitični položaj v Evropi interesantna kot prehodno območje in zbirališče, tudi morebitna organizacijska točka in eno od možnih komunikacijskih središč. Opozorilo na te rizike in vidike v sedanjih čedalje bolj nestabilnih razmerah, ko nas v neposredni soseščini vedno znova presenečajo pojavi in zločini islamskega in drugega terorizma, je iz dneva v dan bolj nujno – ko bo prepozno, ne bo več potrebno.

> Popolnoma očitno se je razkrilo, da na ravni EU izza proklamiranih varnostnih zahtev v resnici ne obstaja nič, da se je ob prvem večjem pritisku čez noč razpršila ne le zunanja meja EU, marveč tudi Schengen, t.j. njena notranja meja praviloma nekontroliranega prehajanja ljudi in blaga, meja, katere del varuje tudi naša država.

S precejšnjim presenečenjem pa obenem zaznavamo tudi številna aktualna svetovna in evropska politična dogajanja – ne le ob medijskem spremljanju današnje neverjetno grobe in populistične tekme med obema kandidatoma za predsedniški položaj v eni izmed treh, štirih svetovnih velesil[2], pač pa tudi ob javnih pozivih vodilnih politikov osrednjih evropskih držav, naj si prebivalstvo pripravi deset-dnevne zaloge vode in druge pijače ter hrane[3]. Ali danes tudi v Evropi že živimo v izrednih razmerah? Presenečenje ljudi je veliko, enako pa tudi nejevera, kar kažejo njihovi odzivi v medijih. Z osuplostjo lahko v zvezi s temi dogajanji obenem spremljamo v svetovnem spletu komaj verjetne komentarje s strani domnevno dobro poučenih strokovnjakov, za katere prav tako ne vemo, ali so resnični ali prav tako le domnevni. Ni jasno, kje se nahajamo - komu lahko zaupamo in komu ne. Očitno pa je, da se nas opazno dotika vrtinec fanatizma, nacionalnega in družbenega razslojevanja in vojn.

V teh razmerah se popolnoma na novo odpira stara dilema o tem, kakšna je vloga zasebnega varovanja v sodobni družbi, konkretno v okviru držav Evropske unije. Kot je bilo v preteklosti že opozorjeno[4], je dosedanji evropski razvojni trend potisnil to dejavnost na široko področje gospodarskih dejavnosti, resda z določenimi posebej predpisanimi pogoji in omejitvami, ki pa jih je doslej Sodišče EU v vrsti svojih judikatov maksimalno relativiziralo. Ob lanskem velikem emigrantskem valu (ko so prišleki iz arabskega polotoka in Afrike nekontrolirano prehajali predvsem na grške otoke v bližini Turčije in nato s pohodom najprej iz Grčije prek Srbije in Madžarske ter Avstrije v Nemčijo, kasneje pa, ko je Madžarska z ograjami

*avtor je član Slovenskega združenja korporativne varnosti

preprečila nekontrolirano prehajanje njenih mej in so se ti množični prehodi teh ljudi preusmerili iz Srbije na Hrvaško in Slovenijo do Avstrije in Nemčije) je bilo nenadoma potrebno za varovanje obmejnih področij skupno angažirati poleg policije in vojske tudi zasebno varnostne službe. Evropa je bila na to dogajanje množičnih migracij popolnoma nepripravljena. Reagirala je neodločno, zmedeno in predvsem neenotno. Jasno se je pokazalo, kako zlahka je njena obstoječa državna in varnostna konstrukcija ranljiva. Popolnoma očitno se je razkrilo, da na ravni EU izza proklamiranih varnostnih zahtev v resnici ne obstaja nič, da se je ob prvem večjem pritisku čez noč razpršila ne le zunanja meja EU, marveč tudi Schengen, t.j. njena notranja meja praviloma nekontroliranega prehajanja ljudi in blaga, meja, katere del varuje tudi naša država. Prav tako se je razkrila tudi notranja neenotnost EU, še prav posebej s tem, ko se je Velika Britanija (ki je emigrantom popolnoma zaprla svoje meje) izločila iz EU, ter po drugi strani z nasprotovanjem držav Višegrajske skupine, da sprejmejo emigrante iz islamskih držav. Položaj je danes – po neuspešno izvedenem vojaškem udaru v Turčiji - še posebej nevaren in nejasen. V večini članic EU, še zlasti v Nemčiji se je čez noč spreobrnila njena dosedanja politika krčenja policijskih kapacitet v smer njihovega pomembnega povečevanja, podobno tudi pri nas v Sloveniji. Kot smo pri poskusih obvladovanja nedavnih množičnih emigrantskih prihodov doživljali, je tudi danes za takšne primere še vedno v igri možnost, da ob takšnih dogodkih množičnega nekontroliranega prehajanja mej s policijo aktivno sodeluje vojska – ne glede na to, da je bil takšen predlog nemške zvezne ministrice za obrambo[5] nedavno zavrnjen. O vlogi in potrebah po večjem angažiranju družb za zasebno varovanje v takšnih primerih, še posebej ob nevarnostih terorističnih in amok napadov, pa ne zasledimo nikakršnih razmišljanj in predlogov, ne v okviru pristojnih organov in institucij EU ne pri nas. Ali za to resnično ni nobene potrebe?

Če drugega ne, je očitno, da te nove razmere – ko se srečujemo z bistveno novimi (vnaprej organiziranimi samomorilskimi) napadi - zahtevajo tudi dodatno, bistveno zahtevnejšo usposobitev varnostnega osebja. Ali pač ne? V ustreznih strukturah, zlasti policiji, se ob teh bistveno novih varnostnih razmerah v Evropi pojavljajo tudi popolnoma nasprotna stališča, ki dejavnost zasebnega varovanja marginalizirajo in ji zavestno krčijo področja njenega delovanja. Tako n.pr. zvezni nemški policijski sindikat zahteva za policijo ne le čimprejšnje pomembne kadrovske in tehnične okrepitve, pač pa tudi ponovno izključno pristojnost za delovanje na posameznih sektorjih[6] , kjer se je do sedaj namesto policije uveljavilo zasebno varovanje.

Ob takšnih različnih stališčih se moramo vprašati :

Stojimo, kar zadeva razvoj na področju zasebnega varovanja, na razpotju ?

Razvoj gre – kot se zdi – v popolnoma nasprotni smeri, kot smo ga še pred nedavnim lahko spremljali v praksi in predvidevali v prihodnosti. Še nedavno tega so v državah EU, zlasti v Nemčiji (pa tudi pri nas) krčili policijske kapacitete. Številni samomorilski teroristični oz. amok napadi in napadi na osebno integriteto in spolno nasilje, ki smo jim sedaj priča[7] so kardinalno preusmerili dosedanjo politiko na tem področju. Še večje število od izvršenih terorističnih dejanj pa je število dejanj, ki so bila v tem zadnjem času v Evropi načrtovana in tudi že v pripravi, pa so bila še pravočasno preprečena. Sicer se pa spomnimo, da spremljamo v zadnjem času takšne vnaprej natančno načrtovane in izvedene velike teroristične napade na cilje v razvitih delih sveta že od napada v letu 1983[8] in nato celo verigo takšnih napadov preko 11. septembra 2001 do danes. Med temi napadi jih je bilo v preteklosti, t.j. že pred letom 2015, izvršenih več s tragičnimi posledicami, tudi z zelo hudimi, tudi na področju EU[9]. Vprašanje, ki se zastavlja, je, zakaj se Evropa ni že takrat, t.j. pred več kot desetimi leti, ustrezno pripravila na te očitne, zelo nevarne teroristične napade – napade, ki bi jih morala že vnaprej zaznati in preprečiti ! Nedvomno je, da je EU - kot tudi vsaka od njenih članic - nevarnost teh napadov popolnoma nedopustno podcenila. Šele danes, ko se neposredno soočamo s t.i. begunsko krizo, dejansko pa z množičnim prihodom ljudi iz zelo različnih razlogov in z zelo različnimi motivi (t.j. od resničnih beguncev, do ekonomskih migrantov ter do posebej motiviranih





Sedanja umiritev razmer je zelo krhka in, kot vse kaže, tudi samo začasna. Izzivi, pred katerimi stojijo v teh razmerah varnostne družbe, so zaradi očitnih navedenih rizikov opazni, zaradi nezadovoljive in nerazčiščene pripravljenosti nanje, pa vse premalo definirani. Tako je seveda komaj mogoče pričakovati, da bi se varnostne družbe na morebitne ponovne krizne situacije na tem področju lahko pravočasno in ustrezno pripravile.

teroristov) in še posebej po vrsti naklepno izvršenih množičnih pomorih, so se vodstva držav v EU zganila. Zaenkrat pa ostaja v javnosti še vedno popolnoma neodgovorjeno vprašanje, kakšne ukrepe za obvladovanje tega najbolj akutnega problema načrtuje EU Komisija – razen njenega prizadevanja da bi se obdržal v veljavi sklenjen dogovor s Turčijo o zadržanju teh prišlekov in njihovem sprejemanju nazaj po njihovi napotitvi iz območja EU. Razen tega zelo majavega dogovora s Turčijo (ki veže njegovo veljavnost na neuresničljiv pogoj skorajšnjega prostega vstopa njenih državljanov na področje EU) pa vse doslej ni videti drugih učinkovitih ukrepov. Zadržanje morebitnega novega nekontroliranega množičnega navala teh prišlekov ostaja še vedno izjemno velik problem. Določena preusmeritev tega navala na področje Italije je v zadnjem času zaznavna, ostaja pa za zdaj še v mejah obvladljivosti. Vprašanje, ki se nam vsak dan znova zastavlja, je, ali gre pri tej umiritvi tega navala v resnici za dolgoročno stanje? In še posebej, ali bodo državni proračuni prizadetih držav dolgoročno zmogli prevzemati tako povečana finančna, materialna in kadrovska bremena za delovanje in razvoj njihovih nacionalnih policijskih in vojaških kapacitet? Vsekakor ta povečana pripravljenost države ne bo namenjena za potrebe tistih subjektov v njej, katerih varnostne zahteve so zahtevnejše oziroma specifične, zlasti če je njihova glavna dejavnost na tehnološkem področju. Utemeljeno namreč lahko domnevamo, da bo tudi to sedaj v več državah načrtovano povečano policijsko varovanje ostalo le na ravni osnovnih potreb prebivalstva in državne infrastrukture.

Sedanja umiritev razmer je zelo krhka in, kot vse kaže, tudi samo začasna. Izzivi, pred katerimi stojijo v teh razmerah varnostne družbe, so zaradi očitnih navedenih rizikov opazni, zaradi nezadovoljive in nerazčiščene pripravljenosti nanje, pa vse premalo definirani. Tako je seveda komaj mogoče pričakovati, da bi se varnostne družbe na morebitne ponovne krizne situacije na tem področju lahko pravočasno in ustrezno pripravile. Vsekakor lahko te težave v veliki meri razreši ustrezna pravočasna planska razporeditev nalog v primerih takšnih kriznih situacij s strani Vlade in pristojnih resornih ministrstev - in upam, da se to že dogaja. Te obstoječe rizične razmere, s katerimi smo se prvič resno spopadli šele pred kratkim in na ponovitev katerih je glede na krhkost obstoječe situacije vsekakor potrebno računati, pa obenem ponovno odpirajo tudi nekatera temeljna vprašanja organiziranosti same dejavnosti zasebnega varovanja. Pomen varnosti je v teh današnjih razmerah ponovno posebej poudarjen in zato viden tudi iz tistih vidikov, ki jih običajno zanemarimo.

Nedvomno je v kriznih situacijah, kot smo jim bili še nedavno priča, odločilna ustrezna usposobljenost varnostnega osebja. Da je ta danes v teh razmerah – pa tudi sicer, če govorimo o drugih rizičnih situacijah in sposobnostih ustreznega odzivanja na vrsto različnih izzivov – v veliki meri nezadovoljiva, je več kot oči-

tno. Za profesionalno izvajanje dejavnosti varovanja, ki je nedvomno povezano s čedalje večjimi riziki, po drugi strani pa s popolnoma novimi in tudi z zelo zahtevnimi področji (varnostne tehnike, varnostnega svetovalnega inženiringa, kibernetike na področju varovanja idr.), je potrebno ponovno preveriti obstoječo zakonsko ureditev te dejavnosti. Pri tem ne gre le za ustrezno uskladitev zahtevnosti poklicev v tej dejavnosti in ravni usposabljanja zanje, marveč tudi principielno za premislek o samem statusu te dejavnosti. Čedalje bolj nevzdržna postaja njena čista komercialna usmeritev in vztrajanje na ravni konkurence najnižje cene, minimalnih strokovnih zahtev za opravljanje nalog varnostnika ter njegovega bednega plačevanja. Prav tako je tudi nesprejemljivo, da lahko družba, ki opravlja dejavnost varovanja, hkrati opravlja tudi še katero koli drugo dejavnost. V teh današnjih specifičnih razmerah postaja premislek o statusu dejavnosti varovanja posebej aktualen.

Čedalje bolj nevzdržna postaja njena čista komercialna usmeritev in vztrajanje na ravni konkurence najnižje cene, minimalnih strokovnih zahtev za opravljanje nalog varnostnika ter njegovega bednega plačevanja.

Nedvomno je nujno, da zahteva opravljanje te občutljive dejavnosti poleg ustreznih strokovnih sposobnosti in učinkovitega delovanja tudi izpolnjevanje visokih etičnih kriterijev. Izpolnjevanja teh kriterijev v obstoječih zakonskih okvirih, s katerimi sta opredeljena pomen in opravljanje te dejavnosti, v pogojih tržnega gospodarstva objektivno ni mogoče zagotavljati. V sedanjih zelo nestabilnih razmerah, še posebej, ko se na področju varovanja že desetletja bije zelo neizprosen konkurenčni boj, je to tudi praktično nemogoče. Sedanje socialno zelo občutljive in tudi posebej rizične razmere v okoliščinah teh velikih prehajanj ljudi iz tujih kultur in okolij v naš prostor, zahtevajo popolnoma drugačno naravnanost vseh subjektov, ki sodelujejo pri uravnavanju teh gibanj. Terjajo - kot je bilo povedano – sodelovanje, in sicer optimalno sodelovanje na najvišji profesionalni ravni. Takšno sodelovanje bi morala biti tudi stalna maksima vseh subjektov, ki jim je zaupana naloga, da poklicno skrbijo za varnost. Da bi ta cilj, ne dosegli, ampak sploh omogočili, je potrebna temeljita preureditev naše zakonodaje na področju zasebnega varovanja, to je njeno koncipiranje iz bistveno drugega zornega kota. V sedanjih nestabilnih, nevarnih razmerah je takšno opravljanje varovanja, kot ga imamo sedaj, kontraproduktivno in izključno odvisno od osebnih lastnosti, kulture in pripravljenosti posameznega varnostnika.

Seveda zahteva takšna konceptualna sprememba zakonskega urejanja zasebnega varovanja tudi premislek o vrsti sedanjih zakonskih predpisov, ki pa se tudi v dosedanji praksi že dalj časa izkazujejo kot neustrezni, še posebej z vidika pomena te dejavnosti. V današnjem času, v katerem se pojavljajo popolnoma novi riziki z neposrednim srečevanjem s tujimi kulturami, je sedanja ureditev pogojev za opravljanje dejavnosti varovanja očitno nezadovoljiva. Nevzdržno je, da se lahko z varovanjem ukvarja praktično vsakdo, tudi če opravlja še vrsto drugih dejavnosti (celo takih, ki so v razmerju do dejavnosti varovanja izrazito neustrezne), samo če izpolni minimalne pogoje za pridobitev licence. Prav tako je nevzdržno, da je število subjektov v okviru posameznih zvrsti varovanja popolnoma neomejeno, ne oziraje se niti na dejanske potrebe. Strokovno usposobljenost in osebnostno preveritev varnostnega osebja in lastnikov družb je z vidika današnjih rizičnih razmer prav tako nujno potrebno preverjati po ustreznih višjih kriterijih. Zasebno varovanje, ki naj bi po definiciji pomenilo nadstandard varovanju, ki ga vsakomur zagotavlja policija, pa zahteva tudi sicer – ne le glede na današnje posebej rizične razmere – izpolnjevanje bistveno višjih kakovostnih kriterijev, predvsem na področju strokovne usposobljenosti osebja, kot to velja doslej. Naloge, ki jih opravlja, so že doslej prvenstveno namenjene potrebam posebne klientele. V okviru obstoječih razmer, ki jih posebej označujejo povečani riziki, povezani z množičnim priseljevanjem ljudi iz popolnoma drugih okolij, postajajo te naloge zasebnega varovanja – poleg morebitnih dodatnih v okviru potreb zagotavljanja nacionalne varnosti – še toliko bolj zahtevne.



[1] Nenačrtovan, iz osebnostne motnje spodbujen napad.

[2] Predsedniška volilna tekma v ZDA med demokratsko kandidatko go. Hillary Clinton in republikanskim kandidatom g. Donaldom Trumpom.

[3] Najprej s strani zveznega ministra za notranje zadeve Nemčije g. dr. Thomasa de Maiziere-ja.

[4] V mojem zapisu »Zavrte razvojne možnosti zasebnega varovanja« obj. v št.10/2015 te revije.

[5] ge. Ursule van der Leyen

[6] Zlasti pri kontrolah potnikov na letališčih.

[7] V Parizu, v Bruslju, v Münchnu, v Londonu, v Nici.

[8] Dva napada Hezbolaha na ameriško veleposlaništvo v Bejrutu (s približno 300 mrtvimi).

[9] V Madridu 2004, v Londonu 2005, v Toulousu 2012, v Bruslju 2014. ■

Varno v nov dan



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

ZARJA ELEKTRONIKA

Avtorica: Marta Štefanič/Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI-CERT)*



HEKERJI VDIRAJO V ELEKTRONSKO POŠTO SLOVENSKIH PODJETIJ

Geslo za elektronsko pošto je najpomembnejše med vsemi. Pogosta izjava »Pa kaj, če mi vdrejo v moj mail, saj nimam ničesar za skrivati«, se v večini primerov izkaže za še kako zgrešeno.

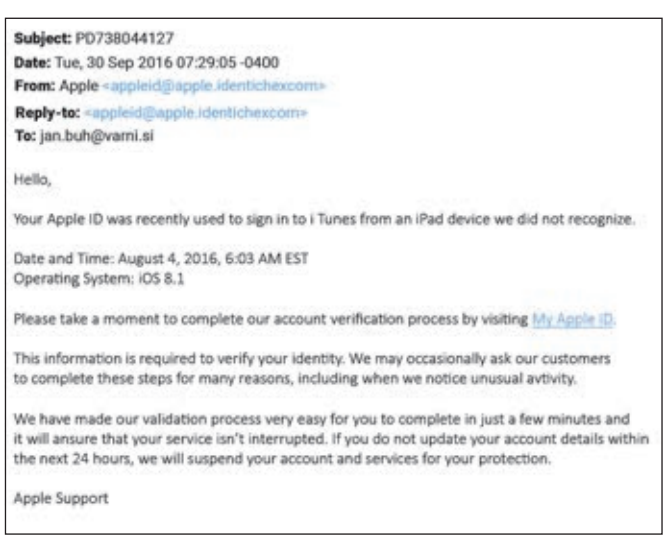
V osebni elektronski poštni predal ponavadi romajo vse povezave za ponastavitev gesel, ki smo jih pozabili; geslo za Paypal, za Dropbox, Facebook. Tisti, ki dostopa do naše e-pošte, dostopa tudi do vsega ostalega. Ko pa govorimo o vdoru v elektronsko pošto podjetja, so posledice lahko veliko hujše. Takšni vdori so že nekaj let stalnica povsod po svetu, nič drugače ni niti v slovenskem podjetniškem okolju. Samo v zadnjem času smo na SI-CERT prejeli več prijav zlorab elektronske komunikacije med slovenskimi podjetji in njihovimi poslovnimi partnerji iz tujine. Ne gre za pravilo, a na udaru so predvsem podjetja, ki poslujejo s tujino v velikih zneskih, saj napadalci lahko podatke o podjetjih enostavno pridobijo iz javno dostopnih evidenc.

Glavni razlog za vdor so občutljive poslovne informacije o prodajnih procesih. Ko napadalci zberejo dovolj potrebnih podatkov, lahko v ključnem trenutku prodaje aktivno posežejo v komunikacijo, kupcu pošljejo sporočilo o spremembi transakcijskega računa in s tem preusmerijo plačevanje računov in drugih stroškov na svoje lažne bančne račune. Do trenutka, ko podjetja ugotovijo, da je nekaj narobe, hitro nastane velika škoda, od nekaj 1000 do več 10000 EUR.

Kako pride do vdora v e-pošto?

Kriminalci se poslužujejo različnih načinov. Vdrejo v nadzorno ploščo pri ponudniku poštnih storitev ter preusmerijo pošiljanje pošte na svoj e-naslov (od tam nato neopaženo spremljajo komunikacijo podjetja). Lahko okužijo računalnik enega od zaposlenih, najpogosteje pa se do gesla za dostop do e-pošte dokopljejo s pomočjo ciljanega phishing napada.

***Običajni phishing napadi** so v obliki generičnih sporočil razposlani na veliko število naslovov in poštni strežniki jih bolj kot ne uspešno filtrirajo v vsiljeno pošto. Sem spadajo sporočila tipa ‚Ponovno se vpišite v vaš račun zaradi preverjanja pristnosti/ zaradi posodobitev/ ker smo zaznali nenavadne aktivnosti na vašem računu/ Če se ne vpišete ponovno, bomo vaš račun izbrisali.‘ Grožnja je prazna, to zelo splošno obvestilo pa znak, da sporočilu ne gre zaupati. Če bi sledili gumbu oz. povezavi in se skušali vpisati v svoj račun, bi podatke (up. ime in geslo) v resnici vpisovali v lažno spletno stran in jih s tem sami posredovali goljufom.



Subject: PD738044127
Date: Tue, 30 Sep 2016 07:29:05 -0400
From: Apple <appleid@apple.identichexcom>
Reply-to: <appleid@apple.identichexcom>
To: jan.buh@varni.si

Hello,

Your Apple ID was recently used to sign in to i Tunes from an iPad device we did not recognize.

Date and Time: August 4, 2016, 6:03 AM EST
Operating System: iOS 8.1

Please take a moment to complete our account verification process by visiting My Apple ID.

This information is required to verify your identity. We may occasionally ask our customers to complete these steps for many reasons, including when we notice unusual avtivity.

We have made our validation process very easy for you to complete in just a few minutes and it will ansure that your service isn't interrupted. If you do not update your account details within the next 24 hours, we will suspend your account and services for your protection.

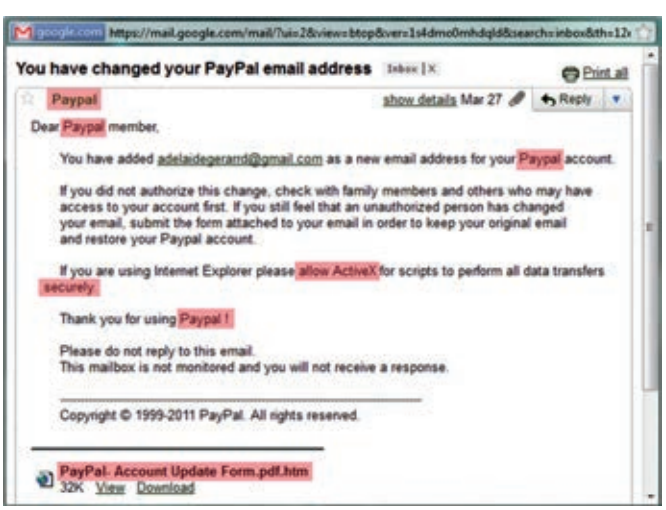
Apple Support

[Primer običajnega phishing sporočila.]

***Ciljani phishing napadi** so izvedeni veliko bolj sofisticirano: napadalec izbrani žrtvi pošlje personalizirano sporočilo, ki se izogne poštnim filtrom in obenem deluje bolj verodostojno, zaradi česar je takšen napad tudi bolj ‚uspešen‘.

*ustanova je korporacijski član Slovenskega združenja korporativne varnosti





[Primer ciljanega phishing napada. Napadalčevo sporočilo je bilo napisano za točno določenega naslovnika. Ker se vsebina sporočila dejansko navezuje na njegove aktivnosti je veliko bolj verjetno, da bo naslovnik takšnemu sporočilu tudi nasedel.]

Ko kriminalci dobijo dostop do e-pošte, lahko komunikacijo spremljajo direktno iz poštnega predala ali pa nastavijo preusmeritve vseh sporočil na svoje elektronske račune. Posebej za ta namen jih kreirajo pri enem od brezplačnih ponudnikov (gmail, yahoo, hotmail). Brezplačne ponudnike izberejo premišljeno: ob kreiranju računa lahko uporabijo lažne osebne podatke in s tem zakrijejo svoje sledi.

Nekaj časa nato neopaženo spremljajo celotno komunikacijo da ugotovijo, na kakšen način poteka poslovanje, plačevanje in čakajo na ključni trenutek prodaje ali plačilo večjega računa. Takrat aktivno stopijo v komunikacijo, pri čemer prevzamejo vlogo zaposlenega v podjetju. To lahko dosežejo tako, da pišejo iz njegovega elektronskega predala, a ker v tem primeru obstaja večja verjetnost, da bi zaposleni to opazil, poskušajo še na druge načine.

Pri enem od brezplačnih ponudnikov registrirajo elektronski naslov z imenom in priimkom zaposlenega v podjetju (npr. janez.novak@podjetje.si kar naenkrat postane janez.novak@gmail.com). Iz tega naslova žrtvi pošljejo podatke o spremenjenem TRR računu za nakazilo. Kot razlog za spremembo bančnega računa navedejo različne izgovore, od tega, da imajo težave s svojo banko, da bo plačilo hitreje sprovedeno, če plačajo na račun v bližnji državi, da raje nakažite na račun njihovega lokalnega zastopnika ipd. In ker večinoma nismo pozorni na domeno, na kateri je e-poštni naslov kreiran, ali pa je naslov v sporočilu celo delno zakrit, tako ponarejen naslov pogosto zadostuje.

S takšnim sporočilom denarna nakazila preusmerijo na svoje TRR račune, na njihove elektronske račune se preusmeri tudi komunikacija s stranko. Ker uporabniki običajno nismo pozorni na el. naslov sogovornika ali pa je ta celo delno zakrit, žrtev redko opazi spremembo.

Nakazan denar iz računov hitro izgine

V vseh obravnavanih primerih pri nas je šlo za nakazila na bančne račune fizičnih oseb iz EU, vendar to ne pomeni, da bodo oškodovani izgubljeni denar dobili nazaj ali organi pregona lažje prišli na sled kriminalcem. Vsi fizični računi so bili v lasti t.i. denarnih mul, ki so nakazan znesek takoj dvignile in po neki drugi denarni poti, ponavadi z nakazilom preko sistema Western Union, naprej nakazale goljufom. Na ta način pa se sled za denarjem zelo hitro izgubi.

Tudi sicer kriminalci denarne mule pogosto uporabljajo za prenakazovanje denarnih sredstev sumljivega izvora. V svojo mrežo jih zvabijo s pomočjo raznih zvijač, da pogosto še same ne vedo, s čim imajo opravka. Se spomnite oglasov za dobro plačano delo od doma; nekaj v stilu ‚Kako slovenska mama samohranilka zasluži 20.000 € z delom od doma? Preveri tukaj!' Oglasi so tipično v angleškem jeziku, na njih pa naletimo med brskanjem po kakšni potrošni spletni strani. Gre za lep primer prikritega oglaševanja dela denarne mule - sicer bogato plačanega, a z visokim rizikom – velik delež jih odkrijejo, pogosto morajo zaradi vpletenosti v kaznivo dejanje svoj del kazni odsedeti.



Svetujemo

- Če poslujete s tujino, bodite še posebej pozorni na morebitna nenadna odstopanja od utečenih praks. Vsako spremembo občutljivih podatkov, sploh tistih za nakazilo denarja, preverite na različne načine, tudi preko telefona, faksa, skypa ipd.



- Preverjajte el. naslove vaših partnerjev. Nekateri programi za el. pošto kot pošiljatelja prikažejo zgolj ime in priimek, ki pa si ju lahko vsakdo nastavi po svoje. Če pa se z miško postavimo na ime, se nam prikaže tudi el. naslov. Je ta morda spremenjen? Se namesto naslova ime.priimek@podjetje.com kar naenkrat pojavi ime.priimek@gmail.com? To je že lahko znak za alarm.

- V nastavitvah vašega el. računa redno preverjajte, ali se vaša el. pošta preusmerja na kakšen neznan el. naslov. V Gmailu to preverite v nastavitvah pod zavihkoma »Filtri« in »Posredovanje«, če uporabljate el. pošto drugega ponudnika se pri njem pozanimajte, kje najdete to nastavitev (preverite posredovanje in filtre).



Se vaša e-pošta preusmerja na neznan naslov?

- Če vam vaš ponudnik el. pošte omogoča dostop do vpogleda iz katerih IP naslovov je bilo dostopano do vašega predala, redno preverjajte te podatke. Na podlagi IP naslova lahko ugotovimo, kateremu ponudniku dostopa pripada, v nekaterih primerih pa tudi približno lokacijo. V primeru kazenskega pregona pa se lahko na podlagi IP naslova ter točnega časa prijave pridobi tudi podatke o uporabniku tega IP naslova.

- Ne zanemarjajte morebitnih obvestil o sumljivem dogajanju v el. računu, ki vam jih pošilja vaš ponudnik. Vsako tako obvestilo je potrebno analizirati in ugotoviti vzroke, zakaj je do tega prišlo (pri tem morate paziti, da prepoznate lažna, phishing sporočila, ki na prvi pogled izgledajo, kot da vam jih je poslal vaš ponudnik).

- Eden najpogostejših načinov kraje gesel so phishing sporočila, ko svoje geslo in up. ime napadalcem posredujemo kar sami. Razširjeni pa so tudi ‹trojanci›, ki prestrezajo shranjena in vpisana gesla. Trojanci se na računalnik naselijo, ko odpremo okuženo priponko v elektronski pošti, ali pa iz spleta prenašamo sumljive vsebine. Je možno, da ste v preteklosti naredili kakšno od teh napak?

- Kakšna je politika gesel v vašem podjetju? Uporabljajte kompleksna gesla in nikoli naj istega gesla ne uporablja več uporabnikov. Posebej skrbno ravnajte z geslom za dostop do nadzorne plošče za el. pošto vašega podjetja. Kraja enega gesla ima lahko za posledico zlorabo prav vseh el. predalov. Zato za dostop do nadzorne plošče uporabljajte 2-faktorsko avtentikacijo , če vam vaš ponudnik to omogoča. ■

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



KAKO POSKRBETI ZA VARNOST OMREŽJA

Izredno pomembna dejavnika za celovito normalno delovanje podjetja sta ustrezna omrežna in informacijska varnost. Različne prekinitve ali oslabitev delovanja sistema zaradi zlonamernih dejanj, sistemskih ali človeških napak, lahko kritično vplivajo na celotno delovanje in kot tako, tudi na poslovanje.

V svetu bitov in bajtov, ali danes rečeno drugače v kibernetskem prostoru, se dogajajo različna »bojevanja«, ki prinašajo različne varnostne izzive. Informacijski sistemi so postali eden izmed ključnih temeljev, na katerih sloni uporaba različnih storitev, ter predstavljajo različne elemente, vse od enostavnih in do bolj zapletenih protokolov pri zagotavljanju varnosti.

Varnost omrežij je le eno področje kibernetskega prostora, ki bije bitko v celotni problematiki pri zagotavljanju informacijske varnosti. Glede na razširjenost omrežij, le-ta predstavlja eno izmed ključnih vlog pri obrambi pred neželenimi vplivi, saj so rezultati napada lahko uničujoči, zato je varnost omrežij pomembna za vse deležnike, ne glede na to kako veliko je omrežje.



Kaj vse lahko ogroža varnost omrežja?

Na motnje v delovanju celotne omrežne infrastrukture lahko vplivajo različne kibernetske grožnje. Nepoznavanje segmenta groženj in napačno odzivanje na le-te, lahko prinese posledice, ki omejijo funkcionalnost celotnega sistema.

Trojanski konji, virusi in črvi

Računalniški trojanski konji so vrsta grožnje, ki so zasnovani tako, da se uporabniku predstavijo kot uporaben program, v ozadju pa delujejo z nelegitimnimi nameni. Pogosto delujejo kot stranska vrata (ang. »backdoor«), kar napadalcu omogoča oddaljen dostop do uporabnikovega računalnika.

Računalniški virus je zlonamerna programska koda, ki je dodana obstoječi datoteki v računalniku. Najpogosteje napadejo izvedljive datoteke in dokumente. Glede na namen in škodo, ki jo lahko povzročijo, poznamo takšne, ki so lahko zelo nevarni, saj lahko namenoma izbrišejo datoteke s trdega diska in takšne, ki ne povzročajo resne škode.

Računalniški črv je program, ki vsebuje zlonamerno programsko kodo in se od virusa razlikuje po tem, da se lahko širi sam, kar pomeni, da ni odvisen od gostiteljskih datotek. Črvi izkoristijo varnostne pomanjkljivosti omrežja ali pa se širijo prek elektronskih sporočil.

Napredne trajne grožnje

Napredne trajne grožnje (ang. »Advanced Persistent Threat (v nadaljevanju APT)«) so set »nevidnih« in ponavljajočih se računalniških procesov, ki jih pogosto upravlja človek. APT se uvršča v kategorijo usmerjenih napadov in so oblikovani posebej za ciljnega posameznika ali organizacijo. Namen APT je ostati neviden v sistemu čim dlje časa, ter so zasnovani tako, da se v sistemu pomikajo počasi, da se izognejo odkritju.
APT uporablja različne vrste napadov, tako izvajalcu napada omogoča, da v primeru neuspelega napada uporabi drugačen pristop izvedbe le-tega. Najbolj pogoste kombinacije groženj, ki jih APT uporablja so:

- Okužbe od zunaj (izkoriščanje ranljivosti sistema, vdori preko brezžičnih omrežij, izkoriščanje ranljivosti ponudnikov gostovanj)
- Okužbe z zlonamerno programsko kodo (priponke elektronske pošte, deljenje datoteke, okuženi podatkovni mediji)

*avtorica je članica Slovenskega združenja korporativne varnosti



Porazdeljena ohromitev storitve

Porazdeljena ohromitev storitve (ang. »Distributed Denial of Service« (v nadaljevanju DDoS)) in ohromitev storitve (ang. »Denial of Service« (v nadaljevanju DoS)) je napad s ciljem ohromiti storitev in preprečiti njeno neprekinjeno delovanje, tako da je le-ta nedosegljiva uporabnikom. DoS se običajno doseže s »poplavo« ciljne naprave ali storitve z odvečnimi zahtevami s ciljem preobremeniti sistem in preprečiti nekatere legitimne zahteve.

DDoS je podoben napad kot DoS, s tem da je virov napada več kot samo eden. Napadalec ima več računalnikov imenovanih »zombiji«, ki sledijo njegovim ukazom. Dostop do le-teh pa si je napadalec najverjetneje pridobil z nelegalnim dostopom. Tako napadalec »svojim« računalnikom z določenimi ukazi sporoči naj z določeno kapaciteto podatkov napadejo tarčo. Pri tej obliki napada je podatkov bistveno več kot pri DoS napadu, saj podatke pošlje več računalnikov hkrati, zato je tudi obremenitev sistema veliko večja.

Omrežje robotskih računalnikov

Robotski računalnik je avtomatiziran zlonamerni program, ki okuži ranljive računalnike. Več povezanih robotskih računalnikov skupaj tvori omrežje robotskih računalnikov (ang. »Botnet«) in predstavlja omrežje slabo zaščitenih računalnikov, ki jih napadalec, brez vednosti uporabnika, s pomočjo zlonamerne programske opreme poveže v omrežje. Napadalec na takšen način nadzira in do njih dostopa preko odkritih ranljivosti v sistemu.

Botnet lahko napadalec upravlja na dva načina:

- Center za ukazovanje in nadziranje (ang. »Command and Control« (C & C))
- Omrežje komunicira preko glavnega strežnika, na katerega se po vnaprej določenem ključu vsak od okuženih računalnikov povezuje na glavni strežnik, kjer prejme ukaze za delovanje. Vse več napadalcev uporablja protokol za varno povezavo (HTTPS), s čimer se odkrivanje take povezave med glavnim strežnikom in računalnikom še težje odkrije.
- Nadziranje vsakega z vsakim (ang. »Peer to Peer« (P2P))
- Hierarhija komuniciranja med računalniki in glavnim strežnikom je necentralizirana, kar še dodatno oteži njegovo odkritje.

Ko uporabnik na svoj računalnik nevede namesti zlonamerno programsko opremo, le-ta postane del robotskega omrežja, ki ga upravlja napadalec, tako se lahko tak računalnik uporabi za izvajanje različnih avtomatiziranih opravil prek interneta brez vaše vednosti.

Vsekakor obstaja še množica drugih groženj, s katerimi bi lahko bila ogrožena varnost omrežja. Zato je potrebno neželene dogodke, ki so posledica groženj, preprečevati in omejevati, saj lahko le-ti povzročijo velike izgube in gledano z vidika podjetja, tudi resno ogrozijo njegovo eksistenco.

Pametno je upoštevati večplastno zaščito, kjer je več plasti varnostnih kontrol postavljenih skozi celoten informacijski sistem, kar omogoča redundanco v primeru, da katera varnostna kontrola odpove.



Kaj torej lahko storimo?

Za zagotavljanje varnejšega omrežja poznamo različne preventivne ukrepe, ki lahko pripomorejo k večji omrežni varnosti. Pametno je upoštevati večplastno zaščito, kjer je več plasti varnostnih kontrol postavljenih skozi celoten informacijski sistem, kar omogoča redundanco v primeru, da katera varnostna kontrola odpove.

Ocena tveganja
To je proces, pri katerem definiramo in analiziramo tveganja, ki lahko ogrožajo posameznike, podjetja ali vladne organizacije. Nenehno ocenjevanje tveganja lahko pripomore k zmanjšanju varnostnih tveganj, tako, da preučimo tveganja, s katerimi se srečujejo uporabniki in organizacija. Ocena tveganja je lahko kvantitativna ali kvalitativna.

Kvantitativna ocena tveganja poskuša numerično določiti verjetnost različnih neželenih dogodkov in morebiten obseg izgub, ki se lahko pojavijo v primeru, da se določen dogodek zgodi. Pri kvalitativni oceni tveganja pa ne gre za numerične verjetnosti, temveč vključuje opredelitev različnih nevarnosti, ki določajo obseg ranljivosti v primeru, da pride do kakršnega koli napada.

Varnostna politika
Predstavlja ključno varovalo pri zaščiti in varovanju informacij v organizaciji pred različnimi zunanjimi in notranjimi vplivi, saj zajema vse dejavnike, organizacijska pravila in postopke, s pomočjo katerih lahko omogočimo varno in zanesljivo delovanje celotnega informacijskega sistema, ter podaja ključne zahteve, ki morajo biti izpolnjene za učinkovito varovanje ljudi, informacij, strojne in programske opreme.

Izobraževanje uporabnikov
Če se uporabniki omrežja zavedajo varnostnih incidentov, groženj in napadov, bo verjetnost, da bodo vedeli kaj storiti in kako ukrepati pred, med in po napadu, veliko večja. To je lahko ena izmed najbolj učinkovitih protiukrepov za varnost omrežja. Zavedanje o varnostnih tveganjih je kritičen del informacijske varnosti organizacije, saj je človeško znanje in vedenje tisto, kar organizacija uporablja za zaščito pred različnimi varnostnimi tveganji. Izobraževanje uporabnikov lahko močno dvigne raven splošnega znanja med uporabniki omrežja.

Tehnični vidik zaščite omrežja
Vzpostavitev varnega omrežja in implementacija različnih tehnologij neposredno vpliva na povezovanje v splet. Implementacija filtriranja paketkov na usmerjevalniku, implementacija požarnega zidu, uporaba DMZ (ang »Demilitarized Zone«) omrežja za strežnike, ki potrebujejo dostop do interneta, uporaba VPN (ang. »Virtual Private Network«) vse to pripomore k večji varnosti omrežja. Požarne pregrade in filtrirni mehanizmi praviloma delujejo do četrtega nivoja OSI referenčnega modela, zato lahko onemogočijo uporabo določenih aplikacij, dostope do dovoljenih aplikacij pa vsebinsko ne morejo nadzorovati, zato je potreben nadzor nad uporabo aplikacij s strani uporabnikov.

Glede na razširjeno uporabo brezžičnega omrežja, je za le-te z varnostnega vidika potrebna dodatna pozornost. Pri lokalnem omrežju mora uporabnik imeti fizičen dostop do omrežnega priključka, pri brezžičnem omrežju pa se uporabnik lahko povezuje iz drugega prostora ali celo stavbe.

Pri vseh omenjenih ukrepih je ozaveščanje vsekakor prvi korak do preprečevanja različnih groženj in napadov. Da bi zmanjšali možnost tovrstnih napadov, pa je velikega pomena usposabljanje in izobraževanje zaposlenih o morebitnem socialnem inženiringu ter o vrednosti in shranjevanju zaupnih podatkov in njihovi učinkoviti zaščiti. Spoštovanje varnostne politike ter nadzor nad uporabo virov informacijskega sistema je zelo pomembno, saj lahko kakršno koli odstopanje predstavlja grožnjo za podjetje.

Varnosti ni mogoče doseči zgolj z vzpostavitvijo različnih varnostnih sistemov ali orodij, vendar so varnostne napake veliko manj verjetne, če izvajamo varnostno politiko, procese in procedure, ter poskrbimo za večplastno zaščito celotnega sistema. Vsaka organizacija bi zato tovrstne ukrepe morala videti kot nujen ukrep ker saj veste kako pravi star pregovor: »Bolje preprečiti kot zdraviti«. ■



NADZOR NA DELOVNEM MESTU

17. november 2016, Bled

PLANET GV

ICS

Želite izvedeti več o naslednjih vsebinah:

- Novosti, ki jih prinaša nova uredba EU o varstvu osebnih podatkov.
- Dopustnost uporabe različnih oblik tehničnega nadzora (videonadzor, biometrične kontrole, GPS).
- Dileme dopustnosti uporabe socialnih omrežij na delovnem mestu in nadzor službene e-pošte.
- Kako učinkovit kadrovski postopek zmanjša kasnejša tveganja vezana na ključne kadre v podjetju?
- Pravni vidiki pri disciplinski obravnavi zaposlenih, sodna in nadzorna praksa.
- Nadzor nad pogodbenimi sodelavci in outsourcing storitvami.
- Ekonomski vidiki učinkovitega obvladovanja tveganj.
- Pogled strateškega managementa.

Pridružite se nam
17. novembra v hotelu Astorija na Bledu.
Organizatorja sta Planet GV in Inštitut za korporativne varnostne študije.
Prijave so možne na spletnih straneh
www.planetgv.si in www.ics-institut.si.

PLANET GV

ICS
Institut za korporativne varnostne študije

Avtorja: Robert Kompan / vodja oddelka za promet, DARS d.d.*
Drago Dolenc / uradnik za varnost v predorih, DARS d.d.*





TEHNOLOŠKI IN ORGANIZACIJSKI UKREPI DARS-A ZA POVEČANJE VARNOSTI AVTOCESTNIH PREDOROV V SLOVENIJI

Z vedno večjimi prometnimi tokovi se soočamo tako rekoč po vsej Evropi, zato je upravljanje s prometom veliko več kot samo krmiljenje s sistemi ter napravami. Dogovori s sosednjimi državami pri upravljanju prometa ter uvajanje novih tehnologij in standardov, kot je povezljivost infrastrukture z vozili (C2I), bo vodilo k zagotavljanju večje prometne varnosti ter pretočnosti. Rezultati vpetosti naše družbe na evropskem prostoru že kažejo pozitivne rezultate, tako na varnosti kot na kvaliteti opremljenosti avtocestne mreže.

Prometna stroka pridobiva na veljavi v vseh državah sveta, kar gre pripisati predvsem temu, da je promet gonilna sila gospodarstev.

V zadnjih letih je upravljanje s prometom in prometno varnostjo dobilo velik pomen tudi v Sloveniji, saj se je pokazalo, da lahko z organiziranim in strokovnim pristopom pridemo do velikih dosežkov in izboljšav. Rezultati aktivne vloge družbe DARS d.d. pri upravljanju prometa se kažejo na vseh področjih, saj smo neposredno povezani s šolami, ministrstvi, univerzami, različnimi strokovnimi inženirskimi podjetji, zavodi, agencijami, tudi v mednarodnem prostoru.

Posodobitev avtocestnih predorov

Minimalne varnostne zahteve za predore v vseevropskem cestnem omrežju določa Direktiva Evropskega parlamenta in Sveta 2004/54/ES z dne 29. aprila 2004 (Direktiva 2004/54/EC), ki jo v slovenski pravni red prenaša Uredba o tehničnih normativih in pogojih za projektiranje cestnih predorov v Republiki Sloveniji (Uredba UL RS 48/2006) sprejeta 11. maj 2006.

Vsi predori na slovenskih avtocestah (razen predor Karavanke, kjer gradimo drugo cev) so od leta 2015 opremljeni v skladu z Direktivo 2004/54/EC (med evropskimi državami, ki imajo večje število predorov je Slovenija med prvimi, ki je to uredila).

S tem je zaključen sedemletni cikel ureditve predorov skladno s to direktivo. V tem času je bilo izvedenih več projektov v skupni vrednosti 25 mio. EUR. Predori so opremljeni z vso potrebno opremo, ki samodejno zaznava izredne dogodke. Prav tako so vsi predori povezani v nadzorne centre in nadzorovani z nadzorno krmilnim sistemom, ki ob izrednih dogodkih v predoru avtomatsko odreagirajo in izvedejo potrebne varnostne ukrepe (zaprtje predora, omejitve hitrosti, obveščanje udeležencev v prometu...). Prometno stanje v predorih spremljajo ekipe visoko usposobljenih nadzornikov prometa 24 ur na dan. Na nevarnih odsekih, kjer je pred predori vzpostavljen sistem za nadzor in vodenje prometa (SNVP), je le ta povezan tudi s sistemi v predoru, tako, da se v primeru izrednih dogodkov avtomatsko sprožijo omejitve in obvestila že pred predorom.

V novejših predorih so izvedeni določeni ukrepi boljši od minimalnih zahtev, saj se s tem želi doseči še višji nivo varnosti. Prav tako se neprestano izvajajo analize tveganja za predore, ki nam podajo dodatne podlage za izboljšanje varnosti.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Dobro opremljenost predorov na slovenskih avtocestah potrjuje tudi dejstvo, da ne beležimo večjih izrednih dogodkov s hujšimi posledicami. Prav tako to potrjujejo tudi ocene projekta EuroTAP (European Tunnel Assessment Programme), kjer so bili v preteklosti slovenski predori zelo dobro ocenjeni.



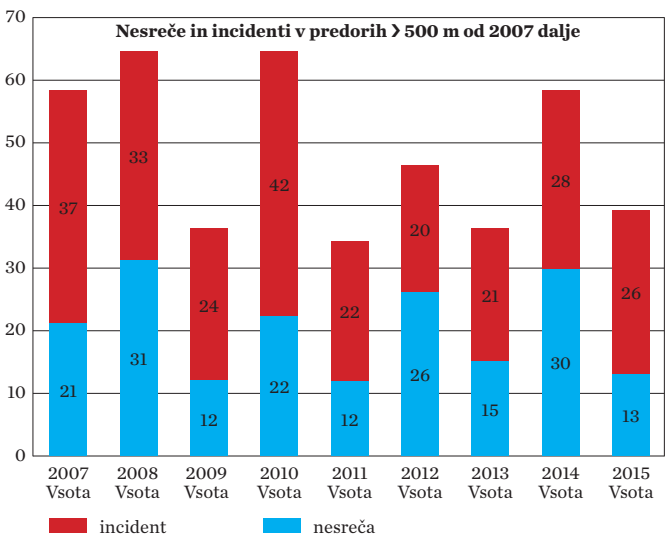
Predor Markovec, vir: DARS d.d., 2015

Varnost v slovenskih avtocestnih predorih

V času od 1.1.2007 do 30.4.2016 beležimo v daljših slovenskih avtocestnih predorih v povprečju 47 izrednih dogodkov na leto, ko je bilo potrebno začasno izločiti iz prometa del predora. Trendov naraščanja oziroma zmanjševanja absolutnega števila dogodkov ne zaznavamo, glede na nenehno povečevanje prometne obtežbe pa lahko zaključimo, da se število dogodkov vseeno zmanjšuje. Med dogodki prevladujejo prometne nesreče (37,7% od vseh dogodkov) in okvare vozil (21,2%). Požarov, ki poleg nesreč z nevarnimi snovmi predstavljajo za predore posebno nevarnost, je bilo po pričakovanjih relativno malo (2,71%). V 25% vseh dogodkov so bile za posredovanje aktivirane posebne gasilske enote, ki so usposobljene in opremljene za reševanje ob nesrečah v avtocestnih predorih in katerih delovanje sofinancira DARS.



Preko dneva se dogodki intenzivneje pojavljajo med 6. in 19. uro, beležimo pa jih vso leto.



Nesreče in incidenti v predorih, vir: DARS d.d., 2016

Da pridemo do dobre prometne varnosti v predorih, je potrebna dobra tehnologija in dobre ekipe v nadzorih centrih ter vzdrževanju

Darsova Služba za upravljanje s prometom ter prometno varnostjo prevzema veliko odgovornosti kot ključen upravljavec cestnega prometa v Sloveniji. Pomemben člen te službe so nadzorni centri (NC), ki predstavljajo jedro Oddelka za promet. V zadnjih treh letih so bile izvedene natančno načrtovane naloge, med katerimi smo ponosni predvsem na poenotenje dela nadzornikov prometa v NC. Natančna navodila so privedla do njihovega usklajenega ukrepanja. Nadzorniki prometa skrbijo za najvišjo stopnjo prometne varnosti ne samo v predorih, ampak tudi na trasi. Njihovo letno usposabljanje je natančno načrtovano (tudi na simulatorju), izvaja

Dobro opremljenost predorov na slovenskih avtocestah potrjuje tudi dejstvo, da ne beležimo večjih izrednih dogodkov s hujšimi posledicami. Prav tako to potrjujejo tudi ocene projekta EuroTAP (European Tunnel Assessment Programme), kjer so bili v preteklosti slovenski predori zelo dobro ocenjeni.

se na različnih področjih in v različni intenziteti glede na pomembnost posamezne vsebine.

V začetku prihodnjega leta bo DARS pristopil k pridobitvi nacionalne poklicne kvalifikacije (NPK) za nadzornike prometa, s katerim se bo nivo znanja v nadzornih centrih še dodatno dvignil. Nadzorniki prometa bodo s tem pridobili višjo stopnjo izobrazbe, kot se jo sicer zahteva za njihovo zaposlovanje.

Pomemben premik naprej pomeni tudi spremenjena strategija dela v nadzorih centrih, v katerih se v prihodnosti načrtuje tudi integracija sistemov. V preteklosti je bila prevečkrat načrtovana nepremišljena implementacija posameznih naprav ter sistemov, kar je skoraj privedlo do neobvladljivega dela nadzornikov prometa v NC, saj so bile naprave ter sistemi med seboj precej razkropljene. Razlog temu je predvsem to, da so se sistemi dobavljali ob izgradnji infrastrukturnih objektov v različnih časovnih obdobjih in se niso sistemsko integrirali.

Družba DARS ima v planu integracijo sistemov v NC, saj bodo ukrepanja nadzornikov prometa s tem še hitrejša in učinkovitejša. Z integracijo sistemov bo možno tudi natančno načrtovanje optimalnega števila nadzornih centrov ter strokovno potrebnega osebja, kar je cilj vsake sodobne avtocestne družbe.

V ustanavljanju je tudi Glavni nadzorni center DARS (GNC DARS), ki bo predstavljal jedro upravljanja prometa na slovenskih cestah. S strokovnim osebjem, katerega družba DARS že usposablja, bo GNC

DARS opravljal najpomembnejše naloge tako mednarodnega kot državnega prometa, tudi v koordiniranem sodelovanju z Nacionalnim centrom za upravljanjem prometa (NCUP).

Vsak dogodek, ki se zgodi v predorih, je potrebno evidentirati na način, da je zagotovljena najvišja stopnja prometne varnosti. Pomembni sistemi, ki so nameščeni v predorih so premišljeno in strokovno implementirani v tri glavne sklope:

- avtomatska detekcija prometa,
- video nadzorni sistem ter
- nadzorno krmilni sistem.

S pomočjo teh treh sistemov nadzorniki prometa v nadzornih centrih zaznavajo posebnosti v predorih. Vsak tak dogodek je potrebno obravnavati v skladu z Načrti zaščite in reševanja - NZiR, ki morajo biti predhodno usklajeni z Upravo za zaščito in reševanje. Za vsak izmed dogodkov je predviden poseben algoritem, ki se sproži avtomatsko, nekaj pa je takšnih, ki jih sproži nadzornik prometa v NC ročno. Vsa ukrepanja nadzornikov prometa v NC, ki običajno prvi zaznajo odstopanja v predorih, so natančno opredeljena v NZiR. V NZiR so opredeljene tudi naloge ostalih udeležencev pri reševanju morebitnih dogodkov. Nadzorniki prometa morajo biti posebej usposobljeni, da dogodke v predorih in izven njih rešujejo hitro, strokovno ter v skladu z navodili. Za usposabljanje nadzornikov prometa in ostalih interventnih skupin, ki sodelujejo pri reševanju dogodkov v predoru, skrbi osebje Oddelka za promet, ki takšna usposabljanja vrši vsaki dve leti.

Da predori funkcionirajo, je nujno potrebno redno vzdrževanje infrastrukture in vseh sistemov. Hitrost odprave napak na sistemih, zanesljivost sistemov in njihova nenehna posodabljanja, so ključnega pomena pri varnosti. Zato družba DARS namenja veliko pozornosti rednemu vzdrževanju infrastrukture in pripadajočih sistemov ter njihovemu nenehnemu strokovno usklajenemu obnavljanju.



Nadzorni center – primer integracije sistemov vodenja prometa, vir: DARS d.d., 2016



Predorske vaja; vir: DARS, 2016

Predorske vaje

Da se ob predorskih nesrečah lahko hitro odzovejo vse naše službe in zunanji partnerji (nadzorniki prometa, gasilci, reševalci, vzdrževalci, policija, inšpekcijske službe,...), se redno izvajajo predorske vaje. V skladu z direktivo 2004/54/ES, ki določa, da se vaje opravijo vsaj vsaka štiri leta v predorih daljših od 500 metrov v celotnem obsegu ter v čim bolj realističnih razmerah.

Z vajami želimo v praksi preveriti učinkovitost ukrepanja osebja predora in reševalnih služb ob izrednem dogodku, delovanja prezračevalnega sistema v primeru požara ter pridobiti predloge za izboljšave.

Usposabljanje in urjenje opravijo vsi zaposleni, ki so aktivno vključeni v izvajanje nalog zaščite, reševanja in pomoči po načrtu ZIR, najmanj enkrat na dve leti. Prav tako izvajamo delne simulacijske vaje vsako vmesno leto.

Cilj vaj je ugotoviti slabosti na vgrajenih sistemih v predoru, alarmnih načrtih, načrtih enot za reševanje, analizirati sisteme alarmiranja, dostopne poti in dostopne čase enot za reševanje, ukrepanje enot za reševanje ob prihodu na kraj dogodka, vzpostavitve skupnega vodje intervencije, komunikacije med nadzornim centrom Dars, ukrepi prometne policije »113«, gasilci in reševalci »112«, ter posebnosti pri uporabi in delovanju predorske opreme in varnostnih sistemov.

DARS nenehno prenaša svoja znanja in izkušnje tudi na tuje upravljavce avtocest, kjer smo npr. v letu 2014 uspešno usposobili ekipo nadzornikov prometa iz Sarajeva.

Zaključek

DARS se zaveda svoje vloge pri zagotavljanju optimalne prometne varnosti v predorih, zato nenehno vlaga velika finančna sredstva v to vrsto infrastrukture, pripadajoče sisteme in organiziranost.

Pri tem pa moramo sodelovati z vsemi deležniki, ki kakorkoli vplivajo na proces predorske prometne varnosti. To sodelovanje smo v Sloveniji zelo dobro uredili, plod tega pa se že kaže v stanju predorske prometne varnosti. Tudi vedno večja usklajenost infrastrukture in sistemov, optimizirana organiziranost in usposobljenost reševalnih enot ter uvajanje enotnih evropskih standardov in smernice nam prinaša pozitivne rezultate.

Na koncu pa ne smemo pozabiti na uporabnike avtocest. Brez njihovega sodelovanja bi bili tudi rezultati veliko slabši.

Tega se zavedamo, zato skupaj z nevladnimi organizacijami, šolami, fakultetami, avto-šolami ter v koordinaciji Javne agencije RS za varnost prometa, izvajamo veliko preventivnih akcij za uporabnike. ■



Preventivna akcija – razvrščanje; vir: DARS 2015

Avtor: Branko Skrbinek / vodja Centra za varovanje in zaščito, Policija



OBISK PREDSEDNIKA RUSKE FEDERACIJE V SLOVENIJI

Obisk predsednika Ruske federacije je predstavljal enega izmed dogodkov visokega rizika pred katerimi se je znašla Republika Slovenija in njene pristojne institucije. Kompleksno varnostno okolje, ki v zadnjem obdobju pred nas postavlja cel niz izpostavljenih tveganj je to nalogo naredilo še bolj zahtevno.

V zadnjih letih je bilo v javnosti veliko govora na kakšen način primerno obeležiti 100. obletnico spomina na smrt ruskih vojakov, ki jih je zasul snežni plaz med gradnjo ceste čez gorski prelaz Vršič. V določenem času se je zelo veliko govorilo tudi o srečanju poglavarjev Rimskokatoliške in Ruske pravoslavne cerkve. Po srečanju papeža Frančiška in patriarha Kirila v februarju letošnjega leta na Kubi je bilo jasno, da obiska v takem formatu v Sloveniji ne bo. V policiji smo se nekoliko oddahnili, saj predstavlja varovanje dveh cerkvenih poglavarjev v naši državi precejšen varnostni zalogaj. Vendar je tak občutek trajal le krajši čas, saj je predsednik države na počastitev obletnice povabil predsednika Putina, ki je povabilo tudi sprejel. S potrditvijo obiska, ki je povzročil kar nekaj negodovanja v diplomatskih krogih, se je policija znašla pred novim izzivom, ki je pomenil načrtovanje in izvedbo varovanja po najvišji stopnji.

Varovanje oseb so poznale že najstarejše kulture človeške civilizacije, v katerih so varnost zagotavljali posebej pomembnim članom določenih skupnosti. Omenjajo se staroegiptovski faraoni, inkovski vladarji, in rimski cesarji, za katere so poznali različne oblike osebnega varovanja, tako za čas življenja in za čas po smrti. Razvoj varovanja je potekal od skupinske zaščite in samozaščitnih ukrepov posameznikov do organiziranih oblik vojaške obrambe. Bolj ko so se v družbi pojavljale razlike med ljudmi oziroma razslojenost prebivalstva, večja je bila potreba po varovanju vodij in tistih, ki so povzročali te razlike. Z nastankom države kot organizirane politične skupnosti, ki ima na prostorsko omejenem ozemlju suvereno oblast, je to dejstvo pripeljalo do organiziranosti specializiranih enot za varovanje legitimnih predstavnikov države. Po razmahu terorističnih napadov na politične in diplomatske predstavnike v sedemdesetih letih prejšnjega stoletja je Generalna skupščina OZN sprejela Konvencijo o preprečevanju in kaznovanju kaznivih dejanj zoper mednarodno zaščitene osebe, vštevši diplomatske agente (Konvencija)[1], ki jo je prevzela tudi Republika Slovenija na osnovi Akta o notifikaciji nasledstva mednarodnih pogodb in obveznosti SFRJ ter s tem vse obveznosti iz te Konvencije.

Bolj ko so se v družbi pojavljale razlike med ljudmi oziroma razslojenost prebivalstva, večja je bila potreba po varovanju vodij in tistih, ki so povzročali te razlike. Z nastankom države kot organizirane politične skupnosti, ki ima na prostorsko omejenem ozemlju suvereno oblast, je to dejstvo pripeljalo do organiziranosti specializiranih enot za varovanje legitimnih predstavnikov države.

Policija je tako na podlagi mednarodno sprejetih aktov dolžna zagotavljati ustrezno varnost tako imenovanim mednarodno zaščitenim osebam. Med te akte štejemo omenjeno Konvencijo in domače pravne akte kot sta predvsem Zakon o nalogah in pooblastilih policije (ZNPPol)[2] in Uredba o varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija (Uredba)[3] ter nekaj podzakonskih aktov, ki so varovani na podlagi Zakona o tajnih podatkih (ZTP)[4] in govorijo predvsem o metodi in taktiki varovanja. Poleg navedenih pravnih aktov je policija, oziroma njena notranje organizacijska enota, Center za varovanje in zaščito (CVZ), aktivna članica dveh mrež in sicer v evropskem prostoru v mrežo za varovanje javnih osebnosti European



Network for the Protection of Public Figures (ENPPF) in v svetovnem prostoru v zvezo služb za varovanje Association of Personal Protection Services (APPS). V obeh mrežah CVZ aktivno sodeluje na področju izmenjave operativnih podatkov, dobrih praks in usposabljanj.

Priprave in izvedba varovanja predsednika Ruske federacije

Po najavi udeležbe predsednika Ruske federacije na spominski slovesnosti se je policija odzvala s prvimi aktivnostmi za pripravo obiska. V okviru Centra za varovanje in zaščito, Uprave za policijske specialnosti, Generalne policijske uprave je bila ustanovljena delovna skupina, ki je pričela z načrtovanjem varnostnih ukrepov. Podlaga za načrtovanje varnostnih ukrepov je bila stopnja varovanja in izdelana preliminarna ocena ogroženosti v katero so bili vključeni vsi podatki, ki so bili v tistem trenutku na razpolago in je glede na vrednotenje informacij in podatkov na podlagi veljavnih pravil za pripravo ocen ogroženosti, varnostnih informacij in ocen tveganj pri varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija bila ocenjena z visoko stopnjo ogroženosti. Na podlagi strokovne ocene delovne skupine je bila predlagana ustanovitev koordinacijske skupine na nivoju Generalne policijske uprave, ki je glede na razsežnost varnostnega dogodka skrbela za aktivnosti usklajevanja tako na nivoju policije kot nivoju medresorskega usklajevanja ministrstev vključenih v izvedbo spominske slovesnosti na Vršiču. V tem kontekstu je koordinacijska skupina skrbela za:

- spremljanje varnostnih razmer v Sloveniji in v svetu;
- sodelovanje z drugimi ministrstvi in drugimi državnimi organi;
- nudila kadrovsko, logistično in materialno tehnično podporo operativni skupini Centra za varovanje in zaščito ter ostalim enotam policije;
- skrbela za izvedbo načrtov varovanja;
- usklajevala aktivnosti policije za zagotovitev varnosti udeležencev srečanja, ter za varen in nemoten potek in
- pomoč in koordinacijo drugih dejavnosti ter ukrepov, ki so potrebni za zagotovitev varnosti.

V prvi fazi je CVZ na podlagi Uredbe sodeloval z ostalimi državnimi organi pri pripravi preliminarne ocene ogroženosti in pripravil predlog varnostnih ukrepov za pripravo načrta varovanja. Pri pripravi načrta varovanja so bili vključeni ukrepi preventivno operativnega, tehničnega in fizičnega varovanju v skladu z veljavnimi predpisi. Glede na obsežnost varnostnih ukrepov je bilo nujno potrebno za optimalno realizacijo določene pristojnosti prenesti na koordinacijsko skupino. Koordinacijska skupina je poskrbela, da je določene zahteve CVZ realizirala v okviru kadrovske pomoči znotraj policije, nekatere pa v okviru sodelovanja z drugimi ministrstvi. Določene aktivnosti je bilo mogoče izvesti v okviru podpisanega sporazuma o sodelovanju med Slovensko vojsko in Policijo, za nekatere (omejitev obratovanja letališča in omejitev letenja) pa je bilo potrebno pripraviti gradivo za vlado, ki je odločila v skladu s svojimi pristojnostmi.

Načrtovanje in sama izvedba varovanja je zahtevala pripravljenost in sodelovanje vseh ministrstev, vladnih služb, državnih organov in ostalih, ki so vključeni v organizacijo takega obiska, kar je predvideno in v skladu z Uredbo. Glede na stopnjo varovanja in oceno ogroženosti je bilo nujno potrebno izvesti



Varovanje predsednika Ruske federacije je bil za policijo velik strokovni in organizacijski izziv.

akreditacijski postopek, ki je pomenil večji varnostni standard in posledično izvajanje določenih varnostnih ukrepov, ki so zahtevali potreben dodatni čas in večje človeške resurse. Prav tako je bilo potrebno izvesti zaporo prometa na trasi potovanja varovane osebe, kar je pomenilo pričakovane prometne zastoje. Oba navedena ukrepa sta bila s strani načrtovalcev varovanja prepoznana kot ukrepa, ki lahko povzročita največ problemov in negodovanja med državljani in uporabniki cestnih povezav. Zaradi tega je bil sprejet sklep koordinacijske delovne skupine, da se prične s pravočasnim obveščanjem domače in tuje javnosti o cestnih zaporah v času obiska Ruskega predsednika v Sloveniji. Ta sklep se je kasneje izkazal kot zelo uspešen, saj v času obiska ni bilo omembe vrednih zastojev na cestnem omrežju Republike Slovenije, kljub drugačnim predvidevanjem.

CVZ (prej Urad za varnost in zaščito) ima dolgoletne izkušnje z varovanji po najvišji stopnji pomembnih svetovnih voditeljev in je tudi v tem primeru izvedel varovanje v skladu z veljavnimi mednarodnimi in domačimi predpisi. Za izvedbo varovanja je uporabil vse razpoložljive resurse (materialne in človeške) in kadrovsko pomoč vseh policijskih enot policije. Pri izvedbi varovanja je sodeloval z vsemi ministrstvi in državnimi organi ter še posebej z Društvom Slovenija Rusija, in varovanje izvedel na najvišji strokovni ravni, za kar je dobil priznanje vseh naštetih in še posebej Ruske varnostne službe.

Zaključek

Zagotavljanje varnosti oseb, ki so v nacionalnem interesu, predstavlja element zagotavljanja varnosti demokratične ureditve z izvajanjem varnostnih ukrepov preventivno operativnega, tehničnega in fizičnega varovanja. Izvajanje navedenih ukrepov temelji na Ustavi Republike Slovenije, spoštovanju človekovih pravic in temeljnih svoboščin ter demokracije in načel pravne države in spoštovanju vseh predpisov domačega in mednarodnega pravnega reda. Na podlagi zapisanega lahko zaključimo, da je danes pri varovanju oseb in objektov pravni izziv večji kot operativno taktični. Še posebej, ko se soočimo z izzivom, kako zagotavljati varnostne standarde ob pogoju zakonitosti in racionalnosti ter pri varovanju uporabljati le tiste metode in sredstva, ki so izrecno dovoljena. Varovanje predsednika Ruske federacije je bil za policijo velik strokovni in organizacijski izziv. Strokovni je bil predvsem zaradi priprave ocene ogroženosti glede na trenutne razmere v svetu in Evropi, glede terorističnih groženj in migrantske problematike ter optimalnega načrtovanja ukrepov ob racionalni uporabi proračunskih sredstev. Organizacijski pa predvsem zaradi kadrovske podhranjenosti, ko že večje akcije, v tem primeru varovanje predsednika Ruske federacije, zahtevajo izdatno kadrovsko pomoč policijskih uprav.

[1] *Konvencija o preprečevanju in kaznovanju kaznivih dejanj zoper mednarodno zaščitene osebe, vštevši diplomatske agente*, (Konvencija), Uradni list SFRJ, št.: 54/1976.

[2] *Zakon o nalogah in pooblastilih policije,* (ZNPPol), Uradni list RS, št.: 15/2013 in nasl.

[3] *Uredba o varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija*, (Uredba), Uradni list RS, št.: 63/2013.

[4] *Zakon o tajnih podatkih*, (ZTP), Uradni list RS, št.: 87/2001. ■

Avtorja: Metod Budna, mag. obramboslovja / Gorenje Group*
Alma Ribič, mag. varstvoslovja / Gorenje Group*





OBVLADOVANJE VARNOSTI Z OCENJEVANJEM TVEGANJ

Ocenjevanje tveganj pridobiva vedno večjo vlogo pri obvladovanju vseh varnostnih pojavov, tako na nivoju nacionalne varnosti kot tudi poslovnih sistemov. V Gorenju smo se za namen ocenjevanja tveganj na operativni ravni varovanja ljudi in premoženja odločili poiskati lastni sistem ocenjevanja. Na podlagi izkušenj in znanja v podjetju smo ubrali svojstven pristop oz. metodologijo za ocenjevanje tveganj v varovanih območjih Gorenja.

Uvod

Zavedamo se, da so gospodarske družbe in druge organizacije (v nadaljnjem besedilu podjetja) izpostavljene različnim negativnim vplivom iz ožjega (notranjega) in tudi iz širšega okolja. Ob tem se pojavljajo večji ali manjši škodni dogodki z materialnimi in finančnimi posledicami, nemalokrat še huje, torej s posledicami za zaposlene in pa za zunanje osebe, ki se v trenutku neželenega dogodka nahajajo na varovanem območju podjetja. Škodno delovanje in neželeni dogodki tako za podjetje predstavljajo določeno tveganje, ki ga lahko imenujemo tudi skozi funkcijo nevarnosti oz. ogroženosti podjetja.

Škodni (negativni, neželeni) dogodki, ki se pojavljajo v daljšem časovnem obdobju, ne glede na obseg, predstavljajo za podjetje in za zaposlene negotovost, pojav strahu in v skrajnih oblikah celo paniko. Prav tako je potrebno razmišljati tudi o latentnih škodnih dogodkih. Posledice škodnih dogodkov lahko sežejo vse do zastojev poslovnih in proizvodnih procesov, odhoda strokovnih kadrov, ukinitev investicijskih vlaganj, do zastojev v razvoju idr. Škoda se na koncu izrazi predvsem v finančnem smislu, prav tako pa je zelo pomembno zavarovalniško področje, kar pa lahko vse skupaj predstavlja grožnjo za nadaljnji obstoj podjetja.

Za funkcijo neprekinjenega poslovanja in delovanja podjetja je zelo pomembno identificiranje različnih tveganj in v nadaljevanju njihova analiza ter ocenjevanje, seveda vključno z vsemi ostalimi koraki celovitega obvladovanja tveganj, kjer so opredeljeni tudi »lastniki tveganj« in povezava tveganj s strategijo podjetja. Na področju zasebnega varovanja ljudi in premoženja smo se za lastne potrebe varovanja družbe Gorenje d.d. in glede na pretekle izkušnje ter vedenje, lotili obvladovanja tveganj z uporabo modelov in metod poznanih iz teoretičnih del različnih avtorjev ter s pomočjo lastnega znanja. To ocenjevanje oz. prepoznavanje tveganj (nabor možnih tveganj) je v podjetju obvladovano skupaj z drugimi delovnimi področji. Za operativno ocenjevanje stopnje tveganja (na področju varovanja ljudi in premoženja) za lastna varovana območja in tudi stopnje tveganja za varovanje javnih zbiranj pa smo ubrali svojstven pristop, ki je rezultiral v izdelanih obrazcih s kriteriji, ki temeljijo na prej omenjenih prepoznanih tveganjih. Vodilo pri izdelavi teh obrazcev je bila predvsem uporabna, praktična vrednost za naše podjetje (dejanska takojšnja uporaba rezultatov ocene tveganja v praksi). Obrazci so v celoti prilagojeni poznavanju problematike lastnih varovanih območij in so dobra podlaga za izdelavo načrtov varovanja in pomoč odločevalcem v podjetju o tem,

Za funkcijo neprekinjenega poslovanja in delovanja podjetja je zelo pomembno identificiranje različnih tveganj in v nadaljevanju njihova analiza ter ocenjevanje, seveda vključno z vsemi ostalimi koraki celovitega obvladovanja tveganj, kjer so opredeljeni tudi »lastniki tveganj« in povezava tveganj s strategijo podjetja.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

kaj je potrebno na področju zasebnega varovanja v podjetju še postoriti.

Tveganja in obvladovanje le-teh

Za pojem tveganja obstaja veliko definicij. Nekatere med njimi pravijo, da je tveganje lahko vsako zmanjšanje koristi podjetja. Prav gotovo govorimo o stanju podjetja, kjer gre za negativno razliko med načrtovanimi cilji in pričakovanimi rezultati. Tveganje vsebuje verjetnost nastanka nekega dogodka, ki bi lahko imel (predvsem) negativne posledice za uresničitev planiranih ciljev podjetja. V strokovni literaturi je zaznati, da se negativni pojavi/dogodki poimenujejo različno, kot npr. grožnje, spet drugič kot tveganja, tudi kot nevarnost, nekateri te pojave ocenjujejo kot izziv ali celo priložnost. Če vsa ta poimenovanja damo pod skupni imenovalec, lahko to imenujemo tveganje za varnost, torej tisto tveganje, ki bi v podjetju povzročilo grožnjo za varnost ljudi in premoženja, podatkov, informacij, znanja, skratka grožnjo funkcijam za realizacijo planiranih ciljev in uspešnih finančnih rezultatov.

Tveganjem na vseh področjih življenja se enostavno ni moč izogniti, zato jih je zelo pomembno znati prepoznavati, analizirati, ocenjevati in obvladovati, kar pomeni iskati možnosti preventivnega in korektivnega ukrepanja za zmanjševanje stopnje tveganja. Pri tem se ne sme zanemariti vidika povezanosti tveganja s kakovostjo izvedbe procesov. Pomeni, da če želimo proces izvesti z rezultatom čim bolj kakovostnih izdelkov ali kakovostne storitve, ne smemo zanemariti aktivnosti za zmanjšanje tveganj na vseh načrtovanih in izvedbenih točkah procesa.

Sprejemanje tveganja je povsem normalen in nujen poslovni pojav, ker bi v nasprotnem primeru to nesprejemanje pomenilo nesposobnost in nepripravljenost odgovornih oseb spopasti se z nevarnostmi, izzivi in priložnostmi.

Celovito upravljanje s tveganji – risk management vsebuje prepoznavanje tveganj – risk identification, analiziranje tveganj – risk analysis, ocenjevanje tveganj – risk assessment, zavarovanje tveganj – risk insurance in vse druge aktivnosti za zmanjševanje tveganj v vseh poslovnih procesih podjetja. Obvladovanje tveganj zahteva organizirane, načrtne in dolgoročne pristope. Zahteva znanje, sposobnost in delovanje odgovornih oseb v podjetjih, da prevzemajo in nadzirajo tveganja, da ne bi prišlo do ogrožanja poslovanja, obratovanja podjetja in da ne bi tveganja onemogočila nadaljnjega razvoja podjetja. Sprejemanje tveganja je povsem normalen in nujen poslovni pojav, ker bi v nasprotnem primeru to nesprejemanje pomenilo nesposobnost in nepripravljenost odgovornih oseb spopasti se z nevarnostmi, izzivi in priložnostmi.

Tveganja na področju varovanja ljudi in premoženja v podjetju

Na področju varovanja ljudi in premoženja v podjetju je bistvenega pomena identifikacija različnih tveganj, njihova vsebinska opredelitev ter iskanje vzrokov za njih in nazadnje poskus odprave ali vsaj zmanjšanja vplivov teh tveganj. Potrebno jih je povezati s temeljno strategijo podjetja in jim nenazadnje določiti tudi »skrbnika«.





Katera tveganja bi lahko bila povezana s področjem varovanja ljudi in premoženja? Obstaja jih precej, nekatera med njimi: neustrezna organizacija fizičnega varovanja, pomanjkljivo dokumentirani postopki delovanja, nezadostno število varnostnega osebja, pomanjkljivo znanje – usposobljenost varnostnega osebja, nezakoniti vstopi v prostore oz. varovano območje, izdaja – zloraba poslovnih skrivnosti in drugih podatkov s strani zaposlenih, koruptivna tveganja varnostnega osebja, neustrezen interni nadzor nad delom varnostnega osebja, nezakonito nošenje in nepravilna hramba ter evidenca službenega orožja, inkriminirana dejanja, terorizem in še veliko drugih. Omeniti velja tudi tveganja na področju zaščite in reševanja v podjetju, kot so npr. tveganja zaradi naravnih nesreč (potresi, poplave, ...) in tveganja zaradi industrijske nesreče. Pri slednjih lahko pri vzrokih za ta tveganja govorimo o odsotnosti rednih kontrol, navodil za delo, odsotnost rednega vzdrževanja in izvajanja pregledov delovne opreme, cevovodov, ventilov ..., odsotnost vzdrževanja celovitega in učinkovitega obveščanja in alarmiranja, nezagotavljanje materialnih pogojev za delo civilne zaščite, opustitev usposabljanja zaposlenih, idr. Tudi to področje je nerazdružljivo z varovanjem ljudi in premoženja, čeprav sta funkciji zasebnega varovanja in civilne zaščite v Gorenju, d.d. ločeni.

Operativno ocenjevanje tveganj varovanih območij Gorenja, d.d.

Pri vsakem poskusu ocenjevanja tveganj se je najprej potrebno zavedati, da je vsako ocenjevanje tveganj, tveganje. Kljub še tako izdelani metodi, temelječi na vseh možnih teoretičnih podlagah, matematičnih modelih ipd., je na koncu vsaka izdelana ocena tveganja subjektivni izdelek presojevalca. Niti dva presojevalca ne bi nekega tveganja ocenila enako zaradi različnih interpretacij posameznih elementov tveganja in osebnih preferenc posameznika, saj ne obstaja nek univerzalni (matematični) model za katerega bi lahko rekli, da upošteva vse možnosti, kaj šele naključja, ki so vedno prisotna pri varovanju ljudi in premoženja, tudi če sami menimo, da v celoti obvladujemo vse vidike varnosti ljudi in premoženja v podjetju.

V Gorenju, d.d. je tako izdelan katalog tveganj, ki vsebuje zaznana tveganja na področjih, ki se ukvarjajo s poslovanjem in z varnostjo podjetja. Ta področja so: varnostna politika, varnostni sistem, varnost in zdravje pri delu, varstvo pred požari, varovanje okolja, fizično in tehnično varovanje, varovanje osebnih in poslovnih podatkov, varovanje poslovnih skrivnosti, varovanje intelektualne lastnine, zaščita in reševanje (civilna zaščita), informacijska varnost, zavarovanja idr. Področja, ki jih pokrivajo različne službe, sama razčlenjujejo prepoznana tveganja in sprejemajo ukrepe za minimaliziranje teh tveganj.

Kot je že bilo omenjeno, smo tako tudi v službi Varovanja izdelali svojo metodologijo (obrazec) za ocenjevanje tveganj na svojem delovnem področju. Izdelane ocene uporabljamo kot pripomoček pri vsakodnevnem delu, kaj in kje je potrebno izboljšati, da bo naša služba bolje, bolj učinkovito delovala in obvladovala tveganja znotraj svojega delokroga. Vodilo pri izdelavi je bila predvsem praktična vrednost (ne izdelava zaradi same izdelave, prav tako ne čisto znanstveni pristop).



Obrazec je zasnovan tabelarično, da zagotovimo preglednost. Prav tako lahko vsak vodja oz. odgovorni takoj poišče tisti del ocene, ki ga zanima in začne z odpravljanjem pomanjkljivosti na svojem področju. V glavi obrazca najdemo rubriko za osnovni opis lokacije varovanega območja/objekta in podatke o presojevalcu. V nadaljevanju pa so razdelani elementi, kriteriji, ki jih presojamo pri vsakem varovanem območju (elementi prepoznani kot pomembni za varovana območja Gorenja, d.d. na področju varovanja ljudi in premoženja). Ti elementi zajemajo vrsto proizvodnje oz. dejavnosti na varovanem območju, sistem že vzpostavljenega varovanja, fizično varovanje, ograje, oznake varovanega območja, urejenost gibanja po območju (tako zaposlenih kot tudi zunanjih oseb), nadzor nad delom varnostnega osebja, dostopi do in varovanje posameznih objektov, dostopi do in varovanje ključnih oseb, dostopi do in varovanje blagajn, sefov/trezorjev, dostopi do in varovanje informacijsko komunikacijske tehnologije, dostopi do in varovanje osebnih, zaupnih podatkov, poslovnih skrivnosti, dostopi do in varovanje arhivov, dostopi do in varovanje skladišč, skladišč/objektov z nevarnimi snovmi, dostopi do energetskih vodov, instalacij ipd., ustreznost tehničnega varovanja območja (videonadzor, alarmni sistemi, požarni sistemi, pristopna kontrola, registracija delovnega časa ipd.), ustreznost nadzornega centra ipd., obvladovanje ključev, evidenc, varovanje parkirišč, garaž, ustrezna urejenost materialnega poslovanja (del, ki zadeva varovanje ljudi in premoženja), kriminalna tveganja (zaznana, potencialna) in druga pomembna varnostna ogrožanja. V procesu ocenjevanja se preverijo tudi načrtovani ukrepi v primeru protivlomnega alarma, sprožitve tipke za osebni napad, požarnega alarma, v primeru izrednega dogodka (vlom, tatvina, prometna nesreča, grožnja, zastoj v dvigalu, nedovoljeni prehodi, vdori itd.), v primeru naravne ali industrijske nesreče ipd.

Pri vsakem obravnavanem elementu se opiše ogroženost, ranljivost, možne škodne posledice, verjetnost škodnih dogodkov. Poda se opis varovanja, postopkov in stanja posameznega elementa. V naslednjo rubriko pa se dodajo predlogi za varovanje, varnostni ukrepi, možne izboljšave, rešitve, priporočila in druge morebitne opombe. Pri vsaki rubriki se določi tudi številčna stopnja tveganja od 1 do 3, pri čemer 1 pomeni nizko stopnjo, 2 srednjo in 3 visoko stopnjo tveganja. Na koncu se točke seštejejo in dobljeni rezultat se interpretira kot končna ocena tveganja, vendar pa je še vedno možnost, da presojevalec poda še subjektivno oceno mimo seštevka točk.

Možnost je tudi ta, da se presojevalec sam odloči katere rubrike so pomembne (če je ena rubrika ocenjena kot tako zelo pomembna za oceno, se ji lahko prisodi večja teža ipd.), prav tako daje možnost izpustitve katere od rubrik itd. Presojevalec ima možnost pojasniti svojo odločitev na koncu ocene, saj kot smo že ugotovili, je ocenjevanje tveganj v večji meri subjektivno. Z raznimi togimi modeli pa spremenljivka, ki je znana samo presojevalcu in je mogoče zelo specifična, ne bi bila upoštevana.

Zaključek

Gorenje, d.d. se zaveda pomembnosti ocenjevanja tveganj na vseh področjih. Od strateškega nivoja do operativnih ravni. V službi Varovanja smo se zato odločili, da bomo na operativni ravni izdelali/uporabljali praktični model ocenjevanja tveganj na področju varovanja ljudi in premoženja, ki nima toliko oz. ima manj opore v znanstvenih modelih. Ker svoje podjetje najbolje poznamo, menimo da smo s tem individualnim pristopom, ki bi se ga z nekaj korekcijami lahko uporabilo tudi drugje, dosegli boljše obvladovanje tveganj in tako izboljšali varnostno sliko podjetja na našem obravnavanem področju.

Viri

- Vršec, M., (2007). Ravnanje s tveganji in spremembami – Risk management. Fakulteta za varnostne vede, Ljubljana.
- Interni viri Gorenje, d.d. ■

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
Elena Blaževič, absolventka magistrskega študija »Management korporativne varnosti«

MANAGEMENT KORPORATIVNE VARNOSTI POMEMBEN POKLICNI PROFIL PRIHODNOSTI

Pogovarjali smo se z absolventko magistrskega študija »Management korporativne varnosti«, ki je kot študentka prve generacije študija na GEA College/Fakulteti za podjetništvo pustila neizbrisen pečat pri začetku tvorjenja pomembne profesije v Republiki Sloveniji.

Nam lahko v kratkem predstavite vaše trenutno delovno okolje in povezanost vašega dela s procesi korporativne varnosti. Prihajate namreč iz okolja zelo uspešnega družinskega podjetja Elita i.b., d.o.o.

Trenutno delam preko študentskega servisa v podjetju, ki ima sedež v Ljubljani, vendar poleg tega vedno pomagam tudi v družinskem podjetju Elita i.b., d.o.o., ki se ukvarja z izdelavo celotne projektne dokumentacije, svetovalnim inženiringom in vodenjem investicij. Podjetje ima ustrezna pooblastila za načrtovanje in nadziranje nad celotno izvedbo tehničnega varovanja v objektih: požarno varnost, protivlomni in video nadzorni sistemi, nalogi iz varnosti in zdravja pri delu ter med drugim opravlja tudi preglede aktivne požarne zaščite, izdeluje zasnove požarne varnosti za požarno manj zahtevne objekte in študije požarne varnosti za požarno zahtevne objekte. Tukaj lahko govorim o korporativni varnosti, saj predstavlja požarna varnost velik del le-te. Tako v manjših kot v večjih organizacijah je potrebna implementacija premišljenega sistema organiziranih in usklajenih ukrepov požarne zaščite. Cilj vsakega sistema varovanja pred požarom je, že v študiji pravilno predvideti vso požarno zaščito, da bi v primeru požara, le tega lahko odkrili pravočasno in ga preprečili, saj le z zgodnjim odkritjem lahko omejimo materialno škodo, zmanjšamo negativen vpliv na delovno okolje, zmanjšamo izredne dogodke v poslovnih procesih ob nastanku požara in tako povečamo varnost premoženja, opreme in ljudi v delovnem okolju.

Nam lahko zaupate kateri so tisti razlogi, ki so prevladali k sprejemu odločitve, da magistrski študij nadaljujete na programu »Management korporativne varnosti«.

Ko je napočil čas vpisa na magistrski študij, sem zasledila na Fakulteti za podjetništvo Gea College, novo smer Management korporativne varnosti. Sprva nisem niti sama vedela kaj pravzaprav je korporativna varnost. Tako sem se odločila obiskati okroglo mizo, ki je bila v Državnem svetu Republike Slovenije. Tam sem imela možnost pobližje spoznati to področje, ki me je takoj navdušilo. Še bolj me je navdušil pogovor s predsednikom Inštituta za korporativne varnostne študije dr. Čaleto, ki mi je na kratko predstavil, kaj me čaka v prihajajočih letih. Bi poskusila? Zakaj pa ne. Zanimivo, zame novo področje, najboljši profesorji, praksa in še in še. Tako je padla odločitev o študiju, seveda tudi v povezavi z domačim družinskim podjetjem.

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

Prvi vtisi so bili odlični in pričakovanja vsekakor dosežena. S profesorji smo se dobro ujeli. Pomagali so nam pri nastalih ovirah, dajali napotke, spodbujali in nas pripravili na svet, ki nas čaka zunaj študijskih klopi. V dveletnem magistrskem programu smo spoznali vse veje

*avtor je član Slovenskega združenja korporativne varnosti



V dveletnem magistrskem programu smo spoznali vse veje korporativne varnosti, od informacijske varnosti do fizične, požarne varnosti, finančne varnosti, varnosti kadrov. Povezovali smo teorijo s prakso in se naučili kako prepoznati, obvladovati oziroma obvladati ter preprečiti različna varnostna tveganja, s katerimi se podjetja srečujejo. Korporativna varnost je še kako pomembna v današnjem svetu, da podjetje lahko preživi.

korporativne varnosti, od informacijske varnosti do fizične, požarne varnosti, finančne varnosti, varnosti kadrov. Povezovali smo teorijo s prakso in se naučili kako prepoznati, obvladovati oziroma obvladati ter preprečiti različna varnostna tveganja, s katerimi se podjetja srečujejo. Korporativna varnost je še kako pomembna v današnjem svetu, da podjetje lahko preživi.

Sam študij je prepleten z različnimi dopolnilnimi možnostmi za izpopolnjevanje in preverjanje teoretičnih spoznanj v neposrednih praktičnih okoljih. Menite, da je za vas možnost udeležbe na različnih dogodkih, v organizaciji Slovenskega združenja za korporativno varnost, lahko dodana vrednost za pridobivanje novega znanja?

Vsekakor. Med študijem smo imeli to izjemno priložnost, da smo se lahko udeležili raznih dogodkov, ki sta jih organizirala Inštitut za korporativne varnostne študije in Slovensko združenje za korporativno varnost. Dogodki kot so Dnevi korporativne varnosti, Mednarodna konferenca »Izzivi zoperstavljanja terorizmu v regiji JV Evrope«, mesečna srečanja**.** Obiskali smo mnoga podjetja in imeli priložnost spoznati najboljše slovenske managerje in korporativne ase s katerimi smo izmenjali mnenja in se od njih veliko naučili. Take priložnosti ne dobiš kar tako in je vsekakor to eden izmed največjih plusov tega študija.

Ocenjujete, da vam bodo nova znanja koristila v nadaljevanju vaše poslovne kariere v vaši organizaciji?

Trenutno sem še v Ljubljani, saj moram še dokončati študij z magistrsko nalogo, a sem prepričana da mi bo to znanje še kako koristilo v domačem podjetju, ali pri iskanju nove zaposlitve in na moji bodoči karierni poti. Vse več bo povpraševanja po tovrstnemu kadru, saj je obvladovanje tveganj ključnega pomena v organizaciji.

Bi izrabila priložnost, če bi se vam ponudila možnost dela na področju korporativne varnosti v mednarodnem okolju?

To bi bil definitivno korak v novo smer, katere se ne bi branila. V tujini se bolj zavedajo nevarnosti in tveganj, ki jih prinaša poslovno okolje in bi pridobila, najverjetneje, neprecenljivo znanje.

Ali po vašem mnenju poslovno okolje v Sloveniji dovolj dobro pozna vlogo korporativne varnosti kot enega izmed osnovnih predpogojev za učinkovito delovanje organizacij?

Poslovno okolje Slovenije v primerjavi s poslovnim okoljem po svetu še ne pozna dovolj dobro vlogo korporativne varnosti. Podjetja in organizacije, ki so v tuji lasti so veliko bolj ozaveščena, čeprav je bilo razvidno na vseh konferencah in seminarjih, srečanjih, da se vodilni kadri tudi pri nas vse bolj zavedajo, da bi morali vzpostaviti varnostni sistem v samem poslovanju podjetja, da bi zaščitili notranjo varnost podatkov s sodobnim informacijskim sistemom, varnostno kulturo zaposlenih, ter vedno bolj tudi s tehničnim in fizičnim varovanjem. O varnosti na delovnih mestih in o varovanju delovnih mest, pa smo, po mojem osebnem mnenju, že na visokem nivoju, saj so v novejših objektih in v javnih ustanovah predvidena varnostna varovanja pred požari že v študijah, ki so lahko že del projektne dokumentacije. Poklic managerja korporativne varnosti je po svetu zelo razširjen, a v Sloveniji je to nekaj novega. V naši bližnji prihodnosti bodo večja podjetja iskala tovrsten kader, ki poleg direktorja predstavlja ključno funkcijo v podjetju.

Pogosto pri obravnavanju varnostnih problemov naletimo na pomisleke glede spolne enakopravnosti in vloge žensk na področju korporativne varnosti. Menite, da bi bilo potrebno za podiranje teh stereotipov v javnosti vložiti več napora? Na samem študiju tega programa na GEA College je zastopanost nežnejšega spola izredno uravnotežena.

Menim, da smo ženske v enakopravnem položaju skoraj v vseh poklicih, vendar nismo enako ocenjene, ali cenjene. Večina nas ocenjuje kot »multipraktik« saj smo sposobne delati veliko stvari naenkrat kvalitetno in natančno, z odgovornostjo in preudarnostjo. Na področju korporativne varnosti, žal še nismo, oziroma še nismo dovolj uveljavljene saj je po mojem mnenju potrebno imeti poleg izobrazbe še delovne izkušnje, mogoče v sodelovanju z že uveljavljenim korporativno usposobljenim managerjem, kar je seveda tudi moja velika zaposlitvena želja. ■

Med študijem smo imeli to izjemno priložnost, da smo se lahko udeležili raznih dogodkov, ki sta jih organizirala Inštitut za korporativne varnostne študije in Slovensko združenje za korporativno varnost.Take priložnosti ne dobiš kar tako in je vsekakor to eden izmed največjih plusov tega študija.



Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Management korporativne varnosti

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj **Management korporativne varnosti**?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

- *Management človeških virov*
- *Okoljski vidiki korporativne varnosti*
- *Metode raziskovanja varnostnih pojavov*
- *Zavarovalništvo v procesih zagotavljanja gospodarske varnosti*
- *Gospodarsko poizvedovanje in varovanje poslovnih informacij*
- *Informacijska varnost*

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

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

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

CENTER VIŠJIH ŠOL

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

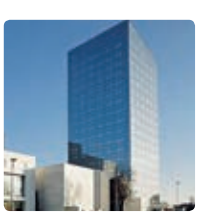
FAKULTETA ZA PODJETNIŠTVO

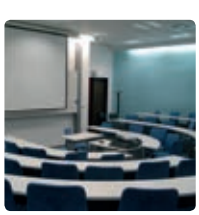
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo

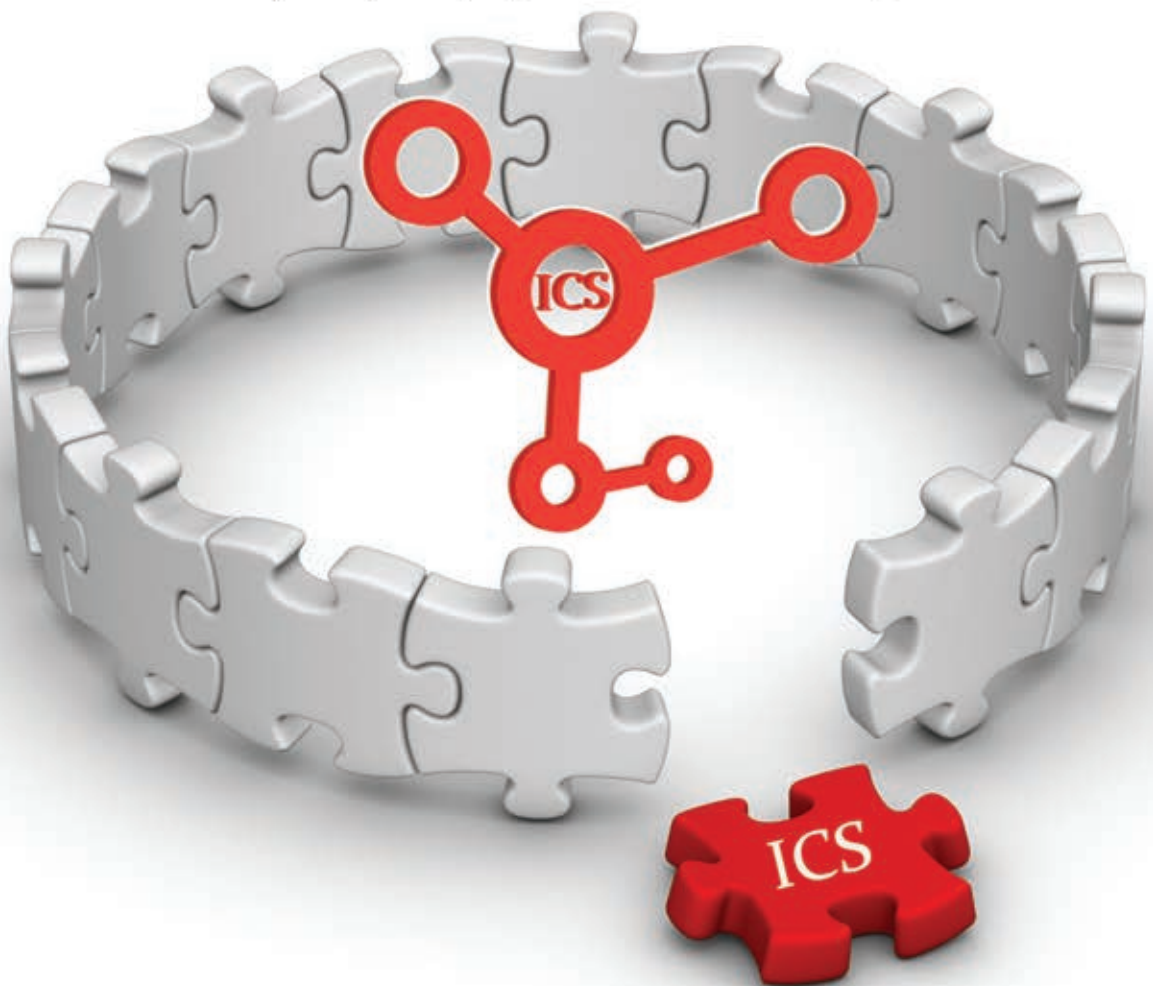
8. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 15.—16. marec 2017



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