Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

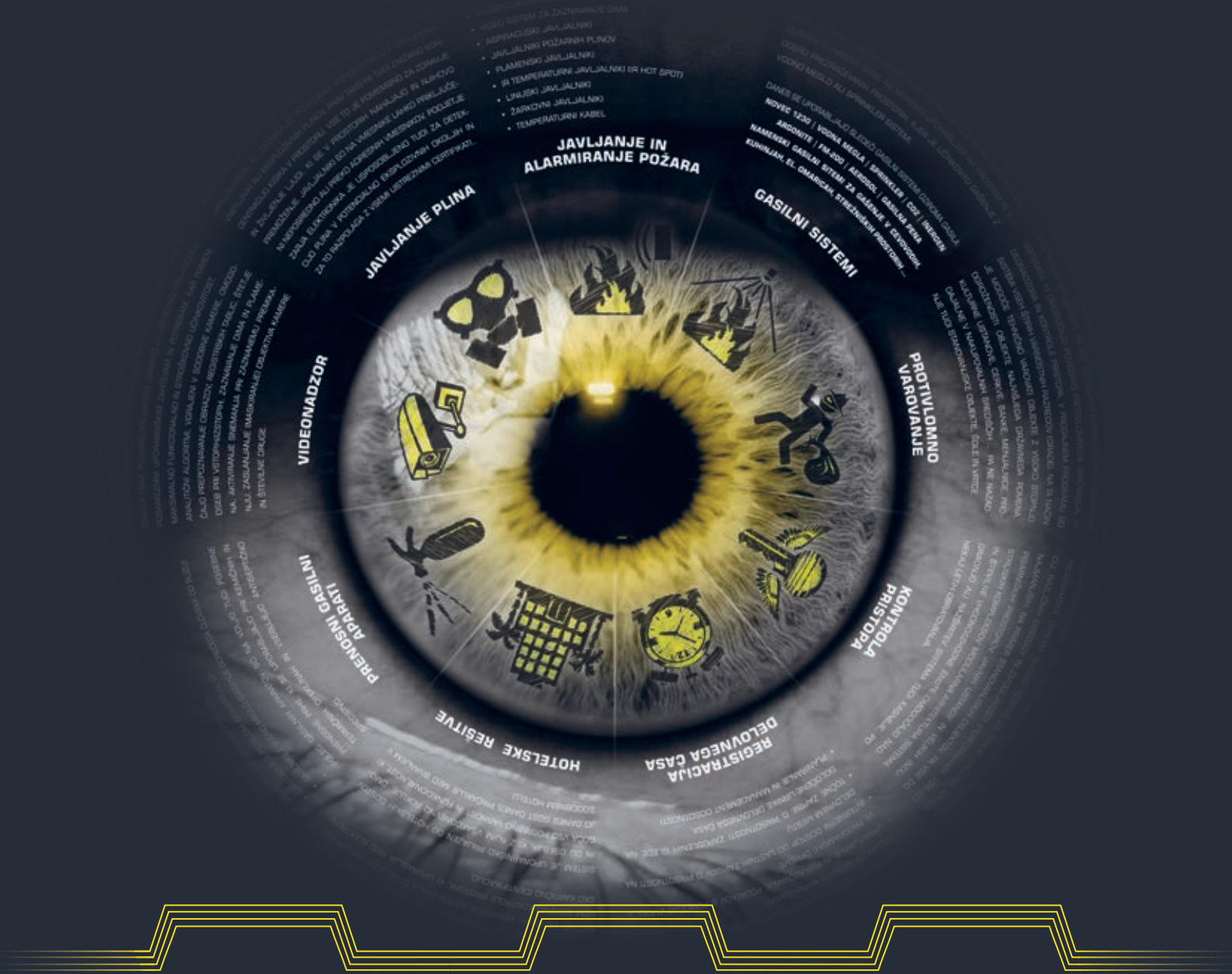
Letnik 2018, marec • št. 16



Magistrski študijski program »Upravljanje s tveganji in korporativna varnost«

GZS na čelu gospodarskega razvoja Slovenije

Mag. Sonja Šmuc, generalna direktorica Gospodarske zbornice Slovenije



Varno v nov dan

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

www.zarja.com

ZARJA ELEKTRONIKA





Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
marec 2018

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

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

Letos je pred nami vsekakor vsebinsko najbolj bogata mednarodna konferenca Dnevi korporativne varnosti. Udeleženci na konferenci prihajajo kar iz desetih držav, kar daje konferenci vedno večjo mednarodno prepoznavnost. Posebej pa je potrebno izpostaviti pomen, ki ga ima dogodek v nacionalnem okolju, saj že dolgo časa velja za kvalitetno najbolj prepoznaven dogodek s področja varnosti. To vsekakor dokazuje tudi udeležba najpomembnejših gostov iz poslovnega, političnega in strokovnega okolja. Razmah konference in vedno večje število udeležencev kaže na to, da se zavedanje o pomenu varnosti počasi a vendar vztrajno dviguje. Najbolj prepoznavna rast udeležencev je zaznana ravno iz gospodarskega okolja, k čemur verjetno pripomore dejstvo, da je varnostno okolje v katerem delujejo organizacije vedno bolj zahtevno. Učinkovitega poslovanja si enostavno ni mogoče zamisliti brez dejstva, da je pomembno težišče namenjeno obvladovanju dinamičnih tveganj s katerimi se soočajo na globalnih trgih. Dodatno prepoznavnost dogodku daje tudi podelitev prestižne nagrade Slovenian Grand Security Award, ki se vsako leto tradicionalno podeljuje v okviru otvoritvene slovesnosti omenjene konference.

V zadnjem obdobju smo tudi v Republiki Sloveniji priča nekaterim pomembnim procesom, ki bodo v prihodnje zaznamovali področje, ki je povezano z zagotavljanjem varnosti. Na začetku leta je bil sprejet Zakon o kritični infrastrukturi, ki bo od vseh udeleženih na tem področju zahteval velike napore za učinkovito implementacijo. V tem delu bodo izredno pomembne izkušnje, ki jih prinaša Institut za korporativne varnostne študije in neposredno tudi Slovensko združenje za korporativno varnost. Poleg navedenega je v zaključni fazi implementacija evropske uredbe o varstvu osebnih podatkov GDPR, saj je mesec maj praktično pred vrati. Še vedno pa je odprtih nekaj pomembnih dilem, ki jih bo potrebno reševati in bo končne odgovore prineslo šele obdobje ob njihovem neposrednem uveljavljanju. Posebej pa bi želel izpostaviti tudi pomen javne razprave, ki poteka ob pripravi Zakona o informacijski varnosti. Posebno dejstvo, ki ga pripravljavci ne smejo spregledati, je vsekakor medsebojna usklajenost in sistemskost sprejetih zakonskih rešitev, tako na področju kritične infrastrukture, kakor tudi s tem neobhodno povezane informacijske varnosti. Za konec pa velja izpostaviti kripto valute in blokchain tehnologijo, ki vedno močneje vstopa v določene procese. Varnostna tveganja, ki jih prinaša uporaba, predvsem neosveščenih uporabnikov, pa vedno pomembneje nastopajo v vsakdanjem življenju.

V tokratni številki, ki je posvečena mednarodni konferenci Dnevi korporativne varnosti smo odprli cel niz aktualnih tem. V kolumni smo varnostne vidike postavili v širši geopolitični prostor regije v kateri živimo in poslujemo. K pogovoru smo povabili več zanimivih in izpostavljenih sogovornikov, ki so vsak iz svojega strokovnega stališča pomembno obogatili tokratno številko revije.

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

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
Stanislav Veniger, svetovalec za korporativno varnost, Zavarovalnica Triglav d.d.

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

17



KOLUMNA
Vojko Volk, veleposlanik

SLOVENIJA – SMER SEVER-SEVEROZAHOD

Usoda majhnih gospodarstev, kakršno je slovensko, je močno odvisna od zunanjega sveta. Poznavanje sveta in razmer v njem je zato ključnega pomena za uspešno gospodarjenje in razvoj, predvsem pa za ...

21



KAKO IZBRATI USTREZNO OSEBO ZA VARSTVO OSEBNIH PODATKOV (DPO)?

Pred vrati je uveljavitev Splošne evropske uredbe o varstvu podatkov, ki jo strokovna javnost pozna pod nazivom GDPR (General Data Protection Regulation). Uredba prinaša nekaj pomembnih novosti, katera pred zavezance postavlja resno zavezo za vzpostavitev vseh mehanizmov, ki bodo zagotavljali učinkovito varovanje zaupanih osebnih podatkov.

26



VAROVANJE PRVENSTVA UEFA FUTSAL EURO 2018

Veliki športni dogodki nudijo poleg svojih ekonomskih in socialno - kulturnih priložnosti, ki ugodno vplivajo in dvigujejo perspektive mestnih gospodarskih entitet oz. celo držav, tudi povečano varnostno tveganje lokalnih, nacionalnih, lahko tudi internacionalnih dimenzij.

43



PASTI IN ZAŠČITA V SVETU KRIPTOVALUT

Virtualne valute ali morda bolje poznane kot kriptovalute so postale znani globalni fenomen za veliko ljudi. Preden pa se podate v svet kriptovalut, je dobro poznati pasti, ki vas na tej poti lahko čakajo in kako se zaščititi, ko boste na le-te naleteli.

55

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

INTERVJU
mag. Sonja Šmuc, generalna direktorica Gospodarske zbornice Slovenije

GZS NA ČELU GOSPODARSKEGA RAZVOJA SLOVENIJE

Gospodarska zbornica Slovenije je ključen dejavnik pri dvigovanju varnostnega zavedanja, kot pomembnega predpogoja za učinkovito poslovanje slovenskih organizacij. O izzivih in priložnostih razvoja slovenskega gospodarstva smo se pogovarjali z mag. Sonjo Šmuc.

Gospodarska zbornica Slovenije predstavlja največje interesno združenje na področju gospodarstva. Nam lahko v kratkem predstavite glavne pristojnosti in naloge GZS.

Doslej je bila vizija GZS biti največja, najmočnejša in najvplivnejša organizacija gospodarstva v Sloveniji, sedaj temu dodajamo še dimenzijo povezovalnosti in sodelovanja. Gospodarsko zbornico Slovenije vidim kot krovno, povezovalno, konstruktivno gospodarsko organizacijo, ki učinkovito zastopa najboljše v gospodarstvu in najboljše za gospodarstvo.

GZS bo najbolj koristila svojim članom in Sloveniji, če bo v družbi prepoznana kot konstruktiven partner, katerega fokus je reševanje težav, s katerimi se soočajo podjetja, ker ima to pozitiven učinek na družbo kot celoto.

Grajena je mrežno in temelji na tipalkah, ki prve zaznavajo potrebe in zahteve članstva, saj so v neposrednem stiku z dnevnim življenjem slovenskega gospodarstva. To so njeni »deli« na terenu območne in regionalne zbornice ter panožna združenja in zbornice.

> Korporativna integriteta je prava smer razvoja in ključni predpogoj trajnostnega razvoja vsakega gospodarstva.

Konjunkturo v Sloveniji moramo nujno izkoristiti za nov razvojni zagon. Slovenija je zaradi globoke recesije, kljub ugodnim trendom, šele pred meseci dosegla raven realnega BDP na prebivalca iz leta 2008. Obenem po produktivnosti, navkljub odličnim izvoznim rezultatom, še vedno preveč zaostaja za povprečno produktivnostjo v EU-28. Zato je čas za srednjeročni nacionalni razvojni sporazum, ki bo okrepil zdrave gospodarske trende, s tem pa omogočil tudi višji življenjski standard prebivalk in prebivalcev Slovenije. Na Vrhu slovenskega gospodarstva 2017 smo s tematiko o Razvojnem partnerstvu treh generacij 2018-25 odprli novo razpravo, ki temelji na viziji razvoja gospodarstva do leta 2025. Želimo, da je dokument z Vrha slovenskega gospodarstva eden ključnih prispevkov za razvojno partnerstvo s socialnimi partnerji za obdobje 2018-25. V tem obdobju mora biti naš cilj, da dodano vrednost na zaposlenega dvignemo s sedanjih 42.000 na preko 60.000 evrov, izvoz pa z lanskih 35 milijard na 50 milijard evrov v letu 2025. V tem obdobju bi Slovenija morala realizirati svoje prednosti skozi okrepljen socialni dialog. Cilj mora biti hitrejši gospodarski razvoj kot podlaga za večjo kakovost življenja prebivalcev Slovenije.

V nastavkih za Razvojno partnerstvo 2018-25 smo zato postavili ključne cilje za tri slovenske generacije: mlade do 30. leta starosti, aktivno popula-

*avtor je član Slovenskega združenja korporativne varnosti



cijo in generacijo 55+. V letu 2018 bo Razvojno partnerstvo 2018-25 naša ključna naloga in naš ključni izziv.

Ustrezno stabilno in varno poslovno okolje je pomemben dejavnik za uspešno delovanje slovenskih podjetij. Ali na strateškem nivoju sodelujete s posameznimi javnimi in zasebnimi strokovnimi institucijami pri poglabljanju razumevanja globalnega varnostnega okolja in izdelavi strateških varnostnih ocen, ki so pomembne za vaše člane?

Strinjam se z vami. Stabilno in varno poslovno okolje je del upravljanja tveganj, ki zelo vpliva na odločitve slovenskih podjetij, sploh tistih, ki poslujejo v tujem poslovnem okolju.

Sodelujemo s pristojnimi državnimi inštitucijami, prav tako z nekaterimi iz komercialnega sektorja, da te rizike obvladujemo in omejujemo na sprejemljivo raven in, da lahko gospodarstvo tudi na tej osnovi sprejema kompetentne odločitve.

Seznanjeni smo z aktivnostmi Eurochambresa, katerega tudi član smo, ki nas seznanja z evropskim pogledom gospodarstva tudi na to problematiko. Aktivno sodelujemo tudi v njegovih organih.

V zadnjem obdobju so tudi naša podjetja izpostavljena vedno pogostejšim dejavnikom, ki jih prinaša kompleksno mednarodno varnostno okolje. Posebej so izpostavljena informacijska tveganja, tveganja povezana s kadrovskim potencialom, tveganja, ki jih prinaša naravno okolje in seveda tveganja, ki so povezana z organiziranim kriminalom in grožnjami terorizma. Menite, da je odgovornost zagotavljanja varnega in neprekinjenega poslovanja poslovnih subjektov izključno njihova naloga ali menite, da lahko GZS na tem področju naredi določene korake v smeri dvigovanja zavedanja o pomenu celovitih pristopov k obvladovanju varnostnih tveganj?

Vsak dober gospodar bo pred sprejemom poslovne odločitve preveril informacije preko več različnih virov. Za slovenska podjetja je GZS prav gotovo eden izmed teh virov.

V praksi se srečujemo s tovrstnimi povpraševanji in jih individualno naslavljamo. Pri tem uporabljamo svoje zbornične kanale po svetu, prav tako druge kanale, od družb s področja poslovne inteligence do posameznikov, ki imajo znanje in izkušnje pri določeni temi oz. trgu.

Ustreznih in pravočasnih informacij nikoli ni dovolj. Tako lahko GZS na tem področju skupaj s partnerji in strokovnjaki iz prakse, prispeva k dvigu zavedanja o pomenu obvladovanja varnostnih tveganj preko vzpostavljanja smernic in priporočil dobre prakse. Krepi se tudi razmišljanje, da bi na področju kibernetske varnosti država morala vzpostaviti center, ki bo varoval internetno infrastrukturo pred vdori, ki postajajo čedalje večja skrb.

Mikro, mala in srednje velika podjetja imajo, na področju virov na-

menjenih za obvladovanje tveganj, določene omejitve. Menite, da bi lahko ta segment podjetij določen del podpore, predvsem v smislu znanja in nasvetov, dobival tudi preko GZS?

Podporo, o kateri govorite, že danes dobivajo preko GZS. Tako preko seminarjev, srečanj, kot tudi individualnih sestankov, ki jih na GZS redno organiziramo. Je pa res, da so pri obvladovanju tveganj pri MSP v ospredju predvsem tveganja finančne narave, manj pa tveganja cyber kriminala ter drugih. Trenutno je zelo vroča tema GDPR, ki straši tako velika kot mala podjetja.

Za uspešnost delovanja korporativne integritete in posledično korporativne varnosti imajo vodilni v organizaciji izredno pomembno vlogo, saj je vodenje s svojim zgledom najmočnejši motivacijski dejavnik, da se temu podredijo tudi ostali zaposleni v organizaciji. Kako bi lahko po vaši oceni skozi vzvode GZS pristopili k motivaciji strateškega in srednjega managementa, ki je v vsakem sistemu ključen za uspeh uveljavljanja sprememb, še posebej kadar govorimo o organizacijski in varnostni kulturi v slovenskih podjetjih?

> Naši člani vlagajo v nova znanja tudi na področju korporativne varnosti, kar je nujno za izpolnjevanje pogojev, da za izvajanje storitev na kritični infrastrukturi sploh lahko konkurirajo.

Korporativna integriteta je prava smer razvoja in ključni predpogoj trajnostnega razvoja vsakega gospodarstva. Pomeni poslovanje ne le v skladu z zakonodajo, ampak tudi v skladu z dobrimi poslovnimi običaji in visokimi etičnimi standardi do vseh deležnikov v poslovnem svetu.

Predstavniki Gospodarske Zbornice Slovenije, Združenja Manager, Združenja nadzornikov Slovenije in Ekonomske fakultete Univerze v Ljublja-



ni smo zato v letu 2015 pod pokroviteljstvom predsednika RS Boruta Pahorja oblikovali »Slovenske smernice korporativne integritete«. Na 9. Vrhu slovenskega gospodarstva, ki smo ga organizirali istega leta, se je 28 predsednikov uprav, članov uprav in direktorjev – Ambasadorjev korporativne integritete - s podpisom javno zavezalo, da bodo gospodarske družbe, ki jih vodijo, spoštovale in sledile načelom, zapisanim v Slovenskih smernicah korporativne integritete.

Med podpisniki so bili: Gorenje, NLB, Lek, Zavarovalnica Triglav, Petrol, Telekom Slovenije, Slovenske železnice, Intereuropa, Kolektor Group, SKB, Domel Holding, Siemens, Pozavarovalnice Sava, Zavarovalnica Maribor, Luka Koper, ELES, Studio Moderna, RIKO, BTC, Trimo, PricewaterhouseCoopers, SID Banka, Elektro Maribor, InterEnergo, Steklarna Hrastnik, Vzajemna, Elektro Gorenjska in Actual I.T. Kasneje se je krogu Ambasadorjev pridružila tudi družba A1 (prej: Si.mobil). K smernicam so in še vedno lahko pristopijo vse tiste gospodarske družbe, ki se odločno zavzemajo in si želijo za vključitve etičnih poslovnih praks in bodo dosledno delovale v smeri povrnitve ugleda v slovensko gospodarstvo.



Skratka, kakor vidite, to temo nekatera vodilna podjetja in organizacije že danes ustrezno naslavljajo. Verjamemo, da se bo zgled pozitivnih učinkov, skupaj z aktivnostjo podpornega okolja, širil dalje tudi na druga podjetja. Gre pa seveda za tek na dolge proge.

Veliko gospodarskih subjektov, ki so med drugim tudi člani GZS, posluje v globalnem poslovnem okolju. Zaznavate določene primere, da se omenjena podjetja k vam obračajo glede informacij o varnostni situaciji in razmerah na določenih kriznih žariščih? Imate vzpostavljene določene mehanizme za izvajanje takšne strokovne asistence?

V Sloveniji imamo okoli 8.000 podjetij, z več kot 100.000 EUR izvoza, vendar 500 največjih ustvari polovico vsega blagovnega izvoza. Od izvoznih podjetij je po naši oceni približno 10 odstotkov takih, ki že poslujejo ali pa želijo širiti svoje poslovanje tudi na območja, kjer je vprašanje varnostnih razmer še vedno pereče. Zato se seveda obračajo na nas z vprašanji tudi glede varnostne situacije in razmer na določenih kriznih žariščih. Predvsem gre za vprašanja oz. informacije o t.i. tretjih trgih. V ospredju so Afrika, Bližnji in Srednji vzhod, prav tako so tveganja povečana v Ukrajini oziroma celotnem območju bivše Sovjetske zveze.

Ker so stopnje odprtosti posameznih gospodarstev na teh območjih zelo specifične, kot tudi njihov institucionalni ustroj, je pomembno, da imamo kot GZS dostop do formalnih in neformalnih mrež ter na ta način našim članom posredujemo relevantne informacije, ki jim omogočajo boljše poslovno odločanje. Pri tem sodelujemo tako z mrežo ministrstva za gospodarski razvoj in tehnologijo, ministrstvom za zunanje zadeve ter lokalnimi gospodarskimi združenji in predstavniki.

Ob koncu leta 2017 je v veljavo stopil Zakon o kritični infrastrukturi, kjer imajo upravljavci le te infra-

strukture pomembno vlogo pri neprekinjenosti delovanja ključnih funkcij za delovanje širše družbene skupnosti. Večina teh upravljalcev kritične infrastrukture sodi v okvir poslovnih subjektov. Imate na GZS določene načrte kako okrepiti javno zasebno partnerstvo in sodelovanje gospodarstva in države na tem konkretnem področju?

Večina upravljavcev kritične infrastrukture je v članstvu Gospodarske zbornice Slovenije. To so družbe, ki upravljajo z energetsko prenosno in distribucijsko infrastrukturo, plinsko prenosno infrastrukturo, telekomunikacijsko infrastrukturo in družbe, ki upravljajo z energetskimi proizvodnimi objekti. Po drugi strani pa so v članstvu GZS tudi ključna inženiring podjetja, ki projektirajo, gradijo in vzdržujejo kritično infrastrukturo za javni sektor. To sodelovanje je tradicionalno zgledno in rezultira v učinkovitem sodelovanju v primeru naravnih nesreč.

Najbolj znan primer je žledolom pred leti, kjer smo s skupnimi močmi preprečili električne mrke širokih razsežnosti in preprečili veliko gospodarsko škodo. Izboljšanje korporativne varnosti je stalna naloga, pojavljajo se vedno novi izzivi, pa tudi nove nevarnosti predvsem zaradi vpetosti slovenskega energetskega sistema v mednarodne energetske tokove in naše izpostavljene lege. Naši člani vlagajo v nova znanja tudi na področju korporativne varnosti, kar je nujno za izpolnjevanje pogojev, da za izvajanje storitev na kritični infrastrukturi sploh lahko konkurirajo.

Na GZS javno zasebno partnerstvo krepimo s strokovnimi posveti na temo kritične infrastrukture in sodelujemo pri novih konceptih razvoja energetske, prometne in informacijske infrastrukture. Javno-zasebno partnerstvo je v Sloveniji še vedno relativno slabo uveljavljen koncept, predvsem zaradi pomanjkanja dobrih praks, deloma nezaupanja ter tudi pomanjkljivega znanja na področju ureditve pogodbenih obveznosti obeh strank. Večina podjetij, ki upravlja kritično infrastrukturo, je še vedno v pretežno državni lasti, še posebej telekomunikacije, energetika in deloma transport. Seznanjeni smo s tem, da imajo, na primer na Nizozemskem, osrednjo vlogo na področju zaščite kritične infrastrukture javno-zasebna partnerstva, kar sicer ni posebej uzakonjeno.

> Verjamem pa, da bi lahko sodelovanje z Institutom za korporativne varnostne študije in Slovenskim združenjem za korporativno varnost prispevalo h krepitvi zavedanja o pomenu varnosti v poslovnem okolju.

Slovensko združenje korporativne varnosti v svojem obsegu združuje večino slovenskih podjetij, ki upravljajo z določenimi segmenti kritične infrastrukture v Republiki Sloveniji. Menite, da bi tesnejše sodelovanje omenjenega združenja z GZS lahko prineslo pozitivne rezultate v smeri dvigovanja zavedanja o pomenu obvladovanja tveganj in pomembnost ustreznega varnostnega okolja na neprekinjenost delovanja in poslovno uspešnost poslovnih organizacij?

Seznanjeni smo s tem, da naši člani, ki upravljajo s kritično infrastrukturo, sodelujejo s Slovenskim združenjem za korporativno varnost in so tudi prejemniki nagrad in priznanj.

Tesnejše sodelovanje GZS s Slovenskim združenjem korporativne varnosti, pri tem mislim predvsem njenih združenj oz. zbornic, lahko prinese dodatne koristi, predvsem nova znanja in izboljšanje varnostne kulture, pri obvladovanju tveganj za naše člane in uporabnike naših storitev.

Institut za korporativne varnostne študije in Slovensko združenje za korporativno varnost že vrsto let podeljujeta nagrado »Slovenian Grand Security Award« tudi v kategoriji najbolj varno podjetje. Menite, da bi tesnejše sodelovanje omenjenih dveh institucij skupaj z GZS, pri podeljevanju in nominacijah za omenjeno nagrado, zavedanje o pomenu varnosti v poslovnem okolju lahko še okrepilo?

Namen nagrad je, da osvetlijo in širijo dobre prakse. GZS tako podeljuje številne nagrade, ki so v prvi vrsti usmerjene predvsem v promocijo gospodarskih in podjetniških dosežkov ter spodbujanje inovativnosti. Take so Nagrade GZS za izjemne gospodarske in podjetniške dosežke ter priznanja za najboljše inovacije na regionalnem in nacionalnem nivoju. Poleg tega nekatera združenja in območne oz. regionalne zbornice podeljujejo nagrade in priznanja na svojih specifičnih področjih dela.

Znotraj GZS nimamo posebej oblikovane organizacijske enote, ki bi se ukvarjala prav z varnostjo. Verjamem pa, da bi lahko sodelovanje z Institutom za korporativne varnostne študije in Slovenskim združenjem za korporativno varnost prispevalo h krepitvi zavedanja o pomenu varnosti v poslovnem okolju. Blagovna znamka GZS bi ta pomen še okrepila.

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

Upravljanje s tveganji je v današnjem poslovnem svetu eno izmed pomembnejših področij dela, ki iz dneva v dan še bolj pridobiva na pomenu. Del tega je tudi upravljanje z varnostnimi tveganji. Če smo v preteklosti imeli izziv, kako sploh pridobiti informacije, ki nam bodo pomagale pri odločitvah, je danes usmerjenost predvsem v to, kako iz nabora tisočerih virov pravočasno izluščiti verodostojne in zanesljive informacije. In tu se bo najbrž tudi v Sloveniji, kot je to primer v številnih drugih državah, v prihodnje še bolj razvil t.i. »business intelligence sektor«, ki bo podpiral odločitve različnih deležnikov v tem pogledu. ■

Slovensko združenje korporativne varnosti

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



Namen združenja je uresničevanje interesov članstva, ki so:

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

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

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

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

CETIS · ELES · NZS · gorenje group VAROVANJE · LMP d.d. · hse Holding Slovenske elektrarne d.o.o. · TES Termoelektrarna Šoštanj · LUKA KOPER Port of Koper · lek član skupine Sandoz · REISSWOLF secret. service. · BTC · A1 · Občina Slovenska Bistrica · MARIBORSKI VODOVOD · PHILIP MORRIS LJUBLJANA D.O.O. · univerzitetni klinični center ljubljana · GASILSKA ZVEZA SLOVENIJE · si-cert · INFORMACIJSKI POOBLAŠČENEC

www.ics-institut.si

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI

vam olajša obvladovanje tveganj v vaših organizacijskih sredinah.

SKUPAJ SMO MOČNEJŠI!

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

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Roman Žnidarič, izvršni direktor, Cetis d.d.*

UČINKOVITO OBVLADOVANJE TVEGANJ KLJUČ ZA USPEŠNO POSLOVANJE PODJETJA

Podjetje CETIS je dobitnik prestižne nagrade Slovenian Grand Security Award v kategoriji najbolj varno podjetje za leto 2017. Prizadevanja za učinkovito obvladovanje varnostnih tveganj se kažejo v dobrih rezultatih poslovanja, smeri novih izzivov in poslovnih priložnosti. O ključnih izzivih, ki jih prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Romanom Žnidaričem.

CETIS d.d. predstavlja enega od vodilnih evropskih podjetij na področju rešitev varnostnih in komercialnih tiskovin. Nam lahko prosim podrobneje pojasnite, katera so glavna težišča vaših rešitev, ki na trg varnostnih tiskovin prinašajo dodano vrednost?

Na področju rešitev varnostnih tiskovin smo eden izmed redkih proizvajalcev, ki svoje izdelke in storitve tržimo globalno, smo pa tudi integrator, ki se je iz klasične tiskarne z večstoletno zgodovino v zadnjem desetletju razvil v ponudnika celovitih rešitev. Tako danes, ob tisku varnostnih dokumentov, ponujamo celovite rešitve; od ustrezne programske opreme (npr. rešitev e-vlada, zajem in upravljanje podatkov, centralni registri, itn.), integracije programske in strojne opreme za izdajo dokumentov, pa do svetovanja vladnim organom na področju izdaje dokumentov.

Zaradi ostrejšega nadzora identitete posameznikov proizvajalci potovalnih dokumentov razvijamo nove, še trajnejše in še bolj zaščitene rešitve, zato smo razvili številne inovacije na področju grafike, pa tudi celovitih rešitev, s katerimi otežujemo ponarejanje oziroma prenarejanje dokumentov in tako prispevamo k večji globalni varnosti.

Trenutne varnostne razmere v svetu namreč zaostrujejo varnostne postopke na potovanjih, sprožajo dodatne aktivnosti glede preprečevanja zlorab dokumentov in povzročajo uveljavitev dodatnih varnostnih standardov. Zaradi ostrejšega nadzora identitete posameznikov proizvajalci potovalnih dokumentov razvijamo nove, še trajnejše in še bolj zaščitene rešitve, zato smo razvili številne inovacije na področju grafike, pa tudi celovitih rešitev, s katerimi otežujemo ponarejanje oziroma prenarejanje dokumentov in tako prispevamo k večji globalni varnosti.

S svojim poslovanjem ste močno prisotni v mednarodnem okolju, med drugim tudi na delih sveta, kjer so varnostna tveganja globalnega varnostnega okolja še posebej izpostavljena. Ali svoje odločitve o širitvi

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



poslovanja na določene trge temeljite tudi na strateških analizah varnostnega okolja ali bolj upoštevate poslovne možnosti?

Naše proizvodne in kadrovske kapacitete bistveno presegajo potrebe domačega trga. Zato smo sprejeli strateško odločitev, da moramo zadržati slovenski trg, ki je za nas še vedno najpomembnejši, obenem pa rasti na ciljnih trgih v tujini. Odločitve, kam se usmeriti, temeljijo predvsem na poslovnih priložnostih, saj so naše ciljne države (npr. v Afriki, Srednji Ameriki in na Bližnjem Vzhodu) pogosto tehnološko podhranjene in je pri njih potreba po naših storitvah večja kot v razvitih državah. Po drugi strani pa je varnostno okolje v teh državah bistveno kompleksnejše, saj smo neprestano izpostavljeni velikim (varnostnim, zdravstvenim, političnim, ...) tveganjem. Za vsako državo in projekt skrbno pretehtamo tveganja in naredimo ustrezno analizo, na osnovi katere se odločimo, kako pristopiti k sodelovanju in kako ta tveganja obvladovati. Ta tržišča zaradi neurejenih sistemov in slabe zaščite dokumentov predstavljajo največje globalno tveganje, kar se je tudi izkazalo v času večjih migrantskih pritiskov na staro celino.

Poslovne informacije, znanja in stike ščitimo tudi s tem, da sodelujemo z zvestimi sodelavci in poslovnimi partnerji, tehnično in tehnološko znanje pa zaščitimo tudi v okviru zaščite intelektualne lastnine. Ena najučinkovitejših zaščit pa je zagotovo hitra izvedba projektov v praksi.

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

Zaščito naših internih informacij in informacij naših poslovnih partnerjev jemljemo zelo resno. Zato smo že pred leti pristopili k ustreznemu obvladovanju informacij v celotni življenjski dobi, pri čemer si pomagamo z mednarodnimi standardi (npr. ISO 27001, ISO 14298) in najboljšimi praksami. Prav vsi v družbi CETIS imamo redna letna izobraževanja o varovanju informacij, ustreznih varnostnih klasifikacijah in obvladovanju od nastanka do uničenja. To zahtevamo tudi od naših dobaviteljev. Če želite sodelovati z nami na takšnih projektih, je dogovor o nerazkrivanju informacij (t. i. NDA) začetek, nekatere dobavitelje pa povabimo tudi na varnostno predavanje. Poslovne informacije, znanja in stike ščitimo tudi s tem, da sodelujemo z zvestimi sodelavci in poslovnimi partnerji, tehnično in tehnološko znanje pa zaščitimo tudi v okviru zaščite intelektualne lastnine. Ena najučinkovitejših zaščit pa je zagotovo hitra izvedba projektov v praksi.

Varnostne in vrednostne tiskovine so lahko predmet potencialnih in realnih groženj odtujitve, sabotaž in drugih nesreč. Nam zaupate kako strateško upravljate s tveganji, ki jih prinaša izdelovanje takih tiskovin?

V družbi CETIS smo ponosni, da smo lastnik številnih mednarodnih certifika-

Zavedamo se, da nam je zaupana pomembna dejavnost in pri tem si ne smemo dovoliti napak.

tov s področja varnosti in kakovosti, med katerimi so najpomembnejši: ISO 9001 - Certificiran sistem vodenja kakovosti, ISO 14001 - Certificiran sistem ravnanja z okoljem, ISO 27001 - Certificiran sistem upravljanja informacijske varnosti, Certificiran sistem MasterCard/Visa za zagotavljanje fizične in logične varnosti v skladu z zahtevami PCI (Payment Card Industry), Certificiran sistem kakovosti CQM (Card Quality Management System) MasterCard za zagotavljanje kakovosti bančnih kartic, FSCC (Facility Security Clearance Certificate) Varnostno potrdilo vlade Republike Slovenije, Urada za varovanje tajnih podatkov, ki je v skladu z varnostno politiko Evropske unije, Certificiran sistem vodenja varovanja za izdelavo visoko varovanih dokumentov Intergraf ISO 14298 (Central Bank Level), DPG Certifikat Deutsche Pfand Gesellschaft, sledimo pa tudi standardu ICAO. Zaradi rednih internih kontrol, predvsem pa zunanjih revizij naših procesov in aktivnosti s strani mednarodno priznanih inštitucij, kar zagotavlja nepristranskost, moramo aktivno spremljati trende, slediti zadnjim varnostnim smernicam, nenehno izboljševati naše procese in investirati v najsodobnejše varnostne sisteme. Zavedamo se, da nam je zaupana pomembna dejavnost in pri tem si ne smemo dovoliti napak.



V sistemu poslovanja imate vzpostavljen cel niz politik med katerimi imata politika varovanja informacij in politika varovanja posebno pomembno mesto. Nam lahko podrobneje pojasnite pomen navedenih politik za celovitost pristopa do obvladovanja varnostnih tveganj?

Naš pristop k obvladovanju varnostnih tveganj s politikami sledi znanemu Demingovemu krogu. Ko identificiramo določeno področje (bodisi na podlagi internih izkušenj, novih zahtev projekta ali sprememb standarda), zapišemo ugotovitve in navodila v obliki interne politike. Če sprememba zahteva interno izobraževanje, je za izvedbo zadolžen skrbnik politike. Skladnost naših internih procesov s politikami redno pregledujemo in morebitna odstopanja zapišemo ter ukrepamo. Na ta način uspešno zmanjšujemo tveganja in pridobivamo nova znanja.

Dinamično varnostno okolje pred vsako organizacijo prinaša cel niz tveganj. Tveganja povezana s kadrovskim potencialom so v tem okviru še posebej izražena. Smatrate, da je proces uvajanja korporativne integritete lahko eden izmed učinkovitih dejavnikov obvladovanja navedenih tveganj?

Tveganj, povezanih s kadrovskim potencialom, se zavedamo. Predvsem v zadnjem času smo v Sloveniji priča povečani gospodarski rasti, manjši brezposelnosti in pa večji fluktuaciji kadra, kar seveda pomeni določen pritisk na beg znanja. Naši zaposleni imajo specialna znanja, ki jih je na trgu izredno težko najti (šola za tiskarje, denimo, sploh ne obstaja več), pa naj bodo to specialna tehnična znanja (smo edina tiskarna varnostnih dokumentov v Sloveniji) ali pa znanja s področja delovanja na globalnem trgu in na ravni prodaje storitev vladam (business to government).

Proces uvajanja korporativne integritete je lahko eden izmed učinkovitih dejavnikov navedenih tveganj, saj si zaposleni želijo dela v urejeni in ugledni organizaciji, ki pa ima korenine v osnovnih etičnih načelih, ki jih kot družba zagovarjamo. V letošnjem letu smo sprejeli »Etični kodeks – Zlata pravila ravnanja«, ki nas vse zaposlene v Skupini CETIS nagovarja k spoštovanju temeljnih vrednot in tako pomembno vpliva na naše dojemanje medsebojnih razmerij znotraj organizacije in v odnosu do našega okolja.



Za uspešnost delovanja korporativne integritete imajo vodilni v organizaciji izredno pomembno vlogo saj je vodenje s svojim zgledom najmočnejši motivacijski dejavnik, da se temu podredijo tudi ostali zaposleni v organizaciji. Kako ste v vašem podjetju pristopili k motivaciji srednjega managementa, ki je v vsakem sistemu ključen za uspeh uveljavljanja sprememb, še posebej kadar govorimo o organizacijski kulturi?

Vodilni v organizaciji si s promocijo temeljnih načel, zapisanih v kodeksu, in pa predvsem z zgledom, ki ga dajemo našim sodelavcem in poslovnim partnerjem, prizadevamo graditi dolgoročen partnerski odnos in motivirati sodelavce. V Skupini CETIS redno izvajamo letne razgovore z vsemi zaposlenimi in pa tudi merjenje organizacijske klime in kulture. Na osnovi povratnih informacij skupaj dorečemo ukrepe, za katere se potrudimo, da jih tudi uresničimo. S pomočjo povratnih informacij usmerjamo naše aktivnosti v nenehno izboljševanje odnosov, ki jih gradimo med drugim tudi s pomočjo različnih aktivnosti za zaposlene, ki jih organiziramo med letom. Kot že omenjeno, smo pomemben korak naredili z izdajo etičnega kodeksa, k spoštovanju katerega smo se zavezali vsi v Skupini CETIS.

V tako razvejani organizaciji je uvajanje sprememb v organizacijski kulturi zaposlenih izredno zahteven proces. Nam lahko zaupate dobre prakse in izkušnje kako ste se tega procesa lotili v družbi Cetis d.d.?

Skupina CETIS je del skupine MSIN in na ravni celotne skupine MSIN smo pristopili k enotnemu in celovitemu pristopu k uvajanju sprememb v organizacijski kulturi. Na ravni Skupine uvajamo enotne smernice delovanja, poročanja in nadzora, glede organizacijske kulture pa je temeljni dokument »Etični kodeks - Zlata pravila ravnanja«, s katerim smo dobili jasna priporočila in usmeritve, kakšno ravnanje je v Skupini zaželeno in naj bi ga izvajali vsak dan. Bistvena komponenta pa je izobraževanje – ob uvedenih spremembah poskrbimo, da so naši sodelavci z njimi seznanjeni in da jih razumejo.

Korporativni varnostni manager mora zaradi izvajanja svojih specifičnih procesov obvladovanja tveganj imeti določeno ustrezno organizacijsko umeščenost in neposreden dostop do strateškega managerja organizacije. Kako je to urejeno v vašem podjetju?

Pooblaščenec za varnost in skladnost odgovarja neposredno upravi oz. izvršnemu direktorju, zadolženemu za to področje. Obenem pa je izvršni direktor (v tem primeru jaz) aktivno vpleten v vse procese, povezane z obvladovanjem tveganj. Pri tem je pomembna predvsem nepristranskost in strokovnost osebe, zadolžene za to področje.

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?

Vsekakor je združevanje strokovnjakov s področja korporativne varnosti nujno, saj gre za ozek krog specialistov z določenimi znanji in menim, da je zelo dobrodošlo, da si strokovnjaki izmenjujejo dobre prakse. V veliko čast nam je bilo tudi, da smo imeli možnost gostiti člane združenja v Cetisu, kjer smo članom na kratko prikazali, na kakšen način obvladujemo to področje. V vsakem podjetju so prisotne določene posebnosti, tveganja med podjetji se razlikujejo, skupna pa nam je predvsem zavest, da moramo tveganja zaznati in najti učinkovit način, kako jih v največji meri obvladujemo. ■



Vodilno globalno podjetje na področju varovanja

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

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

CE FC ISO 9001:2000

www.dahuasecurity.com

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

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

INTERVJU
Stanislav Veniger, svetovalec za korporativno varnost,
Zavarovalnica Triglav d.d.*

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

V današnjem poslovnem svetu je zagotavljanje korporativne varnosti naših organizacij tesno povezano tudi z ustreznim zavarovanjem določenih varnostnih tveganj. Celovitost obvladovanja vseh tveganj je praktično nemogoče zagotoviti. Zato je zavarovanje določenih tveganj ena od ustreznih rešitev.

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Nam lahko poveste katera so ključna področja pristojnosti, ki ste jih v svoji bogati karieri konkretno izvajali?

Po zaključku kadetske šole sem se zaposlil v slovenski policiji, kjer sem deloval 35 let. Izkušnje sem pridobival preko celotnega ustroja, na različnih področjih. Kot policist, pomočnik in vodja varnostnega okoliša, na področju prometne varnosti, preiskovanja kaznivih dejanj itd. Zaključil sem študij na višji šoli in prevzel zadolžitve pomočnika komandirja, kmalu za tem komandirja policijske postaje, tudi med osamosvojitveno vojno. Ravno to obdobje bi opisal kot izjemno stresno in zahtevno, a tudi eno od najlepših na karierni poti. Kasneje sem opravljal delo direktorja policijske uprave, direktorja uniformirane policije, sekundanta v mednarodni organizaciji, nazadnje pa sem deloval kot generalni direktor policije. Za tem me je pot vodila v gospodarstvo. Celotna moja kariera je torej povezana z različnimi ravnmi varnosti in dejansko poznam najširši nabor varnostnega delovanja. Tudi zaradi tovrstnih izkušenj verjamem, da je najbolje sprejemati pragmatične odločitve, tudi tiste najbolj zahtevne.

V zadnjem obdobju ste zelo močno vpeti v zagotavljanje določenih procesov korporativne varnosti v zavarovalnici. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost podjetja, ki se v osnovi ukvarja z zavarovalniškim področjem? So v tem okviru priložnosti za nove produkte?

Absolutno je korporativna varnost izjemno pomembna za vsak sistem, ne glede na to ali gre za poslovnega ali javnega, za storitveno ali proizvodno naravnanega, kritično infrastrukturo... Še posebej re-

g. Stanislav Veniger je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2017«

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Prepričan sem, da se strateški management v slovenskih podjetjih vedno bolj zaveda, kako pomembno je obvladovanje varnostnih tveganj, ki lahko precej vplivajo na ranljivost podjetij, in s tem povzročeno veliko škodo.

cimo za velika in uspešna podjetja. Ker so varnostna tveganja vedno bolj številna in pogosta, je prav, da organizacije v Sloveniji vedno bolj stremijo k njihovemu aktivnejšemu upravljanju. Imamo pa prostor za napredek, še posebej ko potegnemo primerjavo z razvitejšimi sistemi.

Z vidika zavarovalništva je ustrezno razumevanje in obvladovanje korporativne varnosti zagotovo prav tako vedno bolj pomembno, tudi z vidika konkurenčnosti. Živimo namreč v času, ko smo priča novim izzivom skorajda na vseh področjih in je včasih težko napovedati, v katero smer in s kakšno hitrostjo se bo kaj razvijalo (npr. električni avtomobili, ali jih bo čez 20 let več kot dizelskih in bencinskih, ali bo vožnja avtomatska, se bomo oz. bodo naši otroci ali vnuki vozili z droni...., robotizacija, informacijska varnost, kripto valute...). Dejstvo je, da tisto, kar smo pred 20 leti pojmovali kot znanstveno fantastiko, postaja realnost. Zato je ves čas potrebno iskati rešitve, da se bomo znali in zmogli odzvati na prihajajoče izzive in seveda zaposliti ljudi, ki bodo to obvladovali. Kajti, če sistem ali del sistema ne deluje, lahko hitro pride do finančnih in tržnih izgub, izgube ugleda, povečanja tveganj in podobno.

Zavarovalnica Triglav d.d. predstavlja regionalno podjetje, ki se ukvarja z zelo specifično dejavnostjo. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?



Skupina Triglav je vodilna zavarovalno-finančna skupina v Sloveniji in regiji Adria. Prisotni smo na Hrvaškem, Bosni in Hercegovini (Sarajevo in Banja luka), Srbiji, Črni gori in Makedoniji. Zavarovalništvo je z vidika tveganj še nekoliko bolj specifično, saj na njih temelji osnovni posel. Kot celota smo usmerjeni v poenoteno obvladovanje tveganj, tudi varnostnih, ob upoštevanju določenih posebnosti. A sistem je jasen, za varnostna tveganja je potrebno skrbeti v vseh naših poslovnih procesih, jih spremljati, meriti in se na njih odzivati.

Zavarovalniške goljufije ne poznajo državnih mej zato je mednarodno sodelovanje pri odkrivanju in preprečevanju le teh izrednega pomena. Vam pri tem pomagajo vaše dolgoletne izkušnje v Policiji?

Zavarovalniške goljufije ne poznajo meja, a so določene ocene, da so relativno enakomerno porazdeljene glede na teritorialnost in upoštevanje obsega posla na določenem trgu. Seveda gre v teh primerih običajno za večje goljufije, za katerimi stojijo organizirane mednarodne kriminalne združbe. Te lahko povzročajo škodo tudi na drugih področjih in je potrebno storiti vse, da jih ustrezne institucije čim prej izsledijo. Če gre za takšne združbe, pa seveda morajo med sabo operativno sodelovati in izmenjavati informacije.

Moje izkušnje, tudi mednarodne, ki sem jih pridobil kot sekundiranec v Centru za demokratični nadzor oboroženih sil (DCAF) v Ženevi, ko smo z izpostavo v Ljubljani pokrivali tudi jugovzhodno Evropo, so seveda lahko določena prednost in v pomoč. Še posebej v smislu, da smo takrat skrbeli za vzpostavljanje učinkovite mejne kontrole ter sodelovanja med policijami, v primeru izvrševanja kaznivih dejanj, iskanja storilcev in podobno. Zaradi narave dela sem v tem času precej potoval po celotnem balkanskem polotoku in širše, vse s ciljem krepitve sodelovanja med policijami, prenosa dobrih praks, izboljšanj zakonodaj... In izredno pomembno je, da so vse države na tem območju, tako članice EU kot tudi tiste, ki k temu stremijo, po letu 2006 pričele pristopati h Konvenciji o policijskem sodelovanju v jugovzhodni Evropi, ki dopušča tudi izmenjavo osebnih podatkov, informacij...

Nam lahko zaupate kako pomemben je v takih primerih učinkovit sistem varovanja ključnih poslovnih informacij?

S prevarami in podobnimi kaznivimi dejanju se ukvarjajo vse zavarovalniške družbe po svetu. Pri nas je bila podana ocena, ki še vedno v poprečju drži, da vsakdo plača na račun prevar okoli 80 evrov več. Zaradi tega je nujno in potrebno, da si industrija izmenjuje informacije glede prevar in drugih negativnih dejanj, sooblikuje primerne osveščevalne aktivnosti ter da snuje skupne ukrepe za preprečevanje, odkrivanje in raziskovanje. V Sloveniji sodelovanje poteka preko Slovenskega zavarovalnega združenja in menim, da ne bi smelo biti prikrivanja informacij glede načina izvajanja prevar. Za vse je namreč pomembno, da se znajo boriti proti tem dejanjem. Vzporedno je pomembno, da imaš ustrezno urejen sistem, procese in odgovornosti v podjetju, saj je potem tveganje izgube ključnih poslovnih informacij ustrezno upravljano in minimizirano ter z vidika izmenjave podatkov ne bi smelo biti problematično.

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

Moram priznati, da sem prišel iz javne uprave v gospodarsko družbo, ki deluje odlično na osnovnem področju kot tudi na področju korporativne varnosti. Sistem je celovito upravljan in urejen, na podlagi sprememb v zunanjem in notranjem okolju pa se ga nenehno nadgrajuje in dopolnjuje. Imamo službe, ki se s tem področjem uspešno ukvarjajo. Strateški management se absolutno in popolnoma zaveda svoje odgovornosti tudi na tem področju, se tekoče seznanja z razmerami in temu primerno sprejema ustrezne odločitve.

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?

Stanje na tem področju me zelo zanima in ga redno spremljam preko različnih virov. Prepričan sem, da se strateški management v slovenskih podjetjih vedno bolj zaveda, kako pomembno je obvladovanje varnostnih tveganj, ki lahko precej vplivajo na ranljivost podjetij, ki jih vodijo, in povzroči veliko škodo. Še posebej, ker smo bili lansko leto priča takim dogodkom ne samo po svetu, ampak tudi v Sloveniji. Zaradi tega se v ta področja vlaga vedno več energije, izdeluje se varnostne ocene, načrte, sprejema notranje akte, vzpostavlja nadzorne mehanizme... Še posebej pa bi se morali vedno bolj zavedati, da za sisteme skrbijo in jih sooblikujejo ljudje, zato je izjemnega pomena poiskati primerno mešanico usposobljenih kadrov, ki znajo uporabljati napredne tehnologije ter vlagati v informacijsko varnost v najširšem pomenu besede. Vsi vemo, da je možno preko informacijskih sistemov priti do ogromno informacij o konkurenčni družbi, možni so razni prisluhi preko različnih programov, snemanja sestankov in razgovorov na neviden način. Poglejmo samo kaj vse lahko naročimo preko spleta v cilju zlorab (nevidne kamere, USB snemalnike, svinčnike za snemanje....) in prepričan sem, da se premalo ljudi zaveda te dimenzije.



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

Absolutno so tovrstna vlaganja potrebna in prepričan sem, da se večina podjetij tega vse bolj zaveda. Za korporativno varnost bo vedno bolj pomembno, da podjetja z vidika doseganja ustreznega nivoja splošne varnosti, nadaljujejo z izobraževanji vseh zaposlenih. Hkrati pa se morajo zavedati, da je potrebno vlagati tudi v razvoj specifičnih znanj zaposlenih, ki so specialisti in zadolženi za razvoj naprednih pristopov na področju varnosti. Še posebej, ker se spremembe dogajajo nerazumljivo hitro. Včasih težko razumeš, da postane podjetje, ki se ukvarja z informatiko ali kibernetiko, žrtev takega napada, kar pomeni, da obstaja mnogo neznank in varnostnih rizikov. Zaradi tega je odločitev, ene od slovenskih fakultet za podjetništvo, da v sodelovanju z inštitutom, ponudi študentom na voljo novo smer Management korporativne varnosti, zagotovo ustrezna in pomembna odločitev za prihodnji razvoj varnosti v slovenskih podjetjih.

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?

Predvsem je pomembna izmenjava izkušenj in znanj, kar omogočajo ravno platforme kot je Slovensko združenje korporativne varnosti. Še posebej v času, v katerem živimo in v prihodnost, v katero gremo. Vsa predavanja, predstavitve, razgovori in izmenjava informacij zagotovo pozitivno vplivajo na delovanje posameznikov, ki se s tem področjem ukvarjamo. Ko nove informacije odprejo več varnostnih vprašanj, pa strokovnjak ve, da je na pravi poti in da bo poiskal primerne rešitve, da te dileme razreši. ■

SISTEMSKE REŠITVE PRED POŽARI, – Z ENO BESEDO BONPET!

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



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

NOVO
v ponudbi: BONPET SAMODEJNI GASILNIK 2, 4, 6 ali 12L.

SAMODEJNE GASILNE AMPULE BONPET

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



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

Bonpet® systems

Zanesljivi gasilni sistemi

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

Avtor: Vojko Volk / veleposlanik



KOLUMNA
vojko.volk@gov.si

SLOVENIJA – SMER SEVER-SEVEROZAHOD

„V svetu marketinga ni laži, je samo koristno pretiravanje.“

/Iz filma A.Hitchcocka, „Sever, severo-zahod“/

Usoda majhnih gospodarstev, kakršno je slovensko, je močno odvisna od zunanjega sveta. Poznavanje sveta in razmer v njem je zato ključnega pomena za uspešno gospodarjenje in razvoj, predvsem pa za načrtovanje in usmerjanje pri ključnih odločitvah in še zlasti investicijah.

Zdaj je že povsem jasno, da bi v primeru pravočasnega odziva Slovenije na krizo leta 2008 slovensko gospodarstvo in država lahko utrpela neprimerno manjšo škodo, kot jo je in bi slovenskim davkoplačevalcem lahko prihranili breme poplačila ogromne bančne luknje, katere vrednost je presegla polovico letnega proračuna države. Namesto, da bi kot majhno in okretno gospodarstvo s pravočasnimi ukrepi utrpeli najmanj škode, smo bili žal med tistimi, ki smo je utrpeli največ. Med tistimi, ki so se znašli bolje kot mi, so bili še zlasti Čehi, ki so nas tudi zato prav v zadnjih 5 letih razvojno najprej dohiteli in poslej tudi prehiteli. In to po domala v vseh kriterijih, vključno z BDP na prebivalca in tudi z mnogimi indeksi družbenega razvoja, vključno z bolj uspešnim bojem zoper korupcijo. Za primerjavo; ob „letu nič“, ob propadu komunizma in prehodu na tržno gospodarstvo, je takratna Češkoslovaška komaj presegala polovico BDP na prebivalca takratne Slovenije. Že samo ta podatek je dovolj, da razumemo kako bolj ambiciozni in preprosto boljši bi morali vsa ta leta biti, da bi ohranili vsaj nekaj prednosti pred Češko, poslej pa tudi Slovaško, ki nas tudi že dohiteva.

Samo z nekaj več znanja in volje ter nekaj več interesa po pridobivanju ustreznih informacij in z nekaj več kulture analitičnega pristopa k poslovnim odločitvam, bi si lahko prihranili neverjetno lahkotno in nespametno financiranje projektov ter še posebej vlaganj v nepremičnine na Balkanu v času, ko je bil razkroj tamkajšnjih finančnih trgov že povsem očiten. A je bila prav tam v kratkem času izgubljena še vsaj poldruga milijarda denarja iz slovenskih bank in skladov v večinski javni lasti. Mnogo slovenskih podjetij in bank je propadlo zato, ker so tvegali brez potrebe, namesto, da bi se ustrezno informirali in zavarovali. Z več znanja in volje bi se lahko izognili katastrofalni odločitvi o prodaji Mercatorja takrat že de facto bankrotiranemu hrvaškemu podjetju Agrokor in lahko bi se izognili tej množični razprodaji slovenske živilske industrije hrvaškim podjetjem (Droga Kolinska-Atlantic Grupa, Žito-Podravka) ravno v letih, ko se je v sosednji Avstriji uresničila nacionalna odločitev o zdravi hrani (bio in organic) kot strateški dobrini prihodnosti. Rezultat slabih odločitev je, da je danes polovica hrane na policah slovenskih trgovin uvožena iz Hrvaške, in to hrane slabše kakovosti, medtem ko kvalitetna slovenska hrana vse bolj odhaja na police avstrijskih in zadnja leta tudi italijanskih trgovin. Potrošniki to seveda opazijo in reagirajo, kar potrjuje padanje tržnega deleža Mercatorja in rast tržnega deleža konkurenčnih trgovin.

EU po Brexitu postaja vse bolj neka druga skupnost, v kateri je predvsem več zavedanja o nujnosti reform in več jasnosti glede prihodnjih korakov.

Od slovenskih načrtov po prevzemanju strateških pozicij na Balkanu ni ostalo veliko, na koncu se je zgodilo ravno obratno; zdaj podjetja z Balkana prevzemajo tudi slovenske banke, z vsemi tveganji, ki jih prinašajo poslovne prakse in običaji podjetij, ki so bila v svojih domačih okoljih navajena na posebne pogoje poslovanja in bila pogosto politično privilegirana. Izkušnja in usoda koncerna Agrokor je trajen poduk o tem, da ima ambicija po nenehnih širitvah in koncentracijah svoje meje in da ob poslovanju z večinsko dolžniškim kapitalom vsako podjetje postane nazadnje Ponzijeva shema in s tem tempirana bomba. Če smo se v Sloveniji iz napak zadnjih let česa naučili je zdaj skrajni čas, da se opravi strateške premisleke na podlagi katerih bodo morali slovenska država in gospodarstvo že v kratkem sprejemati pomembne odločitve; o nastajanju bolj povezane EU, o primernosti in varnosti ciljnih trgov in ukrepih za preskok Slovenije v tehnološko prihodnost.

Balkan

Obseg blagovne menjave Slovenije z državami Balkana je po osamosvojitvi močno upadel, predvsem zaradi vojne, zaradi česar so bila slovenska podjetja prisiljena povečati svoj izvoz na zahod. Odtlej je slovenska menjava z zahodom z nekdanjih slabih 60 odstotkov narasla na današnjih skoraj 80 odstotkov, kar štejemo za najbolj blagodejno posledico izgube nekdanjih balkanskih trgov. Do leta 2010 je slovenska menjava z Balkanom, takrat še skupaj s Hrvaško, znašala dobre 4.3 mrd eur (1.7 mrd s Hrvaško, 2.6 ostali) potem pa je z vstopom Hrvaške v EU prišlo do velikih razlik. Menjava s Hrvaško je zaradi vstopa v EU že po dveh letih poskočila skoraj za polovico in je lani dosegla 3.6 mrd eur. Z ostalimi državami Balkana (Srbija 1.25 mrd, BiH 1.1, Makedonija 0.26, Črna gora 0.1, Kosovo 0.1, Albanija 0.05) je menjava ves ta čas stagnirala. Med ključnimi razlogi stagnacije so v prvi vrsti kriza in njen pozen odraz na Balkanu ter s tem kasnejše okrevanje zagotovo pa tudi večja previdnost slovenskih gospodarstvenikov.

Obeti krepkejše gospodarske rasti na Balkanu so močno povezani s prihodnjo politično stabilnostjo regije in z obeti posameznih držav v postopkih pogajanj za vstop v EU. Ob Makedoniji in Kosovu, katerih napredovanje je odvisno od na žalost malo verjetne ureditve odnosov s sosednjima Srbijo oziroma Grčijo, sta v primežu notranje političnih težav tudi BiH in Albanija. Zato sta v pogajanjih z EU še najdlje prišli Črna gora in Srbija. Zlasti Črna gora se pri tem zdi kot povsem neproblematična in poslej skoraj vzorna kandidatka za vstop v EU, tudi zavoljo dejstva, da spretno ureja odnose s sosedami in je dejavnik stabilnosti na južnem Balkanu. Ključna težava Srbije je čustvena navezanost na Kosovo, ki postaja zavora za napredovanje obeh držav. Če se bo pat pozicija v odnosih med državama nadaljevala utegne na Kosovu prevladati razpoloženje, ki se že nekaj časa krepi, da je edini izhod povezava Kosova z Albanijo v zvezno državo, z vsemi nevarnimi posledicami, ki na tej podlagi lahko nastanejo za stabilnost sosednje Makedonije, kjer je skoraj tretjina prebivalstva albanske narodnosti. Srbija s tem postaja osrednja točka prihodnje širitve EU na Balkan v vseh pogledih; političnem, ekonomskem in prometnem.



EU bi lahko že samo z okrepitvijo svojih različnih prisotnosti na Balkanu, od političnih do civilno družbenih ter podvojitvijo finančnih vložkov dosegla vidne učinke, ki bi lahko bistveno izboljšali družbeno vzdušje. Takšna je namreč izkušnja iz „prvega vala“ intenzivne podpore EU državam Balkana v letih od 2003 do 2008. Ko je ta podpora ošibila in v zadnjih petih letih, ko se je EU odrekla širitveni agendi, tudi povsem izginila, so se na Balkanu razmere močno poslabšale. Potencialni investitorji na Balkanu bodo zato pozorno spremljali korake EU v regiji ter jim vzporedno a še vedno previdno tudi sledili. Za bistveno povečanje vlaganj pa bo potrebno počakati vsaj do prve naslednje širitve.

Evropska unija

EU po Brexitu postaja vse bolj neka druga skupnost, v kateri je predvsem več zavedanja o nujnosti reform in več jasnosti glede prihodnjih korakov. Brexit je bil očitno nujno potrebna brca v zadnjico zaspane Evrope, ki se prav to leto nahaja pred usodnimi odločitvami. Francoske in nemške volitve so se ugodno iztekle in zdaj se čaka samo še izid volitev v Italiji in na začetek dela nove nemške vlade. Trije dogodki bodo v prihodnosti ključni.

Prvi je vsebina dogovora o bolj povezani in finančno enotnejši EU, kakršno je po izvolitvi predlagal francoski predsednik Macron in čemur se je še pred volitvami priklonila kanclerka Merklova. Nazadnje se je tem ambicijam pridružil še italijanski predsednik vlade Gentiloni, s čimer so dani temeljni pogoji za začetek tesnejšega povezovanja EU na področju finančnega delovanja in na področju skupne varnosti oziroma kar skupne, evropske vojske. Že na prvi pogled je jasno, da bo to točka, v kateri se bo EU razklala na dvoje; na zahodni del, ki je hkrati najrazvitejši in najbolj demokratičen del sveta, ter na vzhodni del, ki se vse bolj utaplja v nazadnjaških populizmih, ob tem pa mladi z vzhoda množično bežijo na zahod, kjer jih ob delu čaka tudi več svoboščin. Za povrh je vzhodni del EU močno pod vplivom vsebin iz ameriške pobude Treh morij (Trimarium), ki je zamišljen kot projekt „vmesne cone“ iz časov po prvi svetovni vojni, ko se je hotelo izolirati predvsem Sovjetsko zvezo. Tokrat je zamisel veliko bolj namenjena nadzorovanju Nemčije, ki je s svojim ogromnim trgovinskim presežkom trn v peti ameriškemu gospodarstvu. Slovenija kot članica evroskupine in Schengna izpolnjuje temeljne pogoje za pristop v zahodni del, seveda pod pogojem, da bo za tem stala tudi potrebna politična volja.

Slovenija skratka živi v svojevrstnem paradoksu; medtem, ko si dobesedno ves svet prizadeva čim več poslovati z EU kot najbogatejšim delom sveta in tja čim več izvažati, je Sloveniji to že davno uspelo! Še več, Slovenija je ena od zgolj štirih evropskih članic EU, ki ima presežek v blagovni menjavi z mogočno Nemčijo. Za Slovenijo je smer torej jasna; smer sever, severo-zahod.



Drug pomemben proces bo oblikovanje skupne evropske politike do migracij. Zahodni del se jasno nagiba k nekakšni „omejeni solidarnosti“ do pribežnikov; za tiste, ki jih lahko sprejmemo, bomo poskrbeli, jim dali izobrazbo, stanovanje in delo, vse ostale pa bomo tako ali drugače zavrnili. Ta načrt se že odraža v koalicijski pogodbi nove nemške vlade, kjer je število pribežnikov na leto omejeno na 230 tisoč oseb. Nemčija je namreč ena tistih držav, ki je med vsemi razvitimi daleč najbolj demografsko ogrožena in se njeno prebivalstvo že desetletje ne povečuje več, potrebe po delovni sili pa so tolikšne, da so pribežniki edina rešitev. Povsem na drugi strani bo spet vzhodni del EU, kjer so vse države nekdanjega trdega komunizma, v katerih je bilo zavračanje vsega tujega in zapiranje meja običajna praksa in domala družbena vrednota realnega socializma.

Tretji projekt je okrepljena skupna varnost oziroma začetek nastajanja evropske vojske. Gre za zelo moder projekt zlasti zato, ker se pri delovanju policijskih ali vojaških varnostnih sil ne postavlja problem odločanja oziroma upravljanja na politični ravni. Ko se vzpostavi enote in odredi vodstvo enot za določeno obdobje, postane vodenje strokovno-tehnično, ne pa več politično vprašanje. Poleg tega je sporočilnost enot z evropskimi simboli izjemna in prodornejša od še tako usklajenih monetarnih ali davčnih politik. Tudi učinkovitost ne bi smela biti pod vprašajem, saj enote različnih članic EU že zdaj skupno delujejo v misijah kot NATO, potem pa bo ta možnost odprta tudi za članice EU, ki niso v NATO.

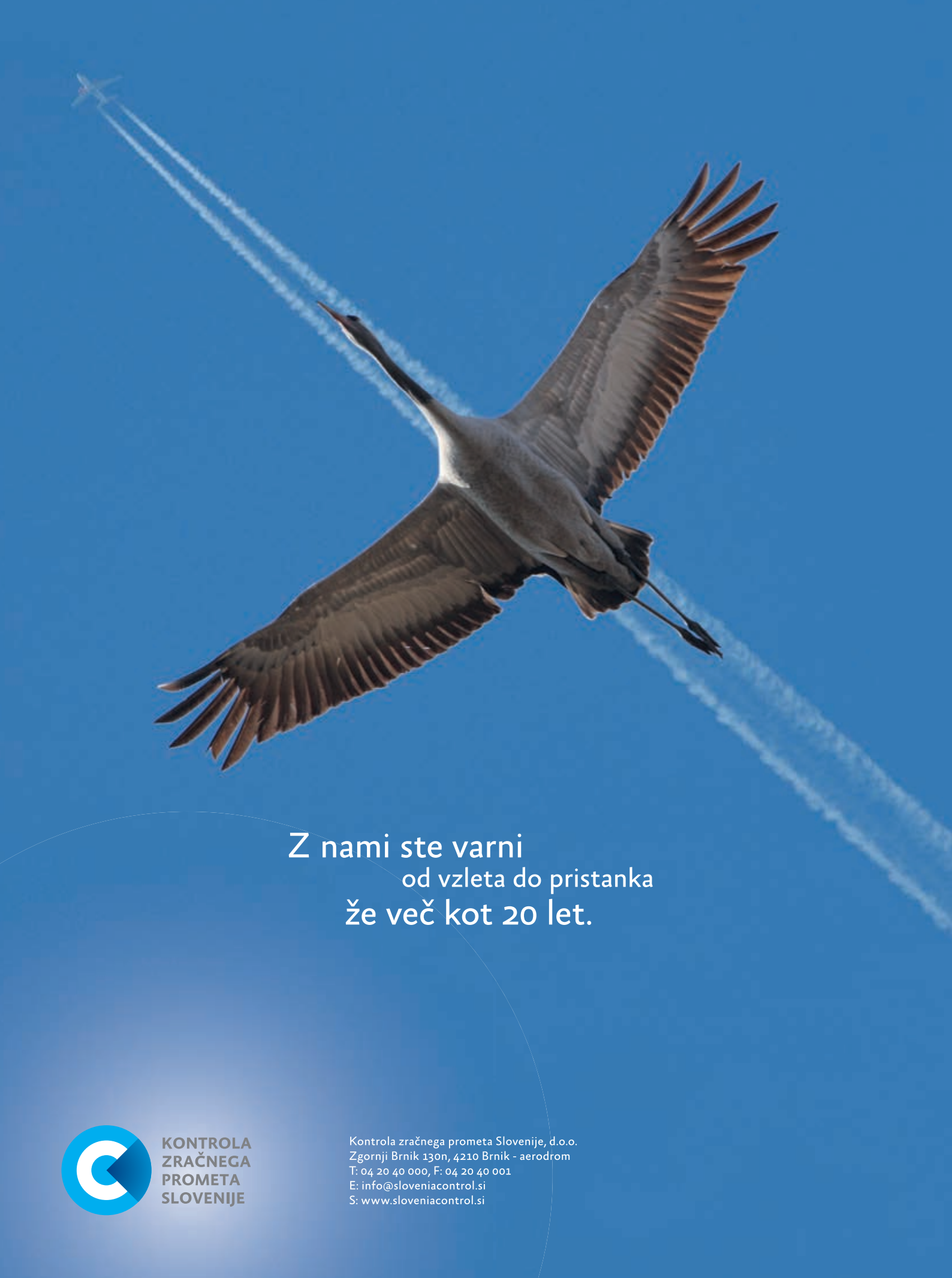


Slovenija

Slovenija je že, vsaj odkar je leta 1849 v Ljubljano pripeljal prvi vlak po novozgrajeni Južni železnici, trdno vpeta v gospodarstvo zahodne Evrope. In to tako trdno, da se ni nič bistveno spremenilo niti v času komunizma, ko so naše ključne trgovinske partnerice ostale Nemčija, Italija in Avstrija in je tako še danes, skoraj 170 let kasneje. V lanskem letu bo samo blagovna menjava z Nemčijo presegla 10 mrd eur, z Italijo dosegla 7 mrd z Avstrijo pa skoraj 5 mrd eur. Zdaj se že skoraj 78 odstotkov blagovne menjave Slovenije opravi znotraj EU, kar pomeni usodno povezanost Slovenije z zahodom. Lahko bi rekli; povej mi s kom trguješ in povem ti, kdo si.

Od nekdanjih političnih ambicij Slovenije, da bi želela več trgovati s svetom, posebej z državami BRICS (Brazilija, Rusija, Indija, Kitajska, Južna Afrika) po soočenju z realnostjo ni ostalo veliko. Kadar politične ambicije in projekti niso usklajeni z realnimi zmožnostmi in predvsem potrebami gospodarstva (demand driven) praviloma nastanejo težave in izgube. Za prodor na nove trge je potrebno imeti ali izjemno posebnost in kakovost ali pa množične, kvalitetne in po možnosti tudi cenejše izdelke, česar pa Slovenija, razen nekaj izjem, praktično nima. Za povrh so prav vsi BRICS tigri že ob prvih znakih krize močno omagali, še najmanj Kitajska, a je tudi ta komaj ohranila tretjino nekdanjih stopenj rasti. Najbolj hudo pa sta bili prizadeti Brazilija in Rusija, ki je v zadnjih 4 letih izgubila več kot tretjino BDP in je iz nekoč osme gospodarske sile sveta pristala na enajstem mestu, povsem skupaj s Španijo. Na te razmere so se slovenska podjetja tokrat dobro odzvala in se hitro preusmerila s teh kriznih in nelikvidnih trgov na sicer zahtevnejše a likvidne in razvojne trge. Nekaj jih je ostalo z velikimi dolgovi v Rusiji, Belorusiji, Ukrajini, nekaj pa jih je uspešno prešlo na zahod ali pa so povečala svoje deleže na zahodu. Kar Sloveniji manjka je hitrejši prenos znanj in prehod na nova orodja tehnološke dobe, a to je tema za naslednji članek.

Slovenija skratka živi v svojevrstnem paradoksu; medtem, ko si dobesedno ves svet prizadeva čim več poslovati z EU kot najbogatejšim delom sveta in tja čim več izvažati, je Sloveniji to že davno uspelo! Še več, Slovenija je ena od zgolj štirih evropskih članic EU, ki ima presežek v blagovni menjavi z mogočno Nemčijo. Za Slovenijo je smer torej jasna; smer sever, severo-zahod. ■



KONTROLA ZRAČNEGA PROMETA SLOVENIJE

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

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



KAKO IZBRATI USTREZNO OSEBO ZA VARSTVO OSEBNIH PODATKOV (DPO)?

Pred vrati je uveljavitev Splošne evropske uredbe o varstvu podatkov, ki jo strokovna javnost pozna pod nazivom GDPR. Uredba prinaša nekaj pomembnih novosti, katera pred zavezance postavlja resno zavezo za vzpostavitev vseh mehanizmov, ki bodo zagotavljali učinkovito varovanje zaupanih osebnih podatkov. Posebno poglavje vzpostavitve ustreznega varstva osebnih podatkov predstavlja imenovanje ustrezne osebe za varstvo osebnih podatkov ali strokovno bolj poznanega kot DPO. Zelo hitro pa ugotovimo, da naloga, ki jo uredba prinaša, v praksi ni ravno najlažje izvedljiva.

Veliko je bilo že, vezano na omenjeno uredbo, povedanega in napisanega, zato se bom v tem kratkem prispevku osredotočil na osnovno dilemo, kako izbrati in določiti pravo osebo za varstvo osebnih podatkov (v nadaljevanju DPO). Izkušnje jasno kažejo, da je človeški faktor, ko govorimo o ustreznem delovanju posameznih sistemov, ki jih prinašajo zakonske rešitve na posameznih pomembnih področjih, tisti najpomembnejši člen. Področje varovanja osebnih podatkov v tem okviru ni nikakršna izjema, zato bo v vsaki organizaciji, ki bo zavezana, da postavi lastnega DPO, zelo pomembno, kakšna oseba bo imenovana na to področje. Od osebe se bo, poleg ustreznih strokovnih referenc, pričakovalo seveda etično, neodvisno in nepristransko delovanje. Že bežno pa lahko skozi te zahteve vidimo, da bo poiskati in določiti pravo osebo na mesto DPO v organizaciji, vse prej kot lahek proces. Naslednja pomembna ugotovitev bo verjetno ta, da se s postavitvijo določene osebe za DPO, njeno strokovno potovanje oz. trnova pot pridobitve vseh ustreznih znanj, ki jih bo potrebovala za učinkovito izvajanje svojega poslanstva, praktično šele začne.

Kratka analiza že imenovanih DPO oz. analiza oseb, ki so po ZVOP-1 skrbele za to področje pokaže, da je v večini primerov ta naloga padla na pravne ali kadrovske službe v organizaciji oz. službe skladnosti poslovanja. Le redko so bili ti omenjeni strokovnjaki vključeni v službe, ki se ukvarjajo s celovitim obvladovanjem varnostnih tveganj, med katerimi je posebej izpostavljena informacijska varnost. Lahko se seveda strinjamo, da mora bodoči DPO poznati pravno področje in ga tudi do te mere razumeti, da lahko ustrezno tolmači določene pravne dileme, ki so vezane na obdelovanje in varovanje osebnih podatkov. Vendar pa to še zdaleč ni edina naloga oz. strokovna kompetenca, ki jo potrebuje. Zaradi določene nedorečenosti in praktičnih dilem, bo šele praksa pokazala, kako bodo določene rešitve zares zaživele v praksi. Zaradi navedenega lahko strokovnjak pravne stroke, s konservativnimi pravnimi stališči, pri učinkoviti implementaciji predvidenih zakonskih mehanizmov, postane velik zaviralni faktor. Še bolj pa postane ta zadeva nevarna, če vzamemo, kot osnovno in edino izhodišče za učinkovitega DPO, samo kompetence in znanja s področja prava. Na žalost živimo v informacijski družbi, kjer se velika večina podatkov obravnava in obdeluje skozi komunikacijsko informacijsko tehnologijo. Nepoznavanje osnovnih podlag informacijske varnosti in procesov obvla-

To pomeni, da bo moral ustrezno kompetentni DPO poleg pravnih znanj, vsekakor obvladati znanja s področja varnosti, osnov informatike, organizacijskih ved in seveda v potankost poznati poslovne procese na katerih temelji uspešno delovanje organizacije.

*avtor je član Slovenskega združenja korporativne varnosti

dovanja varnostnih tveganj je verjetno tako velik hendikep, ki bo področje varovanja osebnih podatkov v organizaciji hitro pripeljal v smer, kjer bo sicer nekaj pravno urejeno, praksa pa bo na žalost zaradi nujnih potreb, predvsem gospodarskega poslovanja, največkrat popolnoma nekaj drugega. To pomeni, da bo moral ustrezno kompetentni DPO poleg pravnih znanj, vsekakor obvladati znanja s področja varnosti, osnov informatike, organizacijskih ved in seveda v potankost poznati poslovne procese na katerih temelji uspešno delovanje organizacije.

Naslednja pomembna komponenta je ustrezna etična in moralna dimenzija, ki bo DPO-ju zagotovila uveljavljanje svetovalne aktivnosti in zahtev za ureditev stanja, tudi v tistih trenutkih, ko za to ne bo podpore vodstva. Še več, prišli bodo namreč trenutki, ko bo vodstvo skozi različne načine pritiskalo na DPO, da določeno stvar spregleda ali naredi izven okvirov strokovnih in normativnih pričakovanj oz. zahtev. Pred kratkim smo namreč slišali, da bi bilo lahko področje DPO primerno za zaposlovanje mladih pravnikov, ki so dovolj neobremenjeni in so produkt informacijske dobe, kateri naj bi zadosti poznali informacijsko in komunikacijsko tehnologijo, da jim razumevanje rešitev na tem področju ne bi bilo tuje. Torej, če na ta predlog pogledamo z dovolj veliko resnostjo, lahko hitro ocenimo, da začetnik, brez izkušenj, predvsem pa z nezmožnostjo kompetenčne in strokovne avtoritete, nikakor ne bi bil ustrezna izbira za potrebno delovanje sistema varovanja osebnih podatkov. DPO mora imeti skozi ustrezne organizacijske poti neposreden dostop do vodstva organizacije. Na tem področju pa se že dotaknemo organizacije procesov v posamezni organizaciji. Seveda bi na vsakem pomembnem področju želeli imeti neposreden dostop do strateškega vodstva. V nekaterih primerih so zakonodajalci ob spretnem lobiranju pripravljavcev določenih pravnih aktov to celo uzakonili. Tudi v tem primeru imamo take nastavke v samem pravnem aktu. Potrebno se je zavedati, da organizacija potrebuje tak procesni ustroj, kjer se tudi področje varovanja osebnih podatkov umešča v učinkovito delovanje in vodenje organizacije. Vsekakor velja predlagati, da je DPO umeščen v tako organizacijsko enoto, ki je že v svojstvu pomembnosti in nujnosti umeščena v neposredno bližino strateškega vodstva oz. mu skozi dodeljene procese v pomembnih trenutkih lahko poroča neposredno, kljub temu, da v normalnem delovanju ni pod njegovim neposrednim vodenjem. V zadnjem času lahko opažamo, da se DPO vedno bolj potiska v organizacijske dele, ki se ukvarjajo z zagotavljanjem skladnosti poslovanja. Osebno sem menja, da bi DPO, v tistih organizacijah, ki imajo ustrezno postavljen sistem korporativne varnosti, sodil ravno v to organizacijsko obliko. Zelo hitro namreč, ko govorimo o informacijski varnosti, ki je bila do nedavno umeščena v službe informatike, pridemo do podobne dileme. Tu pride do kolizije interesov, saj služba praktično nadzira sama sebe. Zaradi navedenega moramo biti tudi pri organizacijski umeščenosti bodočega DPO zelo pozorni in skrbno pretehtati, kam ga, glede na specifične situacije, ki jih imamo v posameznih organizacijah, tudi umestiti.

V vsakem primeru bi bil pri izbiri previden in bi veljalo iskati predvsem tista usposabljanja, ki bodo širila obseg kompetenc na nujno potrebnih področjih informacijske varnosti povezanih z implementacijo zakonskih zahtev varovanja osebnih podatkov.

Za konec pa je potrebno nameniti nekaj besed vprašanju kako zagotoviti nadgraditev in razširitev strokovnih kompetenc postavljenih DPO-jev. V zadnjem obdobju imamo poplavo določenih usposabljanj, delavnic, v nekaterih primerih tudi »certificiranj« bodočih DPO. V vsakem primeru bi bil pri izbiri previden in bi veljalo iskati predvsem tista usposabljanja, ki bodo širila obseg kompetenc na nujno potrebnih področjih informacijske varnosti povezanih z implementacijo zakonskih zahtev varovanja osebnih podatkov. Neposredne izkušnje in primeri dobre prakse morajo biti tisti jeziček na tehtnici potrebnih znanj in novih kompetenc. Golo ponavljanje napisanih pravnih zahtev ne sme biti osnova, na kateri nekdo temelji certificiranje oz. bodoči kompetenčni model DPO. Pri tem vsekakor vidim pomembno nalogo institucije Informacijskega pooblaščenca, ki bo skozi jasne smernice, če ne celo akreditacijski postopek, določil kdo, glede na izkazane reference in strokovnost, lahko izvaja tovrstna usposabljanja. ■



Avtorja: Ksenija Butenko Černe / članica uprave,
mag. Marko Potokar / korporativno varnostni manager, Lek d.d*





OCENJEVANJE TVEGANJ V KORPORACIJAH

Vsak dogodek, ki negativno vpliva na doseganje ciljev organizacije in povzroči moteno poslovanje, je potrebno določiti, analizirati in oceniti njegov vpliv na izvajanje procesov organizacije. Za oblikovanje učinkovitega sistema upravljanja tveganj, je potreben sistematičen pristop, ki mora ustrezati danemu okolju organizacije in biti usklajen s splošnim upravljanjem tveganj v njej. Tudi farmacevtska dejavnost je povezana z nizom tveganj, ki imajo lahko negativni vpliv pri zagotavljanju neprekinjenosti delovanja glavnih poslovnih procesov.

Uvod

Upravljanje tveganj je eden izmed bistvenih procesov vsake organizacije, ki pomaga pri prepoznavanju in analiziranju morebitnih rizikov, ranljivosti in priložnosti. Učinkovito obvladovanje tveganj povečuje verjetnost uspeha in zmanjša verjetnost neuspeha ter stopnjo negotovosti, povezano z doseganjem ciljev organizacije. Pogosto napačno prepričanje je, da obvladovanje tveganj preprečuje strateško rast in ambicije. Podjetja morajo tvegati, da ustvarijo vrednost. Z učinkovitim upravljanjem tveganj zagotavljamo, da so tveganja, ki jih organizacija sprejema, pravilna in da se ustrezno upravljajo (t.i. risk-intelligent decision making). Tudi priložnosti lahko postanejo tveganja, v kolikor jih organizacija ni sposobna zaznati ali ne učinkovito izkoristiti.

Upravljanje tveganj v Novartisu

Lek, kot del mednarodne korporacije Novartis, predstavlja eno od najpomembnejših farmacevtskih podjetij v regiji JV Evrope. V podjetju je močno razvita zavest o pomembnosti korporativne integritete, ki je več kot le izpolnjevanje zakonskih določil, uredb in pravil. Gre za kulturo, ki se prepleta v vse pore delovanja podjetja. Le gospodarske družbe, ki pri svojih standardih poslovanja ohranjajo visoko stopnjo etike in morale, lahko dolgoročno krepijo svoj ugled in zaupanje svojih deležnikov v njihovo delo ter ohranjajo konkurenčnost, stabilno poslovanje in s tem tudi delovna mesta. Za dolgoročno poslovno uspešnost, pa je poleg visokega nivoja organizacijske kulture, bistvenega pomena tudi upravljanje tveganj.

Pogosto napačno prepričanje je, da obvladovanje tveganj preprečuje strateško rast in ambicije. Podjetja morajo tvegati, da ustvarijo vrednost.

Upravljanje tveganj je proces zmanjševanja tveganj na sprejemljivo stopnjo. Je nepretrgan proces, sestavljen iz naslednjih faz:

- identifikacija tveganj,
- analiza tveganj,
- ocena stopnje tveganja,
- priprava načrta za zmanjšanje stopnje tveganja,
- izvedba načrta za zmanjšanje stopnje tveganja,
- spremljanje in ponovna ocena stopnje tveganja.

Ključne kategorije tveganj, ki jih prepoznava Novartis, so tveganja, ki imajo lahko naslednje negativne učinke:

- pravne, med katere sodijo regulatorni in drugi pravni postopki proti organizaciji ali njenim zaposlenim, zaradi katerih se lahko zoper organizacijo in njene zaposlene izreče globe, kazni, zaporne kazni in zasege ali odvzem izdelkov;
- finančne, kot so npr. negativni učinki na vrednost delnic, potencialne prihodnje zaslužke ali izgubo zaupanja vlagateljev;
- poslovne, kot so neželeni dogodki in embargi, ki bi lahko znatno ovirali sposobnost organizacije za delovanje;
- negativni učinki, ki povzročajo škodo ugledu podjetja ali blagovni znamki organizacije, na primer zaradi negativne-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

ga poročanja medijev, izgube zaupanja strank ali zmanjšanja morale zaposlenih.

Upravljanje poslovnih tveganj, in tveganj s področja skladnosti, je v Novartisu del rednega poslovnega procesa in s tem odgovornost vodstva.

Varnostna tveganja

Na seznamu rizičnih podjetniških dejavnikov, o katerih je Novartis tudi poročal v okviru svojega letnega poročila za leto 2016, so med drugim navedena tveganja zaradi neupoštevanja zakonov, kršitev na področju varovanja informacij in informacijskih sistemov ter tveganja zaradi kršitev na področju zasebnosti pri uporabi informacijsko komunikacijske tehnologije, interneta, socialnih medijev in mobilnih tehnologij.

Navedena tveganja sodijo na področje korporativne varnosti, ki ne predstavlja samo fizičnega in tehničnega varovanja ljudi in premoženja, temveč zajema tudi varovanje transportne verige, varnost izdelkov, upravljanje tveganj v zvezi z ekstremističnimi skupinami, izvajanje preiskav, varnostno svetovanje, varovanje posameznikov in skupin na tveganih območjih in tudi varovanje informacij ter osebnih podatkov. Ključna naloga varnostne funkcije je upravljanje varnostnega sistema in s tem obvladovanje varnostnih tveganj, na področju zaščite ljudi in premoženja.

Analiza varnostnih tveganj

Namen analize varnostnih tveganj je ugotovitev, ali uvedene varnostne kontrole uspešno in učinkovito zmanjšujejo tveganja na sprejemljiv nivo. Celovit varnostni sistem je sestavljen iz fizičnih, tehničnih, logičnih in organizacijskih varnostnih ukrepov in je zmožen detektirati grožnjo, oceniti njeno velikost in se ustrezno odzvati, da omeji oziroma prepreči delovanje grožnje na sredstvo, ki ga sistem varuje. Tako se v procesu analize tveganj ocenjujejo naslednja področja:

Namen analize varnostnih tveganj je ugotovitev, ali uvedene varnostne kontrole uspešno in učinkovito zmanjšujejo tveganja na sprejemljiv nivo.

- ***upravljanje varovanja***, v okviru katerega se preverja, ali organizacija ima varnostnega managerja oziroma odgovorno osebo za varovanje in pisno dokumentacijo, v kateri je določeno kako se varujejo viri in informacije.
- ***varnostno preverjanje osebja***, ki je sestavljeno iz postopkov preverjanja kandidatov za zaposlitev in občasnega preverjanja zaposlenih in pogodbenikov.
- ***kontrola pristopa***, ki predstavlja sestav strojne in programske opreme, s pomočjo katere upravljamo s pristopnimi pravicami posameznikov ali skupin na varovano območje, v določene objekte ali prostore.
- ***fizično varovanje***, katerega osnovna funkcija je mehanska zaščita, ki preprečuje oziroma otežuje nepooblaščen dostop do varovanih sredstev. Med fizično zaščito sodi tudi ustrezna struktura in izgradnja objektov, osvetlitev, rezervno napajanje, sistemi upravljanja s ključi ipd.
- ***varnostni postopki***, s katerimi se predpiše in zagotovi izvajanje in preverjanje varnostnih protokolov v okviru posameznih procesov.
- ***informacijska tehnologija in varovanje informacij***, ki zajema preverjanje ustreznosti zagotavljanja celovitosti, zaupnosti in razpoložljivosti informacij in informacijskih sistemov. Pri tem se med drugim ocenjuje sistem upravljanja z uporabniškimi pooblastili in gesli, varnost računalniškega omrežja in obstoj pripadajoče varnostne dokumentacije.



Priprava načrta za zmanjšanje stopnje tveganja

Iz analize tveganj izhaja ocena tveganj in priprava načrta za zmanjšanje stopnje tveganja, ki predstavlja formalni načrt za uvajanje ukrepov za zmanjševanje tveganj, katerih stopnja tveganja je ocenjena kot nesprejemljiva. V načrtu tveganja so opredeljene:

- aktivnosti za zmanjšanje tveganja (KAJ),
- odgovorni za izvedbo aktivnosti (KDO),
- roki za izvedbo aktivnosti (KDAJ),
- prioritete,
- stroški uvedbe in izvajanja ukrepov,
- potrebe po človeških virih,
- potreb po novih tehnologijah,
- potrebno delo za vpeljavo in izobraževanje.

Izvedba načrta za zmanjšanje tveganj

Ko je načrt pripravljen, sledi odločitev za izvedbo načrta, katerega cilj je zmanjšanje stopnje tveganja na raven, določeno s kriterijem sprejemljivosti. Vsa tveganja, ki so nad postavljeno ravnijo, so nesprejemljiva in morajo biti zmanjšana z:

- odstranitvijo vzroka tveganja,
- izbiro ustreznih kontrol (nadzorstev),
- zavarovanjem tveganj pri zavarovalnici,
- prenosom tveganj na drugo osebo s pogodbo.

Vsa tveganja pod izbrano ravnijo sprejemljivosti zavestno sprejmemo, saj so premajhna, da bi upravičila stroške za njihovo zmanjševanje.

Spremljanje in ponovna ocena tveganja

Ta faza procesa upravljanja tveganj, velikokrat podcenjena ali celo pozabljena, zajema ocenjevanje uspešnosti izvedbe načrta za zmanjšanje stopnje tveganja in se nadaljuje v naslednji krog izvedbe analize in ocene stopnje tveganja.

Zaključek

Bistvo pri določanju stopnje tveganja je negotovost neželenega dogodka. Poznamo dva osnovna načina za analizo in oceno tveganja: kvantitativni in kvalitativni. Oba načina imata svoje prednosti in pomanjkljivosti. Prednost kvantitativnih modelov je v njihovi objektivnosti in eksplicitnosti dobljenih rezultatov. Podprti so s statistično analizo. Pomanjkljivost tovrstnih modelov je v težavnosti pridobivanja dovolj velike količine merodajnih podatkov in uporaba kompleksnih matematičnih izračunov. Dodatna težava je oblikovanje primerne interpretacije rezultatov za vodstvo, ki se odloča o sprejetju oziroma zavrnitvi določenih aktivnosti za zmanjšanje tveganja. Lažji za razumevanje so kvalitativni modeli za analizo tveganj. Njihovi rezultati so sicer v osnovi subjektivne narave, a nam ti modeli omogočajo dobro predstavo, kaj določeno tveganje pomeni za dani proces. Da bodo rezultati jasni in pot do njih razumljiva, moramo v procesu analize tveganja in njegovi oceni uporabljati ustrezna orodja.

Predvsem pa je za stabilnost poslovanja in učinkovito upravljanje tveganj bistvena kultura organizacije, z vgrajenimi standardi integritete in skladnostmi v vseh procesih delovanja. Kultura organizacije in zavedanje poslovodstva ter vseh zaposlenih krepi poslovno odgovornost za prevzem pametnih tveganj pri izvajanju aktivnosti, za pravi razlog in na pravi način. In predvsem to je tisto, kar zagotavlja dolgoročno stabilnost poslovanja organizacij. ■









POPOLNA SPROSTITEV JE BLIŽJE, KOT SI MISLITE

17 BAZENOV • 14 SAVN • CENTER AZIJSKIH MASAŽ
STROKOVNI CENTER ZDRAVJA • RESTAVRACIJA

ATLANTIS
VODNO MESTO

01 585 21 00 | www.atlantis-vodnomesto.si

BTC, D.D., ŠMARTINSKA 152 • SAATCHI & SAATCHI

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Srečko Zajc, generalni direktor Direktorata za obrambne zadeve, Ministrstva za obrambo

SPREJET JE NOV ZAKON O KRITIČNI INFRASTRUKTURI REPUBLIKE SLOVENIJE

Pogovarjali smo se z generalnim direktorjem, g. Srečkom Zajcem, o pomenu sprejetja ustrezne zakonodaje s področja kritične infrastrukture in ukrepih, ki jih bo, na podlagi zahtev zahtevnega varnostnega okolja, potrebno izpeljati na tem področju.

Ob koncu leta 2017 je bil sprejet nov Zakon o kritični infrastrukturi. Glede na potrebnost omenjenega sistemskega akta ste verjetno zadovoljen z njegovim sprejemom.

Glede na dejstvo, da se v Republiki Sloveniji z zaščito »nacionalne« kritične infrastrukture bolj ali manj prizadevno ukvarjamo že več kot desetletje, me izredno veseli, da je zdaj to področje tudi sistemsko urejeno z enovitim krovnim zakonskim predpisom. Zakon o kritični infrastrukturi, ki ga je potrdil Državni zbor 12. decembra 2017 na svoji 36. redni seji z nevsakdanje visoko podporo s 65 glasovi za in nobenim proti, torej z absolutno kvalificirano večino, in je objavljen v Uradnem listu RS, št. 75/17 z dne 22. 12. 2017, ureja ugotavljanje in določanje kritične infrastrukture državnega pomena, načela in načrtovanje njene zaščite, naloge organov in organizacij na področju kritične infrastrukture ter obveščanje, poročanje, zagotavljanje podpore odločanju, varovanje podatkov in nadzor na področju kritične infrastrukture. S sprejetjem zakona je Slovenija naredila pomemben korak v svojem večstranskem prizadevanju za krepitev ravni odpornosti slovenske družbe na sodobne varnostne grožnje in tveganja. Zakon je pristojnost strokovnega usmerjanja in usklajevanja, na področju kritične infrastrukture, naložil Ministrstvu za obrambo, čemur je botrovalo predvsem dejstvo, da to ministrstvo skrbi za usklajevanje dejavnosti na tem področju že vse od leta 2006.

Kakšni so načrti v naslednjem obdobju vezano na izdelavo potrebnih podzakonskih predpisov, ki bodo nekatere stvari vezane na določila zakona še dodatno opredelili?

Vsebino zakona in predvsem naloge za njegovo uresničevanje smo sredi februarja 2018 predstavili predstojnikom in strokovnim delavcem direktoratov in organov v sestavi ministrstev, ki so predvidena za nosilce sektorjev kritične infrastrukture, kot jih določa 4. člen Zakona o kritični infrastrukturi (sektor energetike, prometa, prehrane, preskrbe s pitno vodo, zdravstva, financ, varovanja okolja in informacijsko-komunikacijskih omrežij in sistemov). Prva naloga, ki izhaja iz določil zakona, je določitev nosilcev sektorjev kritične infrastrukture in z njimi sodelujočih državnih organov pri izvajanju njihovih zakonskih nalog ter prioritete delovanja sektorjev kritične infrastrukture. Določiti bo treba sektorske in medsektorske kriterije za ugotavljanje kritične infrastrukture ter njihove mejne vrednosti. Na njihovi podlagi bo treba izvesti postopek ugotavljanja kritične infrastrukture in v devetih mesecih po uveljavitvi zakona na novo določiti kritično infrastrukturo državnega pomena z njenimi upravljavci. V letu dni od uveljavitve zakona bo treba sprejeti navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture. Na podlagi slednjega in strokovnih usmeritev nosilcev sektorjev kritične infrastrukture bodo upravljavci izdelali oceno tveganj za delovanje kritične infrastrukture, katero upravljajo.

Za usklajevanje tako pomembnega procesa kot je zaščita kritične infrastrukture bo verjetno potrebno zagotoviti dodatne kadrovske vire. Menite, da boste uspeli prepričati vrh ministrstva, da vam nameni dodatno strokovno pomoč pri izvedbi teh nalog?

Usmerjanje in usklajevanje na področju kritične infrastrukture ter aktivnosti za uveljavitev določil Zakona o kritični in-

*avtor je član Slovenskega združenja korporativne varnosti

frastrukturi v Direktoratu za obrambne zadeve že izvajamo z obstoječim strokovnim kadrom. Uresničevanje z zakonom naloženih nalog ter pristojnosti in odgovornosti je nova, zahtevna strokovna naloga Ministrstva za obrambo kot skrbnika tega področja v državi. Za njihovo izvajanje bo potreben dodaten strokovni kader. Prepričan sem, da bo vodstvo ministrstva to potrebo prepoznalo in tej problematiki namenilo ustrezno pozornost. V naše delovno okolje bo treba pritegniti ne samo dodatne kadre, ampak tudi za področje zaščite kritične infrastrukture strokovno že kompetentne osebe, če želimo biti kos tako povečanemu obsegu operativno-tehničnih nalog kot tudi (bolj) zahtevnim razvojnim izzivom na posebnem strokovnem področju, ki je z obrambnim samo v daljnem sorodstvu.

Kaj bi bilo po vašem mnenju potrebno narediti, da bo razumevanje pomena javno-zasebnega partnerstva na področju zaščite kritične infrastrukture prišlo na višji nivo?

S sprejemom Zakona o kritični infrastrukturi je vzpostavljena tudi temeljna podstat tako za boljše razumevanje pomena javno-zasebnega partnerstva kot za vzpostavitev partnerskih razmerij.

Zakon o kritični infrastrukturi namreč opredeljuje načelo odgovornosti na področju kritične infrastrukture, po katerem so za krepitev zaščite kritične infrastrukture odgovorni vsi pristojni organi in organizacije v skladu z zakonom, torej ne samo upravljavci kritične infrastrukture kot gospodarske družbe in javni zavodi, ampak tudi organi državne oblasti, kar že samo po sebi kaže na nujnost sodelovanja med javnim ter zasebnim in/ali poslovnim okoljem, če upoštevamo, da je v naši državi večina kritične infrastrukture še zmeraj v javni lasti.

Zakon o kritični infrastrukturi namreč opredeljuje načelo odgovornosti na področju kritične infrastrukture, po katerem so za krepitev zaščite kritične infrastrukture odgovorni vsi pristojni organi in organizacije v skladu z zakonom, torej ne samo upravljavci kritične infrastrukture kot gospodarske družbe in javni zavodi, ampak tudi organi državne oblasti, kar že samo po sebi kaže na nujnost sodelovanja med javnim ter zasebnim in/ali poslovnim okoljem, če upoštevamo, da je v naši državi večina kritične infrastrukture še zmeraj v javni lasti. Poleg tega načelo izmenjave podatkov in informacij ter varovanje podatkov zahteva visoko stopnjo zaupanja pri vseh pristojnih organih in organizacijah ob hkratnem doslednem varovanju podatkov, povezanih s kritično infrastrukturo. Z udejanjanjem teh dveh temeljnih načel zaščite kritične infrastrukture se bo prav gotovo okrepilo ne samo zavedanje o pomenu javno - zasebnega partnerstva pač pa se bodo vzpostavile tudi različne oblike medsebojnega sodelovanja, usklajevanja in sporazumevanja na podlagi vzajemnega interesa in zaupanja.





Strokovna javnost ves čas opozarja, da je največja težava na področju sektorskih koordinatorjev v resornih ministrstvih, ki jim zakon prinaša zelo pomembne pristojnosti usklajevanja zaščite kritične infrastrukture v posameznih sektorjih. Kaj bi bilo po vašem mnenju potrebno narediti, da bi na ta odgovorna mesta prišli ustrezno usposobljeni strokovnjaki?

Prepričan sem, da ministrstva razpolagajo s strokovno usposobljenim kadrom, ki izvaja naloge na delovnih področjih iz njihove pristojnosti. Za udejanjanje njihovih pristojnosti kot nosilcev sektorjev kritične infrastrukture in izvajanje nalog, ki jim jih nalaga novo sprejeti Zakon o kritični infrastrukturi, pa bo verjetno terjalo dodatno usposabljanje že zaposlenih. V Ministrstvu za obrambo v okviru izvajanja projektov s podporo Evropske unije iz Sklada za notranjo varnost zaključujemo projekt z naslovom Potrebna znanja in predlog programa usposabljanj upravljavcev kritične infrastrukture (PROPU), katerega cilj je med drugim pripraviti predlog programa usposabljanj upravljavcev kritične infrastrukture in vzpostaviti podlage za izvajanje usposabljanj upravljavcev in njihovih odgovornih oseb za izvajanje nalog na področju kritične infrastrukture. Udeležbo na takih osnovnih izobraževanjih in usposabljanjih, sicer namenjenih v prvi vrsti upravljavcem, bi lahko ponudili tudi odgovornim osebam za področje kritične infrastrukture v ministrstvih.

Sicer je od vodstev ministrstev odvisno v kolikšni meri prepoznajo pomen neprekinjenega delovanja kritične infrastrukture državnega pomena za sektor, katerega nosilec so, in da za izvajanje nalog, na področju dejavnosti sektorja kritične infrastrukture ter usmerjanje upravljavcev kritične infrastrukture pri njihovem načrtovanju zaščite kritične infrastrukture, imenujejo izkušene, strokovne in kompetente ljudi. Ministrstva so namreč skladno z Zakonom o kritični infrastrukturi odgovorna za stanje v »svojem« sektorju kritične infrastrukture z vidika njegove zaščite.

V pripravi je nov zakon o Informacijski varnosti. Bo po vaši oceni težko uskladiti omenjeni predlog zakona z že sprejetim Zakonom o kritični infrastrukturi? Strokovna javnost namreč opozarja na nujne korake tesnejšega usklajevanja rešitev, ki jih urejajo posamezni zakonski predpisi s področja zaščite kritične infrastrukture.

Direktorat za obrambne zadeve si je z vidika (zaščite) kritične infrastrukture močno prizadeval, da so bili v Predlog zakona o informacijski varnosti med zavezance, po navedenem zakonu, umeščeni tudi upravljavci kritične infrastrukture državnega pomena, saj menimo, da bi morale zahteve zakona, katerega namen je dvigniti nivo varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, veljati oziroma biti zavezujoče tudi za celoten nabor kritične infrastrukture Republike Slovenije. Infrastruktura, ki ima status kritične infrastrukture oz. njeni upravljavci bi po našem mnenju morali – tudi ali celo prvi med vsemi – zadostiti vsem standardom informacijske varnosti, ki jih bo prinesel Zakon o informacijski varnosti. Ker so pisci Zakona o informacijski varnosti končno le sprejeli ustrezno dopolnitev, ki jo je predlagalo naše ministrstvo, lahko govorimo o ustreznem jamstvu, da ne bo morebitnemu (ne)srečnemu naklju-

Infrastruktura, ki ima status kritične infrastrukture oz. njeni upravljavci bi po našem mnenju morali – tudi ali celo prvi med vsemi – zadostiti vsem standardom informacijske varnosti, ki jih bo prinesel Zakon o informacijski varnosti.

čju prepuščeno, ali bodo zavezanci po Zakonu o informacijski varnosti tudi organizacije in organi, ki so za zagotavljanje nacionalne varnosti in drugih ključnih družbenih funkcij najpomembnejši subjekti v državi.

Vodite Direktorat za obrambne zadeve, kjer je pomemben del vaših pristojnosti tudi koordinacija kriznega upravljanja. Kako tesno so po vašem mnenju povezani procesi zaščite kritične infrastrukture in nacionalnega sistema kriznega upravljanja?

V Republiki Sloveniji je v kriznih razmerah vsako ministrstvo do določene ravni odgovorno za izvajanje nalog na svojem področju, glavni organ za usklajevanje kriznega odziva pa je vlada. Kriza po Zakonu o kritični infrastrukturi pomeni, da stanje, v katerem so zaradi prekinitve delovanja kritične infrastrukture nastale oziroma lahko nastanejo posledice, ki presegajo mejno vrednost vsaj enega medsektorskega kriterija za ugotavljanje kritične infrastrukture ne pomeni nujno tudi krize nacionalnih razsežnosti, ko se uporabijo vsi mehanizmi kriznega odzivanja. Hkrati pa je kriza, kot je razumljena v zakonu, več kot stanje, kadar pride do resnih motenj v delovanju kritične infrastrukture ali do prekinitve njenega delovanja.

Ob zaznani povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi na področju kritične infrastrukture, upravljavci, ki načrtujejo in izvajajo stalne ukrepe za zaščito kritične infrastrukture, izvajanje le-teh lahko stopnjujejo. Ukrepi za zaščito kritične infrastrukture so dejavnosti, katerih namen je zagotoviti varnost kritične infrastrukture, preprečiti motnje v njenem delovanju ali prekinitev njenega delovanja in ublažiti posledice tega, po potrebi vzpostaviti nadomestno ali obhodno delovanje kritične infrastrukture in zagotoviti njeno čimprejšnje ponovno nemoteno delovanje. Delijo se na stalne in dodatne.

Če stalni ukrepi, tudi če so stopnjevani, ne zadostujejo, lahko upravljavci in po potrebi tudi nosilci sektorjev kritične infrastrukture, ko gre za ukrepe za zaščito kritične infrastrukture na ravni sektorja kritične infrastrukture iz njihove pristojnosti, sprejmejo dodatne ukrepe. Ko gre za ukrepe, ki presegajo pristojnost posameznega nosilca sektorja kritične infrastrukture lahko dodatne ukrepe na njihov predlog sprejme tudi Vlada Republike Slovenije.

Opisani procesi pravzaprav predstavljajo krizno upravljanje na področju kritične infrastrukture, v katerem ima svojo vlogo tudi Nacionalni center za krizno upravljanje (NCKU), ki v skladu s pristojnostmi v takih razmerah nudi podporo odločanju na navedenem področju.

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

Ministrstvo za obrambo bo glede na zakonsko pristojnost in nalogo kot skrbnik področja kritične infrastrukture v državi še bolj poudarjeno usmerjalo in koordiniralo pristojne organe in organizacije na področju kritične infrastrukture državnega pomena in tudi kot kontaktna točka za zaščito evropske kritične infrastrukture v Republiki Sloveniji. V tej luči jih bo seznanjalo z dobrimi praksami in izkušnjami drugih pri zaznavanju, ocenjevanju in obvladovanju tveganj za delovanje kritične infrastrukture ter načrtovanju njene zaščite ter drugimi vsebinami z navedenega področja. Vse pristojne organe in organizacije na področju kritične infrastrukture bo seznanilo z navodilom za ocenjevanje tveganj za delovanje kritične infrastrukture, s primeri rešitev na tem področju v drugih državah, usmeritvami za izdelavo ocene tveganj za delovanje kritične infrastrukture, ki jo upravljajo itd. Naštete aktivnosti bo ministrstvo lahko izvajalo tudi ob opori na Slovensko združenje korporativne varnosti. Slednje bo za ministrstvo dobrodošel sogovornik pri skrbi za izmenjavo dobrih praks in izkušenj ne samo na področju obvladovanja tveganj za delovanje kritične infrastrukture, ampak tudi na področju zaščite kritične infrastrukture nasploh, torej od sistemskih do bolj operativnih ukrepov za zagotavljanje njenega neprekinjenega delovanja. Ministrstvo si bo tudi v prihodnje prizadevalo za krepitev partnerskega odnosa z združenjem, premislek v smeri formalnega vstopa v združenje pa je v pristojnosti vodstva ministrstva. ■

Opomba: avtor fotografij je Bruno Toič.



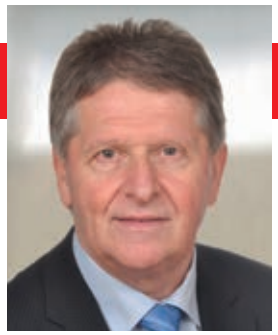
spica

Pripravljeni na digitalno transformacijo?



Obiščite www.spica.si in preglejte ponudbo
sodobne kontrole pristopa in registracije delovnega časa.

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



ZANESLJIVOST ZAPOSLENEGA IN DELOVANJE KRITIČNE INFRASTRUKTURE

Vpliv zaposlenega na delovanje kritične infrastrukture v sodobni državi je eden izmed najbolj nezanesljivih in nepredvidljivih dejavnikov, zato pomeni zanjo stalno nevarnost, ki je ne smemo podcenjevati. Postavlja se vprašanje, koliko si prizadevati za še večji tehnološki napredek, da bi bile tehnološke in fizične sestavine kritične infrastrukture varnejše, po drugi strani pa, kako obravnavati zaposlenega pri upravljanju teh kompleksnih sistemov, saj ta postaja vse pomembnejši referent za njeno zanesljivo delovanje.

Uvod

Obravnavanje zanesljivosti zaposlenega na delovanje kritične infrastrukture ni novo, v zadnjem času pa se je zaradi odmevnih škodnih dogodkov, groženj in terorističnih napadov za to področje močno povečalo. Ob predpostavki, da razpolagamo s tehnološko dovršeno kritično infrastrukturo in da lahko na učinke iz zunanjega okolja vplivamo le delno, je zaposleni eden najpomembnejših dejavnikov tudi pri zagotavljanju neprekinjenosti njenega delovanja. Če se je ta v preteklosti nanašala pretežno na tehnične rešitve, se je danes treba osredotočiti tudi na družbeno socialne in korporativno varnostne vidike.

Kritična infrastruktura je dosegla točko, ko bo izboljšano varnost mogoče doseči le na podlagi boljšega razumevanja tveganj in možnosti za nezanesljivost zaposlenega. V okviru verjetnostnih varnostnih analiz se ugotavlja, kateri scenariji groženj kritične infrastrukture se lahko zgodijo, kako verjetno je, da se zgodijo, kako hude so lahko njihove posledice in kakšna je pri tem zanesljivost zaposlenega.

Ob predpostavki, da razpolagamo s tehnološko dovršeno kritično infrastrukturo in da lahko na učinke iz zunanjega okolja vplivamo le delno, je zaposleni eden najpomembnejših dejavnikov tudi pri zagotavljanju neprekinjenosti njenega delovanja.

Zanesljivost zaposlenega

Pregled številnih opredelitev kritične infrastrukture po državah kaže, da večina držav posebej ne opredeljuje zanesljivosti zaposlenega, kot bistvenega pogoja za neprekinjeno delovanje kritične infrastrukture. Pomembnost njene zaščite, preglednost obravnave in sistematičen pristop na tem področju se kaže zlasti v varnostni politiki ZDA. Sprejet je bil Nacionalni načrt zaščite infrastrukture (NIPP, 2013), ki predstavlja celostni izbor programov, ukrepov in dejavnosti, ki potekajo med njenimi različnimi sektorji. Analiza tveganja se nanaša na fizične, računalniške in človeške elemente. Posebna pozornost je namenjena pretoku informacij in usposabljanju udeležencev na vseh ravneh delovanja.

V vsakem sistemu, ki je podvržen entropiji in homeostazi, je prednostna naloga sistemskega inženiringa določiti zahteve glede zanesljivosti in razpoložljivosti. Zanesljivost je sposobnost kritične infrastrukture, da ohrani svoje delovne parametre. Ti se nanašajo na zaupanje v sposobnost in zanesljivost kritične infrastrukture, da opravi kakovostno storitev na določenem območju in v določenem času. Pojem zanesljivost kritične infrastrukture lahko obravnavamo s treh povezanih vidikov, in sicer lastnosti, ogrožanja in povečanja zanesljivosti (kazalniki so prikazani na sliki 1). Lastnosti se nanašajo na razpoložljivost, gotovost, varnost, zaupnost, neokr-

*avtor je član Slovenskega združenja korporativne varnosti

njenost in vzdržljivost. Pri ogrožanju je lahko kritična infrastruktura izpostavljena napakam v poslovnih procesih, kršitvam, pomotam in/ali malomarnosti ter pohlepu zaposlenega. Zanesljivost kritične infrastrukture je mogoče zagotavljati s preprečevanjem napak, povečanjem odpornosti na napake, z odstranjevanjem odkritih napak in predvidevanjem pomanjkljivosti pri delovanju (Avizienis idr., 2001).

ZANESLJIVOST		
Lastnosti:	**Ogrožanja:**	**Povečanje zanesljivosti:**
Razpoložljivost	Napake	Preprečevanje napak
Gotovost	Kršitve	Povečanje odpornosti na napake
Varnost	Pomote	Odstranjevanje odkritih napak
Zaupnost	Malomarnost	Predvidevanje pomanjkljivosti
Neokrnjenost	Pohlep	
Vzdržljivost		

Slika 1: Kazalniki zanesljivosti (prirejeno po Avizienis idr., 2001)

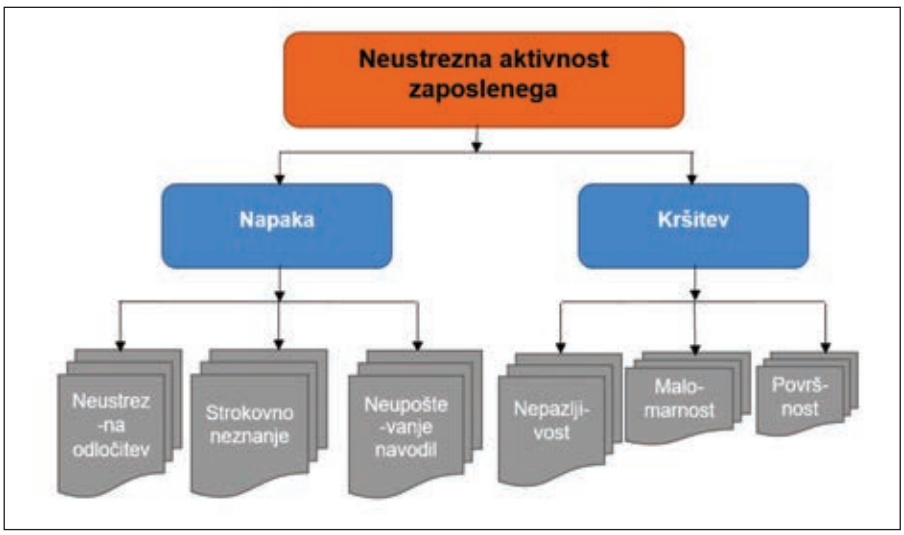
Na zaposlenega vpliva več dejavnikov, kot na primer, družbeni, socialni, okoljski, fiziološki, organizacijski, fizični, varnostni ipd. Osnovna domneva sistemskega pristopa je, da je zaposleni zmotljiv in napaka se pojavlja kot posledica in ne kot vzrok. Protiukrepi temeljijo na domnevi, da, če ne moremo spreminjati stanja zaposlenega, lahko pa spremenimo razmere (poslovno okolje), v katerem ta opravlja poslovne procese. Menim, da je kritična infrastruktura s tehnološkega vidika varna, zaščititi pa jo je treba pred nezanesljivim zaposlenim.

Napaka zaposlenega je bila navedena kot glavni vzrok ali pomemben dejavnik pri prekinitvi delovanja kritične infrastrukture, na primer v jedrski industriji (nesreče v jedrskih centralah Three Mile Island leta 1979, v Černobilu leta 1986 in Fukušimi-Daiči leta 2011), v letalstvu (padec letala Air France 447 sredi Atlantskega oceana leta 2009, padec letala v Franciji zaradi samomora kopilota leta 2014), pri raziskovanju vesolja (nesreči vesoljskih plovil Challenger,1986 in Shuttle Columbia, 2003), medicini (z raziskavo Inštituta za medicino ZDA, 2000, so ugotovili, da je bilo zaradi zdravniških napak od 44.000 do 100.000 naključnih smrti vsako leto in približno 1.000.000 naključnih poškodb), kemiji (kemični nesreči v Bophalu leta 1984 in Exxonu leta 1989), pri nafti (izliv nafte v Mehiškem zalivu leta 2010), v prometu (železniški nesreči v Nemčiji in Italiji leta 2016), energetiki (incident v TEŠ 6 v Sloveniji leta 2016) in informacijski tehnologiji (IBM, 2014, meni, da 95 odstotkov vseh napak povzroči zaposleni).



Napaka zaposlenega

Dekker (2005) je opozoril, da je pojem napaka zaposlenega zavajajoč. Stari pogled na napako, izhaja iz predpostavke, da je zaposleni nezanesljiv, njegova napaka pa lahko povzroči neobičajne razmere in škodni dogodek. Nov pogled obravnava napako kot učinek ali simptom globljih težav, napaka pa je sistematično povezana z delovnimi orodji, poslovnimi procesi, delovnim okoljem ipd.



Slika 2: Mogoče posameznikove neustrezne dejavnosti (lastni vir)

Na sliki 2 so predstavljene nekatere posameznikove neustrezne dejavnosti, ki lahko povzročijo neobičajne razmere. Neustrezne dejavnosti lahko delimo na namerne ali nenamerne oziroma naključne, ki se zgodijo zaradi napak ob neustrezni odločitvi, strokovnem neznanju, neupoštevanju navodil ali zaradi napačne zaznave, nepazljivosti, malomarnosti ali površnosti.

Raziskave zanesljivosti zaposlenega

Raziskave zanesljivosti zaposlenega so v tuji strokovni javnosti že dalj časa znana orodja za napovedovanje njegovih zmogljivosti. Uporabljajo se za analizo, kje lahko v kritični infrastrukturi nastanejo neobičajne razmere kot posledica nezanesljivosti zaposlenega. Pri proučevanju ogrožanja in ranljivosti gre torej za razumevanje, kaj, zakaj, kako in kdaj lahko nastanejo neobičajne razmere. Ta pristop spodbuja analitično razmišljanje, ki temelji na analizah, simulacijah in dobri praksi, žal pa tudi na analizah po škodnem dogodku. Analiza različnih metod raziskovanja zanesljivosti se do zdaj nanaša na kar 39 pristopov. Raziskava zanesljivosti zaposlenega je pogosto sestavljena iz treh ločenih faz (Boring, 2009):



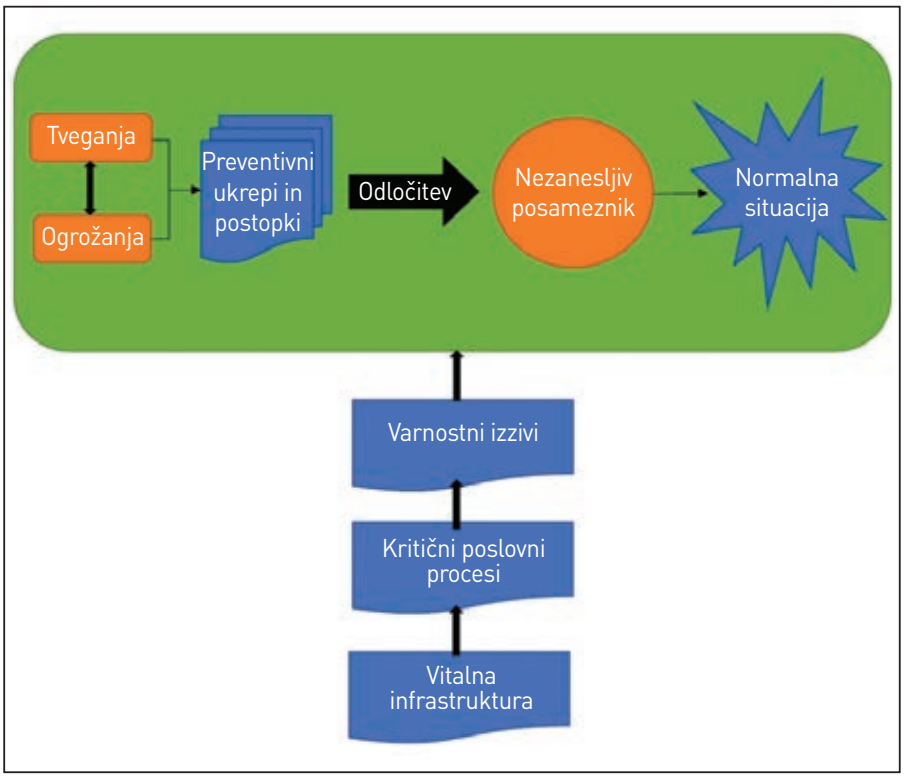
- modeliranje in opredelitev mogočih napak zaposlenega. Ta faza navadno obsega različne mogoče scenarije ogrožanja kritične infrastrukture zaradi napake. V navedeni dejavnosti ni splošno sprejetega standarda, kar lahko vodi do različnih pristopov;
- identifikacija mogočih ogrožanj neprekinjenega poslovanja kritične infrastrukture. Pristopi in metode raziskave zanesljivosti zaposlenega so zelo različni. V zadnjem času so vzpostavljeni standardi dobre prakse;
- količinska analiza napak, pri čemer je verjetnost napake tudi izračunana. Vsaka metoda raziskovanja zanesljivosti ima nekoliko drugačen pristop h kvantifikaciji, vključno s strokovno oceno, uporabo multiplikatorjev in simulacij. Količinsko se določa verjetnost za nastanek neobičajnih razmer. Napaka verjetnosti od enega primera na 100.000 dogodkov pomeni visoko zanesljivost sistema, srednje vrednosti pa se gibljejo od približno enega primera na 1.000 do enega primera na 100 dogodkov. Sistem pod temi vrednostmi je nezanesljiv.

Okvir modela zanesljivosti zaposlenega na delovanje kritične infrastrukture

Obravnavanje zanesljivosti zaposlenega na delovanje kritične infrastrukture zahteva interdisciplinarni pristop, saj so za obravnavanje tega vprašanja potrebni tako tehnično, sociološko, družboslovno, psihološko znanje in poznavanje korporativne varnosti oziroma smiselno upoštevanje dobre prakse.

Na sliki 3 je predstavljena možnost nastanka neobičajnih razmer v kritični infrastrukturi. Poudarek je na kritičnih poslovnih procesih, varnostnih izzivih, ogrožanju in tveganju ter preventivnih ukrepih in postopkih. Pred ugotavljanjem tveganj je treba analizirati kritičnosti poslovnih procesov, in sicer tako, da se upošteva njihov najslabši mogoč scenarij. Ta metodološki okvir tveganj

zagotavlja, da bodo prepoznani vsi pomembni viri negotovosti, določeni vzroki za tveganja in mogoče posledice tveganj.



Slika 3: Okvir modela zanesljivosti zaposlenega na delovanje kritične infrastrukture (lastni vir)

Posebna značilnost neobičajnih razmer je njihova sorazmerna nepredvidljivost, bolj ali manj verjetnost, ki pa ne dopušča stalne pripravljenosti in pozornosti zaposlenega. Menim, da zaposleni o tem razmišlja kot o negotovem dogodku nizke verjetnostne narave, kar vpliva na njegovo delovanje in posledično na rutino poslovanja.

Zaključek

Napaka ali malomarnost zaposlenega je univerzalna in neizogibna, kar pomembno vpliva na zanesljivost delovanja kritične infrastrukture. Lahko zmanjšamo verjetnost napake, vendar pa se je popolnoma ne more odpraviti. Zavedati se moramo, da je težko spremeniti osebnosti in stanje zaposlenega, lahko pa spremenimo pogoje, v katerih dela. Uspešno upravljanje tveganj zaposlenih mora preprečiti vrsto njihovih »neprimernih« aktivnosti, bodisi naključnih ali zlonamernih.

Med bolj uporabljenimi metodami za analizo zanesljivosti zaposlenega je tehnika za napovedovanje človeške napake,



ki je povezana s programom za vrednotenje nesreč. Različne metode po posameznih sektorjih kritične infrastrukture v zadnjem času postajajo vse bolj univerzalne.

Menim, da je za zanesljivost zaposlenega v neobičajnih razmerah pomembna ustrezna konstruktivna strategija spoprijemanja z ogrožanjem in tveganji. Uspešnost ali neuspešnost spoprijemanja pa je tesno povezana z njegovimi osebnostnimi lastnostmi (zlasti osebna čvrstost), kompetentnostjo, zaznavo ogrožanja in odzivom. Ta se nanaša na realno oceno in zavestno razčlenjevanje neobičajnih razmer, zaupanjem v svoje sposobnosti in v preventivne dejavnosti organizacije ter državnih organov. Ob tem je pomemben aktiven odnos do razmer, prilagodljivo iskanje rešitev, konstruktivno sodelovanje z drugimi (namesto pasivnega pričakovanja pomoči) ter sprejemanje in prenašanje čustvene obremenitve (namesto neorganiziranosti in panike).

Obravnavanje zanesljivosti zaposlenega na delovanje kritične infrastrukture zahteva interdisciplinarni pristop, saj so za obravnavanje tega vprašanja potrebni tako tehnično, sociološko, družboslovno, psihološko znanje in poznavanje korporativne varnosti oziroma smiselno upoštevanje dobre prakse.

Viri

- Avizienis, A., Laprie, J. C. in Randell, B., 2001. Fundamental Concepts of Dependability (Research Report No 1145), LAAS–CNR.
- Boring, R. L., 2009. Human reliability analysis in cognitive engineering. Frontiers of Engineering: Reports on Leading–Edge Engineering from the 2008 Symposium (103–110). Washington, DC: National Academy of Engineering.
- Dekker, S. W. A., 2005. Ten Questions About Human Error: a new view of human factors and systems safety, Lawrence Erlbaum Associates.
- NIPP, 2013. Partnering for Critical Infrastructure Security and Resilience, https://www.dhs.gov/, 12.1.2017. ■





POSVET

NADZOR NA DELOVNEM MESTU

26. september 2018, Ljubljana

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

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

www.planetgv.si

www.ics-institut.si

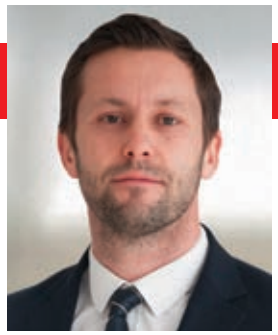
ORGANIZATORJA POSVETA

PLANET GV

ICS
Institut za korporativne varnostne študije

BREZPLAČNA ŠTEVILKA
• 080 33 44

Avtor: Martin Koželj / Vodja varnosti in področja integritete NZS*



VAROVANJE PRVENSTVA UEFA FUTSAL EURO 2018

Veliki športni dogodki nudijo poleg svojih ekonomskih in socialno - kulturnih priložnosti, ki ugodno vplivajo in dvigujejo perspektive mestnih gospodarskih entitet oz. celo držav, tudi povečano varnostno tveganje lokalnih, nacionalnih, lahko tudi internacionalnih dimenzij.

V nadaljevanju je predstavljena organizacija UEFA evropskega prvenstva v futsalu – UEFA Futsal EURO 2018, ki jo je Nogometna Zveza Slovenije (v nadaljevanju NZS) organizirala med 30. januarjem in 10. februarjem 2018 v Ljubljani in je v dvorano Stožice med prvenstvom privabila preko 100.000 obiskovalcev.

Varnostna tveganja povezana z velikimi športnimi dogodki imajo v povezavi z zgodovino tudi svojo temnejšo plat. Na to nas opominjajo teroristični napad na Izraelsko moštvo na olimpijskih igrah leta 1972 v Münchnu, teroristični napad 9/11 in vse, kar je bilo v zadnjih letih povezano z njim. V povezavi z nogometom je potrebno izpostaviti dva bombna napada, ki sta se zgodila v preteklih letih in smo ju preučili med pripravami na naš dogodek. Prvi bombni napad se je zgodil leta 2016 v Istanbulu v Turčiji, med katerim je bilo ubitih 38 ljudi in preko 160 ranjenih. Drugi bombni napad je bil uperjen na avtobus Borussia Dortmund v letu 2017. Za Slovenijo lahko trdimo, da je varna država, in je verjetnost tovrstnih napadov izjemno majhna. Tudi ocena Global »peace indexa« Slovenijo postavlja na 7. mesto. Stabilnost v našem okolju je rezultat mnogih faktorjev, predvsem geografske umeščenosti ter urejenosti in učinkovitosti našega varnostnega sistema. Kljub vsemu je stopnja varnostnega tveganja na nivoju Evrope visoka in vsaj v delu terorističnih potencialov Slovenija nikakor ni nek osamljen otok. Teroristični tokovi, in z njimi povezana tveganja, so v globaliziranem svetu izjemno dinamični in adaptivni, kar pomeni, da so ob povišani stopnji izpostavljenosti, ki je prisotna v Evropi, ves čas realna grožnja. UEFA, kot mednarodno visoko cenjena in hkrati s tem izpostavljena globalna znamka, je lahko potencialna tarča možnih varnostnih tveganj in v skladu s tem je bilo potrebno tudi delovati. Eden izmed ukrepov, ki jih je visoko strokovno izvajala policija, je bil vsakodnevni protibombni pregled celotne dvorane Stožice. Nič ni bilo prepuščeno naključju.

NZS je leta 2016 pridobila zaupanje UEFA za organizacijo omenjenega prvenstva. Takoj po izkazanem zaupanju za organizacijo UEFA Futsal EURO se je pričelo z izvajanjem vrste aktivnosti, ki so se neposredno navezovale na vse segmente organizacije. Zagotavljanje varnosti je bilo eno izmed njih. Pri tem je potrebno poudariti, da se segment varnosti neposredno deli na tri vzporedna integrirana področja. Tristebrni sistem sestoji iz področij varnosti (Safety), varovanja (Security) in storitev (Services). Na lokalnem področju se integriran pristop odraža kot vzajemno sodelovanje lokalnih oblasti, NZS in policije. Cilj je zagotavljanje varnega okolja, v katerem lahko obiskovalci uživajo ob gledanju nogometnega spektakla kot celostnega dogodka v vsej njegovi prvinskosti in brez prisotnosti ali izpostavljenosti tveganjem in motečim elementom. Stremimo k temu, da se nogomet odvija v okolju, v katerem so prisotni visoki standardi - tako infrastrukturnih pogojev kot na drugi strani kombinacije primernega upravljanja varnostnega managementa. Varnost kot temeljni postulat je determinirana z ukrepi, ki omogočajo varno izvedbo prireditve. Ustrezna infrastruktura, efektivni management upravljanja z obiskovalci, vidne označbe, požarno varovanje, proste evakuacijske poti, delujoči elektronski in mehanski sistemi (požarni sistemi, sistemi beleženja vstopa ...), proste vstopne in izstopne poti, nedrseča podlaga (čas obilnega sneženja in nizkih temperatur), ter še mnogo tovrstnih področij. Varovanje, ki predstavlja drugi steber, je neposredno povezano s samim segmentom opravljanja varnostnih storitev gospodarskih subjektov, je integriran in ves čas

Varnostna tveganja povezana z velikimi športnimi dogodki imajo v povezavi z zgodovino tudi svojo temnejšo plat.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

delujoč sistem. Pri tem je pomembna primerna izpostavljenost in zaznavnost ter aktualno vrednotenje tveganj in politika takojšnjega odziva, ki temelji na proaktivnem delovanju. Samoiniciativni pristop in dobro vodenje, ki sta v jedru podprta s strokovnostjo, se kažeta v res dobri komunikaciji in koordinaciji vseh udeleženih varnostnih subjektov. Za zagotavljanje nemotenega poteka prireditve je poleg dobrega in vestnega dela posebno pozornost potrebno nameniti tudi ukrepom, kot so opozarjanje in v skrajnih primerih tudi morebitna zavrnitev ali izključitev motečih obiskovalcev ali prepovedanih predmetov. Kvaliteta, strokovnost, doslednost, zavzetost in še mnogo drugih elementov, ki se odražajo v vestnem, zakonitem in strokovnem delovanju, so aksiom dobrega zagotavljanja varnosti. Zadnji del tripartitnega dela je področje storitev. Tovrstno področje je najbolj izpostavljeno in vidno, saj obiskovalci v večini prepoznajo in neposredno občutijo le tovrstni segment. Pri tem je pomembna dobra in vljudna komunikacija varnostnega osebja. Ključno za vse tovrstne dogodke je uravnotežen pristop, ki v obzir poveže vse tri elemente. V kolikor tovrstno delovanje ni vzajemno uglašeno in upravljano, se rezultat lahko kaže tudi v potencialnih resnih posledicah in različnih dojemanjih javnosti. Psihologija množice je prav gotovo generator določenih aktivnosti in je kot taka zelo pomemben del predvidevanja, vrednotenja in delovanja.

Priprava na prihajajoče UEFA Futsal EURO je bila sistematična in postopna. Razdeljena je bila na več faz. V prvi fazi je bilo potrebno teoretično in plansko pripraviti načrte in različne naloge in tveganja, ki bi lahko bila prisotna. V samem začetku je bilo potrebno pripraviti oceno tveganja prihajajočega prvenstva. Ocena tveganja je obsegala vrsto elementov, med katerimi lahko izpostavimo mednarodno strukturo obiskovalcev, potencialno število obiskovalcev, prisotnost organiziranih navijaških skupin, infrastrukturo športnega objekta Stožice, objektov in okolice, kjer so bila nastanjena moštva, prisotnost uradnih oseb in visokih gostov, transporta vseh deležnikov, vitalnih točk v varovanem in nevarovanem delu objekta, vpliv vremenskih razmer, odpoved posameznih elementov (induktivna in deduktivna metoda), potencialne možnosti terorističnega napada in izrabe dogodka kot političnega, verskega ali drugega dogodka.

Ocena stopnje tveganja je bila izdelana postopoma z upoštevano vrsto potencialnih možnosti. Pri sami oceni tveganja je sodelovala tudi policija, s katero NZS izredno dobro sodeluje. Na koncu izdelave ocene tveganja je bilo ugotovljeno, da je le-ta za prihajajoče prvenstvo nizka. V skladu s tem je bilo potrebno izdelati varnosti koncept oziroma načrt. Koncept je sestavljen iz večjega števila vsebin kot so: varnostno organizacijska struktura, akreditacijski sistem, varovanje namestitvenih kapacitet, policijsko spremstvo moštev, varovanje objektov za trening, ki so bili na sekundarnih lokacijah, transport igralcev, sodnikov in uradnih oseb, glavni varnostni ukrepi, preventivni varnostni ukrepi, proti-bombni pregled dvorane, tiskanje in prodaja vstopnic ter potencialna prepoznava ponarejenih vstopnic, varovanje vstopnih in izstopnih točk, vnos nevarnih in prepovedanih predmetov na prireditev, hišni red, varnostne službe in njihovo delovanje ter še nekatera druga področja. Poleg koncepta varovanja je bil izdelan tudi podrobnejši koncept, v katerem smo eksplicitno definirali na-





mestitvene prostore, uradne dogodke in dvorane za trening. Prav tako je bil izdelan natančen mikro lokacijski načrt položaja posameznih varnostnikov (na posamezni tekmi jih je bilo preko 160). Za dobro linijo vodenja in upravljanja je bil vzpostavljen glavni varnostni štab, ki je skrbel za načrtovanje, organiziranje, implementacijo, koordinacijo in kontrolo vseh varnostnih elementov na evropskem prvenstvu. Prav tako je bil odgovoren za zbiranje, obdelavo, vrednotenje in distribucijo vseh podatkov in informacij, ki so bile pomembne za varno izvedbo prireditve. Poleg glavnega varnostnega štaba je bil na posamezni dan sestavljen tudi varnostni operativni center, ki je skrbel za operativno organizacijo, vodenje in nadzor.

Najpomembnejši segment nogometa so prav gotovo gledalci. Nogomet se igra zaradi njih in v skladu s tem je temu posvečena posebna pozornost. Na UEFA Futsal EURO so bila prisotna moštva iz držav Slovenije, Srbije, Rusije, Poljske, Portugalske, Romunije, Španije, Francije, Kazahstana, Ukrajine, Italije in Azerbajdžana. Pluralnost evropskih kultur se sociološko odraža tudi v raznolikosti in raznovrstnosti dojemanja in delovanja. Priprava hišnega reda in pravil vedenja je bila naslednja aktivnost, ki je definirala prepoved vnosa nevarnih predmetov in pravila obnašanja na prireditvi. Vzpostavitev hišnega reda temelji na oceni tveganja in s tem potencialnih morda tudi hipotetičnih tveganjih, ki lahko vplivajo na zagotavljanje varnosti na posameznem dogodku. Ravno zaradi izpostavljenosti dogodka ter različnosti nacionalnih identitet je bil v hišnem redu prepovedan vnos vrste predmetov, kot so na primer nezložljivi dežniki s konico, večje torbe od 25 x 25 cm, kape, ki omogočajo zakritje obraza, vnos hrane in tekočin (možnost potencialnega odvrženega predmeta) ...

> Tekme so bile odigrane v vznemirljivem športnem duhu in z vedno prisotnim »fair-play«-om. Izvedba tovrstnega tekmovanja je bil največji projekt NZS do sedaj in je predstavljal organizacijsko usklajenost celotne ekipe zaposlenih, ki so pokazali izredno predanost projektu in NZS kot organizaciji.

Predmete, s katerimi ni bilo dovoljeno vstopiti, je bilo možno začasno odložiti v prostor za oddajo predmetov, v katerem je varnostnik v skladu s svojimi pooblastili pregledal vsak oddan predmet, ga nato do konca prireditve shranil v varovanem prostoru ter zanj izdal potrdilo za prevzem.

Neuradna generalka pred prihajajočim UEFA Futsal EURO je bila prijateljska tekma med Slovenijo in Portugalsko v futsalu, ki se je prav tako kot kasneje tekmovanje, odvila v Stožicah. Omenjena tekma je bila dobra popotnica pred prihajajočim prvenstvom, saj je pokazala določena tveganja in izzive na nekaterih področjih. V skladu s tem smo na NZS k temu pristopili sistematično in metodično ter predvsem z jasno vizijo, kaj želimo doseči. Določili smo cilje, strategije in vizijo, vse v želji po čim boljšem rezultatu, in to je bilo organizirati najboljše prvenstvo doslej. V želji po čim boljši implementaciji vseh elementov smo s predstavniki varnostnih služb izvedli



vrsto sestankov in usklajevanj. Podrobno poznavanje dvorane je bilo ključno za dobro in efektivno delovanje. Številna usklajevanja in terensko delo je imelo rezultat v natančni določitvi vseh nalog, ki so jih opravljali posamezni varnostniki na svojih delovnih točkah. Zadnji teden pred UEFA Futsal EURO je bilo izvedeno tudi izobraževanje za sodelujoče varnostnike, ki so med prvenstvom skrbeli za varnost. Usposabljanja se je udeležila večina varnostnikov (150) iz vseh varnostnih podjetij, ki so sodelovala na prvenstvu. Predstavniki NZS so podrobno predstavili časovnico prvenstva, vsa delovanja in ravnanja, želeni videz in vedenje, komunikacijo z obiskovalci, delovanje v primeru posebnih razmer (evakuacija) in kritičnih situacij (sumljiv nenadzorovan predmet, požar ...), zaščiti igralcev in igralnega prostora, vnosa transparentov s prepovedanimi simboli, potencialna pričakovanja obiskovalcev, hišni red, delovanja v primeru izgube predmetov ali oseb (med prvenstvom se je izgubil otrok, vendar ima zgodba srečen konec, saj je otrok ob pomoči varnostnikov kmalu našel svojega očeta). Želeno in pričakovano vedenje je bilo, da je bil varnostnik profesionalen, ustrežljiv in vljuden, točen in zanesljiv, osredotočen na dolžnosti, strikten ter se je poslu-ževal osnovnega bontona za delovanje v družbi. Varnostniki na svojih položajih niso smeli jesti, piti, kaditi ali uporabljati mobilne telefone. Na koncu usposabljanja so predstavniki NZS predali varnostnikom v reševanje tudi test, ki je povzel vsa področja, ki so bila predstavljena med izobraževanjem. Vsi varnostniki so test rešili uspešno. Ob začetku prvenstva je posamezni varnostnik dobil tudi knjižico z vsemi nujnimi informacijami, ki so nudila odgovore na najpogostejša vprašanja (parkirne akreditacije, urnik, karte in podobno). Omenjeno izobraževanje se je izkazalo kot zelo primerno, saj je naročnik, v tem primeru NZS, podal natančna navodila in zahteve o tem, kako si želi, da je segment varovanja izvajan v vsem obsegu. Varnostne službe so seveda omenjeno delo opravile zelo strokovno in z visoko stopnjo zavzetosti. Tovrstno delo varnostnega protagonista je ustvarilo varno okolje, ki je imelo za posledico prvenstvo brez enega samega incidenta. Vsi sodelujoči v UEFA Futsal EURO 2018 so imeli le en sam najpomembnejši cilj, in to je, ustvariti varno ter prijazno okolje za vse udeležence. Najbolj zahtevne in obsežne so bile tekme, na katerih je igrala Slovenija, ter zadnji, deseti dan prvenstva, ko sta bili na vrsti tekma za tretje mesto in finale. Na posamezni tekmovalni dan sta bili izvedeni dve tekmi, in sicer ena ob 18. uri in druga ob 20.45 uri. Poseben izziv je predstavljalo tudi beleženje vstopa in izstopa obiskovalcev s pomočjo statičnih in prenosnih elektronskih čitalcev, saj je bilo tokrat izvedeno prvič. Običajna praksa je, da se beleži le vstop obiskovalca. Ker sta bili dve tekmi ena za drugo in je bil vstop mogoč le z eno karto, je bilo tudi zaradi natančnega pregleda nad številom obiskovalcev izvajana kontrola vstopa in izstopa.

Eden najpomembnejših segmentov delovanja posameznega prvenstva je bila tudi vzpostavitev akreditacijskega sistema. Bistvo implementacije je bilo definiranje con dostopa za posamezne deležnike. Najpomembnejše je bilo prav gotovo igrišče, na katerega ima na takšnih prireditvah z razlogom dostop omejeno število ljudi. Naslednja so bila tekmovalno območje, delovno območje, območje za gledalce, območje za delo medijev, VIP območje in območje za pogostitev in TV območje. Akreditacijski model, ki je definiral osebe in območja, je predstavljal osrčje celotne organizacijske strukture posamezne tekme. Velika fluktuacija ljudi v času 10 tekmovalnih dni je morala biti sistematično upravljana. Pravilno vrednotenje posameznika v okviru njegovih delovnih nalog je bilo pomembno za določitev in dodeljevanje akreditacijskih dostopov. Pri tem je bila izredno pomembna pravilna in predvsem natančna določitev posameznega območja. V okviru tega so morali varnostniki striktno in dosledno izvajati svoje naloge.

Prvenstvo so obiskali tudi številni visoki gostje, med drugim tudi predsednik UEFA Aleksander Čeferin. Obsežnost projekta so nakazovali tudi vsi deležniki. Poleg obiskovalcev so bili tu prisotni tudi lokalna skupnost, VIP gostje, sponzorji, moštva, uradniki UEFA in delegati, mediji, osebje in dobavitelji, prostovoljci, reševalne službe, policija, predstavniki dvorane in predstavniki NZS. Ravno zaradi vseh prisotnih je bilo poznavanje dvorane in celotnega sistema zelo pomembno, saj je omogočalo varnostnikom suverenost v varnostnih elementih in na področju usmerjanja in komunikacije z obiskovalci.

Zaključeno UEFA Futsal EURO 2018 je bilo prvenstvo, ki ni samo doseglo, temveč tudi preseglo številna pričakovanja. 101.934 obiskovalcev v 10 tekmovalnih dneh je doživelo izjemen spektakel s številčnim obiskom in čudovito atmosfero. Tekme so bile odigrane v vznemirljivem športnem duhu in z vedno prisotnim »fair-play«-om. Izvedba tovrstnega tekmovanja je bil največji projekt NZS do sedaj in je predstavljal organizacijsko usklajenost celotne ekipe zaposlenih, ki so pokazali izredno predanost projektu in NZS kot organizaciji. Zadovoljni obrazi obiskovalcev, odlična promocija Ljubljane kot mesta gostiteljice prvenstva in na koncu Slovenije, je najboljša promocija, ki bo prav gotovo pustila neizbrisan pečat. ■

Opomba: fotografije so iz arhiva NZS in UEFA.

INFORMACIJSKA VARNOST

V podjetju Unistar PRO pod blagovno znamko PRO.ASTEC združujemo rešitve in storitve iz področja informacijske varnosti in skladnosti. Že od leta 2007 vam zagotavljamo izvajanje storitev skladnosti z zahtevami standarda ISO/IEC 27001 za varovanje informacij. S svojimi izkušnjami, znanjem in partnerskimi vzpostavljamo procesne in logično – tehnične informacijske varnostne rešitve.

Naše kompetence delimo na področji vzpostavljanja in upravljanja varnega informacijskega okolja:

- Svetovalne aktivnosti na področju sistemov upravljanja varovanja informacij in neprekinjenega poslovanja.
- Rešitve in storitve za upravljanje varovanja informacij, neprekinjenosti in skladnosti poslovanja.
- Storitve s področja Splošne uredbe o varstvu osebnih podatkov (ang. GDPR).
- Sistemi za upravljanje varnostnih dogodkov in varnostnih tveganj.
- Napredne varnostne rešitve podatkovnih centrov.
- Napredne varnostne rešitve roba omrežja.
- Napredne varnostne rešitve dostopov do informacijskih virov.
- Napredne varnostne rešitve končnih uporabnikov in naprav.

- 24/7/365 nadzor in odziv na informacijske varnostne incidente.
- Oddaljena asistenca ali asistenca na lokaciji z dogovorjenim odzivnim časom.
- Zagotovljena razpoložljivost strokovnjakov iz področja informacijske varnosti.
- Preiskovanje in analiza informacijskih varnostnih incidentov.
- Prilagoditev varnostnih pravil in postopkov na nove poslovne modele in glede na novo zaznane grožnje ter s tem povezana tveganja.
- Potrjevanje ustreznega nivoja informacijske varnosti preko varnostnih, penetracijskih testiranj in pregledov.
- Gostovanje in upravljanje poslovnih in varnostnih sistemov.
- Usposabljanje in ozaveščanje uporabnikov o informacijski varnosti.

take a challenge
UNISTAR PRO
Challenge, Passion, Trust.

PRO.astec

Alterna Intertrade d.d. skupina www.unistarpro.si

Unistar LC d.o.o., Ljubljana | Litostrojska cesta 56 1000 ljubljana | Tel 01-4755 502 | Fax 01-4755 600 | info@unistarpro.si

www.posta.si

Za vsako zgodbo, **samo en naslov je pravi!**



KRAFT&WERK

ZANESLJIVO Z VAMI!

Ko za posel v oblaku ste pravi in vas na poti k uspehu nič ne ustavi. Ko potrebujete rezervni del ali partnerja, ki bo za vas vsak dan poskrbel. Če ste prepozni za banko ali želite v zbirko dodati novo znamko. Ko želite razveseliti z voščilom ali presenetiti z lepim darilom. **Za vsako zgodbo, samo en naslov je pravi!**

Pošta Slovenije
Zanesljivo z vami!

Avtor: Rok Novak / Reisswolf Slovenija*



GDPR-PRILOŽNOSTI IN IZZIVI NA PODROČJU ARHIVIRANJA IN UNIČEVANJA DOKUMENTACIJE

V življenjskem ciklu papirne dokumentacije pomemben delež predstavljata procesa arhiviranja in uničevanja papirne dokumentacije, do katerih so imela podjetja do sedaj praviloma precej mačehovski odnos. Nova uredba o varstvu osebnih podatkov (v nadaljnjem besedilu: GDPR) zahteva varno obdelavo osebnih podatkov v njihovem celotnem življenjskem ciklu, torej tudi v času arhiviranja in uničenja. Pri tem je še posebej pomembno poudariti dejstvo, da gre pri arhiviranju in uničevanju papirne dokumentacije prav tako za obdelavo osebnih podatkov, zato bo potrebno tema dvema procesoma v bodoče posvečati bistveno več pozornosti in tudi v teh procesih zagotoviti ustrezen nivo varnosti osebnih podatkov.

Po podatkih raziskave uslužbencev podjetja Senzing, ki so v raziskavo vključili 1.015 družb iz petih največjih evropskih držav, kar 60 odstotkov večjih podjetij, ki imajo več kot 250 zaposlenih še vedno ni pripravljenih na GDPR, 44 odstotkov jih skrbi, ali jim bo do 25.5.2018 uspelo urediti sezname osebnih podatkov, 12 odstotkov pa jih sploh ne ve, kje hranijo osebne podatke (vir: Finance, 31.1.2018).

Kakšno je stanje na področju arhiviranja dokumentacije z vidika GDPR

Pri nas imajo podjetja različno urejeno področje arhiviranja papirne dokumentacije. Do sedaj je veljalo splošno prepričanje, da je papirno dokumentacijo sicer potrebno hraniti, saj tako določa različna zakonodaja in predpisi, ni pa se v zadostni meri (ali pa sploh ne) poskrbelo za ustrezno (varno) hrambo dokumentacije.

Z vidika arhiviranja papirne dokumentacije je pomembno izpostaviti naslednjo problematiko:

- Podjetja nimajo izdelanih klasifikacijskih načrtov, ali pa so le-ti precej splošni;
- Označevanje dokumentacije, ki bi zagotovilo preglednost in sledljivost dokumentacije v fazi arhiviranja je pomanjkljivo in nesistemsko;
- Dokumentacija se ne hrani v ustreznih škatlah, ki zagotavljajo potrebno kakovost hrambe na dolgi rok;
- Prostori, ki se uporabljajo za hrambo dokumentacije niso klimatsko in lokacijsko primerni – so v kleteh, zakloniščih, kurilnicah in drugih neprimernih prostorih, kjer obstaja velika nevarnost pojava vlage, plesni, izlitja vode, poplave, požara in uničenja dokumentacije zaradi vdora raznih zajedavcev;
- Prostori v katerih se hrani dokumentacija (arhivski prostori) niso varovani po predpisih, ki urejajo varstvo dokumentarnega in arhivskega gradiva ter arhivov– praviloma ni nadzora vstopov in upravičenosti gibanja po prostorih;
- Dokumentacija ni ustrezno popisana in upravljana s programsko opremo, ki bi zagotavljala sledljivost in revizijsko sled upravljanja z dokumentacijo – sledljivost vnosov in iznosov dokumentacije, sledljivost rokov hrambe ipd.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

To je le nekaj ključnih ugotovitev, ki glede na zahteve GDPR predstavljajo resne kršitve varnosti. Pri tem je kljub vsemu potrebno poudariti, da obstaja kar nekaj ozaveščenih podjetij, ki imajo to področje zgledno urejeno, zato bodo ta podjetja potrebovala le manjše izboljšave v obstoječih rešitvah, ki jim bodo zagotavljale skladnost arhiviranja dokumentacije z GDPR.

Kakšno je stanje na področju uničevanja dokumentacije z vidika GDPR

Na področju uničevanja dokumentacije obstaja še večji prepad med zahtevami GDPR in dejanskim stanjem v praksi. Omenimo naj samo akcije zbiranja odpadnega papirja, ki nam omogočajo čiščenje prenatrpanih kletnih ali celo drugih poslovnih prostorov, kjer se hrani nakopičeni papir, med katerim se lahko nahaja tudi dokumentacija s poslovnimi in/ali osebnimi podatki. Ni bilo malo primerov, ko so otroci v vrtcih pisali in risali na papir, ki so ga starši prinesli iz svojih podjetij, na katerih so se znašli celo podatki o plačah zaposlenih ali kakšni drugi občutljivi poslovi podatki, ali pa primer kurjenja kresov, na katerih so med drugim sežigali tudi odvečno (odvrženo) dokumentacijo.

Če pogledamo na trg ponudnikov uničevanja dokumentacije lahko ugotovimo, da se z zbiranjem in uničevanjem dokumentacije ukvarjajo pretežno podjetja, katerih temeljna dejavnost je zbiranje in ločevanje odpadkov, uničevanje dokumentacije pa le kot postranska dejavnost. Redka so podjetja, ki se profesionalno ukvarjajo z varnim zbiranjem in uničevanjem dokumentacije skladno tudi z zahtevami GDPR.

> Zavedati se je potrebno, da GDPR zahteva varno obdelavo osebnih podatkov v njihovem celotnem življenjskem ciklu, torej tudi v procesu arhiviranja in uničenja, v okviru katerih se prav tako izvaja obdelava osebnih podatkov.

Na področju uničevanja dokumentacije je potrebno izpostaviti naslednjo problematiko:

- Dokumentacija se zbira na hodnikih in drugih skupnih in prosto dostopnih prostorih;
- Zbiralniki dokumentacije niso ustrezni – vreče, kartonaste škatle in plastični zabojniki, ki omogočajo nepooblaščen dostop do dokumentacije;
- Prevozi dokumentacije na uničenje se izvajajo z neustreznimi vozili, ki ne zagotavljajo ustrezne varnosti prevoza dokumentacije;





- Prostori za hrambo dokumentacije pred uničenjem niso varnostno ustrezni in omogočajo dostop nepooblaščenim osebam do dokumentacije;
- Uničenje dokumentacije ni ustrezno in skladno z zahtevami standardov.

Ugotavljamo torej, da navedene ugotovitve stanja na področju uničevanja dokumentacije kažejo na resne pomanjkljivosti, ki jih bo nujno potrebno odpraviti, da se zagotovi skladnost z zahtevami GDPR.

Rešitve za zagotovitev skladnosti arhiviranja osebnih podatkov z GDPR

Podjetje Reisswolf Slovenija zagotavlja uporabnikom celovito rešitev na področju arhiviranja dokumentacije. Celoten proces od prevzema dokumentacije do arhiviranja v lastnih arhivskih prostorih je skladen z zahtevami GDPR. Celo več, obstoječe rešitve zagotavljajo tudi forenzično sled upravljanja z arhivirano dokumentacijo, ki naj bi bila tudi ena od pomembnih zahtev novo nastajajočega Zakona o varstvu osebnih podatkov ZVOP-2.

Uničenje dokumentacije je zadnja faza v procesu obdelave osebnih podatkov, in je po pomembnosti enakovredna ostalim fazam obdelave osebnih podatkov, zato tudi ta terja resnost obravnave in ustreznost izvedbe, saj se le tako lahko tudi v tej fazi zagotovi skladnost z zahtevami GDPR.

Naj poudarim le nekaj ključnih rešitev:

- Izdelava celovitih klasifikacijskih načrtov;
- Ureditev skladnosti popisov dokumentacije s klasifikacijskim načrtom;
- Vnos popisov dokumentacije v RWAS programsko opremo;
- Varen transport dokumentacije iz prostorov naročnika v arhivske prostore Reisswolf;
- Varna hramba dokumentacije v namensko zgrajenih prostorih;
- Enostavno in učinkovito upravljanje z dokumentacijo s programsko opremo RWAS;
- Varnost, preglednost, sledljivost in forenzično sled upravljanja z dokumentacijo;
- Več nivojska dostopnost do arhivirane dokumentacije;
- Stalna 24 urna dostopnost do arhivirane dokumentacije preko RWAS programske opreme.

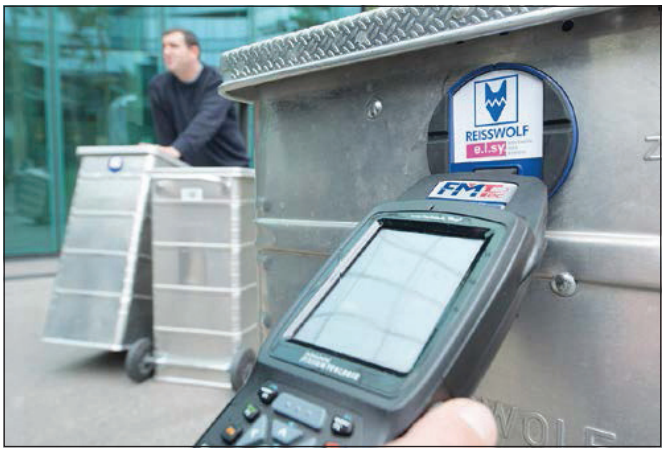
Pri vzpostavljanju varnega upravljanja z arhivirano dokumentacijo ne gre zanemariti tudi stroškovni vidik. Ob pravilnem pristopu ustvarjamo tudi ekonomsko dodano vrednost, ki se izkazuje skozi zakonitost, celovitost, varnost in učinkovitost upravljanja. Celovito in varno arhiviranje z dokumentacijo podjetjem povečuje učinkovitost upravljanja z dokumentacijo in posledično zmanjšuje stroške upravljanja z arhivirano dokumentacijo tudi za več kot 50 odstotkov.

Rešitve za zagotovitev skladnosti uničenja dokumentacije z osebnimi podatki z GDPR

Na področju uničevanja dokumentacije ima podjetje Reisswolf Slovenija razvit sistem zbiranja in uničevanja dokumentacije, ki tudi na tem področju zagotavlja skladnost uničevanja dokumentacije z zahtevami GDPR.

Naj poudarim le nekaj ključnih rešitev:

- Izdelavo celovite rešitve sistema uničevanja dokumentacije;
- Namestitev varnostnih ALU zabojnikov s sistemsko ključavnico, ki omogoča enostavno in varno odlaganje dokumentacije (lahko tudi celotnih registratorjev);
- Varnostni ALU zabojniki onemogočajo nepooblaščenim osebam dostop do vsebine zabojnika, tudi če se la ta nahaja na skupnih površinah podjetja;
- Namestitev ALU varnostnih zabojnikov z Elsy elektronsko ključavnico dostopno preko sistema kontrole pristopa;
- Varen in sledljiv transport dokumentacije iz prostorov naročnika do lokacije uničenja;
- Uničenje dokumentacije v varovanih prostorih, kjer je dostop omogočen le za to pooblaščenim osebam;
- Zagotavljanje skladnosti uničenja dokumentacije z varnostnimi standardi;
- Izdaja potrdila o varnem uničenju dokumentacije.



Rešitve Reisswolf na področju arhiviranja dokumentacije ob dejstvu, da zagotavljajo skladnost upravljanja arhivirane dokumentacije z GDPR, uporabnikom zagotavljajo tudi enostavnost uporabe in stroškovno učinkovitost, saj znižujejo stroške arhiviranja dokumentacije tudi za več kot 50 odstotkov.

Dejavnost uničevanja dokumentacije je ena od treh temeljnih dejavnosti podjetja Reisswolf Slovenija, povezanih s celovitim upravljanjem z dokumentacijo, kar je dodaten garant za visoko kakovost, strokovnost in zakonitost izvedbe ponujenih rešitev.

Sklepna misel

GDPR zagotovo prinaša nov veter v sisteme in procese upravljanja s podatki. Lahko celo rečemo, da GDPR v bistvu predstavlja »standard« za države EU in za ves svet. Gre torej za poenotenje filozofije, politike in upravljanja s podatki na vseh ravneh in področjih družbenega življenja in dela. Tako se bo marsikaj moralo spremeniti tudi v globalnih, regionalnih in lokalnih elektronskih in klasičnih komunikacijah ter v računalniški varnosti. Tako je GDPR vsestranski (zlasti pa varnostni) izziv tudi za menedžment in strokovnjake korporativne varnosti, ki bi se morali vključiti v obvladovanje ranljivosti, groženj in varnostnih tveganj pri upravljanju papirne dokumentacije. V tem kontekstu so vsekakor dobrodošle organizacijske, poslovne, varnostne, tehnične, stroškovne in druge rešitve arhiviranja in uničevanja papirne dokumentacije, ki jih je razvila skupina Reisswolf. ■

REISSWOLF®

Rešitve za upravljanje z digitalnimi dokumenti

Digitalna storitev



Rešitve za upravljanje s fizičnim arhivom

Fizična arhiva



Uničenje dokumentacije

Uničevanje dokumentacije



REISSWOLF® digital. service.
REISSWOLF® archive. service.
REISSWOLF® secret. service.

REISSWOLF d.o.o.
Pod gabri 15
1218 Komenda, Slovenija
T: +386 (0)1 5412266, **M:** +386(0)41 401650
E-mail: info@reisswolf.si, htpp//www.reisswolf.si

Avtor: mag. Luka Keršič / Zavarovalnica Triglav d.d.*

KIBERNETSKA TVEGANJA

Napredek že po definiciji predstavlja nekaj pozitivnega in v tem smislu priložnost, tudi za področje zavarovalništva. Toda po drugi strani nosi s seboj nekatere stranske učinke – nova tveganja, katerih potencialna nevarnost, škodna pogostost in sama škoda, nam še niso povsem znane.

Pozavarovatelji in zavarovatelji tako svoje pozornosti ne namenjajo le tveganjem, ki so na obzorju, temveč usmerjajo svoj pogled tudi čez obzorje. Nihče v (po)zavarovalni panogi si namreč ne želi, da bi spregledali nove, šele nastajajoče rizike, ki jih nosijo klimatske spremembe, demografski razvoj, množični spori (npr. class actions v ZDA), terorizem, nova tehnologija, nove kemikalije, staranje prebivalstva, kibernetska tveganja (ang. cyber risks) itd.

Kaj so t. i. nastajajoča tveganja (ang. emerging risks)? Gre za rizike, ki so po pojavnosti novi ali spreminjajoči se, že obstoječi riziki, ki jih je težko oceniti in imajo velik vpliv na družbo in industrijo. Skupna značilnost slednjih, z vidika zavarovalništva, je, da jih spremlja negotovost in da o njih ni na voljo dovolj relevantnih podatkov. Pomanjkljiv je tudi zakonodajni okvir, prav tako še ni izoblikovana dobra praksa. V panogi še ni bil vzpostavljen enotni pogled na novo nastajajoča tveganja, v smislu enotne ocene stopnje rizičnosti, ki naj bi jo določena dejavnost ali proizvod predstavljala.

Kibernetska tveganja

V prispevku se bomo posvetili kibernetskim tveganjem, ki spadajo v skupino t. i. tehnoloških tveganj (npr. nanotehnologija, droni ipd.). Izpostavljenost kibernetskim napadom kot posledica širjenja elektronskega poslovanja, tehnologije, računalništva v oblaku, množenja informacij in občutljivih podatkov, s katerimi upravljamo, razpolagamo in jih hranimo, se namreč vse bolj povečuje.

Zavarovanje kibernetskih tveganj (ang. cyber risks) je zavarovanje, po katerem je vse več povpraševanja. Kot rečeno nam danes razvoj tehnologije omogoča razpolagati z vse večjimi zbirkami podatkov, jih obdelovati in shranjevati. Od teh podatkov je soodvisna večina današnjega poslovanja. Gre za podatke, ki jih ustvari podjetje samo (strategija, razvoj produktov, uspešnost poslovanja, plače ...) ali za podatke, ki mu jih zaupajo stranke (osebni podatki, podatki o premoženju, kreditiranju ...). S tem se odpira povsem novo polje kriminalnih dejanj, in sicer od tatvin podatkov, brisanja podatkov ali blokade sistemov, tatvine denarja, oškodovanja ugleda podjetja, prevar, poškodovanje sredstev podjetja, izsiljevanje, terorizem ... Informacije, s katerimi razpolagamo, imajo namreč lahko za nekoga določeno vrednost, ne da bi se mi tega zavedali. Če je poslovna informacija v končni posledici izpostavljena, zlorabljena ali spremenjena, ima to lahko predvsem negativne finančne posledice za podjetje. Kibernetska tveganja so torej v širšem kontekstu sinonim za informacijsko tehnologijo (IT) in v tem smislu poslovni riziko, vezan na uporabo, lastništvo, delovanje, vplivanje, vključevanje in privzemanje IT v poslovanje podjetij. Gre torej za kombinacijo verjetnosti in posledic takšnega dogodka (kibernetskega napada) v sferi informacijskega sistema.

Allianzov barometer tveganj na podlagi raziskave med 1900 strokovnjaki iz 80 držav ugotavlja, da so kibernetska tveganja takoj za izpadom poslovanja drugi največji poslovni rizik za leto 2018 in lahko povzročijo največjo dolgoročno škodo. Na 3. mestu so naravne nesreče. Leta 2013 so bila kibernetska tveganja uvrščena šele na 15. mesto.

Zavarovanje pred kibernetskimi napadi

Podjetja imajo danes na voljo več orodij, s katerimi lahko blažijo učinke kibernetskih napadov, pri čemer predstavlja enega od (vse bolj) ključnih tudi t.i. cyber zavarovanje. Povpraševanje po zavarovanju teh rizikov je iz leta v leto večje, saj je osveščenost o tveganjih vse boljša. To je posledica vse agresivnejših in bolj sofisticiranih oblik kibernetskih

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

napadov, vse večje specializiranosti napadalcev, zahtev regulatorjev po objavi napadov in po večji zaščiti potrošnikov ter tudi posledica povpraševanja že obstoječih zavarovancev po višjih zavarovalnih limitih. Vse navedeno vpliva, da je zavarovalni trg na področju kibernetskega zavarovanja v porastu in je trenutno ocenjen na dva bilijona dolarjev (v naslednjih petih letih naj bi narasel celo na pet bilijonov).

Poglejmo, kako se zavarovalnice spoprijemajo z omenjenimi riziki. Zavarovalnice so skozi čas prilagajale in razvijale svoje zavarovalne produkte. (Po)zavarovalnice so sprva razvile t. i. Technology E&O police, ki so bile namenjene e-poslovanju in podjetjem, ki so tehnološko omogočala takšno poslovanje (ponudniki internetnih storitev, različni tehnološki svetovalci, razvijalci računalniške (software) opreme itd.). Ti produkti pa so sčasoma, ob ustreznih prilagoditvah, prešli v kibernetsko zavarovanje, namenjeno podjetjem, ki se ne ukvarjajo s tehnološkimi storitvami. Podjetja, kjer je škoda posledica tehnoloških izdelkov ali storitev, danes praviloma sklepajo zavarovanja, kot so Tech E & O, Internet E & O, Information systems business interruption (ISBI) ipd., medtem ko se podjetja, kjer je škoda posledica uporabe informacijsko-tehnološke infrastrukture, odločajo za kibernetska zavarovanja. Ne glede na omenjeno pa (po)zavarovalnice še nimajo izdelanega unificiranega načina sklepanja tovrstnih zavarovanj. Tako vsaka (po)zavarovalnica pristopa k temu po svoje, po svoje ocenjuje, katera tveganja prevzeti, kako jih kontrolirati, jih še ustrezno umestiti z vidika izpostavljenosti, kumuliranja rizikov itd. Oblikujejo različne rešitve – bodisi kibernetsko zavarovanje kot samostojno polico ali kot razširitev obstoječih zavarovanj, ločeno zavarovanje za first party, third party in krizno svetovanje (ang. crisis consulting), podlimiti, kombiniranje zavarovanj itd.

Ne glede na različne pristope, ki so jih ubrale (po)zavarovalnice, pa je vsem skupen temeljit pregled rizika in ocena izpostavljenosti podjetja.

Polica po meri stranke

(Po)zavarovatelji se pri zavarovanju kibernetskih rizikov zavedajo njihove kompleksnosti. Kar je z vidika zavarovanja pomembno za enega zavarovanca, morda ni pomembno in je celo neuporabno za drugega. Zato so zavarovanja za zdaj do določene mere še zmeraj bolj ali manj narejena po meri (ang. tailor made) za vsakega posameznega zavarovanca. Da pa bi (po)zavarovatelji lahko zagotovili ustrezno kritje in pravilno ocenili stopnjo rizičnosti posameznega zavarovanca morajo, kot rečeno, od njega dobiti čim več informacij. Več kot je informacij in kakovostnejše kot so, laže se (po)zavarovatelj odloči za zavarovanje in hkrati ponudi kritje, ki bo ustrezalo potrebam in izpostavljenosti posameznega zavarovanca. Velja torej pristop: »Learn client's business to design best cover.«

Večina omenjenih kibernetskih rizikov se pravzaprav ne razlikuje toliko od tistih, ki smo jih poznali že do zdaj. Vendar pa se je izpostavljenost tveganjem v





vse bolj digitalizirani družbi pomembno spremenila. Z dostopnostjo do informacij, brezmejnim poslovanjem, obdelavo podatkov, digitalnim povezovanjem različnih virov itd. se povečuje število škodnih dogodkov in predvsem stopnjuje vpliv, ki ga slednji imajo na ekonomijo in družbo v celoti. Razumevanje rizikov, ustrezen pristop (t. i. upravljanje tveganj) in pa mednarodno sodelovanje bodo pri obvladovanju teh rizikov ključni.

Pripravljeni na tehnološki napredek

Zdajšnji čas prinaša tveganja, ki jih vsi vpleteni – regulatorji, (po)zavarovalnice itd. – trenutno šele poskušamo razumeti, sprejeti in se jim prilagoditi. Nekatera standardna zavarovalna »orodja« zavarovatelji že imamo na voljo (franšizo, sprožilce kritja, podlimite, premijo, rezervacije...) in jih moramo ob pravilni oceni tveganj preudarno uporabiti. Razvoj zavarovalnih produktov pa bo terjal tudi določeno stopnjo inovativnosti. Na splošno velja, da so riziki danes bodisi bolj ali manj dobro poznani, jih razumemo in so dobro upravljani, bodisi pa šele nastajajo in so posledično kompleksnejši ter slabše upravljani. Nova tehnologija je v interakciji s svetom na več različnih načinov, ki jih ni bilo in jih ni moč predvideti. Tako se bodo vse posledice tehnološkega napredka (tako pozitivne kot negativne) razkrile šele sčasoma, saj nam v vsem njihovem obsegu danes še niso znane in doumljive.

Jasno je, da vstopamo v novo fazo tehnološkega napredka, ki bo prinesel nove oblike izpostavljenosti, ki jih ne predvideva in ne vsebuje nobena od današnjih zbirk podatkov. Posledica tega je, da bomo morali zavarovatelji razviti modele, ki bodo temeljili bolj ali manj na ocenah in predpostavkah in ne toliko na preteklih izkušnjah. Pri tem bo zaznava, predvsem pa pravilna ocena tveganj, ki jih prinašata nova tehnologija in razvoj, priložnost za zavarovalnice, da se na te »grožnje« odzovejo z razvojem novih zavarovalnih produktov. Zavarovalna panoga bo s svojim znanjem in obvladovanjem tveganj vsekakor odigrala pomembno vlogo pri uveljavljanju in uporabi nove tehnologije in razvijajočih se dejavnosti.

Allianzov barometer tveganj na podlagi raziskave med 1900 strokovnjaki iz 80 držav ugotavlja, da so kibernetska tveganja takoj za izpadom poslovanja drugi največji poslovni rizik za leto 2018 in lahko povzročijo največjo dolgoročno škodo. Na 3. mestu so naravne nesreče. Leta 2013 so bila kibernetska tveganja uvrščena šele na 15. mesto. ■

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



PASTI IN ZAŠČITA V SVETU KRIPTOVALUT

Virtualne valute ali morda bolje poznane kot kriptovalute so postale znani globalni fenomen za veliko ljudi. Preden pa se podate v svet kriptovalut, je dobro poznati pasti, ki vas na tej poti lahko čakajo in kako se zaščititi, ko boste na le-te naleteli.

Kaj sploh so kriptovalute?

Satoshi Nakamoto, gre za izmišljeno ime razvijalca ali skupine razvijalcev, je leta 2008 ustvaril prvo kriptovaluto, ki jo poznamo po imenom Bitcoin. Uporabljajo se kot virtualno plačilno sredstvo in so digitalna valuta, ki za varnost uporabljajo kriptologijo. Imajo podobne lastnosti kot papirnati denar, omogočajo pa takojšnjo transakcijo poljubnih vsot na druge naslove, ne glede na državo prejemnika. O kriptovalutah se danes vse bolj govori, zato je želja po nakupu in preizkušanju tega virtualnega sveta še toliko večja. Preden pa zamika tudi vas, se pred kakršnim koli nakupom dobro informirajte, preberite kakšno knjigo ali članke na spletu ter se vključite v skupine na raznih družabnih omrežjih. Tako boste dobili informacije in nasvete, ki vam bodo pomagali pri vaši nadaljni odločitvi.

Na kaj moramo biti pozorni

Ko se odločite, da bi tudi vi kupili kakšen kripto kovanec, je izbira prave denarnice prva stvar na katero je potrebno pomisliti.

1. Hladne denarnice

Če imate v mislih večje vsote, potem le-te hranite v t.i. hladnih denarnicah. To so denarnice, ki niso povezane v internet, zato hladne denarnice veljajo za najbolj varne. Kraja iz takšne denarnice je tako možna le v primeru, če ima napadelc fizični dostop do nje. Med hladne denarnice pa se uvrščajo tudi papirnate denarnice. Takšne denarnice natisnemo in jih varno shranimo, na primer v sef. Denarnica je dejansko le zasebni ključ kriptovalute. Z zasebnim ključem ustvarimo tudi javni ključ, ki pa kreira naslov kriptvalute. Takšno denarnico sestavljata dve alfanumerični kodi, ki se ju ponavadi zapiše v obliki QR kode. Prva je javni naslov denarnice, kamor nam nekdo lahko nakaže sredstva (kot neke vrste številka bančnega računa), druga pa zasebni ključ, ki omogoča upravljanje s sredstvi na tem računu. Če izgubimo zasebni ključ, izgubimo tudi vsa sredstva na računu.

Vse bolj pa so priljubljene tudi strojne denarnice, ki jih prav tako uvrščamo med hladne denarnice. Najbolj poznana sta Trezor in Ledger (Nano S). To so majhe naprave, v velikosti USB ključa in omogočajo varno shranjevanje, pošiljanje in prejemanje transakcij na spletu. Njihova bistvena lastnost je, da je iz njih nemogoče ukrasti zasebne ključe denarnic.

2. Mobilne denarnice

Mobilni telefon danes uporabljamo že skoraj za vse, tako lahko za sprotno uporabo kripto kovancev in žetonov uporabljamo tudi mobilne denarnice. Pomembno je, da izberete eno od pri-



*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



znanih in preverjenih aplikacij, ki jo namestite iz uradne spletne strani oziroma uradne trgovine. Denarnico obvezno zaščitite z geslom ali s PIN kodo.

3. Spletne denarnice

Kot že pove samo ime, so te denarnice na voljo na spletu in jih ponujajo tretje osebe. Pri tovrstnih denarnicah se je potrebno zavedati, da vi niste lastnik zasebnega ključa, temveč je to upravljalec storitve. V primeru, da se le-ta iz različnega razloga odloči, da vam onemogoči uporabo storitve, lahko ostanete brez vseh sredstev. Zato v spletnih denarnicah hranite le zgolj nujno potrebna sredstva oziroma le toliko, kot si lahko privoščite, da jih izgubite. Med spletne denarnice uvrščamo tudi kripto borze.

Število uporabnikov kriptovalut se je v zadnjem času zelo povečalo, konec leta 2017 naj bi namreč bilo že več kot 21 milijonov naslovov denarnic. Tako so se močno povečale tudi dejavnosti kriminalcev. Napadi, ki ciljajo na posameznika (tako imenovani phishing napadi), oziroma bolj natančno na njegovo denarnico, so med najpogostejšimi. Po nekaterih izračunih naj bi v letu 2017 prišlo do več 100-milijonskih izgub preko takih napadov. Phishing napad poteka tako, da napadalci postavijo prepričljive kopije spletnih storitev na katere nato žrtve preusmerijo na različne načine. Če uporabniki na lažni strani vpišejo svoje podatke, jih tako sporočijo napadalcem. Zato do storitev nikoli ne dostopajte preko ponujenih povezav. Napadalci zelo pogosto lažne spletne strani s pomočjo Google oglaševanja uvrstijo na vrh iskalnih rezultatov, zato je najbolje, da vedno uporabimo zaznamke.

S popularizacijo kriptovalut in Blockchain tehnologije, so se razcvetele tudi oblike množičnega financiranja ICO (ang. »Initial Coin Offering«), pri katerem vlagatelji v času investiranja v kripto denarnico podjetja, ki zbira sredstva za zagon nekega produkta, nakažejo svoje kripto kovance. Nakazila so ponavadi v kriptovaluti Ether ali Bitcoin, podjetje pa jim v nekem delilnem razmerju vrne njihove kripto žetone. Zaradi pričakovanega visokega donosa je vlagateljev v ICO projekte izredno veliko, zato so zelo zanimivi tudi za goljufe. Ti postavijo lažne spletne strani projekta s spremenjenim naslovom kripto denarnice, nato pa poskušajo vlagatelje prepričati k obisku strani, ponavadi pod pretvezo, da bodo hitreje lahko vložili kot drugi in s tem pridobili dodatni bonus. Na različnih družabnih omrežjih se tudi lažno predstavljajo kot zaposleni v podjetju in vlagatelje preko zasebnih sporočil vabijo k nakazilu sredstev v njihovo kripto denarnico. Če zelimo sodelovati v ICO projektu, pred nakazilom vedno preko različnih kanalov preverimo naslov denarnice, kamor bomo nakazali svoja sredstva. V primeru, da jih nakažemo na napačni naslov, so namreč za vedno izgubljena.

Osnovna zaščita in varnostni napotki

Da bi vašo denarnico čim bolj zaščitili, je naprej potrebno poskrbeti za osnovno zaščito vašega računalnika in mobilne naprave. Če boste vse povprek odpirali priponke elektronske pošte od neznanih pošiljateljev, klikali na vse možne povezave, ne boste zaklepali zaslona, potem vam še tako dobra zaščita denarnice ne bo pomagala.





Zato upoštevajte:

- Zaklepajte zaslon z geslom, PIN kodo ali prstnim odtisom
- Nameščajte preverjene aplikacije iz uradnih virov
- Sistem in aplikacije redno posodabljajte
- Uporabljajte protivirusno zaščito

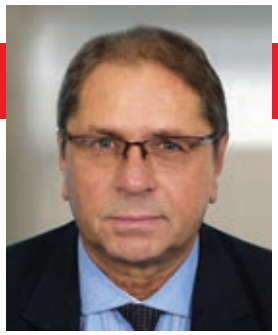
Pred prvim nakazilom denarja, obvezno naredite varnostno kopijo denarnice. Zelo hitro se lahko namreč zgodi nezaželen dogodek (izguba papirnate denarnice , okvara računalniškega diska, izguba ali kraja telefona...), ki pripelje do izgube denarnice. Varnostno kopijo denarnice ne hranite na računalniku, v oblaku ali še slabše v elektronski pošti, temveč na vsaj dveh različnih zunanjih medijih (USB ključ, zgoščenka, zapis na papirju). Varnostna kopija je običajno niz 12 – 24 angleških »seed« besed. Denarnica ima lahko različen način izdelave varnostne kopije, zato se pozanimajte na kakšen način le-to storite za vašo denarnico.

Za dodatno zaščito pa se priporoča tudi uporaba 2-faktorske avtentikacije (2FA), ki jo nudijo vse spletne borze. 2FA vam omogoča, da pri prijavi poleg gesla vpišete tudi unikatno kodo, ki jo zgenerira aplikacija na telefonu ali leto prejmete preko SMS sporočila na svojo mobilno številko. S tem namreč zelo povečate varnost vašega računa, saj napadalec brez te kode, četudi mu uspe pridobiti vaše geslo za dostop, do vašega računa ne bo mogel dostopati.

Bodite na tekočem

Kriptovalute so vsekakor zelo priljubljene, saj jih je danes na trgu že več kot 1000, število le-teh pa še vedno narašča. Vendar pa vsaka nova tehnologija potrebuje čas, da se lahko odkrijejo varnostna tveganja. Tudi Blockchain in storitve, ki na tem temeljijo, niso imune pred varnostimi luknjami, saj so prve ranljivosti že bile odkrite. Zelo pogosto pa gre pri storitvah za napake, ki jih naredi človek (razvijalec), ki pa imajo lahko v svetu kriptovalut precejšnje finančne posledice. Zato je pomembno spremljati varnostna obvestila in novosti, da se lahko v pravem trenutku odzovete in ustrezno ukrepate. ■

Avtor: dr. Alojzij Krapež / Ministrstvo za infrastrukturo RS*



LOGISTIKA OBVEŠČEVALNIH DEJAVNOSTI NA EKONOMSKO POSLOVNEM PODROČJU

Logistika obveščevalnih dejavnosti na ekonomsko poslovnem področju je vsekakor tema, katero bi v našem okolju v preteklosti redko srečali. Ekonomsko poslovno področje in logistika sta soodvisni in v uspešen poslovni model povezani dejavnosti. Vendar kako v to soodvisnost spada obveščevalna dejavnost?

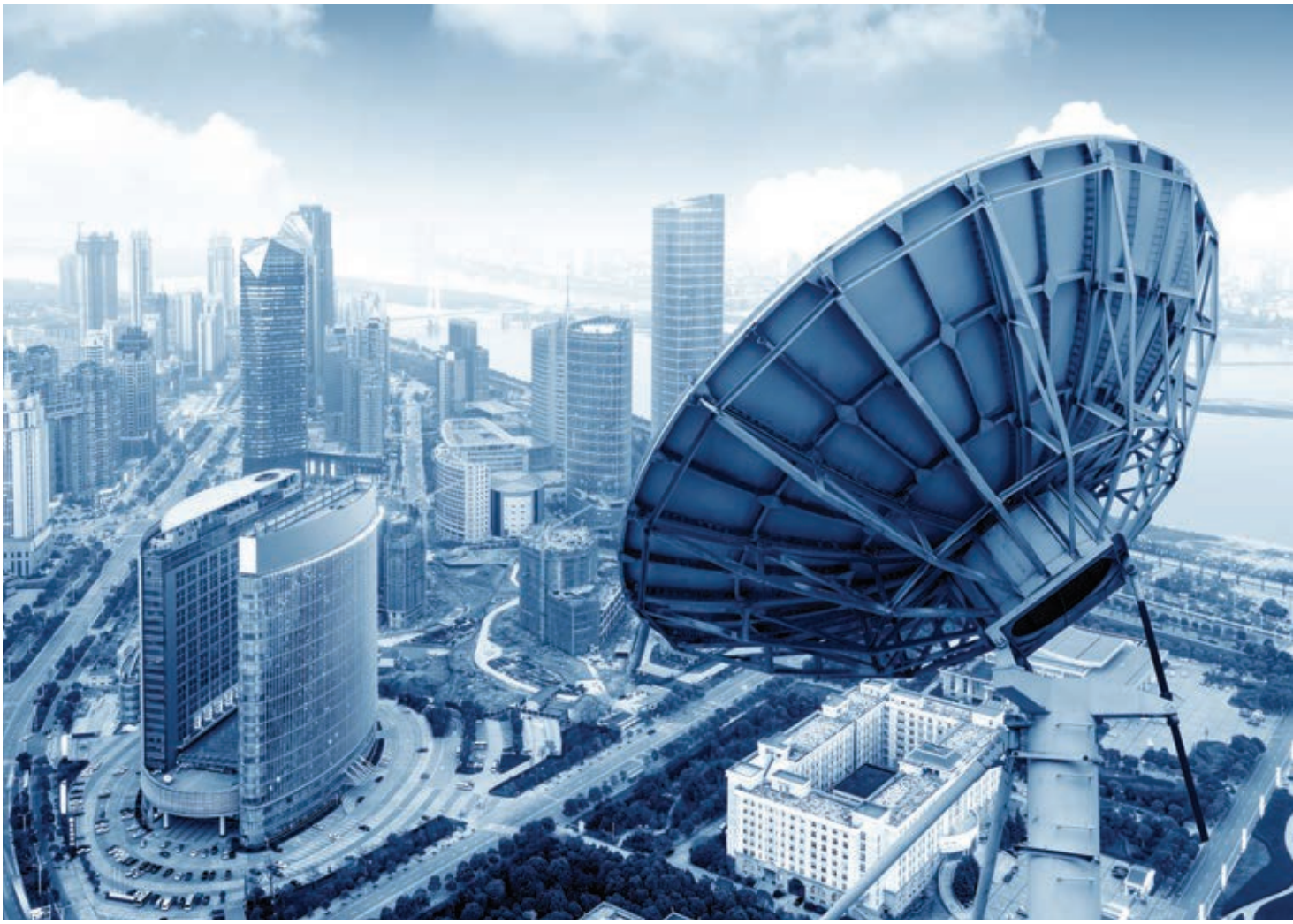
V preteklosti je bila obveščevalna dejavnost organizirana na nacionalnem nivoju in v izključni lasti države. V sodobnem svetu te omejitve počasi izginjajo. Ta kratek pogled nazaj ni pomemben samo zaradi dejstva, da je prišlo do sprememb v varnostni arhitekturi, temveč nakazuje tudi nekaj drugih pomembnih dejstev. Prvo je vsekakor širitev potrebe po obveščevalni dejavnosti na ekonomsko poslovno področje. Kot pravi Podbregar (2008) se posamezniki in organizacije, tako profitne kot neprofitne, v dinamičnem okolju v katerem živimo in ga kreiramo, srečujejo z vse večjo potrebo, ki bi jo na kratko lahko opisali s stavkom: »Potrebujem pravočasne, točne in uporabne podatke za odločanje«. Ta preprost stavek pred nas postavlja velike ovire, zahteva izjemno organiziranost in delovanje različnih timov, skupin ter odlično infrastrukturo, večkrat vezano na najsodobnejše informacijske tehnologije. V sodobni informacijski družbi so nam mnogi podatki na voljo z relativno hitro dostopnostjo. Še vedno pa so nam za ključne odločitve potrebni podatki, ki morda v tistem trenutku niso razpoložljivi, so premalo natančni ali pa jih imajo v posesti ključni posamezniki, ki jih enostavno želijo zadržati zase in jih sami uporabiti za svoje lastne odločitve.

Podjetnik potrebuje na poti do uspeha tudi čedalje več znanja in informacij. Sodobne tehnologije ponujajo neobvladljive količine informacij, a hkrati postaja polje »občutljivih« informacij, ki so zaščitene pred nepooblaščenimi očmi, čedalje obsežnejše. Varujejo jih ne le sofisticirana tehnika in varnostni sistemi, temveč tudi zakon. A načeloma je dosegljiva vsaka, še tako varovana informacija. Vprašanje je le, koliko denarja in časa smo pripravljeni investirati v rušenje ovir. Gre preprosto za vprašanje ekonomije in morale oziroma poslovne etike. Etika ponuja zabrisane meje, ostra ločnica pa je postavljena tam, kjer nemoralno početje prestopi prag zakona in preide na področje kriminalnega početja, točneje na področje poslovnega ali gospodarskega kriminala.

Drugo pomembno dejstvo je, da je prišlo do t.i. privatizacije obveščevalne dejavnosti, ki je bila v preteklosti v ekskluzivni državni pristojnosti. Vse več je subjektov v poslovnem svetu, ki v svojo osnovno dejavnost vključujejo obveščevalno dejavnost, z namenom pridobivanja konkurenčne prednosti na trgu. Obstaja cela paleta subjektov, ki na trgu nudijo storitve, ki so plod obveščevalne dejavnosti. Prav tako deluje tudi veliko subjektov, ki na trgu ponujajo storitve zaščite pred t.i. ekonomskim vohunstvom, pa naj gre zgolj za zaščito vitalnih podatkov ali informacij, ali za bolj kompleksne sisteme t.i. integralne varnosti.

S tem smo prišli do tretjega pomembnega dejstva in to je konkurenčna obveščevalna dejavnost. Konkurenčna obveščevalna dejavnost je sistematični program za zbiranje in analiziranje informacij o aktivnostih vaših tekmecev in splošnih poslovnih gibanj, ki pomagajo k doseganju ciljev poslovnega sistema.

*avtor je član Slovenskega združenja korporativne varnosti



Ugledni Brintov inštitut postavlja ostro ločnico med konkurenčno obveščevalno dejavnostjo (*Competitive Intelligence - CI*) in poslovnim vohunstvom (*Business Espionage*). Konkurenčna obveščevalna dejavnost uporablja namreč javne vire za odkrivanje in razvijanje informacije o konkurenci, konkurentih in tržnem okolju. Za razliko od poslovnega vohunstva, ki razvija informacije z nelegalnimi sredstvi, kot je vdiranje (*hacking*), uporablja konkurenčna obveščevalna dejavnost javne informacije. Torej tiste, ki so lahko legalno in etično identificirane in dostopne.

Poleg znanj s področja obveščevalne dejavnosti potrebujemo tudi znanja s področja logistike. Logistika je zelo široka znanost, ki povezuje organizacijska, ekonomska, finančna, informacijska znanja, znanja o varstvu okolja in mnoga druga, v enoten sistem. Opredeljuje se kot znanost in kot dejavnost, s katero smo obvladali fizični tok blaga, energije, informacij in človeških virov, in tako postane eden glavnih delov poslovne in tržne strategije. Prisotna je v vseh fazah poslovnega procesa v podjetju in je povezana z vsemi temeljnimi poslovnimi funkcijami.

V znanstveni sferi obstaja jasno izražena potreba po definiranju generičnega modela logistike obveščevalnih dejavnosti, ki bo dobra platforma za organiziranje in upravljanje konkretnih aplikativnih modelov znotraj javnega in zasebnega ekonomsko poslovnega sektorja. Odločitev za organiziranje in financiranje takih modelov znotraj javnih in zasebnih gospodarskih družb, je predvsem odgovornost vodstvenih struktur, ki brez take podpore pri poslovnih odločitvah, izgubljajo pomemben del konkurenčnosti ekonomsko poslovnega okolja in s tem pomemben potencialni tržni delež, ki predstavlja materialno osnovo za splošno blaginjo celotne družbe.

Naše raziskovanje je rezultiralo z oblikovanjem procesnega modela logistike obveščevalne dejavnosti na ekonomsko-poslovnem področju kot prvega takega modela v Sloveniji. S tem se je odprl tudi prostor za vse nadaljnje raziskave na tem področju. Količina in kakovost znanj s tega področja je lahko učinkovito orodje managementa podjetij za doseganje konkurenčne prednosti na trgu. Model logistike obveščevalnih dejavnosti na ekonomsko poslovnem področju, je teoretično in empirično kompleksen model, ki omogoča, da je kvaliteta odločitve na osnovi informacij pridobljenih preko mreže obveščevalnih dejavnosti bistveno višja, kot kvaliteta tiste odločitve, ki je sprejeta na osnovi tradicionalnih »instiktivnih« procesov.

Nedvomno lahko zaključimo, da je obveščevalna dejavnost na področju ekonomsko poslovnega sektorja, ena od pomembnejših sestavin vsakega uspešnega poslovnega modela. Pridobivanje pravočasnih in pomembnih informacij je za sprejemanje poslovnih odločitev, v luči konkurenčne prednosti poslovnega subjekta v mednarodnem poslovnem okolju, ključnega pomena.



Odločitev za organiziranje in financiranje takih modelov znotraj javnih in zasebnih gospodarskih družb, je predvsem odgovornost vodstvenih struktur, ki brez take podpore pri poslovnih odločitvah, izgubljajo pomemben del konkurenčnosti ekonomsko poslovnega okolja in s tem pomemben potencialni tržni delež, ki predstavlja materialno osnovo za splošno blaginjo celotne družbe.

Izhajajoč iz zgornje ugotovitve, se sam po sebi ponuja logičen zaključek, da mora logistika obveščevalnih dejavnosti postati del razvojnih načrtov gospodarskih sistemov, sicer bo zgubljanje konkurenčnih prednosti gotovo odvrnilo mnogo potencialnih domačih in tujih investitorjev v nove proizvodne in storitvene zmogljivosti. To pomeni tudi zamujeno priložnost za gospodarsko rast in razvoj oziroma blaginjo celotne družbe.

Dobro definiran model logistike obveščevalnih dejavnosti na ekonomskem in poslovnem področju ter njegova konkretna aplikacija znotraj poslovnih sistemov, ima pomemben vpliv na učinkovito vodenje nacionalnih ekonomij in poslovnih subjektov. Pravočasne in kvalitetne informacije ni mogoče pridobiti brez dobro zastavljenega in delujočega modela izvajanja obveščevalne dejavnosti, ki je vpet v poslovni sistem kot njegov polnopravni del. Ni namreč mogoče pričakovati, da bi občutljive poslovne informacije konkurence pridobili brez organiziranega, sistemskega in visoko profesionalnega pristopa. Tudi naših strateških, konkurenčnih prednosti, ni mogoče zaščititi pred konkurenčno obveščevalno dejavnostjo, če ta zaščita ni vključena v dobro delujoč model, ki ne temelji na naključjih, temveč na sistemsko in dolgoročno zastavljenih ciljih, ki jim sledimo z namenom uspešnega vodenja poslovnega sistema.

Vzpostavitev takega modela logistike obveščevalnih dejavnosti na ekonomskem in poslovnem področju je zahteven proces, za katerega potrebujemo teoretična znanja in praktične izkušnje. V raziskavi, kjer smo preučevali in povezovali rezultate, smo v ospredje postavili tudi tezo, da so motivatorji za obveščevalno tajno sodelovanje in dejavniki v procesu prodaje državnih deležev v slovenskih podjetjih, gradniki modela zaščite gospodarskih družb pred nepooblaščenim oziroma neželenim odtekanjem strateško pomembnih podatkov. Definirali smo osrednje motivatorje obveščevalne dejavnosti in ugotovili, da sta motivatorja materialne koristi in patriotizem uveljavljena v obveščevalni dejavnosti. Motivatorji, kot so rehabilitacija, želja po uveljavljanju, sovraštvo in sorodstvene vezi, pa se lahko občasno pojavijo, kot začasno uporabni v posameznih fazah obveščevalne dejavnosti.

Na podlagi definicije in izgradnje procesa prodaje deležev državnega premoženja smo določili človeške vire, ki kot zunanja ali notranja javnost participirajo v procesu prodaje. Povezali smo človeške vire iz procesa prodaje z motivatorji za tajno sodelovanje v obveščevalni dejavnosti in tako dobili podlago

ter elemente za obveščevalno zaščito gospodarskih družb oziroma njihovih ključnih strateških podatkov v prodajnih procesih.

Ugotavljamo, da v Sloveniji obstaja veliko znanja s področja klasičnih obveščevalnih dejavnosti, ki pa je razpršeno in sistemsko neurejeno, zato bi bilo smiselno ta teoretična in aplikativna znanja sistemsko urediti in prilagoditi ekonomsko poslovnim interesom ter oblikovati generični logistični model, ki bo predstavljal dobro logistično podporo za aplikativno uporabo v javnem in zasebnem gospodarskem sektorju.

Na tej točki bi se usmeril v prihodnost predvsem v luči trenutno perečega vprašanja – prodaje deležev državnega premoženja.

V prihodnjih raziskavah je potrebno posamezne dele procesa prodaje deležev državnega premoženja, povezati s človeškimi viri, ki imajo v posameznem delu procesa prevladujočo vlogo. Letem je potrebno določiti tudi prevladujoč motivator za tajno sodelovanje in tako po posameznih segmentih ugotoviti korelacijo med pomembnostjo človeških virov skupaj z njihovimi motivatorji in v tej kombinaciji njihov vpliv na posamezne dele procesa prodaje državnih deležev v gospodarskih družbah. Prav tako je v prihodnjih raziskavah potrebno določiti vlogo posameznih motivatorjev, glede na zvrsti obveščevalne dejavnosti (predvsem obveščevalno in protiobveščevalno zvrst), in njihove korelacije z deli procesnega modela logistike obveščevalne dejavnosti na ekonomsko-poslovnem področju.

Predlagan procesni model, ki vključuje motivatorje za tajno sodelovanje v povezavi s človeškimi viri, je potrebno znanstveno preveriti tudi na drugih področjih upravljanja deležev državnega premoženja. Predlagamo, da se raziskovanje usmeri predvsem v deleže državnega premoženja, ki predstavljajo kritično infrastrukturo države. ■

Nedvomno lahko zaključimo, da je obveščevalna dejavnost na področju ekonomsko poslovnega sektorja, ena od pomembnejših sestavin vsakega uspešnega poslovnega modela. Pridobivanje pravočasnih in pomembnih informacij je za sprejemanje poslovnih odločitev, v luči konkurenčne prednosti poslovnega subjekta v mednarodnem poslovnem okolju, ključnega pomena.

Vir: Podbregar, Iztok (ur.). (2008). Vohunska dejavnost in gospodarstvo. Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.



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



DUBIOZNI STATUS VAROVANJA

Tuj svet z eksplozijo prebivalstva, socialno izjemno diferenciran, od skrajnega uboštva do izjemnega luksuza – brez vsake eksistenčne varnosti, zasilnimi bivališči in ruševinami ter nekaterimi bohotnimi razkošnimi hotelskimi naselji najvišje kategorije, največkrat pa le na pol dograjenimi počitniškimi otoki ter omejeno komunalno infrastrukturo, leži na dosegu roke Evrope.

Vojno stanje na arabskem polotoku je prek številnih »check point« kontrolnih točk (urejenih ob dvignjenih zanemarjenih kočah na vrhu železnih stopnišč z oboroženim stražarjem - pogosto pa tudi brez njega) neposredno prisotno. Posebej so varovani tudi verski in kulturni objekti - če seveda ob obilici tega varovanja o kakem dejanskem, strokovno zadovoljivem varovanju sploh lahko govorimo. Pogoste kontrole so izjemno pomanjkljive (če piska alarm, greš ponovno skozi nadziran prehod, nato pa enostavno mimo njega, pijačo kljub večkratnim nadzorom brez težave prineseš na letalo). Teroristični napadi so dejansko možni vsak čas.

Navedeno stanje in popolnoma drug ter kulturen svet se nas dotikata iz jugo-vzhodne soseščine prek Turčije in arabskega polotoka in Afrike – ki je pri današnjih prometnih povezavah praktično pred našimi durmi. Nevarnosti ogromnega migrantskega vala, ki je izpred dveh let in pol iz Turčije prek Grčije preplavil velik del Evrope (med drugim tudi našo državo, zlasti pa Nemčijo, kjer se je v največjem delu ustalil) kljub sedanji preusmeritvi čez Sredozemsko morje in Italijo, še zdaleč niso mimo. Večina držav na tej migrantski poti je po zgledu (sprva javno kritizirane) Madžarske postavila obmejne žične ovire. V kritičnem času največjih množičnih vdiranj v Evropo so za njihovo zajezitev in čim hitrejši transport proti Avstriji pri nas nenadoma, ne glede na različne zakonske pristojnosti, hkrati sodelovale vse razpoložljive policijske, obrambne, varnostne, zaščitne, gasilske, reševalne, socialne, zdravniške in prevozniške kapacitete. Zakonsko določene formalne pristojnosti med posameznimi strukturami zagotavljanja varnosti so bile v tej fazi nenadoma zabrisane, pomembne so ostale le strokovne, poklicne.

Seveda se je na državni ravni posebej odprlo vprašanje razmerja med vojsko in policijo, v tej zvezi pa posredno tudi zasebnega varovanja in civilne zaščite.

Razvojne perspektive zasebnega varovanja kot tržne, podjetniške dejavnosti so zaradi hkratnih omejitev pooblastil izvajalcev na tem področju očitno omejene. V verigi subjektov, ki delujejo na področju zagotavljanja varnosti, je njihov status povsem podrejen vsem pristojnim državnim in občinskim službam, izvajanje storitev pa omejeno izključno na pooblastilo vsakogar do samopomoči.

Celo v kritični fazi reševanja najhujših težav obvladovanja takratnih migrantskih navalov, so morali vojaki na hitro opraviti kratko usposobitev in se pri svojih aktivnostih, vsaj formalno, omejiti na področje zalednih delovanj. Te formalne zahteve in omejitve v kritičnem času, sprejete na hitro, ne morejo prekriti čedalje bolj razvidnega vprašanja, ki se odpira danes, v času očitnih groženj svetovnemu miru, grozljivih vojnih območnih spopadov z intervencijami svetovnih velesil ter novodobnega pojava organiziranega podtalnega fanatičnega terorizma :

- kakšna je vloga nacionalnih obrambnih sil v okviru nadnacionalne povezanosti držav v Evropski Uniji ?
- kakšne funkcije policijskega delovanja se povezujejo, prenašajo ali ustanavljajo na ravni evropskih in drugih meddržavnih povezav in inštitucij (Europol, Interpol) ?
- kakšne možnosti nam na obrambnem in policijskem področju prinašajo nove meddržavne povezave v okviru EU, na podlagi konec lanskega leta sklenjenega meddržavnega dogovora PESCO ?
- kakšne so dimenzije in raznovrstne možnosti komunikacij in razvoja ter nevarnosti v kibernetskem prostoru ?

Nobenega dvoma ni, da se v 21. stoletju nahajamo pred bistveno spremenjenimi varnostnimi grožnjami, tako glede strahotnih možnosti oborožitve kot tudi oči-

*avtor je član Slovenskega združenja korporativne varnosti

tne dostopnosti do nje, tudi za majhne, iz okvira svetovnih državnih zvez iztirjene države ter celo fanatične iracionalne združbe in paradržavne tvorbe ter, da po drugi strani na svetovnem odru v odločilni meri prevzemajo besedo večdržavni, večnacionalni veliki sistemi gospodarsko in tehnološko najbolj razvitih državnih subjektov. Po drugi strani se, vedno bolj očitno, znotraj različnih državnih tvorb, razkrivajo družbene elite različnih korenin in interesov ter vedno širše plasti prebivalstva, ki tone pod raven eksistenčnega minimuma. Vse tanjša je vmesna plast ljudi. Etična pravila obnašanja izginjajo za vsiljivimi oblaki številnih preprog enkratnih priložnosti. Nacionalna identiteta se razblinja. Smo prebivalci tega planeta ali vsaj njegovih kontinentov.

Varnost je pomembnejša bolj kot kdajkoli. Zahteva predsednika Trumpa, da EU sama v veliko večji meri poskrbi za lastno varnost, je odprla popolnoma novo poglavje. Predvsem so se najpomembnejši voditelji EU soočili z lastno dosedanjo neaktivnostjo, še zlasti z velikimi odprtimi obveznostmi. Stanje v Sloveniji, tako glede obveznosti do mednarodnih organizacij, zlasti do NATA, kot do lastnih obrambnih, policijskih in varnostnih sil je na določenih področjih celo kritično. Že več kot desetletje. Potrebno financiranje infrastrukture in nalog kritično zaostaja, perspektive zaposlenega temeljnega kadra – na področjih obrambe in varovanja so pogodbe o zaposlitvi sklenjene skoraj izključno le za določen čas in praviloma za plače na minimalni ravni – so skrajno omejene. Tako je eksistenca zaposlenih vojakov ali varnostnikov (mnogokrat pa tudi policistov) praviloma zagotovljena le na najosnovnejši ravni. Nujnost organizacijskih premikov v naših obrambnih, policijskih in varnostnih strukturah je že dolgo prisotna. Kljub sprejetim razvojnim programom, na teh izredno pomembnih področjih obrambne pripravljenosti in zagotavljanja varnosti, ni videti nobenega resničnega premika v smeri konkretne razrešitve teh, v zadnjem desetletju nakopičenih težav. Pred vrati je ponovna stavka policistov (med tem ko možnosti stavke vojakov in varnostnikov le zaradi šibkosti njihove organizacijske strukture ni pričakovati).

Vendar je treba priznati, da je odgovornost za te razvojne zaostanke potrebno iskati tudi v nezadovoljivem delovanju EU, njenega vse preveč zbirokratiziranega upravnega aparata in njeni nedodelani notranji organizaciji, v okviru katere so interesi manjših držav in dežel iz večjih državnih sistemov vse preveč potisnjeni v ozadje. Razvojno zaostajanje EU, še zlasti na področju opravljanja najpomembnejših funkcij na obrambnem in policijskem področju, so podlaga ne le za sprejemanje njenih marsikaterih ad hoc odločitev (kot npr. o obvezni predhodni ureditvi vseh spornih mejnih vprašanj sedanjih balkanskih kandidatk za sprejem v EU, t.j. stališča, ki je v očitnem nasprotju z njeno nekdanjo zahtevo pri reševanju našega mejnega spora z R Hrvaško), marveč predvsem pri zaostajanju njene nujne organizacijske prenove in sistemizacije nalog na navedenih varnostnih področjih. Temeljna reorganizacija vojaških kapacitet članic EU v smislu oblikovanja in delovanja skupnih evropskih obrambnih sil ter celovita izgradnja skupne evropske policijske in varnostne mreže – ki je doslej stkana le v okviru posameznih projektov in inštitucij – vse predolgo zamujata. Konsekvence so očitne: vojaške sile posameznih članic se samostojno povezujejo predvsem v okviru aktivnosti zveze NATO, policijske sile pa v okviru posameznih projektov učinkovite izmenjave podatkov in občasnih skupnih regionalnih aktivnosti. Varnostni mehanizem EU ni le nedovršen, marveč je pri svojem delovanju tudi vse premalo koordiniran in učinkovit.

Razvojne perspektive zasebnega varovanja kot tržne, podjetniške dejavnosti so zaradi hkratnih omejitev pooblastil izvajalcev na tem področju očitno omejene. V verigi subjektov, ki delujejo na področju zagotavljanja varnosti, je njihov status povsem podrejen vsem pristojnim državnim in občinskim službam,



Ni dvoma, da je mogoče, preverjenemu podjetju z dejavnostjo zasebnega varovanja, zaupati izvajanje osnovnih oblik varovanja z usposobljenimi varnostniki, inženirji in tehniki v primerih in ob pogojih običajnih rizičnih situacij. Povsem nekaj drugega pa je, kadar se srečujemo s primeri posebej občutljivih podatkov in rizikov z izjemno velikimi, mnogokrat celo nepredvidljivimi posledicami.

izvajanje storitev pa omejeno izključno na pooblastilo vsakogar do samopomoči. Po drugi strani pa je njihovo gospodarsko delovanje svobodno, tako kar zadeva opravljanje vseh drugih dejavnosti (celo ne glede na njihovo primernost), kot tudi izvrševanje varnostnih storitev na območju vseh držav članic EU. Po evropski zakonodaji so nesprejemljive zakonske omejitve posameznih držav glede obveznosti, da je kraj sedeža podjetja na področju države, kjer opravlja storitve varovanja, da morajo imeti odgovorne osebe teh podjetij svoje prebivališče v teh državah, da mora podjetje za svoje dejavnosti varovanja pridobiti dovoljenje pristojnega organa države, v kateri posluje, in da morajo odgovorne osebe podjetja in varnostni delavci imeti izkaznice notranjega ministrstva države, v kateri delajo. Prav tako so nedopustne tudi vse druge administrativne omejitve, ki otežujejo podjetjem za zasebno varovanje dostop na tržišče druge države, članice EU. Več odločb Evropskega sodišča je ta stališča nedvoumno potrdilo.[1]



Svoboda opravljanja storitev varovanja za gospodarske subjekte iz posamezne države, članice EU, na področju vseh drugih držav v okviru EU izenačuje njihov status z drugimi gospodarskimi subjekti na skupnem evropskem tržišču. To izenačevanje pa ne rešuje bistvenega vprašanja, ki se nujno zastavlja pri varovanju, t.j. dejavnosti, ki še zdaleč ni samo poslovni odnos, marveč zagotavlja uresničevanje ene izmed temeljnih ustavnih pravic in temelji zlasti na osebnem zaupanju. V pogojih svobodnega tržnega gospodarstva, ki je bistveno usmerjeno na ustvarjanje dobička, je zaupanje zelo plaha ptica ali pa neodpustljiva neumnost neizkušenega pogodbenika. Možnost zlorabe zaupnih informacij na pomembnih področjih zaščitenih državnih in gospodarskih skrivnosti, patentov ali drugih oblik intelektualne lastnine, zaradi doseganja lastnih ciljev in koristi izvajalca storitev varovanja, je v takšnih primerih neposredna - ne glede na stopnjo zaupanja in ne glede na dana zagotovila izvajalca zasebnega varovanja.

Ni dvoma, da je mogoče, preverjenemu podjetju z dejavnostjo zasebnega varovanja, zaupati izvajanje osnovnih oblik varovanja z usposobljenimi varnostniki, inženirji in tehniki v primerih in ob pogojih običajnih rizičnih situacij. Povsem nekaj drugega pa je, kadar se srečujemo s primeri posebej občutljivih podatkov in rizikov z izjemno velikimi, mnogokrat celo nepredvidljivimi posledicami. Takšne rizične situacije ne srečujemo le na ravni države, marveč enako v okviru številnih znanstveno raziskovalnih inštitucij ter gospodarstva. Področja inovacij in izumov, razvoja novih tehnologij ali njihovih posodobitev, odkrivanje doslej neznanih naravnih dogajanj in nevarnosti ter možnosti, vključno s čedalje večjim osvajanjem vesolja, so v največjem obsegu strogo varovana skrivnost. Le kanček teh dogajanj in raziskovalnih izsledkov

se bežno dotakne javnosti, največkrat iz določenega razloga in po vnaprej natančno pripravljenem scenariju. Varovanje teh izjemno občutljivih dogajanj in izsledkov je glede na nenehen razvoj in obseg kriminalnega poseganja in prilaščanja podatkov na tem področju prav tako v stalnem razvoju. Nevarnosti se nas v današnjem svetu, ki se je po eni strani s pojavi, kot je t.i. Islamska država, popolnoma neposredno razkril kot grozljivo zločinski in krut, in v katerega po drugi strani človek čedalje globlje posega v njegove neizmerne dimenzije kibernetskega, vesoljskega, podvodnega ali podzemnega prostora, skoraj več ne dotikajo. Sodobni človek je otopel. Giblje se v sferi lastnega interesa. Na rizike, ki ga obkrožajo od vsepovsod, reagira največkrat le, ko je že neposredno ogrožen. Na prizore strahotnih zločinov se komajda odziva.

Svet se je skrčil, odpirajo se popolnoma nove razsežnosti. Rodbinski, gmotni in profesionalni status ter pripadnost določenemu intelektualno in tehnološko razvitemu družbenemu okolju bistveno opredeljujejo današnjega človeka. Nacionalnost in državna pripadnost izgubljata na pomenu. Tisti, ki v tem svetu resnično potrebujejo zahtevne storitve varovanja, poleg osebnega in tehničnega predvsem pa elektronskega in kibernetskega, in imajo v tej zvezi nujne specialne zahteve, ne angažirajo družb za varovanje, kot jih poznamo v evropskem prostoru.

Trg zasebnih varnostnih družb je v največji meri omejen na običajne rizike osebnega varovanja in varovanja premoženja. Visoko izobraženi strokovnjaki in specialisti ter doktorji znanosti s področja varnostnih ved (katerih področje je bistveno širše in zahtevnejše od nalog, ki jih zajemajo veljavni programi usposabljanja in preverjanja varnostnega osebja) so v našem okolju kader, ki že vrsto let le izjemoma najde primerno zaposlitev. Glede na skupno število družb za zasebno varovanje pri nas (144), in v tem okviru posebej glede na število družb za izvajanje tehničnega varovanja (90) in število družb za načrtovanje sistemov tehničnega varovanja (35)[2] lahko ocenimo, da je pri nas v panogi zasebnega varovanja zaposlenih vsega skupaj cca 300 akademsko izobraženih strokovnjakov za izvajanje nalog varovanja. Pri tem je treba upoštevati, da je od navedenega skupnega števila družb in podjetnikov dejansko le manjšina takšnih, ki že tradicionalno, desetletje in dlje, v prevladujočem delu opravljajo dejavnost zasebnega varovanja za naročnike teh storitev na slovenskem tržišču. To, da je konkurenca med temi družbami izjemno ostra in da je kader – predvsem varnostniki kot najštevilčnejši – strokovno minimalno, pogosto tudi nezadovoljivo usposobljen, mnogokrat prekomerno obremenjen, z minimalno plačo in zaposlitvijo le za določen čas, je že dolgo znano. Potreba po takšnem varovanju je podana pri strankah, ki želijo doseči predvsem lastno pokritje v primerih morebitnih škodnih dogodkov. Pogodba za varovanje, sklenjena za najnižjo ceno kot praviloma izključnim kriterijem za izbiro izvajalca, pomeni v teh primerih dejanski dogovor o prenosu odgovornosti zaradi morebitne povzročene škode. S strani naročnika v teh primerih sama kakovost varovanja v resnici sploh ni pomembna. Takšen odnos je prisoten takrat, ko je naročnik – praviloma vodstvo družbe ali inštitucije v neposredni ali posredni državni lasti ali družbi z razpršenim delničarstvom – predvsem zainteresiran, da pokrije lastno odgovornost. Povsem nekaj drugega pa je, ko gre za državni organ, inštitucijo ali podjetje, katerih vodje, lastniki ali sodelavci, na podlagi doseženih izumov in drugih oblik intelektualne lastnine gradijo svoj poslovni uspeh in razvoj ali pa morajo učinkovito zavarovati državno ali poslovno skrivnost. V takšnih primerih je bistvena uspešnost varovanja, saj je kršitev, t.j. odtujitev ali razkritje zavarovane dobrine, praktično nenadomestljiva. Način varovanja takšnih skrivnosti je izziv današnjega časa – pogojno rečeno kibernetske dobe, ki neposredno uveljavlja nujnost takšnih oblik varovanja – in ne pomeni nič drugega kot ustrezno obliko varovanja v okviru samega nosilca skrivnosti – korporativno varovanje. Potrebe po takšnem samo-varovanju so v sedanji dobi, ki je v svojem bistvu razpeta med nenehnim zadrževanjem in uveljavljanjem inovacij, v vzponu, prav posebej v tehnološko najbolj razvitih družbah. Kakovostno, tehnološko in organizacijsko dobro razvito samovarovanje je v današnjem času številnih nepredvidljivih rizikov čedalje pomembnejši pogoj uspešnega varovanja državnih in poslovnih skrivnosti ter ustreznega uveljavljanja načrtovanih ciljev na tem področju.



Trg zasebnih varnostnih družb je v največji meri omejen na običajne rizike osebnega varovanja in varovanja premoženja.

[1] npr. odločitve ES C 114/97, C 355/98, C283/99, C171/02, C 189/03, C 514/03, C 465/05

[2] podatki so povzeti iz preglednice MNZ »Seznam imetnikov licenc« z dne 24.1.2018 ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Upravljanje s tveganji in korporativna varnost

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj Upravljanje s tveganji in korporativna varnost?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

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

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

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

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

CENTER VIŠJIH ŠOL

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

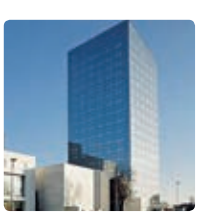
FAKULTETA ZA PODJETNIŠTVO

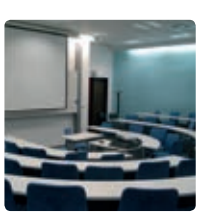
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo



ELES

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.

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

Več kot 2550 km
prenosnega omrežja

Več kot 550
zaposlenih

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

www.eles.si