Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2015, oktober • št. 10



Mednarodna konferenca »Dnevi korporativne varnosti«

Ljubljana, 16-17. marec 2016

Nogomet je kot globalni šport v neposredni soodvisnosti z varnostjo in obvladovanjem tveganj

g. Aleksander Čeferin, predsednik NZS

Nova panorama

družba za integrirano varovanje

www.novapanorama.si

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

IZVIRNA MISEL

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

PRAVA IZBIRA

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

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

GLAVNE DEJAVNOSTI

Poslovno-varnostno svetovanje

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

Integralni varnostni sistemi (celovito varovanje)

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

Varovanje oseb in premoženja

- Varovanje ljudi premoženja
- Prevoz in varovanje denarja ter drugih vrednostnih pošiljk
- Varovanje javnih zbiranj

10 LET ODLIČNOSTI

- Izvajanje sistemov tehničnega varovanja

Kakovost in varnost

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

Krizno vodenje (krizni menedžment)

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

IZOBRAŽEVANJE

Varnostni menedžment

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



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
ICS-Ljubljana

Tisk:
Schwarz print d.o.o.

Datum izida
oktober 2015

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

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

Pred nami stoji 10. številka revije Korporativna varnost, kar vsekakor predstavlja pomemben jubilej in prelomnico v triletnem izhajanju omenjene strokovne revije. Sam razvoj in predvsem pripravljenost avtorjev, da s kvalitetnimi prispevki širijo obzorja na področju korporativne varnosti in preko tega izbranega medija širijo dobre prakse in izkušnje med ciljno skupino bralcev, predstavlja posebno kvaliteto prehojene poti. Tudi odzivi uporabnikov revije so nad vsemi pričakovanji saj z veseljem ugotavljamo, da po reviji in njenih vsebinah posega širši krog bralcev, ki niso ozko omejeni samo na področje korporativne varnosti ter s tem povezanih procesov obvladovanja tveganj, temveč revija v veliko primerih doseže tudi strateški management v organizacijah, ki si revijo vzamejo za svoje redno seznanjanje z novimi pristopi na področju obvladovanja tveganj. Seveda je k temu močno prispevala uredniška politika revije, ki je stalno zagotavljala ustrezno programsko sliko strateških in aktualnih vsebin zanimivih za ta pester nabor bralcev.

Tudi tokratna številka je po vsebini zelo aktualna in se v svojem obsegu dotika zadnjih najbolj perečih dilem in izzivov, ki jih pred nas postavlja moderno varnostno okolje. Posebej bi v tem kontekstu želeli izpostaviti migrantsko krizo s katero se v zadnjem obdobju srečuje Evropa in njene države, med njimi tudi Slovenija. V tokratni številki obravnavamo tudi vlogo strateškega vodstva pri uvajanju ustrezne varnostne kulture v njihove organizacije. Ta primer je še posebej osvetljen skozi nedavno afero »Pirangate« in odtekanja ključnih informacij ter nepopravljivo škodo, ki jo je prineslo pomanjkanje varnostnega zavedanja oz. nizka varnostna kultura zaposlenih v državnih institucijah, kar pa nikakor ne pomeni, da so zasebne gospodarske organizacije v bistveno boljšem stanju. Naslednja pomembna tematika, kateri smo v tej številki namenili pomembno mesto je vsekakor povezana z uporabo brezpilotnih letalnikov in njihove pozitivne in negativne strani uporabe. V mesecu juniju je v organizaciji Instituta za korporativne varnostne študije, ICS-Ljubljana v Državnem svetu Republike Slovenije potekal pomemben nacionalni posvet, kjer so ključni nosilci zakonodajnega urejanja omenjenega področja predstavili načrte in ustrezne poti za učinkovito normativno podlago uporabe brezpilotnih letal, ki so vsekakor izredno uporabna, tudi kot orodje v rokah korporativne varnosti, vendar mora biti ta uporaba ustrezno normativno podprta. Tudi trije intervjuji z vidnimi predstavniki športnega, gospodarskega in izobraževalnega področja prinašajo obilo odličnih priložnosti seznanitve s stanjem v teh sredinah in posredovanja novih idej, katere lahko pripomorejo k večji sinergiji na področju varnosti in s tem učinkovitejših procesov za obvladovanje tveganj. V zaključku pa je potrebno izpostaviti tudi ostale prispevke, ki neposredno bogatijo jubilejno številko in sestavljajo celoto tistega poslanstva, ki ga vseskozi zasledujemo pri tvorjenju programske sheme revije in sicer, da se problematika varnostnih tveganj in dilem odpira z različnih zornih kotov. To nenazadnje odraža tudi osnovno poslanstvo Slovenskega združenja za korporativno varnost, ki predstavlja enega od ključnih bazenov iz katerega prihajajo odlični strokovnjaki in avtorji in se neposredno glasi »Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha«!

V uredništvu revije bomo storili vse, da bo tudi naslednjih deset številk v skladu z vašimi visokimi pričakovanji.

izr. prof. dr. Denis Čaleta
Glavni urednik




INTERVJU

ga. Ksenija Butenko Černe, članica uprave Lek d.d.
mag. Marko Potokar, korporativno varnostni manager

KORPORATIVNA INTEGRITETA IN NJENA VLOGA NA PODROČJU ZAGOTAVLJANJA KORPORATIVNE VARNOSTI 9



INTERVJU
mag. Katja Kraškovic
predsednica uprave GEA College d.d.

PERSPEKTIVE PODJETNIŠKEGA IZOBRAŽEVANJA KOT PODLAGA ZA NOVE RAZVOJNE PRILOŽNOSTI SLOVENIJE 21



DRONI ORODJE ALI NADLOGA?

Eksponenčna rast prodaje dronov za civilno uporabo ter hiter tehnološki razvoj v zadnjh letih napoveduje neslutene možnosti razvoja te nove panoge. Ključna neznanka prihodnosti pa je ravno vidik varnosti, ki zna odločilno vplivati na to, kaj bo v prihodnosti letelo nad našimi glavami. 28



VARNOST MOBILNE TELEFONIJE

Sodobnega življenja si brez mobilnih telefonov praktično ne moremo več predstavljati. Mobilni telefoni nas spremljajo – tudi dobesedno – na vsakem koraku, zato so pomisleki v zvezi z mobilno varnostjo vsekakor na mestu. 36



PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

Institut za korporativne varnostne študije (ICS) je ob soorganizaciji Slovenskega združenja korporativne varnosti in SE European Corporate Security Association (SECSA) v mesecu marcu organiziral tradicionalno mednarodno konferenco z nazivom »Dnevi korporativne varnosti«. Udeležba več kot 120 udeležencev in visokih gostov iz širšega regijskega prostora je ponovno dokazala, da je dogodek nedvomno postal najkvalitetnejši regijski dogodek na področju korporativne varnosti. 54

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



UPRAVLJANJE KONFLIKTA KOT DEL KORPORATIVNE VARNOSTI

V vsaki združbi, kjer se pojavljata vsaj dva posameznika, obstaja možnost konflikta. Živimo v obdobju konfliktov, zato je brezkonfliktna družba iluzija in le želja.

Pojavljanje konfliktov je neizbežno in vsakodnevni pojav v organizaciji. Konflikt ni niti dober, niti slab, naloga vodstva[1] organizacije pa je, da jih skupno z zaposlenimi ustrezno rešuje. Na drugi strani pa je konflikt normalen del zdravih odnosov[2].

Večina resnih konfliktov izvira iz poskusa posameznika, da bi usmerjal mišljenje, spoznanja in vedenje drugega, ki pa tega v skladu s svojo svobodno voljo ne sprejemajo. Ko smo v konfliktu vedno obstaja razlika med tistim, kar bi si posameznik želel in tem, česar je deležen, ne glede na to, kaj stori. Upravljanje konfliktov temelji na teoriji izbire[3], ki omogoča sprejemanje izzivov sodobnega časa ter aktivnejše oblikovanje osebnega in poklicnega življenja. Kako bomo reagirali na dražljaje iz okolja, je odločitev posameznika, ki je za svoje občutke in počutje odgovoren sam. Ne obstajajo psihični in/ali fizični dražljaji, s katerimi bi lahko nadzorovali vedenje drugega. Vsak posameznik prevzema odgovornost za svoja dejanja. Edini, katerega vedenje smo zmožni kontrolirati (pa še to ne vedno), smo mi sami. Vse, kar lahko drugim ponudimo, so informacije. Kaj bodo ali bomo počeli s temi informacijami, pa je stvar izbire.

Konflikti so pogosto težka izkušnja, zato lahko spremenijo naš poslovni in življenjski slog ter dojemanje sveta okoli nas. Prisiljeni smo se namreč neposredno soočiti z drugimi in ponovno opredeliti našo lastno identiteto skozi odnose z ostalimi posamezniki. Konflikti lahko povzročijo, da je med zaposlenimi nezaupanje, želja po maščevanju, sovraštvo ipd. Zaradi negativnega dojemanja drug drugega so aktivnosti bolj

Konflikti so pogosto težka izkušnja, zato lahko spremenijo naš poslovni in življenjski slog ter dojemanje sveta okoli nas.

Pomembno je, da se varnostni managerji naučijo, kako spretno upravljati konflikte, da ti ne škodujejo poslovnim odnosom in varnostnemu sistemu. Za tiste, ki bi konfliktno stanje radi presegli in se iz njih česa naučili, je postalo znanje o reševanju konfliktov zaželena veščina, saj gre za t. i. »mehka znanja«.

kot v uspešno izvrševanje nalog usmerjene v iskanje »zmag« v konfliktih, vse to pa se odraža na manjši poslovni učinkovitosti organizacije. Na drugi strani pa so konflikti pojav, ki jih »pametne organizacije« dojemajo kot možno dodano vrednost in konkurenčno prednost.

Pomembno je, da se varnostni managerji naučijo, kako spretno upravljati konflikte, da ti ne škodujejo poslovnim odnosom in varnostnemu sistemu. Za tiste, ki bi konfliktno stanje radi presegli in se iz njih česa naučili, je postalo znanje o reševanju konfliktov zaželena veščina, saj gre za t. i. »mehka znanja«. Samo znanje pa ni dovolj, ampak je odločilna tudi statusna moč, ki jo posameznik ima. Če je ta moč velika, posameznik (ne)hote vsiljuje svojo voljo drugemu in s tem sproža upor ter konflikte v njem.

Pojem »konflikta« ni strokovno nevtralen, ampak je vrednotno angažiran. Ne gre za katerokoli neskladje človeškega sveta, znotraj katerega razlikujemo posameznike, ki konflikte sprožijo in tiste, ki jih rešujejo[4]. Iršič (2004) opozarja, da je prag zaznavanja konfliktov pri vsakem posamezniku lahko drugačen, vendar pa so reakcije na konflikt podobne.

*avtor je član Slovenskega združenja korporativne varnosti



Pagon (2004) opredeljuje konflikt kot interakcijo soodvisnih posameznikov ali skupin, ki doživljajo nezdružljivost svojih ciljev oziroma oviranje pri doseganju ciljev. Ti posamezniki cilje dojemajo kot nezdružljive oziroma aktivnosti drugih kot oviranje, ne glede na to, ali so te zaznave točne ali ne.

Viri nastanka konfliktov so lahko npr.: različni interesi, zaprta in nejasna komunikacija, razlike med kompetencami posameznikov, različna prepričanja in vrednote, tekmovanje za moč, položaj in priznanje v organizaciji, potrebe po zmanjšanju trenj, prizadevanje za samostojnost, osebno nestrinjanje, različne percepcije posameznikov, nezaupanje ipd.

Dejstvo je, da konfliktov iz vsakdanjega življenja ne moremo odpraviti, zato je toliko bolj pomembno, da jih razumemo, jih znamo sprejemati, obvladovati in upravljati. Konflikte je mogoče razumeti, če preučimo celoten proces posameznega konflikta in vse njegove pomembne faze. V literaturi (npr. Potočan, 2005) različni avtorji omenjajo naslednje faze procesa konflikta:

- faza prikritega konflikta: obstajajo temeljni pogoji za njegov nastanek, vendar konflikt še ni viden in/ali ga udeleženci še ne prepoznavajo,
- faza spoznanja konflikta: udeleženci prepoznajo konfliktno situacijo (in/ali vzroke za njen nastanek oziroma značilnosti konfliktne situacije),
- faza začetka konflikta: nastanejo prve napetosti med udeleženci konflikta, vendar resničnega nasprotovanja med udeleženci še ni
- faza dejanskega konflikta: poteka odkrit spopad mnenj in stališč med udeleženci, njihovo vedenje jasno kaže na obstoj konflikta,
- faza zaključka konflikta: konflikt se reši, kar lahko vodi v ustreznejše prihodnje razumevanje in sodelovanje, in/ali ustavi (oziroma se borba mnenj umiri), kar pa lahko vodi tudi v nastanek novih konfliktov. Proces konflikta vključuje vse navedene faze ali samo nekatere izmed njih.

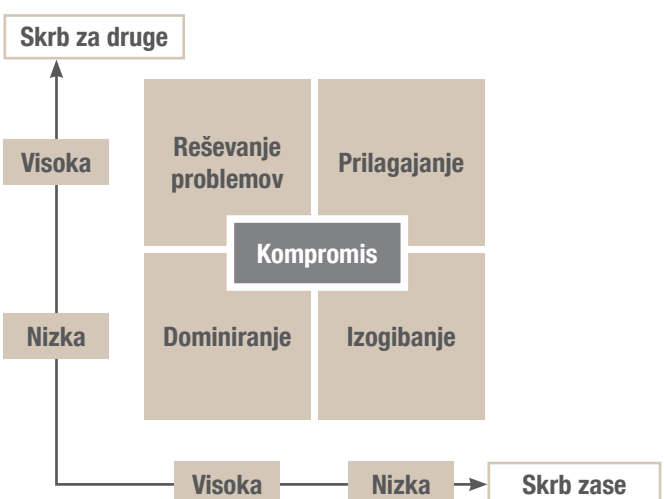
Pagon (2004) loči štiri nivoje konflikta:

- intrapersonalni konflikti se dogajajo v posamezniku, delijo pa se nato na konflikte: (i) privlačenje - privlačenje, med dvema enako privlačnima ciljema; (ii) privlačenje - izogibanje, bolj ko je cilj oddaljen, bolj nas privlači, bliže ko je njegova uresničitev, bolj nas odbija in (iii) izogibanje - izogibanje, med dvema neprivlačnima ciljema,
- interpersonalni konflikti so konflikti med posamezniki, ki se delijo na vsebinske in čustvene. Vsebinski konflikti se dotikajo problematike dela, do njih prihaja ob nestrinjanju glede porazdelitve nalog, načinov opravljanja nalog, ipd., medtem ko do čustvenih konfliktov prihaja zaradi občutkov kot so jeza, razočaranje, strah, ipd. lahko pride tudi do t. i. »trka osebnosti«, pri katerem sta osebnosti dveh posameznikov v interakciji tako različni, da se nikakor ne moreta ujeti in tako tudi ne opravljati skupnih nalog,
- konflikt med skupinami: o tem konfliktu govorimo takrat, ko pride do konflikta med člani ene skupine ali med člani različnih podskupin, znotraj ene skupine, ali pa, ko pride do konflikta med vodjo skupine in posameznikom ali celotno skupino,
- konflikt med skupinami: do tega konflikta pride v primeru konflikta med dvema ali več enotami ali skupinami znotraj organizacije.

Reševanja konfliktov se moramo lotiti čim bolj sistematično, hkrati pa moramo konflikt razrešiti v čim krajšem času. Na splošno so znane tri starejše metode upravljanja s konfliktom (Brajša, 1994):
- »jaz dobivam, ti pa izgubljaš«,
- »ti dobivaš, jaz pa izgubljam«,
- »vsi dobivajo«.

Po metodi »jaz dobivam, ti pa izgubljaš« ustreza rešitev konflikta nam, ne pa tudi drugemu. Rešitev je enostranska, zato jo drugi ne sprejema. V tem primeru prevladuje neenak odnos, saj imamo zmagovalca in poraženca. Po metodi »ti dobivaš, jaz pa izgubljam« ustreza rešitev konflikta drugemu, nam pa ne. V tem primeru drugi dobiva, mi pa izgubljamo. Pri teh dveh metodah gre za zmago in poraz, saj imata obe strani več nasprotujočih si kakor skupnih ciljev. V tem primeru lahko govorimo o vsiljevanju, ne pa o usklajevanju mnenj. Ustrezno je samo tisto ravnanje, ki pripelje do tretje rešitve, še posebej, če je položaj takšen, da »oba dobivata«.

Danes vrednotimo strategije reševanja konfliktov glede na to, v kakšni meri pri tem zadovoljujemo svoja in v kakšni meri stališča (mnenja) nasprotne strani. Strategija reševanja konfliktov je prikazana na spodnji sliki.



Slika: Dvodimenzionalni model stilov reševanja interpersonalnih konfliktov (Rahim, 2002)

REŠEVANJE PROBLEMOV: o tem govorimo takrat, ko kažemo visoko skrb zase in za druge. Strani sta odprti druga do druge in izmenjujeta vse informacije, ki so pomembne, da spoznata, kje so razlike med njima ter na podlagi tega najdeta rešitev v obojestransko korist.

PRILAGAJANJE: pri tem stilu kažemo malo skrbi za sebe in več za nasprotno stran. Uporabljamo ga takrat, ko smo v podrejenem položaju, ko želimo zmanjšati razlike med nami in drugo stranjo, pri čemer je prisoten element samožrtvovanja.

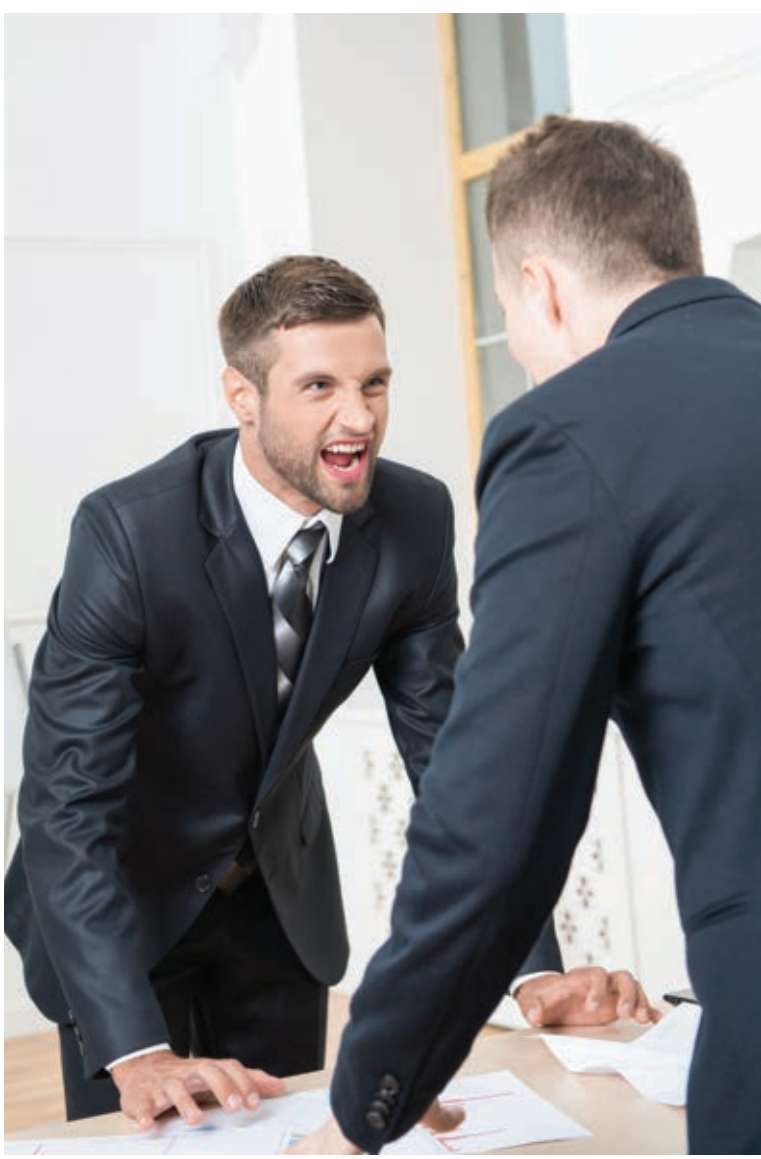
DOMINIRANJE: posameznik rešuje konflikt z veliko skrbi zase in le malo skrbi do drugih. Rezultat uporabe tega stila je, da ena stran dobi vse, druga pa malo ali nič. Dominantni posameznik usmeri napore v to, da doseže svoj cilj, pri čemer se ne ozira na pričakovanja druge strani. Tak stil uporabljamo, ko izkoriščamo moč svojega položaja za pridobitev poslušnosti podrejenih ali takrat, ko svoj položaj zaznavamo kot krivičen in se postavljamo za svoje pravice.

IZOGIBANJE: ko posameznik kaže malo skrbi do sebe in malo skrbi do drugih ter se želi izogniti konfliktu. Ta stil je označen kot izmikanje problemu, preusmerjanje odgovornosti na druge ali pa posameznik ne želi videti, slišati ali govoriti o problemu. Reševanje konfliktov želi preložiti na drug čas ali pa se konfliktu izogne zato, ker se ga boji. S takim stilom ne zadovoljimo svojih, kot tudi ne pričakovanj druge strani.

SKLEPANJE KOMPROMISOV: posameznik, ki uporablja ta stil, je srednje zainteresiran, da bi zadovoljil svoje skrbi, kot tudi skrbi druge strani. To je način sprejemanja dogovora, pri katerem se vsaka stran odpove določenemu delu svojih teženj. Kompromis ne pozna ne zmagovalca in ne poraženca.

Vsaka izbira strategije reševanja konfliktov vodi do sprememb. Spremembe pa v posamezniku povzročajo različne reakcije. Nekateri se spremembam, če je le mogoče, izogibajo in se zato tudi skušajo izogibati konfliktom. Konflikt pa ni rešljiv, če posameznik ni pripravljen sprejeti sprememb.

V zvezi z izbiro strategije reševanja konfliktov se pojavlja več vprašanj: kateri so tisti dejavniki, ki vplivajo na to, da posameznik izbere določeno strategijo, ali posameznik uporablja samo en ali več strategij, ali na izbiro vplivajo značilnosti situacije, v kateri se posameznik znajde in kakšne so osebne posledice uporabe posamezne strategije?



Upravljanje konflikta kot del korporativne varnosti je spretnost, ki se jo je potrebno naučiti, je proces, ki ga je potrebno znati upravljati, vsebina, ki jo je potrebno dobro poznati in dobro razumeti njene okoliščine.

Ovire za konstruktivno reševanje konfliktov so zlasti: napačno razumevanje ali negativen odnos do konflikta, močna čustva, čas, neustrezno komuniciranje, obrambno vedenje, ne znamo se pogajati ipd. Pogoji za konstruktivno reševanje konfliktov se nanašajo na obojestranska pripravljenost sprejemanja novosti, izogibanje ravnanju »zmaga- poraz«, razumevanje narave konflikta ipd.

Upravljanje konflikta kot del korporativne varnosti je spretnost, ki se jo je potrebno naučiti, je proces, ki ga je potrebno znati upravljati, vsebina, ki jo je potrebno dobro poznati in dobro razumeti njene okoliščine.

Na zaključku bralcu priporočam, da razmisli o tem kako bo reševal konflikte v svoji organizaciji (delovni skupini). S skupino se pogovorite o naslednjih vprašanjih:
- kaj je sprejemljivo v primeru konflikta,
- kaj ni sprejemljivo – prepovedi,
- kakšen način govora in višino glasu bi morali uporabljati,
- kako bomo poslušali drug drugega,
- kako je s čustveno vsebino sporočil,
- koga lahko še dodatno vključimo v reševanje konflikta.



Več o tej temi bo predstavljeno na naslednji mednarodni konferenci o korporativni varnosti leta 2016.

[1] Več avtorjev navaja (npr. De Dreu, 2001), da managerji porabijo 20% svojega časa za reševanje konfliktov. Čeprav 20% »izgubljenega« časa predstavlja visok strošek, je ta zanemarljiv v primerjavi s stroški, ki jih lahko povzročijo konflikti, katere obvladujejo čustva in ne več razum.

[2] Konflikti lahko prispevajo vrsto pozitivnih posledic, saj pripomorejo, da spodbujajo spremembe in razbijajo monotonijo, zagotavljajo ustreznejše vsebinske rešitve, prispevajo k poglabljanju razumevanja sveta in življenja, omogočajo bolj intenzivno sodelovanje, omogočajo večje zaupanje, tako sebi kot drugemu.

[3] Teorija izbire trdi, da izbiramo prav vse, vključno z nezadovoljstvom ob konfliktu, za svoja ravnanja pa moramo sprejeti odgovornost. Drugi nas ne morejo niti osrečiti niti onesrečiti, posredujejo nam le informacije, a nas ne morejo pripraviti do tega, da bi nekaj naredili ali občutili. Naši možgani so tisti, ki odločajo, kaj bomo.

[4] Bolj ko nam je pomembna vrednota, ki jo neskladje dražljajske situacije zadeva, intenzivnejša so čustva in bolj smo čustveno odvisni od izida upravljanja s konfliktom. Čustva lahko izrinemo iz zavesti ali jih zadušimo. Lahko jih pa tudi nenadzorovano izrazimo, takrat čustvo usmerja vedenje mimo naše volje, zato nam je pozneje marsikdaj žal, da smo se tako odzvali. ■

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
ga. Ksenija Butenko Černe, članica uprave Lek d.d.
mag. Marko Potokar, korporativno varnostni manager

KORPORATIVNA INTEGRITETA IN NJENA VLOGA NA PODROČJU ZAGOTAVLJANJA KORPORATIVNE VARNOSTI

Gospodarske družbe, ki pri svojih standardih poslovanja ohranjajo visoko stopnjo etike in morale, lahko dolgoročno krepijo svoj ugled in zaupanje v svoje delo ter ohranjajo konkurenčnost, pozitivno poslovanje in s tem tudi delovna mesta.

Lek d.d. kot del mednarodne korporacije Novartis predstavlja eno od najpomembnejših farmacevtskih podjetij v regiji JV Evrope. Med drugim ste tudi nosilci naziva »Ambasador korporativne integritete«. Nam lahko prosim pojasnite točen pomen termina »korporativna integriteta«?

(ga. Butenko Černe) Ko se podjetje oziroma vodstvo v podjetju zave, da je korporativna integriteta edina prava pot za trajnostni razvoj podjetja in za dolgoročno poslovno uspešnost, za zadovoljstvo zaposlenih, strank in poslovnih partnerjev, je to prvi korak na poti korporativne integritete. V Leku, članu skupine Sandoz, kot delu Novartisa posvečamo zelo velik pomen korporativni integriteti. Razumemo jo zelo široko, veliko več kot le izpolnjevanje zakonskih določil, uredb in pravil. Razumemo jo kot kulturo, ki se prepleta v vse pore našega delovanja. Zato etično in odgovorno odločanje bistveno vpliva na to, kako razmišljamo in poslujemo. Zavedamo se namreč, da le gospodarske družbe, ki pri svojih standardih poslovanja ohranjajo visoko stopnjo etike in morale, lahko dolgoročno krepijo svoj ugled in zaupanje v svoje delo ter ohranjajo konkurenčnost, pozitivno poslovanje in s tem tudi delovna mesta.

> Zavedati se moramo, da poslovanje z integriteto ni le narediti tisto, kar je pravilno in zakonsko skladno, ampak tudi tisto, kar je prav in etično.

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 Lek d.d.?

(ga. Butenko Černe) Pomembno je, da je v podjetju vzpostavljen celoten sistem, ki gradi korporativno integriteto in organizacijsko kulturo, ki temelji na etičnem delovanju vseh sodelavk in sodelavcev. Zavedati se moramo, da poslovanje z integriteto ni le narediti tisto, kar je pravilno in zakonsko skladno, ampak tudi tisto, kar je prav in etično.

Področje upravljanja integritete in skladnosti v skupini Novartis zagotavlja učinkovit program integritete in skladnosti, ki podpira vodstvo pri vzpostavitvi, vključitvi in uveljavljanju standardov integritete. Poteka v treh korakih: vzpostavitev sistema, vključitev v sistem in uveljavljanje.

Pri vzpostavitvi sistema smo v Novartisu določili interne standarde s Kodeksom ravnanja in raznimi, iz Kodeksa izhajajočimi politikami ter smernicami, ki ureja-

*avtor je član Slovenskega združenja korporativne varnosti



jo posamezna področja našega etičnega poslovanja. V fazi vključevanja v sistem gre za spodbujanje vodenja z zgledom, izobraževanje in seznanjanje sodelavcev z načeli delovanja z integriteto ter določanje ciljev v skladu z zastavljenimi standardi in vrednotami. Pri uveljavljanju pa preverjamo skladnost s standardi in sistemi internih kontrol, ustrezno upravljamo morebitna poročila o kršitvah ter spremljamo celovito izvajanje programa integritete in skladnosti.

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?

(ga. Butenko Černe) Pri gradnji organizacijske kulture, ki temelji na etičnem delovanju vseh sodelavk in sodelavcev, v Leku stalno poudarjamo, da je skladnost z Novartisovimi vrednotami in standardi osebna odgovornost vsakega sodelavca – in ne more biti delegirana. Odgovorno odločanje je zagotovljeno skozi kulturo integritete, ki temelji na etičnem vodenju in vključitvi etičnih elementov v procese sprejemanja odločitev.

Naš odnos do življenja, družine in prijateljev, do dela in sodelavcev v veliki meri uokvirjajo naše osebnostne lastnosti. Kultura, ki jo gradimo v delovnem okolju, in izobraževanja, ki jih izvajamo, pa pomagajo ta naš odnos utrditi in nas dodatno usmerjati. Zato veliko energije vlagamo tudi v izobraževanja o skladnosti, saj predstavljajo odlično priložnost, da sodelavcem z različnimi konkretnimi primeri prikažemo, katera so neskladna ravnanja, kako se pravilno in pravočasno odzovemo in kako lahko preprečimo ravnanja, ki bi lahko omajala ugled naše družbe ali posameznikov. Pri tem želimo, da zaposleni vedo, da se lahko vedno obrnejo na nas, na skrbnike za skladnost, s kakršnimikoli vprašanji ali dvomi. S tem, ko bomo znali pravilno zaznavati dogajanje okoli nas in delovati preventivno, smo naredili ključen korak na poti skladnega ravnanja.

Kako v vašem podjetju povezujete procese korporativne integritete s korporativno varnostjo in celovitim obvladovanjem varnostnih tveganj?

(ga. Butenko Černe) Kot rečeno v Leku, članu skupine Sandoz, korporativno integriteto razumemo široko. Poleg izpolnjevanja zakonskih določil in pravil ter delovanja v skladu z etičnimi načeli, je del korporativne integritete tudi organizacijska in varnostna kultura podjetja. Tako so procesi korporativne integritete in korporativne varnosti v določenih delih vsebinsko in postopkovno prepleteni. V primeru odstopov oziroma neskladnih ravnanj, pa naj gre za primere kršenja etičnih kodeksov, notranjih pravil podjetja ali za sume storitev kaznivih dejanj, se aktivirata tako skrbnica za skladnost ravnanj (ki sodeluje z nadzornikom poslovnih praks (angl.: *BPO - Bussiness Practice Officer*), kot varnostna služba, ki po potrebi skupaj vodita preiskavo. V določenih primerih se v postopke vključijo tudi druge funkcije, v večini primerov kadrovska služba ali pravna pisarna.

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?

(ga. Butenko Černe) Pri področju upravljanja integritete in skladnosti je zelo pomembno spodbujanje vodenja z

zgledom. Zato vodjem namenjamo še posebej veliko pozornosti. V prvi vrsti so pomembna izobraževanja, kjer jim med drugim pomagamo tudi s smernicami, kako s svojimi sodelavci komunicirati o korporativni integriteti, kako jih k temu spodbujati, kako vključiti razmišljanje o etičnem in odgovornem delovanju v vsakdanjik vsakega zaposlenega. Vedno so jim na voljo tudi različna orodja in gradiva, ki jih lahko uporabijo pri svojem delu, ko s svojimi sodelavci govorijo o korporativni integriteti. Delovanje z integriteto, kot ena izmed ključnih Novartisovih vrednot, predstavlja del ciljev in uspešnosti vseh sodelavcev, in je vključeno v letne razgovore zaposlenih, tudi vodij, kar pomembno prispeva k razumevanju korporativne integritete kot resnično pomembnega dejavnika dela in uspešnosti delovanja vsakega zaposlenega.

Farmacevtska dejavnost je sama po sebi povezana z nizom tveganj, ki imajo lahko negativni vpliv pri zagotavljanju neprekinjenosti delovanja glavnih poslovnih procesov. Ali v podjetju Lek d.d. zagotavljanju varnosti in s tem povezanemu obvladovanju tveganj posvečate dovolj veliko pozornost?

(mag. Marko Potokar) V skupini Novartis in njenih članicah je varnost ena izmed glavnih vrednot. Tako korporativna varnost 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 itd. Za zagotavljanje normativne urejenosti varnostnega sistema ter ustreznega fizičnega in tehničnega varovanja je v Leku, članu skupine Sandoz, vzpostavljena lokalna varnostna funkcija, ki po organizacijski shemi odgovarja vodstvu podjetja, po funkcijski liniji pa varnostni funkciji na nivoju Novartisa. V skladu z Novartisovo varnostno politiko smo za zagotavljanje varnosti odgovorni vsi sodelavci predvsem tudi v smislu preventivnega delovanja in ravnanja z zgledom. Ljudje smo namreč temeljni del varnostnega sistema in tisti, ki na koncu zagotavljamo njegov uspeh. To zavedanje je pri izgradnji varnostne kulture ključno, zato je ena glavnih funkcij varovanja tudi ozaveščanje in izobraževanje o pomenu etičnega ravnanja, ki je skladno z Novartisovim kodeksom ravnanja.

mag. Marko Potokar: V skupini Novartis in njenih članicah je varnost ena izmed glavnih vrednot. Tako korporativna varnost 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 itd.



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 primeru podjetja Lek d.d.?

(mag. Marko Potokar) Kot sem že omenil, je v Leku vzpostavljena varnostna funkcija, ki po organizacijski shemi odgovarja vodstvu podjetja, po funkcijski liniji pa varnostni funkciji na nivoju Novartisa. Organizacijsko je tako varnostna funkcija v Leku konkretizirana v oddelku Varovanje, ki sodi v Upravljanje nepremičnin in storitev, ki je del divizije Novartisove poslovne storitve. V teku je tudi vsebinska reorganizacija varnostne funkcije na globalno in lokalno. Globalni del naj bi tako pokrival področje globalne varnostne strategije, preiskave poneverb in goljufij, varovanje izdelkov, preiskave odstopov in varovanje članov upravnega odbora. Pristojnosti drugega dela varnostne funkcije pa naj bi bile varovanja posameznih lokacij korporacije ter varovanje ljudi in premoženja, upoštevajoč specifične razmere, značilne za posamezna področja.

Nam lahko prosim pojasnite, katera področja spadajo v okvir vaših pristojnosti in ali je področje informacijske varnosti tudi del vaših pristojnosti?

(mag. Marko Potokar) Ključna naloga varnostne funkcije je upravljanje varnostnega sistema in s tem obvladovanje varnostnih tveganj na področju zaščite ljudi in premoženja. Izvajanje varnostne funkcije obsega razvoj in implementacijo učinkovitega sistema varovanja v skladu z zakonodajo Republike Slovenije in standardi podjetja, zagotavljanje in izvajanje vsebine varnostnih načrtov z



vsemi spremnimi dokumenti, skladno s politiko varovanja družbe, pripravo akcijskih načrtov za primere izrednih dogodkov oz. primere dogodkov povečanega tveganja ter aktiviranje in delovanje v okviru kriznega upravljanja. S ciljem izvajanja politike varovanja in zagotavljanja sistema varovanja smo odgovorni tudi za koordinacijo zunanje službe, zadolžene za fizično in tehnično varovanje, ter vodenje, organizacijo in nadzor nad tehničnimi sistemi varovanja. Pomemben del nalog varnostne funkcije zajema tudi svetovanje s področja varnosti in samozaščite za zaposlene, izobraževanje sodelavcev v smislu prepoznavanja in ustreznega ravnanja v primerih izrednih dogodkov ali neprimernih ravnanj, ozaveščanje zaposlenih s pomočjo različnih komunikacijskih kanalov (intranet, prispevki v internem glasilu itd.), kar vse pomembno prispeva k stalni krepitvi poslovne kulture podjetja in zaposlenih. Izvajamo tudi notranje preiskave v primeru odstopov oz. sumov storitve kaznivih dejanj, pri čemer interno tesno sodelujemo s skrbnico za skladnost ravnanj, pa tudi uradnimi organi.

Področje informacijske varnosti je v Novartisu in Leku del funkcije Upravljanja z informacijami v okviru Informacijske tehnologije oz. t.i. *IGM (Information Governance Management)*, s katero prav tako tesno sodelujemo.

Kot del Novartisa ste verjetno vpeti v sistem jasno predpisanih varnostnih standardov in določil krovne varnostne politike. Je v vašem primeru koordinacija delovanja in usmerjanje za zagotavljanje obvladovanja varnostnih tveganj strokovno vodeno iz nivoja Novartis ali ima strateško vodstvo vaše organizacije tukaj neposredne pristojnosti in seveda odgovornosti za uveljavljanje varnostne politike v Lek d.d.?

(mag. Marko Potokar) Novartisova varnostna politika je krovni varnostni dokument, ki opredeljuje poslanstvo varnostne funkcije v zagotavljanju zaščite ljudi in intelektualnega ter fizičnega premoženja organizacije. Pri tem varnostna funkcija deluje družbeno odgovorno in ravna v skladu z etičnimi načeli korporacije Novartis. Vsaka članica skupine Novartis, med njimi tudi Lek d.d., je dolžna uvesti in upoštevati predpisano krovno varnostno politiko in jo prilagoditi zahtevam lokalne zakonodaje, kjer so morda zahteve še strožje. Na lokalni ravni se varnostna politika izvaja skozi varnostni program in predpisane postopke, ki opredeljujejo delovanje lokalnega varnostnega sistema. Pristojnosti in odgovornosti za upravljanje varnostnih tveganj so tako na strani globalnega vodstva, kot predpisovalca globalne varnostne politike, kakor tudi na strani vodstva Lek d.d., kot člana divizije Sandoz.

Glede na dejstvo, da dobro poznate delovanje Slovenskega združenja za korporativno varnost, ali menite, da lahko družba Lek d.d. z vstopom v to asociacijo pridobi ustrezno okolje za izmenjavo dobrih praks in novih spoznanj na področju korporativne varnosti?

(mag. Marko Potokar) Povezovanje in sodelovanje strokovnjakov z določenega področja zagotavlja prenašanje in izmenjavo izkušenj ter dobrih praks iz različnih okolij. Slovensko združenje za korporativno varnost predstavlja praktično edino strokovno združenje s področja korporativnega varovanja v Sloveniji. Kot nekdanji predstavnik mojih prejšnjih delodajalcev v navedenem združenju, lahko samo potrdim dobre izkušnje in koristi delovanja v okviru članstva. V združenju so namreč zbrani strokovnjaki, ki s svojim znanjem, tako strokovnim, kot raziskovalnim in pedagoškim, prispevajo k razvoju in izboljševanju korporativnega varnostnega okolja in kulture korporativne integritete v organizacijah. ■



Slovensko združenje korporativne varnosti

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



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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

Članstvo v SLOVENSKEM ZDRUŽENJU KORPORATIVNE VARNOSTI vam olajša obvladovanje tveganj v vaših organizacijskih sredinah. **SKUPAJ SMO MOČNEJŠI!**

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

Ugodnosti za člane združenja:

- brezplačna udeležba na rednih strokovnih srečanjih;
- popusti pri nakupu izdanih publikacij ICS, Ljubljana;
- popusti pri udeležbah na konferencah, posvetih in drugih dogodkih v organizaciji ICS, Ljubljana;
- popusti pri članarinah za zaposlene, ki prihajajo iz vrst včlanjenih organizacij.
- brezplačna naročnina na revijo Korporativna varnost;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS-Ljubljana

ELES · triglav · NZS · Elita i.b. d.o.o. · Mariborski vodovod · energetika ljubljana · hse Holding Slovenske elektrarne d.o.o. · Kontrola zračnega prometa Slovenije · Luka Koper Port of Koper · IMP d.d. · Republika Slovenija IMP · REISSWOLF secret. service. · Zanesljivo vsepovsod Pošta Slovenije · interblock luxury gaming products · SIEMENS · TelekomSlovenije · DARS · Nova KBM pripravljeni na jutri · univerzitetni klinični center ljubljana · gorenjegroup · si-cert · Informacijski pooblaščenec

www.ics-institut.si

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

INTERVJU
g. Aleksander Čeferin
predsednik Nogometne zveze Slovenije

NOGOMET JE KOT GLOBALNI ŠPORT V NEPOSREDNI SOODVISNOSTI Z VARNOSTJO IN OBVLADOVANJEM TVEGANJ

Nogomet je zaradi svoje globalnosti in razširjenosti neposredno tesno povezan z varnostjo. Novi pristopi in trendi obvladovanja tveganj na športnih prireditvah so ena izmed prioritet krovne nogometne organizacije. Nogometna zveza Slovenije na tem področju predstavlja pomemben primer ostalim športnim organizacijam in zvezam pri zavedanju o pomenu varnosti za učinkovito izvajanje svojega poslanstva.

Pred kratkim ste nastopili svoj drugi mandat na čelu Nogometne zveze Slovenije. Nogomet je globalni šport, zato ima v družbenem okolju poseben pomen. Nam lahko razložite kako zahtevno je voditi tako kompleksno športno organizacijo.

Predvsem je tako veliko in kompleksno organizacijo težje voditi, kot sem si predstavljal. Mislil sem, da je to športna organizacija, ki zahteva občasno prisotnost. Gre pa za pravzaprav resno podjetje. Čeprav je NZS formalno organizirana kot društvo, gre pri vodenju te organizacije za zelo odgovorno delo, ki zame predstavlja še eno službo. Seveda pa je kljub zahtevnosti voditi največjo športno zvezo v Sloveniji to delo tudi zelo zanimivo. Morate vedeti, da sta naša partnerja Evropska nogometna zveza (UEFA) in Svetovna nogometna zveza (FIFA) s proračunom nekaj milijard evrov, organizirani na nivoju multinacionalk. Tudi NZS ni nepomembna po svojem obsegu, saj ima 48.000 registriranih nogometašev oz. toliko članov. Nogomet je namreč globalni šport, ki lahko sproža velike strasti, pomembno pa vpliva tudi na politiko, varnost in druga področja družbenega življenja. Voditi tako organizacijo je pravzaprav zelo velika odgovornost, ki pa je z mačehovskim odnosom države do nogometa, še zahtevnejše. Država nogometu ne pomaga praktično nič, čeprav je praksa v večini drugih držav popolnoma drugačna. V bližnji prihodnosti bomo zgradili reprezentančni trening center na Brdu pri Kranju, kjer država na žalost ni prispevala niti enega evra. Za razliko od kašnih drugih objektov, ki so mnogo manj zasedeni, zgrajeni za manj globalne športe, pa so jih v celoti zgradili z državnim denarjem. Slovenci smo marginalizirali nogomet v bivši državi, verjetno tudi zaradi stališča ostalih, da nismo nogometni narod. Smo pa že večkrat pokazali, da ta stereotip ne drži. Resno mislim, da je prišel čas, ko se bo morala na tem področju zakonodaja drastično spremeniti. Naj omenim samo zadnja primera, katera sta posredno povezana tudi z varnostjo in sicer nogometni tekmi Slovenija : Anglija ali pa Maribor : Chelsea, ki jih državne institucije niso uvrstile v veliki prireditvi mednarodnega pomena. Na drugi strani pa sta Maraton Franja, ki je kolesarski maraton za rekreativce, ali pa Zlata lisica, prireditve, ki sodita v ka-

*avtor je član Slovenskega združenja korporativne varnosti

tegorijo večjih mednarodnih dogodkov. Zakaj je to tako pomembno, kar kaže na nerazumevanje pomena nogometa, kot globalnega športa. Poleg navedenega pa to NZS ter klubom povzroča nerazumno velike stroške, ki jih moramo plačati za angažiranje policije in drugih državnih institucij, ki s svojim poslanstvom zagotavljajo javno varnost in znesejo 20 do 25 tisoč evrov za tak dogodek.

Katera so osnovna težišča vašega drugega mandata na čelu nogometne organizacije?

Vedno poudarjam, da nogomet ni samo A reprezentanca, nogomet niso samo profesionalci. Naše poslanstvo mora biti, da se čim več otrok ukvarja z nogometom, da otroci niso prepuščeni cesti in kriminalu, drogi ali alkoholu. Želimo, da so zdravi, da živijo s športom, da prevzamejo vrednote, ki jih imamo mi, saj tudi sebe smatram za športnika. Najbolj je pomembna množičnost. Kaj pa je pogoj za množičnost? Eden od osnovnih pogojev je sigurno dobra igra A reprezentance. Poglejmo iz večih vidikov primer nogometne šole, ki bo ustvarjala vrhunske igralce. Prvič ti otroci, ki igrajo nogomet, morajo imeti vzornike, morajo videti dobre nogometaše, sicer jih nogomet ne bo zanimal. Drugič pa je otroški oz. mladinski nogomet, predvsem seveda otroški, skoraj v celoti breme staršev. In to je vse večji problem. Zato bo potrebno najti sredstva, vsaj za infrastrukturo, kar tudi delamo. Če povzamem, potrebno bo izboljšati infrastrukturo, hkrati pa dvigniti popularnost nogometa v Sloveniji, kar bo pomenilo tudi večji obisk na stadionih. Lahko vam povem, da imamo primerjalno glede na lansko leto v 1. ligi 40 % večjo obiskanost tekem in preko 100% večjo gledanost na televiziji. To, da nogometna popularnost raste, pomeni posledično možnost pridobitve višjih sredstev, ki jih moramo v nadaljevanju vložiti v mlade selekcije. Če pa se dotaknem še področja varnosti je pomembno zagotoviti da se bo vsak, ki pride na nogometno tekmo katerega koli nivoja, počutil varnega. To pomeni, da bo lahko prišel na tekmo z otroci in ga ne bo strah kateregakoli derbija, pobesnelih navijačev ali drugih izgredov. Mislim, da se stvari obračajo v pozitivno smer, seveda pa se stvari spreminjajo in je treba biti ves čas pozoren. Namreč če počivaš na lovorikah, se ti to lahko hitro maščuje.

Pomembno, da ustvarimo varno okolje, v katerem se bodo vsi udeleženci počutili varno. Po moji oceni pa varnost ni pomembna samo s tega vidika, ampak tudi z vidika »splošne slike« nogometa.

Varnosti v nogometu v svojem programu posvečate eno od težiščnih poudarkov. Nam lahko zaupate osnovne načrte na tem področju.

Pomembno, da ustvarimo varno okolje, v katerem se bodo vsi udeleženci počutili varno. Po moji oceni pa varnost ni pomembna samo s tega vidika, ampak tudi z vidika »splošne slike« nogometa. Če nogometu ne pripisujemo podobe nasilja, potem je to dobro tako za pridobitev sponzorjev, kot tudi npr. za povezovanje s humanitarnimi organizacijami in drugimi smermi promocije predvsem med mladimi. Trdim, da tako v Sloveniji kot po Evropi nogomet ni šport, ki bi privlačil ljudi, ki želijo na tekmah gledati nasilje. Nogomet je zelo spremenil svojo podobo in naša naloga je, da temu tren-





du sledimo. To pomeni, da bo celotna družina prihajala na tekme in bo z nogometom preživela lep nedeljski dogodek, pa naj si gre za prvo ali peto ligo.

Ali lahko podate osnovno oceno kakšen del proračuna NZS je namenjen za zagotavljanje varnosti na tekmah, ki jih igra naša A reprezentanca?

Po zadnjem pregledu nekje med tremi in petimi odstotki proračuna, kar se mi osebno ne zdi malo. Je pa res, da v kolikor bi uspeli doseči spremembo zakona o športu, nov je namreč ravno v pripravi, in bi lahko na mednarodnih tekmah imeli status velike mednarodne športne prireditve, bi lahko mnogo tega denarja prihranili saj nam ne bi bilo potrebno plačevati asistence policiji. v tem primeru bi prihranke lahko investirali v varnost na drugih področjih, ki nujno potrebujejo povečanje finančnih sredstev.

V zadnjem obdobju je bilo predvsem v regiji ponovno zaznati nekaj odmevnih ekscesnih primerov nestrpnosti na nogometnih prireditvah. Ali ta problem navijaške nestrpnosti zaznavate tudi v slovenskem okolju?

Nestrpnost, ne samo navijaško, je zaznati povsod. Slovenija je glede na področje nekdanje Jugoslavije še vedno prava oaza. Mi imamo manj težav z navijači, manj nasilja, manj nestrpnosti kot mnogo drugih evropskih držav. Hkrati pa imamo veliko prednost, ker smo del tega področja in dobro poznamo mentaliteto ostalih. V Srbiji imajo izjemne težave z varnostjo, prav tako v Makedoniji, BiH in Črni Gori, na Hrvaškem pa je to povezano še s pojavom politične nestrpnosti. Menim, da smo lahko dober primer oz. zgled drugim in to se zavedata tako UEFA kot FIFA. Smo popolnoma drugačni in na to sem ponosen. To seveda ni moja zasluga, se pa tudi na NZS trudimo, da se stvari na tem področju še izboljšajo. Smo očitno malo drugačen narod.

Pomembna je preventiva in ker mi sami nimamo dovolj znanja, da bi to lahko obvladovali sami, je vključitev v Slovensko združenje korporativne varnosti absolutno dobra ideja.

Lahko Slovenija s svojim položajem in ugledom v evropski in svetovni nogometni organizaciji pripomore k izboljšanju stanja na področju varnosti na nogometnih prireditvah v Balkanski regiji?

Absolutno. Tako UEFA kot FIFA sta nam že dali iniciativo, da bi mi prevzeli vodilno vlogo na tem področju. Balkan je zelo problematičen na področju varnosti, strasti so hude, hitro pride do incidentov, največ težav v tej regiji je bilo ob igranju reprezentanc. Tako, da so nas v zvezi s tem že angažirali in mislim, da lahko ključno pomagamo pri urejanju stvari.

Velik problem pri doseganju ustrezne varnosti oz. celovitega pristopa do obvladovanja varnostnih tveganj na nacionalni in še posebej klubski ravni predstavlja pomanjkanje kadrovskih in finančnih virov. Kako lahko NZS preko ustreznih sprejetih varnostnih standardov zagotavlja dvig ravni varnosti v tekmovanjih, ki se izvajajo pod njenim okriljem? Kako je v tem okviru s sredstvi UEFE?

Ja, tako kot ste rekli, v klubih denarja ni. Mi jim lahko predpisujemo še tako visoke varnostne standarde, vendar bo v tem primeru kar nekaj klubov zaprlo svoja

vrata. Mi pač moramo biti do neke mere permisivni, predvsem zato, ker ni hudih nevarnosti na naših stadionih. NZS se trudi pomagat klubom z izobraževanji, tukaj je pomembno delo komisije za varnost. Na zvezi imamo vodjo varnosti, ki vsako prvenstveno kolo obišče in pomaga pri organizaciji tistih tekem, ki so potencialno najbolj rizične.

Tako FIFA kot UEFA varnosti posvečata zelo veliko pozornosti, zato tudi obstajajo določena sredstva. UEFA je po tej plati črpanja sredstev malce podobna Evropski uniji. Prepričan sem, da je NZS sposobna od UEFE dobiti sredstva za povečanje varnosti. Namreč finančna sredstva so na voljo, moraš pa imeti dobro idejo, pokazati iniciativo in dobro predstaviti projekt. Na UEFI namenjajo ogromna sredstva za varnost. Če ne bomo aktivni in bomo zasledovali samo svoje interese, potem pač iz tega ne bo nič. NZS ima na tem področju kar velike načrte.

Za zavedanje pomena varnosti in tolerantnosti na in ob nogometnih igriščih je odločilen segment zgodnjega osveščanja in vzgoja mladih nogometašev in tudi njihovih staršev. Menite, da je tukaj možno narediti še kakšen korak naprej, predvsem v povezovanju s posameznimi znanstvenimi in nevladnimi organizacijami s področja varnosti?

Seveda, veliko korakov je možno narediti. Mi si ne delamo utvar, da smo stvari uredili , seveda je treba začeti pri otrocih, pri najmlajših. Je pa kot veste večji problem s starši in izobraževati bi bilo treba tudi starše. Večkrat vidiš na tekmi, kako oče desetletnika lovi drugega očeta zaradi enega prekrška in to predstavlja zelo slab zgled. Na tem področju mislim, da imamo še veliko stvari odprtih. To pomeni, da moramo še veliko postoriti in se povezovati. Na tem področju obstaja še ogromno polje, kjer se da stvari izboljšati. To ne zahteva veliko sredstev. V takih zadevah bi bili pripravljeni sodelovati tudi nogometaši A reprezentance, ki so med drugim izjemno humanitarno usmerjeni. Mislim, da imamo na tem področju še veliko rezerve.

Slovensko združenje za korporativno varnost predstavlja eminentno združbo organizacij in posameznikov s področja varnosti. Menite, da bi lahko NZS s svojo priključitvijo tej asociaciji postavila dober primer, kako se vodilna športna zveza zaveda pomena varnosti in na drugi strani pridobi možnost seznanjanja z dobrimi praksami in najnovejšimi spoznanji na področju varnosti?

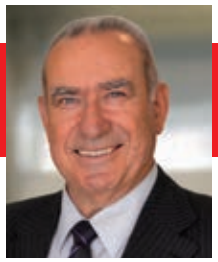
Mnenja sem, da bi bila lahko tovrstna vključitev zelo koristna. Ne samo, da se mi lahko učimo od drugih, ki so že del te asociacije, temveč se lahko tudi drugi naučijo kaj od nas. Prav bi bilo, da se varnost ne uveljavlja samo z represivnimi mehanizmi. Pomembna je preventiva in ker mi sami nimamo vsega znanja, da bi to obvladovali sami, je vključitev v Slovensko združenje korporativne varnosti absolutno dobra ideja. Je pa res da športne organizacije, po mojem mnenju, o tej možnosti nismo kaj dosti obveščene. Če se midva ne bi spoznala preko nogometa, ne bi vedel za delovanje te asociacije in možnosti, ki jih ponuja.

> Vključitev NZS bo dober primer tudi za druge športne zveze.

Drugače pa moram poudariti, da ima NZS podpisan sporazum o sodelovanju s policijo. Tudi to se mi zdi pomembno. Seveda pa to predstavlja drugačen okvir kot članstvo v Slovenskem združenju korporativne varnosti. ■



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





UPRAVLJANJE IN VAROVANJE POSLOVNE DOKUMENTACIJE, DOKUMENTARNEGA IN ARHIVSKEGA GRADIVA TER ARHIVOV

Upravljanje in varovanje poslovne dokumentacije, dokumentarnega in arhivskega gradiva ter arhivov je v bistvu sestavni del celovitega varovanja (korporativne varnosti) organizacije (gospodarske družbe, javnega podjetja, zavoda, državnega organa in drugih), v kateri je varovanje in zaščita osebnih in tajnih podatkov, informacij, elektronskih in drugih komunikacij ter poslovnih skrivnosti pomemben del korporativne varnosti.

V splošnem upravljanje arhivov pomeni skrbno, profesionalno in kakovostno ravnanje s poslovno dokumentacijo, z dokumentarnim in arhivskim gradivom ter z arhivi, varovanje arhivov pa izbira ustreznih prostorov, vzpostavitev zahtevanih pogojev hrambe ter vzpostavitev sistema materialnega varstva to je fizičnega in tehničnega varovanja objekta, prostorov, opreme in arhivskega gradiva. Da je varovanje arhivov zares pomembna kategorija korporativne varnosti je razvidno iz Priporočil Sveta Evrope o prednostnih dejavnostih za večje sodelovanje na področju upravljanja in varovanja arhivov v Evropi (*2005/835/ES, z dne 14. 11. 2005*). Gre za varovanje in preprečevanje poškodb arhivskega gradiva v Evropi, za sprejetje ukrepov za preprečevanje kraje arhivskega gradiva ter za druge ukrepe, ki vnašajo najboljše prakse v sisteme upravljanja in varovanja dokumentarnega in arhivskega gradiva ter arhivov. Upoštevajoč pravno podlago in standarde je upravljanje in varovanje arhivov obvezno v vsaki organizaciji, ki se začne z oceno ogroženosti in tveganj, s sprejetjem varnostne politike in vzpostavitvijo celovitega sistema fizičnega, tehničnega, požarnega, proti kriminalnega varovanja in varovanja pred naravnimi nesrečami. V tem okviru gre tudi za vzpostavitev varnostnega managementa arhivov, ki je v praksi upravljanja z arhivi še zelo šibak.

Pravna podlaga

Upravljanje in varovanje arhivskega gradiva ima kar solidno pravno podlago. Imamo krovni zakon in vrsto podzakonskih predpisov kot npr.:

- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih.
- Uredba o varstvu dokumentarnega in arhivskega gradiva.
- Pravilnik o strokovni usposobljenosti uslužbencev javnopravnih oseb ter delavcev ponudnikov storitev, ki delajo z dokumentarnim gradivom.
- Pravilnik o določanju rokov hranjenja dokumentarnega gradiva v javni upravi.
- Pravilnik o strokovnih izpitih na področju varstva kulturne dediščine in varstva arhivskega gradiva.
- Pravilnik o pridobivanju nazivov na področju varstva kulturne dediščine in varstva arhivskega gradiva.
- Pravilnik o določitvi tarif pri uporabi arhivskega gradiva.

Predstavljena pravna podlaga se v celoti posveča in je tudi nastala z namenom, da bi urejali arhivsko gradivo, dokumentarno gradivo ter arhive in druge subjekte,

*avtorja sta člana Slovenskega združenja korporativne varnosti



ki se ukvarjajo z omenjenim gradivom. Vendar je treba opozoriti, da to še zdaleč niso vsi predpisi, ki bi urejali upravljanje z dokumentacijo in arhivi. Če razmišljamo širše je potrebno upoštevati tudi področno zakonodajo med katero bi predvsem izpostavili Zakon o gospodarskih družbah in Zakon o davčnem postopku, ki določata tudi načine in roke hrambe poslovne dokumentacije in kazensko odgovornost v primeru neupoštevanja in kršitev omenjene zakonodaje.

Standardi

Pravno podlago podpira bogata paleta standardov, ki zagotavljajo enotno metodologijo in procesni pristop k upravljanju in varovanju klasičnega in sodobnega (elektronskega) urejanja arhivskega gradiva in arhivov na evropskem in nacionalnem nivoju. Med njimi bi posebej izpostavili britanski standard BS 5454 – Priporočila za shranjevanje in razstavljanje arhivskega gradiva, ISO 11799 – Zahteve za hrambo arhivskega in knjižničnega gradiva in SIST-TP ISO/TR 15489 Informatika in dokumentacija – Upravljanje zapisov. Poleg navedenih so v uporabi številni standardi za elektronske oblike zapisov pri dolgotrajni hrambi podatkov, standardi za prenos in shranjevanje na mikrofilm in standardi za prenos in shranjevanje na CD-R. Z vidika neprekinjenega upravljanja in varovanja dokumentarnega in arhivskega gradiva ter arhivov pa je uporaben standard neprekinjenega poslovanja BS 25999.

Management korporativne varnosti pa mora poskrbeti, da se v sistem varovanja arhivskega gradiva in arhivov vgradijo tudi standardi kakovosti po ISO 9001:2008 in varnostni standardi med katerimi bi posebej izpostavili standard varovanja informacij ISO/IEC 27000.

Pri vzpostavljanju celovitega upravljanja in varovanja arhivov je potrebno izhajati iz ocene, ranljivosti ogroženosti in tveganj.

Ocena ogroženosti, ranljivosti in tveganj

Pri vzpostavljanju celovitega upravljanja in varovanja arhivov je potrebno izhajati iz ocene, ranljivosti ogroženosti in tveganj. Glavne nevarnosti in grožnje arhivom so naslednje: naravne nesreče – potres, poplava, plaz, obilne padavine, neustrezni prostori, neustrezni klimatski pogoji, malomaren način ravnanja z gradivom s strani zaposlenih in uporabnikov, tveganja odtujitve, tveganja poškodovanja in uničenja (požar), druge nevarnosti in tveganja.

Vsa navedena tveganja je potrebno prepoznati in analizirati ter v načrtu upravljanja in varovanja arhivov opredeliti načine za njihovo obvladovanje.

Varnostni mehanizmi – načrt upravljanja in varovanja arhivov

Poslovno dokumentacijo ter dokumentarno in arhivsko gradivo se hrani v ustrezno varovanih prostorih in opremi, v ustreznih klimatskih pogojih, zavarovano pred nepooblaščenimi vstopi in dostopi, tatvino, vlomom, požarom, vodo, biološkimi, kemičnimi, fizikalni-

Dosedanje dobre prakse tako na lokalnem kot tudi globalnem trgu izkazujejo, da je smiselno razmišljati o outsourcingu tega področja, saj so lahko v tem primeru stroški upravljanja in varovanja arhivov tudi do 50% nižji.

mi in drugimi škodljivimi vplivi. Poleg tega morajo odgovorne osebe poskrbeti, da se pri hrambi, urejanju, popisovanju, uporabi, prevozu in razstavljanju gradivo ne poškoduje, uniči ali kako drugače izgubi. Iz tega izhaja, da načrt upravljanja in varovanja arhivov– upoštevajoč zakonodajo, standarde in oceno ogroženosti – zajema:

- opredelitev zaščite pred naravnimi nesrečami,
- opredelitev zaščite pred biološkimi, kemičnimi, fizikalnimi in drugimi škodljivimi vplivi,
- opis mehansko varovanje,
- način kontrole pristopa,
- ukrepe za preprečevanje nepooblaščenega zajema, iznosa in tatvine gradiva,
- način protivlomnega varovanja,
- način protipožarnega varovanja (sistem aktivne požarne zaščite),
- ukrepe varovanja zaupnega gradiva (osebnih in tajnih podatkov ter poslovnih skrivnosti),
- alarmni in odzivni sistem,
- ukrepe v primeru evakuacije gradiva,
- ukrepe za varno uničevanje gradiva.

Načrt varovanja izdela odgovorna oseba za arhive ob strokovni pomoči managementa korporativne varnosti.

Optimizacija upravljanja z arhivi

Pri vzpostavljanju sistema upravljanja in varovanja arhivov je potrebno upoštevati tudi ekonomski vidik. Dosedanje dobre prakse tako na lokalnem kot tudi globalnem trgu izkazujejo, da je smiselno razmišljati o outsourcingu tega področja, saj so lahko v tem primeru stroški upravljanja in varovanja arhivov tudi do 50% nižji. Pri tem ni zanemarljivo dejstvo, da na ta način podjetje sistemsko uredi register dokumentacije (izdela klasifikacijski načrt) in vzpostavi popolno sledljivost upravljanja in uničevanja dokumentacije.

Zaključna misel

Neustrezno upravljanje in varovanje informacij lahko po eni strani usodno vpliva na poslovanje organizacij, po drugi strani pa to lahko pomeni za poslovodstvo organizacij ali osebe, ki so odgovorne za upravljanje z arhivi moralno, odškodninsko ali celo kazensko odgovornost. Tudi zaradi navedenega je področje upravljanja in varovanja poslovne dokumentacije, dokumentarnega in arhivskega gradiva ter arhivov vse prevečkrat prezrta, vendar izjemno pomembna sestavina korporativne varnosti in upravljanja organizacij nasploh. V eni izmed naslednjih številk bomo ravno iz tega razloga bolj podrobno nakazali možne rešitve za vzpostavitev celovitega sistema upravljanja z arhivi tako na operativnem kot tudi strateškem nivoju.. ■



Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

INTERVJU
mag. Katja Kraškovic
predsednica uprave GEA College d.d.

PERSPEKTIVE PODJETNIŠKEGA IZOBRAŽEVANJA KOT PODLAGA ZA NOVE RAZVOJNE PRILOŽNOSTI SLOVENIJE

Odličnost in novi pristopi izobraževanja bodočih podjetnikov morajo biti temeljna smer razvoja vodilne podjetniške izobraževalne inštitucije v Republiki Sloveniji.

Fakulteta za podjetništvo-GEA College ima v Republiki Sloveniji najdaljšo tradicijo zasebne izobraževalne institucije s področja podjetništva. Pred kratkim ste prevzeli poslovno vodenje te institucije. Nam lahko v kratkih besedah poveste v kakšni kondiciji se nahaja GEA College?

Vodenje GEA College sem prevzela v aprilu, v času torej, ko je študijsko leto še v polnem teku in so več ali manj vsi postopki utečeni. V primerjavi z drugimi zasebnimi inštitucijami na slovenskem izobraževalnem trgu je GEA College v dobri formi, ki jo bomo skušali z dodatnimi aktivnostmi, novimi projekti in ponudbo novih programov v prihodnje še izboljšati. Ne nazadnje pa se kot inštitucija lahko pohvalimo, da se je GEA College – Fakulteta za podjetništvo v letu 2014 uvrstila med 1000 najboljših poslovnih šol na svetu.

V primerjavi z drugimi zasebnimi inštitucijami na slovenskem izobraževalnem trgu je GEA College v dobri formi, ki jo bomo skušali z dodatnimi aktivnostmi, novimi projekti in ponudbo novih programov v prihodnje še izboljšati. Ne nazadnje pa se kot inštitucija lahko pohvalimo, da se je GEA College – Fakulteta za podjetništvo v letu 2014 uvrstila med 1000 najboljših poslovnih šol na svetu.

Kje bodo težišča nadaljnjega razvoja GEA College kot institucije usmerjene v odličnost podjetniškega izobraževanja?

Nadaljnji razvoj GEA College bo potekal v smeri razvoja novih študijskih programov s področja podjetništva, inovativnosti in managementa. Eden od pomembnih ciljev je akreditacija doktorskega študijskega programa, ki bi zagotavljal študentom, ki so nam zaupali na dodiplomski stopnji, nadaljevanje študija do najvišje možne izobrazbe s področja podjetništva. V prihodnjem obdobju bomo nedvomno pristopili tudi k mednarodni akreditaciji Fakultete ali katerega od njenih študijskih programov, kar se nam zdi pomembno pri izkazovanju odličnosti inštitucije v okolju. Prav tako pomembno je, da se usmerimo bolj mednarodno in deloma tudi v študij na daljavo. Trendi v izobraževanju se spreminjajo in pomembno je, da smo v koraku s časom. Pomembno je tudi, da ponujamo študije, ki jih drugi nimajo. Kot primer lahko nevedem magistrski študij Management korporativne varnosti.

*avtor je član Slovenskega združenja korporativne varnosti



Drugo pomembno področje, ki je pri zagotavljanju kakovosti izvedbe študijskih programov nepogrešljivo, je sodelovanje z najboljšimi strokovnjaki različnih področij in razvoj obstoječih kadrov.

Odličnost izvajanja osnovnega študijskega procesa bo še naprej podprta z usmerjenim delovanjem Znanstveno raziskovalnega inštituta, delom mednarodne pisarne in novo nastalega kariernega centra ter ne nazadnje z vstopanjem v različne mednarodne projekte, katerih rezultate bomo lahko uporabili kot orodja pri poučevanju ali kot produkte za prenos v gospodarstvo.

V okviru Fakultete za podjetništvo se izvaja tudi podiplomski magistrski program »Management korporativne varnosti«. Letos se na fakulteto vpisuje druga generacija študentov. Kako ocenjujete prvo leto izvajanja tega programa?

Posebna prednost programa je, da je edini podiplomski študij v Sloveniji, ki izobrazi posameznika v strokovnjaka s področja korporativne varnosti, ki je sposoben izvajati procese celovitega obvladovanja tveganj v organizacijah javnega in zasebnega okolja.

Prva generacija študentov je bila nekoliko manjša od pričakovane, ne glede na to pa smo z rezultatom zadovoljni. Program je bil dobro izveden in študenti so ga zelo dobro ocenili. Imamo zahtevno skupino študentov z veliko znanja, ki veliko zahtevajo od predavateljev. Za leto 2015/2016 so naša pričakovanja višja v smislu števila vpisanih študentov, verjamemo pa, da bo izvedba programa po izkušnji v prvem letu celo boljša. Ker je študij nov je potrebno delati na prepoznavnosti programa. Posebna prednost programa je, da je edini podiplomski študij v Sloveniji, ki izobrazi posameznika v strokovnjaka s področja korporativne varnosti, ki je sposoben izvajati procese celovitega obvladovanja tveganj v organizacijah javnega in zasebnega okolja.

Kje so po vašem mnenju glavne perspektive in dodana vrednost študija na Fakulteti za podjetništvo-GEA College? V tem okviru nas poleg študija podjetništva posebej zanima študij na programu »Managementa korporativne varnosti«.

Dodana vrednost študija pri nas je nedvomno obravnavanje vsakega študenta kot posameznika s potencialom in talenti, ki jih tekom študijskega procesa spodbujamo, nadgrajujemo in dopolnjujemo. V ta namen je vzpostavljen tutorski sistem – vsak študent dobi mentorja, na katerega se lahko obrne po nasvet, pa naj si bo to študijski ali poslovni problem, s katerim se ukvarja. Predavatelji, s katerimi sodelujemo, so strokovnjaki na svojih področjih in imajo poleg akademskih, bogate izkušnje v gospodarski praksi. Veliko študentov izkoristi možnost mednarodne študijske ali delovne izmenjave, ki jo zagotavljamo s sodelovanjem s preko 30 mednarodnimi partnerskimi inštitucijami. Vse več je tudi vključevanja študentov v različne projekte, ki jih izvajamo v okviru Znan-

stveno raziskovalnega inštituta GEA College. Študij bogatijo še izkušnje različnih gostov, ki v predavalnico prihajajo iz podjetij, ekskurzije v uspešna slovenska podjetja in delo kariernega centra. Veliko prednost za naše študente tudi v bodoče vidimo v zagotavljanju stalnega stika s prakso. Verjamemo, da je samo delo tisto, ki daje prave izkušnje za uspešen začetek kariere.

Na enak način smo pristopili tudi pri izvajanju podiplomskega študijskega programa Management korporativne varnosti. Verjamemo, da bo to področje v Sloveniji pridobilo na veljavi, saj je zavedanje o pomenu tega poklica v podjetjih še zelo nizko. Trendi kažejo, da bodo tudi slovenska podjetja na tem področju morala nekaj storiti, da bi zagotovila varnost in uspešnost poslovanja ter hkrati izpolnila zakonske zahteve.

Danes si brez tesnega mednarodnega sodelovanja težko predstavljamo uspešen in učinkovit razvoj izobraževalnih institucij. Kakšni so vaši načrti za povečanje in intenziviranje mednarodnega sodelovanja fakultete na vseh nivojih izobraževanja?



GEA College – Fakulteta za podjetništvo že vrsto let sodeluje v različnih mednarodnih evropskih projektih. S tem se povečuje mreža naših mednarodnih partnerskih inštitucij, s katerimi slej ko prej najdemo, poleg projektov, tudi druge oblike sodelovanja. Še pomembneje pa je, da s tem krepimo bazo znanja, ter omogočamo prenos izkušenj in trendov z najboljših poslovnih šol na svetu v slovenski prostor.

Tudi v bodoče bomo nadaljevali in še povečevali mednarodno sodelovanje v obliki študijskih, akademskih in delovnih izmenjav. Vključevali se bomo v različne projekte na področju podjetništva in poslovnih ved ter skušali angažirati kakovostne kadre, predvsem doktorje znanosti, ki bodo sposobni postati vsebinski nosilci teh mednarodnih projektov.

Predavateljski kader je verjetno eden od dejavnikov, ki je bistvenega pomena kadar govorimo o kvaliteti študija na GEA College. Kako v prihodnosti vidite razvoj predavateljev in raziskovalcev v okviru vaše institucije?

Odličen kader je nepogrešljiv del vsake zasebne izobraževalne inštitucije, ki želi uspešno tekmovati na izobraževanem trgu. Za nas je še posebej pomembno, da imamo predavatelje, ki združujejo akademsko in poslovno delovanje, ter tako strokovno in s pomočjo prakse gradijo študijski predmet na način, da lahko študentje pridobljeno znanje in izkušnje uporabijo neposredno v praksi že med ali takoj po študiju.

Pomembne so tako metode poučevanja kot tudi osebni razvoj predavateljev, in na tem želimo graditi v prihodnje.

Z namenom razvoja in krepitve raziskovalnega in predavateljskega kadra sodelujemo na javnem razpisu za »Spodbujanje in zaposlovanje mladih doktorjev znanosti v letu 2015«. Na takšen način lahko vključimo tudi mlade v delo Fakultete, ter tako pridobimo podmladek,ki lahko s pomočjo mentorja v nadaljevanju okrepi predavateljsko ekipo.

V okviru znanstveno raziskovalnega inštituta imamo namen izvajanja čim večjega števila raziskav s področja podjetništva, seveda pa je to povezano s financiranjem raziskav. Poleg prijave projektov za pridobitev sredstev bomo skušali poiskati za razsikovalni namen tudi sponzorje. Za študijsko leto 2015/16 imamo v pripravi že dve raziskavi, ki jih bomo izvajali. Z eno se bomo osredotočali na srednješolce, z drugo na študente. Ugo-

tovitve bomo uporabili za namen izboljšanja študijskih programov in ozaveščanja okolice z dejstvi s področja podjetništva.

Glede na dejstvo, da je GEA College zasebna podjetniško naravnana institucija nas zanima vaše stališče in ukrepi za boljšo povezljivost teoretičnega znanja in prenos dobrih praks neposredno v podjetniško okolje in nazaj v izobraževalni proces?

Menim, da je za povezljivost teoretičnega znanja in prenos dobrih praks v podjetniško okolje ključno dobro povezovanje in odprtost podjetnikov in inštitucij, ter tudi medsebojno povezovanje podjetnikov. Da lahko prenesemo v izobraževalni proces dobre prakse jih morajo podjetniki deliti z nami, in obratno, tudi inštitucija mora določena znanja deliti s podjetniki. To je precej velik izziv, čeprav se zdi zadeva povsem logična in enostavna.

Osebno menim, da s strogimi ukrepi na tem področju ni možno doseči rezultata, vsekakor pa mora podjetnik oz. direktor v podjetju preko elementov strateškega menedžmenta oblikovati primerno organizacijsko strukturo, procese in kulturo, ki prenose znanja omogočajo in spodbujajo. Če neko podjetje nima razvite kulture prenosa znanja znotraj podjetja je po mojem verjetnost, da bi iskali znanje navzven pri inštitucijah, kot je GEA College, majhna. Takšen način delovanja je še posebej pomemben za manjša podjetja, ki morajo biti v interakcijah z okoljem boljša, da s tem nadomestijo majhnost svojih lastnih virov. Različne raziskovalne inštitucije in fakultete imamo dovolj že evidentiranega znanja v obliki izdelkov/storitev/poslovnih modelov optimizacije poslovanja, ki jih je mogoče prenesti v prakso in podjetju lahko prinesejo konkurenčno prednost.

Na drugi strani pa mora biti vodstvo izobraževalne/raziskovalne inštitucije odprto za sodelovanje s podjetji. Pri tem se je potrebno zavedati, da tudi pri prenosu »univerzalnih znanj« ni enostavnega recepta za prenos v prakso nekega podjetja – vsako zahteva individualen pristop in prilagoditve njihovim zmožnostim, potrebam in ne nazadnje času, ki ga imajo za uvajanje neke novosti. Na Gea Collegu smo za takšna sodelovanja odprti in jih bomo v prihodnje tudi skušali spodbujali preko neke vrste »konzorcija« podjetnikov.

Izkušnje kažejo, da se na raziskovalno razvojne inštitucije in fakultete obračajo velika podjetja, medtem ko mala in srednje velika podjetja, ki jih je v Sloveniji prek 95%, praktično ne sodelujejo. Menim, da je na tem področju še veliko prostora za napredek, hkrati pa je pri tem pomembna vloga države oz. spodbudnega okolja, ki ustvari pogoje za razvoj posameznega področja.

Načrtujete povečanje raziskovalnih projektov z neposredno aplikativno vsebino in njihovo povezovanje s podjetniškimi okolji?

Naša želja je še tesnejša povezanost z gospodarstvom in sodelovanje v več aplikativnih projektih. Verjamemo, da bomo del teh načrtov lahko uresničili skozi uspešno delovanje našega karier nega centra, ki združuje uspešna slovenska podjetja z uspešnimi študenti in ne nazadnje s predavatelji in drugimi zaposlenimi na GEA College.

Veselimo se novega javnega razpisa »Po kreativni poti do praktičnega znanja«, v katerem študenti in njihovi mentorji sodelujejo na praktičnih projektih v podjetjih. Na preteklem razpisu smo bili uspešni z izpeljavo projektov in verjamemo, da lahko z dobrimi idejami pomagamo še kateremu od malih in srednje velikih podjetij v Sloveniji. ■



7. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 16.—17. marec 2016



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI

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



KOLUMNA
denis.caleta@ics-institut.si

BEGUNSKA KRIZA IN NJENI GEOSTRATEŠKI VIDIKI

Migracijski tokovi postajajo stalnica varnostnega okolja v katerem živimo. Pomembno je razumeti tveganja in grožnje, ki jih taki migracijski procesi prinašajo v Evropi in njeni družbi.

V zadnjem času vse svetovne medije zaposluje begunska kriza, ki pljuska v Evropo. Med strokovnjaki je kar nekaj nesoglasij o tem ali gre v zadnjem primeru za begunsko krizo ali gre v večini primerov za ekonomske migracije iskanja boljših življenjskih pogojev. Nismo še pozabili begunskega vala, ki ga je bila Slovenija deležna med vojnimi spopadi na Balkanu. Slika beguncev, ki smo jo poznali, je v marsičem drugačna od slik urejenih mladeničev iz Sirije, ki odgovarjajo novinarjem na njihova vprašanja o razlogih za njihovo pot proti boljšim življenskim pogojem. V ospredju je ves čas humanitarni vidik krize, ki nam zamegli nekatera bistvena vprašanja na katera bi morali v Evropi zelo hitro poiskati odgovore. Gre namreč za pomembno varnostno vprašanje, ki razgalja geostrateška težišča in interese Evrope oziroma bolje rečeno posameznih Evropskih držav. Evropska unija je ponovno dokazala, da v najbolj kritičnih trenutkih, ki lahko dolgoročno pomenijo tudi zaton Evropske ideje in imajo zelo pomemben varnostni vidik, ne more prestopiti pomembne točke preloma sprejemanja ene skupne rešitve. Prevlada parcialnih nacionalnih interesov, pred skupnimi evropskimi, se je pokazala v najbolj črnem scenariju. Evropska unija in njene birokratske strukture pa več tednov niso bile sposobne priprave ustrezne skupne politike spopadanja z valom beguncev. Do včeraj je bila ena od glavnih groženj Evrope, s katero so se ukvarjale vse obveščevalne in varnostne službe držav, radikalizacija in vračanje državljanov evropskih držav z bojišč v Siriji in Iraku. Poudarjeno je bilo izvajanje posebnih obveščevalnih aktivnosti za spremljanje teh oseb pri možnem vračanju v domače države in nevarnost, ki jo predstavljajo zaradi njihove radikalizacije, vojaških izkušenj in travm, katere so doživljali ob moriji v Siriji in Iraku. Le ti predstavljajo veliko tveganje za izvajanje terorističnih aktivnosti. Danes se nam zdi, kot da so meje Evropske unije popolnoma odprte, vsem državam pa je glavni cilj, da veliko količino beguncev čimprej prepeljejo od vstopne točke v njihovi državi do izstopne točke na meji, kjer problem preložijo na naslednjo državo. Nihče se resno ne ukvarja s kontrolo oseb, ki dejansko prihajajo pred naš prag. Trenutna situacija ne more biti boljša priložnost za prehajanje vseh tistih oseb, ki so še do včeraj predstavljale eno od največjih groženj nacionalne in skupne evrospke varnosti. Seveda je potrebno ob poudarjanju tveganj, ki jih prinaša infiltracija nevarnih posameznikov v val begunskih tokov, izpostaviti tudi zdravstvena tveganja, ki se jih vse premalo zavedamo, od možnega prenosa različnih vrst nalezljivih bolezni, katere ob taki nelegalni migraciji oseb niso deležne nikakršne pozornosti. Ko smo skozi prizmo preteklih mesecev gledali kako so pod taktirko nekaterih držav, predvsem Nemčije, institucije Evrospke unije in vlade posamenih držav preko noči sprejemale odločitve v primeru finančne krize v Grčiji, pa danes gledamo podobo popolnoma paraliziranih institucij Evrospke unije, ki niso sposobne sprejeti nikakršnih odločitev. Vsaka posledica dejanj ima vedno neko logično razlago, ki pa si jo je v trenutni situaciji pomanjkanja določenih informacij težko zamisliti in najti prave odgovore. Vendar je potrebno zadevo pogledati z različne perspektive, tudi tiste, ki begunsko krizo ne odslikava samo v črno beli kombinaciji poudarjanja humanitarne krize. Seveda je potrebno na tem mestu jasno poudariti, da je marsikateri primer oseb bežečih pred vojno vihro več kot tragičen in pred nas polaga velik humanitarni čut do pomoči. Pa vendarle poglejmo nekaj dejstev, ki celoten proces

Do včeraj je bila ena od glavnih groženj Evrope, s katero so se ukvarjale vse obveščevalne in varnostne službe držav, radikalizacija in vračanje državljanov evropskih držav z bojišč v Siriji in Iraku.

*avtor je član Slovenskega združenja korporativne varnosti

postavljajo v zelo zanimivo perspektivo, katera delovanje posameznih držav postavlja v zelo zanimiv položaj.

Prav je, da si na tem mestu zastavimo vprašanje zakaj se je ravno sedaj zgodil ta množičen naval »beguncev« v smeri, kjer še pred nekaj meseci ni bilo zaznati tako množičnih migracij. Pri iskanju odgovorov sicer lahko hitro naletimo na nekaj splošnih dilem in sicer ali je to v interesu Rusije, da odvrne pozornost od svojih aktivnosti v Ukrajini, je to interes ZDA, da z begunsko krizo Evropo oslabi v globalni konkurenčni tekmi, kakšen je tukaj interes Turčije in predsednika Erdogana ter njegove želje po povračilu za konstantno, predvsem nemško blokado konkretnemu približevanju EU, ali za tem stoji Nemčija s svojimi multinacionalnimi družbami, ki zaradi gospodarske rasti nujno potrebuje dodatno delovno silo, ali pa je prevladujoč interes bogatih zalivskih držav s finančno podporo omogočil zadnji begunski val, predvsem zaradi prelaganja bremena beguncev čim dlje od njihovih mej. Na žalost je v tem trenutku premalo jasnih odgovorov, ki bi nam potrdili eno od napisanih dilem, vendar pa si lahko skozi nekatere dejavnike ustvarimo sliko, kako v realnosti deluje Evropska unija in kakšna je realna vloga velikih evropskih držav, predvsem Nemčije in kakšna marginalna vloga je prepuščena ostalim državam, ki se morajo soočati predvsem s posledicami igre velikih sil pri zagotavljanju njihovih interesov. Zadnji tok migracij poteka po točno določeni poti v Nemčijo, ki je skoraj pri vseh vprašanjih njihova željena ciljna država. Vendar ravno ta močna želja priti v Nemčijo postavlja nekaj zanimivih dilem.

Širše razumevanje nam kaže na diferenciacijo moči v Evropski družini, katera se dejansko odmika od pričakovanj nas državljanov, predvsem tistih iz manjših držav Evropske unije.

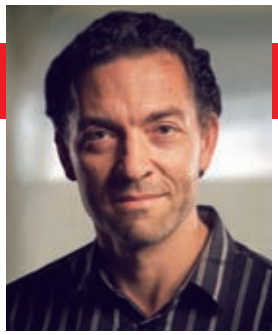
Za zaključek mojih razmišljanj pa vsekakor sodi odprto vprašanje kaj lahko v Sloveniji naredimo za svojo varnost in ali naša politična garnitura sploh razume procese, ki se odvijajo v globalnem varnostnem okoju. Prepričan sem, da bomo na nivoju posameznih institucij poskrbeli za sprejem ustreznega števila tistih beguncev, ki bodo prišli v Slovenijo. Pomembno dejstvo, ki ga seveda nikakor ne moremo spregledati je, da smo še vedno mejna država Shengenskega območja zato je naša naloga in dolžnost, da predvsem zagotovimo ustrezno varnost pri prehajanju naše in evropske meje. Drugo še bolj pomembno dejstvo pa je ali bomo pri prevzemu bremen znali razumeti procese in interese ostalih držav in v pogajanjih tudi ustrezno zagotoviti naše nacionalne interese. Katerakoli od zgoraj postavljenih tez povezanih z begunsko krizo je prava in katera država bo v tej geopolitični igri dobila največje koristi je v tem trenutku še preuranjeno govoriti. Zavedati pa se je potrebno, da stanje begunske krize in njeno pluskanje proti Evropi, ter predvsem nezmožnost skupnega celovitega odgovora kaže na zaton evropske ideje in še en kamenček v njeni eroziji.

Tukaj je še posebej izpostavljena kritična infrastruktura, ki je nujna za delovanje širše družbene skupnosti in je lahko ob zanemarjanju pomembnih varnostnih korakov v takih kriznih trenutkih močno izpostavljena tveganjem.

Čisto za konec pa želim opozoriti, da je problem migracijskih tokov poleg nacionalne in evropske varnosti zelo tesno povezan tudi s korporativnim varnostnim okoljem. Podjetja in druge organizacije morajo zelo resno spremljati in razumeti to krizo, ki lahko v svojih posledicah izredno negativno vpliva na samo poslovanje na kriznih območjih pretoka teh migracij, lahko pa nastanejo tudi neposredne škodljive posledice na premoženju in seveda varnosti zaposlenih v teh organizacijah. Tukaj je še posebej izpostavljena kritična infrastruktura, ki je nujna za delovanje širše družbene skupnosti in je lahko ob zanemarjanju pomembnih varnostnih korakov v takih kriznih trenutkih močno izpostavljena tveganjem. ■



Avtor: g. Janez Kotar / Inprosis, informacijski sistemi, d.o.o.



DRONI ORODJE ALI NADLOGA?

Eksponenčna rast prodaje dronov za civilno uporabo ter hiter tehnološki razvoj v zadnjh letih napoveduje neslutene možnosti razvoja te nove panoge. Ključna neznanka prihodnosti pa je ravno vidik varnosti, ki zna odločilno vplivati na to, kaj bo v prihodnosti letelo nad našimi glavami.

V današnjem času skoraj ni več posameznika, ki ne bi imel vsaj kakšne izkušnje z droni. Tematika se je začela pojavljati tudi v naših medijih, kjer je vzbudila zanimanje predvsem zaradi vidika zasebnosti nenazadnje skoraj ni več javne prireditve, kjer ne bi nad seboj zaslišali značilnega brenčanja multikopterja. Pa vendar so možnosti uporabe dronov mnogo širše zgolj od snemanja videa iz zraka, ki je danes zagotovo najbolj pogosta uporaba.

Zgodovinski pogled na varnost

Izvor dronov za civilno uporabo lahko iščemo v dveh smereh. Prva je že močno uveljavljena vojaška tehnologija brezpilotnih letal, druga pa je svet modelarstva. Modelarska dejavnost in združenja imajo že dolgo zgodovino, pa vendar je ta dejavnost vsa leta obstajala v dokaj ozkem krogu navdušencev. V svojem bistvu modelarstvo od posameznika zahteva dobro poznavanje tehnike ter veščino upravljanja modela – kar ne gre brez dolgotrajnega treninga pod vodstvom učitelja. Proces treninga omogoči, da ob pridobivanju znanja in izkušenj počasi ponotranjiš tudi varnostne vidike dejavnosti. Kršitve (varnostna tveganja) je tudi iz formalnega vidika ustrezno preprečevala organizacija modelarskih združenj. Letalnega modela ni bilo možno uporabljati kjerkoli, saj je bil ključen pogoj za vzlet ustrezno urejena pista.

Predvsem napredek in komercializacija kontrolerjev (elektronike), ki pilotu omogočajo nezahtevno upravljanje, ter pojav celovitih že sestavljenih sistemov na trgu, je omogočila, da je zdaj edina ovira za upravljanje drona v zraku zgolj nekaj sto evrov. Tehnološki napredek je tako v celoti omogočil obvoz tradicionalnega zagotavljanja varnosti modelarstva.



Subjektivni vidik varnosti dronov

Ključno je upoštevati dva subjektivna vidika varnosti. Prvi je motivacijski sistem pilota drona. Osnovni interes tradicionalnega modelarja je bila namreč izgradnja ter upravljanje modela. Preveliko tveganje je imelo za posledico poškodovanje ali celo uničenje modela. Danes je končni cilj pilota drona posneti edinstven video iz zraka – dron je tako zgolj sredstvo za dosego cilja. Prevzemanje večjega tveganja (poškodovanje drona in okolice), je tako za pilota postalo sprejemljivo. Zaradi tega je splet danes poln videov nevarnega upravljanja drona nad skupinami ljudi, nad prometnicami, v neprimernih vremenskih pogojih, v ognjemetih ...

Drugi subjektivni vidik pa je samo zavedanje nevarnosti. Večinska splošna percepcija današnje tehnologije je prekomerno zaupanje v zanesljivost delovanja tehničnih komponent in s tem pomanjkanje razmisleka o posledicah. Prva asociacija na upravljanje drona je namreč igranje računalniških igric, kjer pa imaš neomejeno število življenj, napake upravljanja pa nimajo nikakršne posledice v realnem svetu.



Koristi, ki jih prinašajo droni

Industrijska uporaba dronov pa je mnogo širša od prostočasnega snemanja videov. Ključne prednosti dronov so: cenovna dostopnost, enostavnost upravljanja (vzlet in pristanek se da izvesti skoraj od kjerkoli) ter možnosti delovanja iz majhnih višin. Svojo uporabno vrednost so zato že dokazali na mnogih področjih kot so: geodezija (mapiranje iz zraka), transport (dostava pošiljk, nadzor prometa), arheologija (raziskovanje in vizualizacija arheoloških ostankov), energetika (nadzor električnih dalnovodov, naftovodov, solarnih elektrarn, vetrnic), ohranitev naravne in kulturne dediščine (spremljanje vegetacije, živalskih populacij ...), zaščita in reševanje (iskanje ponesrečencev, pomoč v naravnih nesrečah), kmetijstvo (spremljanje posevkov ter njihovo ciljno tretiranje), varnost in zaščita (nadzor terena), gradbeništvo (nadzor gradnje), rudarstvo (spremljanje količin), filmska industrija (posnetki iz zraka), turizem (nove pespektive fotografiranja in snemanja lokacij).

Večina teh nalog je neposredno povezanih s snemanjem oz. fotografiranjem iz zraka – bodisi z uporabo navadnih senzorjev, bodisi z zajemanjem v nevidnem svetlobnem spektru. Podobne letalne karakteristike kot jih imajo običajni helikopterji, ob sočasnem bistveno manjšem strošku uporabe ter enostavnem upravljanju, omogoča dronom ključno konkurenčno prednost pred snemanjem iz letal in helikopterjev.

Nevarnosti za rast panoge

Napovedi rasti celotne panoge so zelo optimistične. Tehnološki napredek na eni strani ter očitne ekonomske prednosti na drugi strani so ključni pogoj za to. Ne moremo spregledati ključnega tveganja – javnega mnenja. Dovolj resen posamezen incident lahko namreč na globalni ravni ustavi celotno panogo dronov. Začetno navdušenje nad novo tehnologijo je v zadnjem času vedno bolj spremljano z vprašanji varnosti ter posega v zasebnost. Ob sočasnem nedohajanju zakonske ureditve nastaja velik prostor, kjer se pogostost incidetov nenehno veča – oči javnosti pa so vseskozi uprte v to.

Zanesljivost delovanja dronov

Incidenti z droni so dokaj pogosti. Težave pri delovanju pa izvirajo iz dveh vrst dejavnikov: pilota ter tehnike. Daleč največji dejavnik tveganja pri pilotu je njegova neizkušenost in s tem povezane napake, ki se najbolj kažejo pri pripravi na letalske operacije in med izvajanjem operacij. Ključna težava je, da je sistem izobraževanja operaterjev (vsaj tistih, ki drone uporabljajo rekreativno) tudi v državah z urejeno zakonodajo, še zelo v povojih. Tako je samo pridobivanje znanja in izkušenj skoraj v celoti prepuščeno posamezniku. Varnost operacij in s tem povezane posledice, so tako najbolj odvisne zgolj od njegove odgovornosti,
Tehnični vzroki incidentov so bodisi okvara drona (napake v elektronskem ali mehanskem sistemu) ali pa težave v sistemu upravljanja (radijska veza). Tehničnih vzrokov tveganja v večini primerov ne moremo povsem ločiti od vzrokov na strani pilota. Gre namreč za to, da lahko izkušen pilot z ustrezno konfiguracijo sistema, preventivnim vzdrževanjem ter oceno tveganja same letalske operacije v veliki meri prepreči

tudi nastanek tehnične težave ali pa vsaj pomembno ublaži posledice.

Zmanjševanje tveganja strmoglavljenja

Tveganja strmoglavljenja drona zaradi tehnične okvare se regulira z zmanjšanjem vpliva konkretne tehnične okvare na strmoglavljenje. Redundanca je najpogostejši odgovor na ta izziv. Tako recimo multikopter s štirimi motorji nima možnosti obstanka v zraku v primeru odpovedi posameznega motorja ali sistema njegovega krmiljenja - hitrost padanja pa se da omejiti s padalom. Šest ali več motorjev pa ob ostali ustrezni konfiguraciji multikopterja (razmerje med nosilnostjo in vzletno težo, zmogljivost osrednjega kontrolerja ...) tega zadrži v zraku oz. mu omogoči kontroliran pristanek. Podobno je tudi z drugimi kritičnimi komponentami drona.

Minimiziranje nastale škode

Na nastalo škodo se da vplivati zgolj z ustreznim načrtovanjem letalskih operacij oz. z oceno tveganja. Strmoglavljenje nad množico ljudi skoraj zagotovo pomeni telesne poškodbe, v najhujšem primeru pa tudi smrt. Kinetična energija svetovno najbolj prodajanega rekreativnega drona v prostem padu namreč zadostuje za frakturo človeške lobanje. Strmoglavljenje na požarno ogrožen objekt lahko pomeni povzročitev požara – litijev električni akumulator se namreč ob udarcu zelo pogosto vžge. Verjetno daleč najbolj odmeven incident pa bi bil trk s potniškim letalom zaradi nepredvidenega vstopa drona v kontrolirani zračni prostor. Sicer konstrukcija sodobnih potniških letal preživi tudi odpoved posameznega motorja v kritičnih fazah leta (vzlet in pristanek), pa vendar na tem področju še ni bilo opravljenih ustreznih analiz posledic.

Droni kot orožje terorizma

Ne moremo spregledati tudi zlonamerne uporabe dronov. Danes to področje povzroča mnogo sivih las varnostnim organom. Hitrost razvoja dronov je namreč precej prehitela razvoj sistemov zaščite. Tako se je že na mnogih primerih izkazalo, da so obstoječi sistemi protizračne obrambe povsem neučinkoviti pri tovrstnih terorističnih dejanih. Nosilnost dronov, današnji sistemi samodejnega krmiljenja ter avtonomija pa omogočajo dokaj enostavno izvedbo napadov. Razvoj sistemov zaščite trenutno poteka v več smereh: motenje radijskih frekvenc, sestrelitev (tudi lasersko), motenje senzorjev drona (oz. njegovih senzorjev) z zvočnimi valovi, fizično prestrezanje npr. z drugimi droni. Rekreativni droni se kot ceneno sredstvo bojevanja trenutno učinkovito uporabljajo v konfliktih na Bližnjem vzhodu.

Zakonska ureditev za povečanje varnosti

Področje preventive ter ustrezno sankcioniranje kršitev so nujni pogoji za razvoj panoge. Posamezne države so že sprejele prve zakonodaje na tem področju. Te na nek način združujejo vidik javnega mnenja s trenutnim poznavanjem delovanja dronov. Razpon zakonodajnih rešitev posameznih držav gre od popolne prepovedi uporabe dronov v civilne potrebe, pa do zelo okvirnega urejanja v okviru za drone neustrezne letalske zakonodaje. Tako je tudi v EU trenutno popolnoma odsotna harmonizacija nacionalnih zakonodaj, kar zelo otežuje mednarodno delovanje ter razvoj panoge.



Počasi se uveljavljajo izobraževanja s področja letalstva s specifikami dela z droni. Je pa res, da obveza večinoma še ne vključuje rekreativnega področja uporabe dronov, ki pa je daleč največji potencial za nastanek incidentov. Na področju rekreativne uporabe se razvijajo tudi priporočila, s katerimi se poskuša čim bolj učikovito seznaniti kupce dronov.

Skupna EU regulativa

Pomemben korak naprej je priprava skupne EU zakonodaje, ki je v fazi razprave. Osnovni cilji so zagotoviti varnost na eni strani ter omogočiti enotne pogoje za razvoj panoge. Želja pripravljalcev je, da zadostno regulirajo področje, obenem pa se ne spuščajo preveč v tehnične katakteristike, ki se zaradi izjemnega razvoja hitro spreminjajo. Težko je recimo zdaj urejati npr. področja distribucije paketov z droni, saj tehnologija za opravljanje te dejavnosti še ni zrela.

Zahteve za operaterje dronov se večajo z možnimi posledicami. Tako se podobno, kot pri večini nacionalnih zakonodaj uporablja dva osnovna kriterija tveganja: lokacija letalskih operacij ter teža drona. Pomemben dejavnik pa so tudi izkušnje operaterja, ki svoje kompetence pridobiva sprva z manj tveganimi letalskimi operacijami, nato pa z izkušnjami in izpolnjevanjem ostalih pogojev, postopoma napreduje v zahtevnejše. Sankcijski organ na najnižjem in najbolj množičnem področju rekreativne uporabe je policija, v višjih zahtevnejših področjih pa so vključeni tudi ostali organi.

Stanje pri nas

V Sloveniji smo trenutno na področju zakonske ureditve za našimi sosedami. Temu verjetno botruje tudi odsotnost večjega incidenta. Je pa nastanek slednjega ob vse pogostejši nestrokovni uporabi dronov samo vprašanje časa. Trenutno skoraj ni javne prireditve, kjer ne bi bili s strani organizatorja ali pa koga tretjega na spletu dosegljivi posnetki narejeni neposredno nad množico ljudi. Nad odmevnejšimi prireditvami se v zračnem prostoru znajde celo več dronov istočano, kar še dodatno povečuje tveganje. Prav tako je na spletu tudi polno izdelkov začetnikov, ki z neustrezno opremo in pomanjkljivim znanjem letijo po središčih mest.



V Sloveniji smo trenutno na področju zakonske ureditve za našimi sosedi. Temu verjetno botruje tudi odsotnost večjega incidenta. Je pa nastanek slednjega ob vse pogostejši nestrokovni uporabi dronov samo vprašanje časa.

Na ravni današnjega poznavanja tehnike ter tveganj bi bila ustrezna sankcijska intervencija policije, ko gre za evidentno povzročanje splošne nevarnosti. Zgolj trkanje na vest pilotov dronov namreč ni dovolj, saj nekateri hote prevzemajo previsoko tveganje ter s tem ogrožajo splošno varnost. Ravno od ravnanja vseh udeležencev je namreč najbolj odvisno, kakšna bo prihodnost te zelo obetavne panoge.

Nenazadnje – tudi letalstvo je bilo v začetku povsem neregulirano, danes pa v tej izjemno varni panogi vsak pilot ve, da letalo ne leti zaradi vzgona, temveč zaradi papirjev. ■

Avtor: ga. Maja Rožaj / Urad Republike Slovenije za varovanje tajnih podatkov*



NIZKA VARNOSTNA KULTURA NA PODROČJU VAROVANJA PODATKOV – NESPOSOBNOST VODSTVA ALI ODRAZ DRUŽBENEGA STANJA?

Postavitev temeljev za izgraditev ustrezne varnostne kulture je odgovornost vodstva in je torej odvisna od njegovih vodstvenih sposobnosti in razumevanja njenega pomena.

Zadnjo odmevno afero, povezano z dogodki na slovenskem zunanjem ministrstvu (Op. p. gre za kompromitirano komunikacijo med slovenskim članom arbitražnega sodišča in uslužbenko zunanjega ministrstva) bi lahko komentirala z več zornih kotov, začenši z vidika etičnosti in profesionalnosti, pa vendar se bom osredotočila zgolj na vidik neustreznega varnostnega vedenja. Obravnavani dogodek je dodatno potrdil tisto, kar se v javnih razpravah melje zadnjih nekaj let: apatično družbeno stanje v, hočeš nočeš, še vedno tranzicijski državi, pomanjkanje državotvornosti celo pri nosilcih najodgovornejših javnih funkcij in pošastno nizka raven varnostne kulture med slovenskimi javnimi uslužbenci. Pa da ne bodo zgolj javni uslužbenci ves čas izpostavljeni nekemu javnemu linču (kar seveda ne pomeni, da ravnanja dotičnih vpletenih v zgoraj omenjeno afero ne obsojam), z gotovostjo trdim, da situacija ni kaj dosti boljša v zasebnem sektorju. Statistika namreč še vedno kaže, da so zaposleni najpogostejša »varnostna luknja« v varnostnem sistemu. V nadaljevanju podano razmišljanje podajam kot varstvoslovka in uslužbenka Urada Vlade RS za varovanje tajnih podatkov, kjer se že več let trudimo z izvajanjem izobraževanja s področja varovanja tajnih podatkov z namenom dviga varnostne kulture tako v državni upravi, kakor tudi v zasebnih podjetjih. Poleg našega poslanstva in pristojnosti na področju varovanja (državnih) tajnih podatkov je naša usposabljanja mogoče povsem pragmatično razumeti tudi širše: če bodo podjetja znala ustrezno varovati tajne podatke, ki so last Republike Slovenije, je veliko večja verjetnost, da bodo znala ustrezno poskrbeti tudi za zavarovanje lastnih poslovnih podatkov, znanja, idej in inovacij. Ustrezna skrb za lastno konkurenčno prednost namreč posredno pozitivno vpliva na ekonomske interese države. Hitrejši gospodarski razvoj je torej odvisen tudi od sposobnosti države, da lastno znanje in prednosti zaščiti.

Idealni sistem varovanja podatkov in informacij je sestavljen iz ravnotežja ukrepov in postopkov z vseh področij, ki so medsebojno povezana v nekem delovnem procesu, t. j. področje poslovanja, zaposlenih in premoženja. Pri sistemu varovanja tajnih podatkov govorimo o področjih fizične in tehnične varnosti, osebne in dokumentacijske varnosti ter varnosti komunikacijsko informacijskih sistemov. Po analogiji starega slovenskega pregovora lahko

Idealni sistem varovanja podatkov in informacij je sestavljen iz ravnotežja ukrepov in postopkov z vseh področij, ki so medsebojno povezana v nekem delovnem procesu, t. j. področje poslovanja, zaposlenih in premoženja.

* Korporacijski član Slovenskega združenja korporativne varnosti

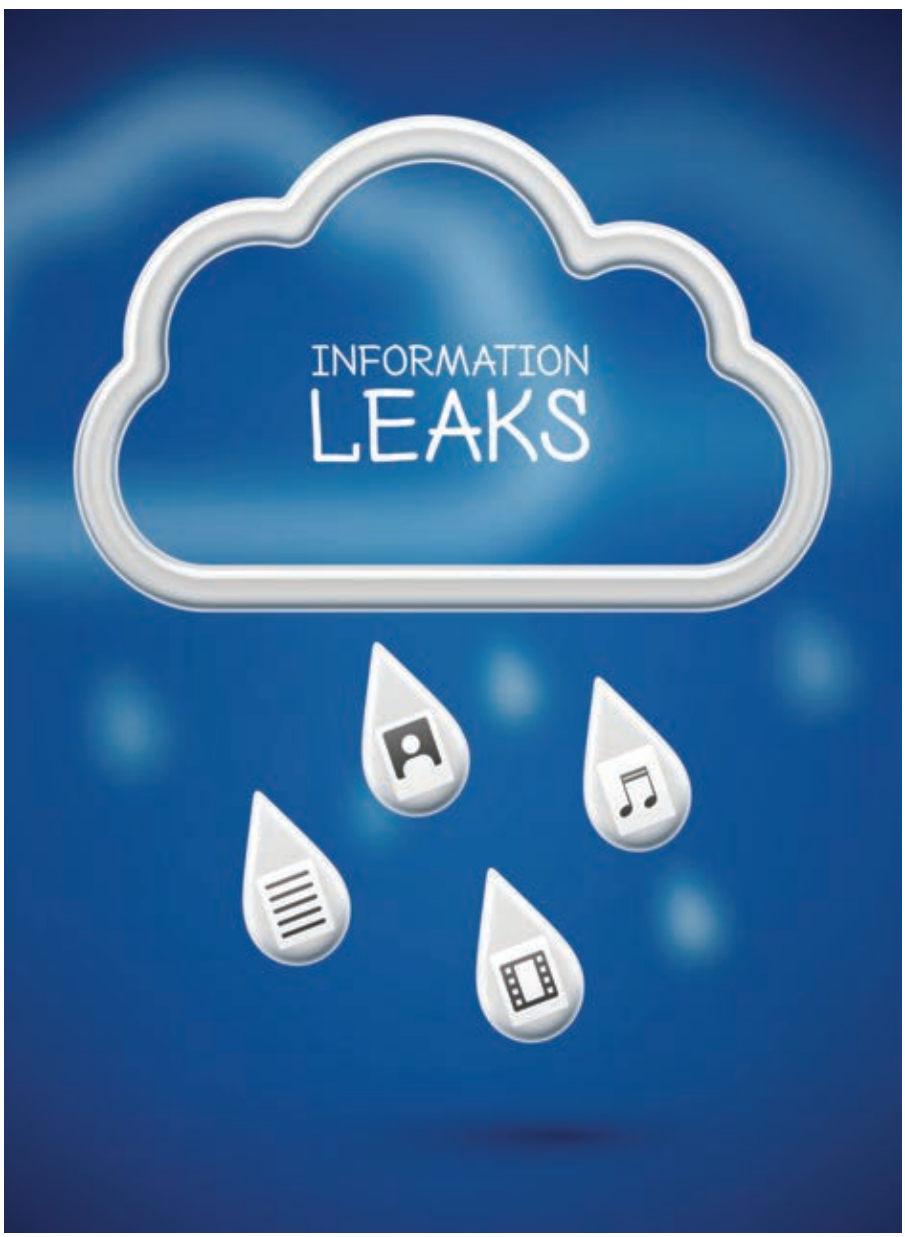


rečemo, da je varnost tako dobra, kot je dober njen najšibkejši člen. Na tej točki se slušatelji mojih predavanj skoraj vedno prikrito muzajo, saj je odgovor na vprašanje »Kaj pa je najpogostejši najšibkejši člen v nekem varnostnem sistemu?« tako smešno enostaven in jasen. Imam občutek, da se nekaterim zdi to vprašanje kar nekako ponižujoče preprosto. Večina namreč ne pomisli na nič drugega kot na to, da je t. i. človeški faktor tisti, ki zamaje ali celo poruši celotno varnostno hišico iz kart. No, z udeleženci smo do tu še nekako na isti valovni dolžini. Ko pa zastavim sledeča tri (bolj kot ne retorična) vprašanja; 1) ali se zavedate dejanske vsebinske vrednosti podatkov, 2) ali se znate ustrezno opredeliti glede podatkov, ki bi jih bilo potrebno zavarovati in 3) ali razumete negativne posledice razkritja tajnih in drugih občutljivih podatkov za interese države in/ali vašega podjetja; pa se obrazi nekoliko zresnijo. Še toliko bolj se zresnijo, ko na koncu predavanja o povsem osnovnih metodah zbiranja podatkov in nepooblaščenega dostopanja do komunikacijsko informacijskih sistemov, navedena vprašanja postavim ponovno. Varnost je namreč pojem, katerega širino večina neukih posameznikov v bistvu niti ne razume. Varnost je tisto, s čimer se ukvarja »naš varnostnik na recepciji«, »z varnostjo naj se ukvarja policija« in »za varnost imamo v Sloveniji malo morje zasebnih varnostnih služb«. Pri razumevanju pojma oziroma koncepta varnosti morda pridemo korak, dva dlje v tistih državnih organih in zasebnih podjetjih (pa še to več ali manj samo pri tistih posameznikih, ki so v to neposredno vpleteni), ki so zaradi spoštovanja določil Zakona o tajnih podatkih dolžni vzpostaviti sistem postopkov in ukrepov varovanja tajnih podatkov. Pri teh je domet razumevanja koncepta varnosti nekoliko širši, če ne zaradi drugega zato, ker že samih normativnih okvirjev navedenega sistema ni povsem preprosto postaviti. Pa vendar je tudi na tem področju logika prepogosto takšna, da se stvari urejajo zgolj zato, ker tako veleva zakon. Področja, kjer je v ozadju nek zakon (npr. Zakon o varstvu osebnih podatkov, Zakon o varstvu pred požarom, Zakon o tajnih podatkih) in, ki sicer niso neposredno povezana z osnovnim delovanjem državnega ali zasebnega subjekta, se po hitrem postopku uredi na način, da se vsaj minimalno zadosti osnovnim zakonskim pogojem. Vsekakor to ni ustrezna varnostna filozofija, saj so v tem primeru interni organizacijski predpisi zgolj neka mrtva črka na papirju, postopki in ukrepi, ki so z njimi predpisani pa v praksi ne delujejo, ker so neživljenjski, zaposlenim in siceršnji organizacijski kulturi neprilagojeni in neprijazni. Še več, interni normativni akti zaradi neprilagojenosti individualnim razmeram celo sprožajo odpor pri zaposlenih, s čimer se morebitna učinkovitost predpisanih ukrepov le še dodatno zmanjša.

Zagotavljanje varnosti, podatkov na primer, je lahko učinkovito samo takrat, ko je vgrajeno v celoten organizacijski sistem postopkov in ukrepov delovanja in poslovanja, zaposlenim in splošni notranji organizacijski klimi. Izgraditev ustrezne varnostne kulture je večplasten in dolgotrajen proces, ki temelji predvsem na ljudeh in na uveljavljanju takšnih

Zagotavljanje varnosti, podatkov na primer, je lahko učinkovito samo takrat, ko je vgrajeno v celoten organizacijski sistem postopkov in ukrepov delovanja in poslovanja, zaposlenih in splošni notranji organizacijski klimi.

tehnoloških in organizacijskih rešitev, ki podpirajo dobre varnostne navade. Postavitev ustreznih temeljev za izgraditev ustrezne varnostne kulture je odgovornost vodstva in je torej odvisna od njegovih vodstvenih sposobnosti in razumevanja njenega pomena. Razumevanje razlogov za varnostni prestopek v zadevi »Pirangate« je torej potrebno obravnavati širše; individualno odgovornost seveda nosita oba vpletena posameznika, del krivde pa je potrebno pripisati tudi predstojniku dotičnega ministrstva (in predstojnikom pred njim), ki ni bil sposoben zagotoviti oziroma vzpostaviti pogojev, ki bi takšno dejanje in ravnanje preprečili. Obravnavani dogodek potrjuje tako teoretično izhodišče, da imajo tudi najmanjše spremembe v posameznikovem vedenju lahko velik učinek na varnost na splošno, kakor tudi ugotovitve, da so varnostne kršitve, katere zaposleni povzročijo namerno, v manjšini. Večina varnostnih prekrškov se namreč zgodi zaradi malomarnosti zaposlenih, zaradi njihove nezadostne varnostne osveščenosti, zato ker se pri »ukvarjanju z varnostjo« zanašajo na druge ali pa imajo preprosto občutek, da imajo drugo, pomembnejše delo. Razloge za nizko raven varnostne osveščenosti je mogoče iskati tudi v širšem družbenem okolju, ki je s tehnološkim razvojem in z njim povezanimi socialnimi omrežji, mejo o tem, katere podatke še obravnavamo kot zasebne in občutljive, potisnil nižje kot kdajkoli prej. Nezanemarljiv je seveda tudi slovenski zgodovinski kontekst, ki je pojmu varnosti dal neko negativno konotacijo.



O ustrezni varnostni kulturi lahko govorimo šele takrat, ko predpisani varnostni postopki in ukrepi postanejo organizacijsko znanje; ko zaposleni začnejo sami zaznavati varnostno relevantne dogodke in situacije ter o njih poročajo pristojnim. S pravočasnim zaznavanjem se hkrati znižujejo dejavniki tveganja, poročanje pristojnim pa pripomore k hitremu in ustreznemu odzivu ter preprečitvi ali zmanjšanju že nastale škode. Potrebno je razumeti, da zagotavljanje varnosti v nekem podjetju ali državnem subjektu v obravnavanem kontekstu ni samo v domeni »varnostnikov« oziroma tistih, ki so »s sklepom predstojnika določeni, da se z njo ukvarjajo«. Za varnost so odgovorni vsi tisti, ki na njo lahko vplivajo, to pa so vsi zaposleni. Ustrezna varnostna drža in samozaščitno vedenje morata postati ponotranjena vrednota zaposlenih. Ponotranjeno varnostno držo bi lahko primerjali s kulturo pripenjanja varnostnega pasu v vozilu: nekaj let nazaj se je veliko voznikov in sopotnikov z varnostnim pasom pripenjalo predvsem zato, da bi se izognili kazni, ki bi jih doletela v primeru policijskega nadzora. Danes večina voznikov in sopotnikov varnostnega pasu ne uporablja zato, da bi se izognili kazni, pač pa zaradi lastne varnosti. Razumevanje tega dela varnosti je postalo ponotranjena vrednota; nekaj let trajajoči proces, pa vendar. Redno opozarjanje na pomen uporabe varnostnega pasu, periodične in kvalitetne, medijsko dobro podprte kampanje za dvig varnostne osveščenosti so navsezadnje obrodile sadove.

Menim, da je v kontekstu zavedanja pomena varovanja podatkov prvi korak k vzpostavitvi nekih osnovnih varnostnih standardov demistifikacija pojma varnosti. Predstavitev osnov metodologije obveščevalnega delovanja običajno zadostuje, da se zaposleni začenjajo zavedati, da grožnje in tveganja obstajajo

ter pripomore k razumevanju, da je zbiranje podatkov, katere želimo iz različnih razlogov zaščititi, nekaj povsem vsakdanjega. Tudi podjetja na primer spremljajo svojega konkurenta (spremljajo njegove poteze na trgu, zanimajo se o cenah, ki jih postavlja ipd), če želijo pridobiti oziroma ohraniti svojo konkurenčno prednost. Na podoben način bi lahko razložili obveščevalno dejavnost, ki v osnovi ni nič drugega kot sestavljanje mozaika, katerega kamenčke se prizadeva pridobiti iz različnih virov. Metode pridobivanja so odvisne od vrste podatkov, katere se želi pridobiti, prag dostopnosti do varovanih podatkov pa je odvisen od znanja, motivacije, vztrajnosti in nenazadnje tudi finančnih in posledično tehničnih sredstev obeh; tistega, ki si jih prizadeva zaščititi in tistega, ki jih želi odtujiti.

Obravnavni dogodek, povezan s slovenskim zunanjim ministrstvom, je šolski primer odtekanja podatkov zaradi malomarnosti, katerega bi bilo mogoče z lahkoto preprečiti, če bi se udeleženca zavedala tveganj, ki izhajajo iz komuniciranja po nezaščitenih sredstvih. Dogodek je zanimiv tudi z vidika proučevanja ravni varnostne osveščenosti posameznikov, katerim so dodeljene tako občutljive in za nacionalno varnost pomembne naloge. Previdnost pri komuniciranju o neprimernih vsebinah na neprimernih krajih in po neprimernih sredstvih je namreč eden osnovnih varnostnih ukrepov. Če vzamemo v ozir kompleksnejše metode pridobivanja podatkov, ki npr. izkoriščajo osnovne značilnosti ali šibkosti človekovega vedenja; če upoštevamo, da ima »napadalec«, t. j. subjekt, ki želi odtujiti varovane podatke, na svoji strani številne prednosti (npr. čas za pripravo, znanje, izkušnje, motiv), ki mu omogočijo, da »napad« izvede premišljeno in skrbno načrtovano, se nam mimogrede postavi vprašanje o tem kako dobro je v resnici samozaščitno vedenje posameznikov (v tem primeru »žrtev«), ki imajo ob napadu v bistvu zelo malo časa, da pravilno odreagirajo.

O ustrezni varnostni kulturi lahko govorimo šele takrat, ko predpisani varnostni postopki in ukrepi postanejo organizacijsko znanje; ko zaposleni začnejo sami zaznavati varnostno relevantne dogodke in situacije ter o njih poročajo pristojnim.

Koncept varnostne osveščenosti je kompleksen in večplasten, saj imamo ljudje na splošno nerealističen optimizem glede naše lastne ranljivosti. Zavedanje oziroma ponotranjenje zavedanja, da je obveščevalna dejavnost realnost, je eden prvih korakov k izoblikovanju lastnega samozaščitnega vedenja. Pri tem seveda ne govorimo o paranoidnosti in paničnosti, pač pa o skepticizmu, pragmatičnosti in profesionalnosti. Vsak zaposleni, bodisi v strukturah državne uprave bodisi v zasebnih podjetjih, je dolžan presojati varnostni pomen podatkov, prepoznati občutljive informacije, se zavedati svoje odgovornosti in poskrbeti za njihovo ustrezno zaščito. Gre za lojalnost do delodajalca (pa naj bo to država ali podjetje), lastno profesionalnost, etičnost in odgovornost. ■



Avtor: dr. Matej Kovačič / Institut Jožef Stefan

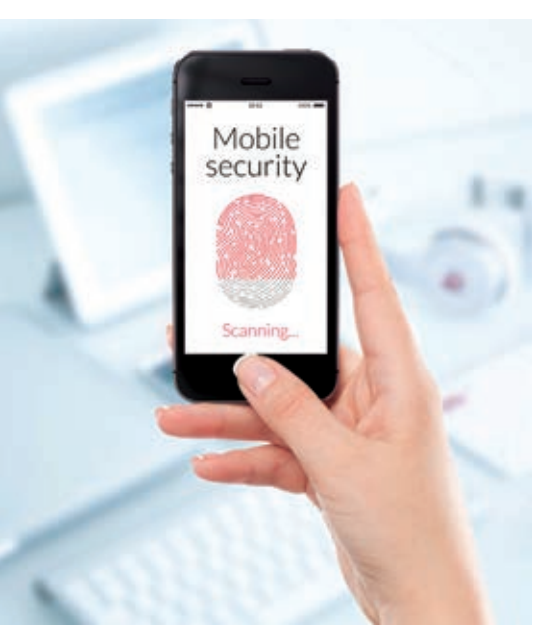


VARNOST MOBILNE TELEFONIJE

Sodobnega življenja si brez mobilnih telefonov praktično ne moremo več predstavljati. Mobilni telefoni nas spremljajo – tudi dobesedno – na vsakem koraku, zato so pomisleki v zvezi z mobilno varnostjo vsekakor na mestu.

Ker je radijske signale mogoče zelo enostavno prestrezati in tako prisluškovati mobilnim komunikacijam, je šifriranje radijskih komunikacij zelo pomembno. Ne preseneča, da je razvoj sodobne kriptografije in zlasti sodobne kriptoanalize močno povezan z odkritjem radijskih komunikacij.

Zgodovina šifriranja zvočnih komunikacij sega v obdobje 2. svetovne vojne, ko je (za današnje razmere) preprosto zvočnio šifriranje radijskih komunikacij pričela uporabljati ameriška vojska. V ta namen so uporabljali napravo SIGSALY, ki je tehtala 55 ton in je napolnila srednje veliko sobo. Za šifriranje telefonskih pogovorov so se kasneje uporabljali posebni telefonski aparati (z vgrajenim modulom za šifriranje in dešifriranje pogovorov), pogosto pa tudi tim. *scramblerji* – samostojne naprave, ki jih je bilo mogoče položiti na telefonsko slušalko, kjer so z vgrajenim mikrofonom "prebrale" vhodni (kodiran) signal, ga dekodirale in nato nekodiranega predvajale na zvočniku (in obratno za mikrofonski del slušalke). Scrambler je sicer naprava, ki omogoča spreminjanje (navadno analognih) signalov, izraz scrambler pa se uporablja tudi za naprave, ki omogočajo šifriranje analognih signalov. A pomemben pospešek šifriranju komunikacij je prinesla digitalna mobilna tehnologija.



Začetki mobilne telefonije sicer segajo že v leto 1946, a prvo komercialno mobilno omrežje so leta 1979 zagnali na Japonskem, leta 1981 pa so na Danskem, Finskem, Norveškem in Švedskem zagnali NMT sistem telefonije (Nordic Mobile Telephone), ki je sprva delovalo na 450 MHz (kasneje so NMT standard razširili še na 900 MHz). Ker pogovori niso bili šifrirani, se jih je dalo poslušati z radioamaterskimi UKV radijskimi postajami.

Leta 1987 je bil razvit standard GSM, ki je bil v osnovi zasnovan tako, da uporabnikom omogoča gostovanje v različnih omrežjih, pogovori v omrežju pa so (praviloma) šifrirani. Prvo GSM-omrežje je bilo postavljeno na Finskem leta 1991, v Sloveniji pa so prvi GSM aparati zazvonili leta 1996. Standardi mobilne telefonije so se kasneje še razširili in danes je tako v komercialni uporabi že četrta generacija mobilne telefonije, tim. 4G ali LTE.

Zaradi nevarnosti prestrezanja GSM telefonija predvideva šifriranje pogovorov – a le med telefonom in bazno postajo. Šifrirni algoritmi, ki se uporabljajo v GSM telefoniji, so bili razviti konec 1980-tih let, žal ob sodelovanju nekaterih zahodnih tajnih služb, ki so poskrbele, da so imeli GSM šifrirni algoritmi vgrajene pomanjkljivosti. Tako so recimo za sejni šifrirni ključ Kc, ki se uporablja za šifriranje GSM pogovorov leta 1997 ugotovili, da je 10 bitov umetno nastavljenih na 0, zaradi česar je bil napad na šifrirni algoritem A5/1 z grobo silo 1024-krat enostavnejši. To ranljivost naj bi odpravile po letu 2001 izdane SIM kartice, a leta 2008 so neodvisni varnostni raziskovalci v okviru A5 Cracking projekta ugotovili še dodatne pomanjkljivosti, ki so pravo velikost šifrirnega ključa Kc v resnici zmanjšale še za dodatnih 10 bitov (tudi na novejših SIM karticah).

Žal podrobnejša analiza pokaže, da pri mobilni telefoniji praktično ni področja, ki ne bi vsebovalo manjših ali večjih varnostnih problemov. Sodobni mobilni telefoni so v bistvu navadni računalniki, morda le s to razliko, da so na nek način še ranljivejši, da ne vsebujejo nekaterih strojnih varnostnih rešitev, ki jih vsebujejo sodobni osebni računalniki. Poleg tega sistem mobilne telefonije, kot tudi telefonskih komunikacij na splošno vsebuje resne varnostne ranljivosti, ki izvirajo iz njegove same zasnove.

Pristopi pri zagotavljanju mobilne varnosti

Varnost mobilnih telefonov se danes načeloma zagotavlja na več ravneh. Prvo predstavljajo metode, s katerimi preprečujemo neupravičen oddaljeni dostop

do mobilne naprave, sledijo metode, s katerimi preprečujemo neupravičen fizični dostop ter metode, s katerimi preprečujemo neupravičeno prestrezanje komunikacij ter beleženje prometnih podatkov.

Eden glavnih mehanizmov zagotavljanja varnosti mobilnih telefonov je uporaba ustrezno ojačanega operacijskega sistema na telefonu. Sodobni mobilni operacijski sistemi tako vsebujejo številne varnostne mehanizme, s katerimi skušajo preprečevati nameščanje neavtoriziranih ali zlonamernih aplikacij, nekateri (zlasti tisti, ki temeljijo na Androidu) pa vsebujejo še številna, pogosto prednastavljena, dodatna varnostna orodja, s katerimi skušajo celovito zagotavljati različne vidike varnosti. Ta orodja so na primer aplikacija za požarni zid, protivirusnik, podpora VPN omrežjem, itd. Neupravičene fizične dostope do mobilnega telefona preprečujemo s šifriranjem notranjega pomnilnika telefona. Verjetno najpomembnejše pa so aplikacije, ki omogočajo šifriranje besedilnih sporočil ter same vsebine pogovorov.

Žal podrobnejša analiza pokaže, da pri mobilni telefoniji praktično ni področja, ki ne bi vsebovalo manjših ali večjih varnostnih problemov. Sodobni mobilni telefoni so v bistvu navadni računalniki, morda le s to razliko, da so na nek način še ranljivejši, da ne vsebujejo nekaterih strojnih varnostnih rešitev, ki jih vsebujejo sodobni osebni računalniki.



Aplikacije za prenos sporočil praviloma uporabljajo podatkovno povezavo (nekatere omogočajo tudi prenos šifriranih SMS sporočil) in če omogočajo šifriranje med končnima komunikacijskima točkama (angl. *end-to-end encryption*, torej med telefonoma obeh komunikacijskih partnerjev), s tem popolnoma onemogočijo prestrezanje oz. dostop do vsebine sporočil med prenosom. Seveda je pri tem pomemben del procesa preverjanje istovetnosti šifrirnih ključev obeh oseb. S preverjanjem šifrirnih ključev namreč preprečujemo napad s posrednikom (tim. *man-in-the-middle napad*), kjer bi se napadalec enemu in drugemu komunikacijskemu partnerju lažno predstavljal in na ta način izvajal prestrezanje njunih šifriranih komunikacij.

Kot standard pri šifriranju zvočnih komunikacij sta se uveljavila protokola ZRTP (Zimmermann Real-time Transport Protocol, gre za sistem, ki omogoča varno izmenjavo šifrirnih ključev med dvema komunikacijskima partnerjema s pomočjo tim. Diffie-Hellmanove izmenjave šifrirnih ključev) ter SRTP (Secure Real-time Transport Protocol, ki se uporablja za šifriranje pogovora). Za šifriranje tekstovnih sporočil se uporabljajo različni protokoli, sodobnejši med drugim uporabljajo tudi mehanizem poudarjene zaupnosti (angl. *perfect forward secrecy), ki omogoča samodejno spreminjanje šifrirnih ključev vsako novo sejo oz. na določeno časovno obdobje. Če napadalec uspe razbiti enega izmed šifrirnih ključev, bo lahko dešifriral le promet, ki je bil šifriran v dani seji.*



Šifriranje zvočnih komunikacij v mobilnih omrežjih sicer predstavlja poseben izziv. Pri uporabi šifrirnih rešitev je namreč pomembna tako izbira kodekov (kodeki skrbijo za kompresijo zvoka), kot tudi kvaliteta prenosa podatkov v mobilnem omrežju.

Raziskovalci iz Johns Hopkins University so namreč leta 2008 ugotovili, da je pri uporabi VBR kodekov - gre za tim. variable bit-rate kodeke, ki različno kompresirajo različne tipe zvokov - mogoče z merjenjem velikosti kompresiranih in šifriranih podatkov z visoko zanesljivostjo identificirati dele besed ali celotne besede paketov brez dešifriranja. Raziskave so pokazale, da je na tak način mogoče v povprečju identificirati 50% besed v pogovoru, za nekatere besede pa je verjetnost prepoznave kar 90%. To velja ne glede na uporabljeni šifrirni algoritem.

Iz tega razloga se je uporabi VBR kodekov pri šifriranih VoIP komunikacijah potrebno izogibati, podobno velja tudi za tehnologije zaznavanja aktivnosti glasu (angl. *voice activity detection* – VAD; gre za tehnologijo, ki zazna tišino in s tem zmanjša nepotrebno kodiranje oz. prenašanje "tišine" preko omrežja). Mimogrede, VBR kodeki, ki omogočajo uhajanje informacij so na primer iSAC, ki ga uporabljajo Skype, Google Talk in Gizmo ter Microsoftov RT Audio, ki se uporablja v aplikaciji Microsoft Office Communicator.

Posebno težavo v mobilnih omrežjih pa predstavljajo zakasnitev oz. latenca (čas, ki preteče od uporabniške zahteve do odziva sistema, od katerega odziv pričakujemo, idealna je latenca do 50 milisekund, nad 250 milisekund zakasnitve že močnovpliva na kvaliteto komunikacije), odmev (tim. echo efekt), problem izgube podatkovnih paketkov (sprejemljivih je do 3% oziroma največ 5% izgube podatkovnih paketkov) ter problem tim. trepetanja sporočil (ang. *jitter,* gre za spreminjanje oz. variabilnost latence pri prenosu podatkovnih paketkov preko omrežja).

Zagotavljanje kvalitetnih šifriranih zvočnih komunikacij v mobilni telefoniji nikakor ni trivialno opravilo, uporabniška izkušnja pri uporabi šifriranih komunikacij pa je pogosto slabša kot pri uporabi nešifriranih komunikacij. Poleg tega morata enaki oziroma združljivi aplikaciji za šifriranje uporabljati oba komunikacijska partnerja. Vse to so razlogi, ki zavirajo širšo uporabo šifriranih komunikacij v mobilni telefoniji.

Zagotavljanje kvalitetnih šifriranih zvočnih komunikacij v mobilni telefoniji nikakor ni trivialno opravilo, uporabniška izkušnja pri uporabi šifriranih komunikacij pa je pogosto slabša kot pri uporabi nešifriranih komunikacij. Poleg tega morata enaki oziroma združljivi aplikaciji za šifriranje uporabljati oba komunikacijska partnerja. Vse to so razlogi, ki zavirajo širšo uporabo šifriranih komunikacij v mobilni telefoniji.

Naprednejši napadi

A kot bomo pokazali v nadaljevanju, navedeni pristopi problema varnosti mobilne telefonije ne rešujejo popolnoma.

Kot rečeno je problematična že sama zasnova mobilne telefonije. Tipičen primer napak v zasnovi je odsotnost mehanizmov avtentikacije mobilnega omrežja mobilnemu telefonu. Mobilna omrežja so bila namreč zasnovana tako, da se je mobilni telefon overil omrežju, omrežje pa se mobilnemu telefonu ni overilo. Razlogi za to so bili verjetno v tem, da je bila vsa logika »skrita« v omrežju, mobilni telefoni pa so se sma-

trali za »neumne odjemalce«. A ta odsotnost overovitve omrežja omogoča uporabo lažnih baznih postaj oz. tim. IMSI lovilcev. S pomočjo IMSI lovilcev je mogoče identificirati uporabnike mobilne telefonije na nekem območju ali pa celo izvesti napad s posrednikom ter na ta način prestrezati mobilne komunikacije brez sodelovanja (in vednosti) operaterja. IMSI lovilce sicer pri svojem delu uporabljajo različne obveščevalne in varnostne službe, a z razvojem tehnologije je lasten IMSI lovilec mogoče sestaviti za nekaj 100 EUR.

Podobno težavo predstavljajo tim. skrita SMS sporočila (angl. *silent SMS*). Gre za posebna SMS sporočila, ki se ne prikažejo na zaslonu prejemnikovega mobilnega telefona, vseeno pa generirajo omrežni promet in celo potrdilo o dostavi. Znano dejstvo je, da je npr. nemška policija v letu 2010 poslala okrog pol milijona tihih SMS sporočil s katerimi je sledila lokacije mobilnih telefonov svojih tarč. Ker se tiha SMS sporočila sprocesirajo na radijskem procesorju mobilnega telefona, jih uporabnik zelo težko zazna. Ta sporočila je mogoče zaznati samo s posebnimi aplikacijami, ki tečejo na tim. odklenjenih Androidnih telefonih s točno določenim naborom radijskih čipov in točno določenimi gonilniki.

Poseben problem pa je lokacijsko sledenje. Temu se praktično ni mogoče izogniti, razen seveda, če onemogočimo kakršnokoli oddajanje radijskih signalov, kar pa pravzaprav onemogoči uporabo mobilnega telefona. Radijski oddajniki mobilnih telefonov namreč oddajajo vsak svoj unikatni identifikator – pa naj bo to Bluetooth, RFID oddajnik, Wi-fi ali mobilni oddajnik. S pomočjo teh identifikatorjev je mogoče z veliko verjetnostjo identificirati lastnika mobilnega telefona, zato ne preseneča, da na območjih konfliktov ameriška vojska navedene identifikatorje uporablja za ciljane napade z droni.

Določene radijske oddajnike sicer lahko izključimo (Bluetooth, RFID), Wi-fi oddajniku lahko spreminjamo MAC naslov, teoretično bi celo lahko spreminjali IMEI številko mobilnega aparata (čeprav je v nekaterih državah to kaznivo), ne moremo pa se izogniti oddajanju IMSI oz. TMSI številke. In če je kdo pomislil, da bi se težavo morda dalo rešiti z odstranitvijo SIM kartice, naj kar takoj povemo, da v tem primeru mobilni telefon v omrežje še vedno oddaja IMEI številko.

Naslednjo skupino napadov, ki si jih bomo ogledali, predstavljajo napadi na šifriran notranji pomnilnik telefona. Prvi tak napad se imenuje Cold Boot napad. Pri tem napadu napadalec pomnilniške čipe mobilne naprave ohladi (na okrog -15 stopinj Celzija), nato pa s pomočjo ustrezne strojne opreme njihovo vsebino prekopira in rekonstruira šifrirne ključe. Uspešen napad so leta 2012 prikazali varnostni raziskovalci Tilo Müller, Michael Spreitzenbarth in Felix Freiling iz Erlangen's Friedrich-Alexander University.

Nekoliko drugačen a s podobnimi posledicami je tim. napad zlobne sobarice (angl. Evil Maid Attack). Napad zahteva fizičen dostop do mobilne naprave, na katero napadalec preko USB vmesnika namesti zlonamerno programsko opremo, ki omogoča prestrezanje gesla za odklep šifriranega telefona. Napad je prav tako leta 2012 uspešno demonstriral varnostni raziskovalec Thomas Cannon. Nekateri mobilni telefoni sicer vsebujejo tehnologijo s katero se takšne napade skuša onemogočiti (od Androida 4.4 dalje je na voljo tim. verificiran zagon – angl. *verified boot*). A tudi te tehnologije napada zlobne sobarice ne rešujejo dokončno, saj je napad še vedno mogoč, le, da se mora napadalec spustiti en nivo nižje. Na primer v tim. ARM Trustzone (Security Extensions ARM procesorjev) ali na nivo SIM kartice.

Najbolj problematični pa so verjetno napadi preko radijskega vmesnika. Mobilni telefoni namreč poleg vsem znanega aplikacijskega procesorja vsebujejo še radijski procesor, ki je praviloma primaren in omogoča neposredni nadzor ostalih delov mobilne naprave (vključno z mikrofonom in kamero). Večina mobilnih telefonov uporablja arhitekturo deljenega pomnilnika, zaradi česar ima radijski procesor dostop do celotne vsebine mobilnega telefona mimo aplikacijskega procesorja.

Kot je že leta 2010 pokazal varnostni raziskovalec Ralf-Philipp Weinman iz University of Luxembourg, radijski procesorji vsebujejo številne varnostne ranljivosti. Njihova izraba omogoča prevzem nadzora nad praktično celotnim mobilnim telefonom, vključno z oddaljenim prisluškovanjem pogovoru v prostoru, kjer se nahaja mobilni telefon. Da tehnologijo uspešno uporabljajo ameriške varnostne službe je znano že vsaj od leta 2006, ko je FBI v okviru kazenskega postopka pred sodiščem razkril, da pri preiskovanju kaznivih dejanj uporablja tim. klateške hrošče (angl. *roving bug*). Glede na povedano pravzaprav ne preseneča odkritje razvijalcev operacijskega sistema Replicant, ki so v programski kodi mobilnega telefona Samsung Galaxy našli namerno vgrajeno varnostno ranljivost, s pomočjo katere je bilo mogoče preko radijskega vmesnika neposredno dostopati do datotečnega sistema v Androidu. In to celo ob uporabi šifriranja.

Zaključek

Mobilna telefonija zato zagotovo ni področje, kjer bi z namestitvijo ene ali dveh varnostnih aplikacij rešili vse težave povezane z mobilno varnostjo. Pomembno se je zavedati katere vse so varnostne ranljivosti v mobilni telefoniji, katere lahko rešimo in katerih ne. Zaradi tempa sodobnega življenja se mobilnim telefonom ne moremo preprosto odpovedati. Ker popolne varnosti mobilnih naprav v svojih žepih ne moremo zagotoviti, je potrebno oceniti nek nivo sprejemljivega tveganja. Predvsem pa se je potrebno zavedati vseh nevarnosti, ki jih mobilna tehnologija prinaša in temu vedenju prilagoditi svoje vedenje. ■



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



ZAVRTE RAZVOJNE MOŽNOSTI ZASEBNEGA VAROVANJA

Dejavnost zasebnega varovanja se nahaja v pomembnem obdobju, ki bo tako na nacionalni kakor tudi evropski ravni potrebovala ustrezne rešitve, katere bodo omogočale ustrezen organizacijski in pravni okvir delovanja in s tem nadaljevanje razvoja.

Uvodoma je treba omeniti, da za področje dejavnosti zasebnega varovanja na področju EU še vedno ni sprejeta ustrezna Direktiva (potem ko je bilo to področje zaradi specifičnosti zahtev teh storitev izvzeto iz Direktive o izvajanju storitev na notranjih trgih). Vendar veljajo tudi za področje zasebnega varovanja v EU določeni skupno sprejeti akti kot npr. Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin ali priporočila evropskega panožnega združenja CoESS (glede oblikovanja kriterijev na področju storitev zasebnega varovanja, tako zlasti za izbiro najboljšega ponudnika glede standardov, licenciranja, usposabljanja). Posebej pomembni pa so judikati Sodišča Evropske unije, ki tudi na področju zasebnega varovanja praktično dosledno odpravljajo omejitve za prosto izvajanje takšnih storitev na tržiščih vseh držav – članic EU. Tako je npr. Sodišče EU že v pravni zadevi C-171/02, t.j. leta 2002, zoper Republiko Portugalsko odločilo, da je prekršila svoje obveznosti iz določb členov 39, 43 in 49 ES (pogodbe o Evropski skupnosti),



s tem ko zahteva, da morajo najprej pod a) tuje gospodarske družbe, ki hočejo na področju zasebnega varovanja opravljati storitve varovanja oseb in objektov, imeti za pridobitev potrebnega dovoljenja ministra za notranje zadeve svoj sedež ali podružnico na Portugalskem, dalje da se ne morejo sklicevati na listine in jamstva, ki so jih že pridobile v državi-članici EU svojega sedeža, dalje da morajo imeti status pravne osebe in da morajo izkazati, da ima družba ustrezen ustanovitveni kapital, in dalje pod b) da mora varnostno osebje tuje družbe, ki namerava izvajati na Portugalskem storitve varovanja oseb in premoženja, pridobiti potrdilo o svoji poklicni usposobljenosti s strani pristojnega portugalskega oblastnega organa. V nasprotju s temi judikati moramo konstatirati, da v zakonodajah držav – članicah EU, tudi Slovenije, še vedno obstaja vrsta takšnih omejitev (zlasti glede obveznosti in pogojev pridobitve zahtevanih licenc, možnosti oziroma pogojev opravljanja občasnih storitev varovanja iz druge države – članice EU idr.)

V tej zvezi je treba pripomniti, da je pristojnost urejanja področja zasebnega varovanja v razmerju med pristojnimi organi EU (Evropski parlament in Svet) na eni strani in pristojnimi organi države – članice EU opredeljena v 4. členu PDEU (Pogodbe o delovanju Evropske Unije), in sicer kot deljena pristojnost med EU in njenimi članicami. To pome-

*avtor je član Slovenskega združenja korporativne varnosti



ni, da članice lahko to področje urejajo samostojno, vendar le ob pogoju, da in dokler ga EU sama ne ureja. V tej zvezi se utegne zastaviti vprašanje, ali države članice EU lahko to področje same urejajo glede na to, da njegova ureditev zaradi njegovih specifičnih zahtev ni bila zajeta z zgoraj omenjeno Direktivo o izvajanju storitev na notranjih trgih (če opustim nekatere parcialne evropske ureditve, kot je nazadnje npr. Uredba (EU) št. 1214/2011 Evropskega parlamenta in Sveta z dne 16. novembra 2011 o profesionalnem čezmejnem prevozu EU gotovine po cesti med državami članicami euro območja). Odgovor je, nikakor, ker je bilo doslej na tem področju sprejeta že vrsta judikatov Sodišča EU, ki imajo posredno tudi ustrezno splošno veljavo.

Zasebno varovanje je v okviru navedenih stališč Sodišča EU opredeljeno kot čista tržna gospodarska dejavnost ne glede na to, da so njene storitve namenjene zagotavljanju varnosti kot eni izmed temeljnih, z ustavo zagotovljenih človekovih pravic. Pri tem za zdaj takšne liberalne opredelitve pogojev in obsega delovanja državnih inštitucij – policije in vojske - , katerih naloga je prav tako zagotavljanje varnosti ljudi in premoženja oziroma obrambe države, nobena zakonodaja ne dopušča. Prav nasprotno, njihovo delovanje je natančno opredeljeno in pogojeno (razen nekaterih izjem v posebnih primerih) izključno na področje zagotavljanja (notranje – policija - in zunanje - vojska) varnosti.

Glede na opisano (še vedno evropsko nezadovoljivo regulirano) stanje je povezanost zasebnega varovanja z navedenimi državnimi organi in institucijami razvidna tudi iz njihove medsebojne komunikacijske in organizacijske povezanosti. Zasebno varovanje je praktično v vseh državah EU organizacijsko uvrščeno v okvir ustreznih državnih organov (Ministrstva za notranje zadeve ali Policije ali Ministrstva za pravosodje), katerih delovno področje je prav zagotavljanje varnosti ljudi in premoženja – z izjemo Nemčije, ki uvršča zasebno varovanje dosledno na področje vladnega resorja, pristojnega za gospodarske dejavnosti. In, če upoštevamo temeljne opredelitve Sodišča EU, ki dejavnost zasebnega varovanja dejansko (popolnoma liberalno) uvrščajo zgolj med eno izmed različnih gospodarskih dejavnosti, moramo pritrditi prav nemškemu zakonodajalcu ter zavzeti kritično distanco do njene posebne opredelitve v večini držav EU.

Ampak dileme ostajajo. Je ta usmeritev dejavnosti zasebnega varovanja dolgoročno, razvojno ustrezna? Vprašanje si sicer res lahko zastavimo, vendar se bojim, da je vlak že odpeljal. Nasproten koncept, ki izhaja iz pomena zagotavljanja varnosti vendar brez posebnih pooblastil, ki jih lahko izvaja le Policija oziroma drug pristojni državni organ, zahteva resnično posebno ureditev te dejavnosti (kot jo ima še večina držav v EU, s tem da so se v tej zakonodaji v zadnjem desetletju – pri nas v obdobju 2007-2008 – že dogodile pomembne spremembe). Druga možnost na tej prekretnici razvoja dejavnosti je bila izključna opredelitev na izvajanje preventivne dejavnosti za onemogočanje oziroma otežkočanje in s tem odvračanje rizičnih in kaznivih aktivnosti z možnostjo, da varnostno osebje v nujnih primerih izvede ustrezne prisilne ukrepe, ki jih sicer v takšnih primerih lahko izvede vsakdo. S takšnim razvojnim konceptom dejavnosti zasebnega varovanja pa je obenem nujno povezana omejitev, po kateri izvajalci te dejavnosti hkrati ne morejo opravljati nalog še na področjih katerihkoli drugih dejavnosti. Njihovo razmerje do vsakokratnega naročnika je namreč mandatno, ki temelji na zaupanju. Zaupanje pa zahteva jamstvo, da morebitne infor-

Zasebno varovanje se je v zadnjem desetletju od navedene naravnanosti bistveno odmaknilo in v velikem zagonu prestopilo na pot čim večje gospodarske uspešnosti – ne oziraje se na vrednote in omejitve, ki jih dejavnost varovanja imanentno vsebuje in zahteva. Strokovna raven absolutno največjega dela varnostnega osebja – varnostnic in varnostnikov - marsikdaj ne dosega niti minimalnih zahtev, njihova delovna obremenitev je mnogokrat prekomerna, njihove plače pa izpod zakonsko določene minimalne višine. Med glavnimi akterji na tržišču varovanja se v ostrem konkurenčnem boju cena varovanja, ki je že desetletja edini kriterij za pridobitev posla, znižuje preko vsake razumne mere.

macije ne bodo zlorabljene v škodo naročnika. Področja delovanja izvajalcev varovanja v tako zastavljenem konceptu te dejavnosti so lahko poleg vseh oblik in nalog varovanja, kot jih poznamo v obstoječi zakonodaji o zasebnem varovanju (v navedenih osmih primerih), še bistveno širše, zlasti na področjih komunikacijskih možnosti, od interneta, elektronskih in drugih sodobnih možnosti, do storitev na različnih socialnih področjih. Prav dejavnostim na teh občutljivih področjih, ki zahtevajo tudi visoko strokovno znanje in specialne izkušnje, mora sodobna družba v času izjemnega tehnološkega razvoja in čedalje večje socialne razslojenosti, prepada med ozkim vrhom komaj predstavljivo premožnim slojem ljudi in ostalo množico prebivalstva, posvetiti posebno pozornost. V današnjem času podivjanega gospodarskega in bančnega grabeža, odprtih vojn in fanatičnih verskih, nacionalnih ter razrednih spopadov in praktično neobvladljivega kriminala potrebujemo bolj kot kdajkoli prej visoko usposobljene strokovnjake z visoko etiko ter zadovoljivo, neodvisno materialno eksistenco.

Ampak možnosti takšnega strokovnega razvoja zasebnega varovanja kot posebne specializirane družbene dejavnosti, so utvara. Zasebno varovanje se je v zadnjem desetletju od navedene naravnanosti bistveno odmaknilo in v velikem zagonu prestopilo na pot čim večje gospodarske uspešnosti – ne oziraje se na vrednote in omejitve, ki jih dejavnost varovanja imanentno vsebuje in zahteva. Strokovna raven absolutno največjega dela varnostnega osebja – varnostnic in varnostnikov - marsikdaj ne dosega niti minimalnih zahtev, njihova delovna obremenitev je mnogokrat prekomerna, njihove plače pa izpod zakonsko določene minimalne višine. Med glavnimi akterji na tržišču varo-



vanja se v ostrem konkurenčnem boju cena varovanja, ki je že desetletja edini kriterij za pridobitev posla, znižuje preko vsake razumne mere. Lastniki glavnih podjetij, ki so v tem konkurenčnem boju za posel varovanja najuspešnejši, pa so med najbogatejšimi osebami v državi. Varovanje se je v tem obdobju etabliralo kot dejavnost z največjimi notranjimi protislovji. Ampak takšen razvoj na področju te dejavnosti, ki bi po svojem pomenu morala biti nasprotje temu, kar je postala – tako v odnosu do lastnih sodelavcev kot do kakovosti svojih storitev, nikakor ni značilen le za Slovenijo. Problem je mnogo širši, zajema praktično vso Evropo, pa tudi številne države na drugih področjih in celinah.

Varovanje se je v obdobju zadnjega desetletja – ponekod pa že prej – razvilo v eno izmed najuspešnejših gospodarskih panog, ki obenem v veliki meri tudi rešuje aktualne probleme brezposelnosti. To, da se je varovanje otreslo svojega nekdanjega statusa dejavnosti posebnega pomena (in omejitev povezanih s takšnim statusom) ter stopilo na tržišče storitev kot vsak drug gospodarski subjekt, v celoti podpirajo oziroma neposredno zahtevajo že omenjena stališča Sodišča EU. Vprašanje, ki se pri tem zastavlja, je seveda zakaj? Ko iščem odgovor na to vprašanje, se ne morem otresti pomisleka, da gre za potrebo oziroma imanentno zahtevo po jasni ločnici med statusom in dejavnostjo gospodarskega subjekta in statusom in nalogami pristojnega državnega organa, t.j. v danem primeru Policije, katere naloge lahko opredeli EU neposredno sama. Status družbe s posebnimi pooblastili posamezne države, članice EU, v ta kontekst ne sodi, je moteč.

Ampak bojim se, da je ta reakcija Sodišča EU v teh letih povzročila prav nasproten razvoj. *Privatizacijo policijskih nalog*. O tem obstaja obsežno delo »Mestno zasebno varovanje« avtorja Thomasa Brunsta, ki podrobno analizira, »kako v Nemčiji panoga varovanja, ki je težka več milijard EUR, pridobiva vpliv in kako njena moč ogroža ustavne pravice«. V tem svojem izjemno obsežnem kritičnem delu avtor na številnih konkretnih primerih (dejansko na ogromni množici takšnih primerov) predstavlja, kako varnostniki, ki so s strani družb, v katerih delajo, brezobzirno izkoriščani, sami s skrajno brezobzirnostjo opravljajo svoje naloge. Za izvrševanje teh nalog so marsikdaj potrebna celo policijska pooblastila, ki so v takšnih konkretnih primerih varnostnikom tudi podeljena. Gre v celoti za dokumentarno gradivo.

Pomembna pa je tudi zelo obsežna raziskava avtorja Joachima Obergfella Fuchsa »Privatizacija policijskih delovnih področij«, izdano s strani Zveznega kriminalističnega urada v letu 2000. Gre za zelo obsežno empirično študijo o tem, kako prebivalstvo v Nemčiji doživlja delovanje služb zasebnega varovanja in kakšno je sodelovanje teh služb s policijo. Na podlagi številnih izsledkov in analiz je mogoče ugotoviti, da gre v veliki meri za korektno, vendar sorazmerno distancirano razmerje, predvsem s policijske strani. Delo naj bi zlasti prispevalo k pričetku varnostno – politične razprave o nalogah, pravicah in pooblastilih zasebno varnostnih služb in njihov pomen za povečanje občutka varnosti pri prebivalcih. Ob tem je danes po 15 letih empirično mogoče ugotoviti, da je razmerje med pripadniki navedenih dveh dejavnosti, t.j. policije in zasebnega varovanja v Nemčiji slej ko prej ostalo na formalni ravni in da med njima ni tesnejšega sodelovanja. Prav tako v vsem tem obdobju – kljub posameznim poskusom nekaterih funkcionarjev - na zakonodajni ravni, kjer je zasebno varovanje obravnavano le v nekaj zakonskih določbah, praktično ni prišlo do nobene spremembe. Glede na povedano k temu ni potreben poseben komentar.

Na podlagi navedenega lahko - še posebej ob prevladujoči javni in/ali politični podpori težnji k t.i. šibki državi - predvidevamo, da se bodo v prihodnosti policijske sile v državah – članicah EU polagoma krčile in da bodo vedno večji del njihovih nalog prevzemale za to usposobljene gospodarske organizacije, ki sicer tudi že sedaj opravljajo naloge varovanja. ■

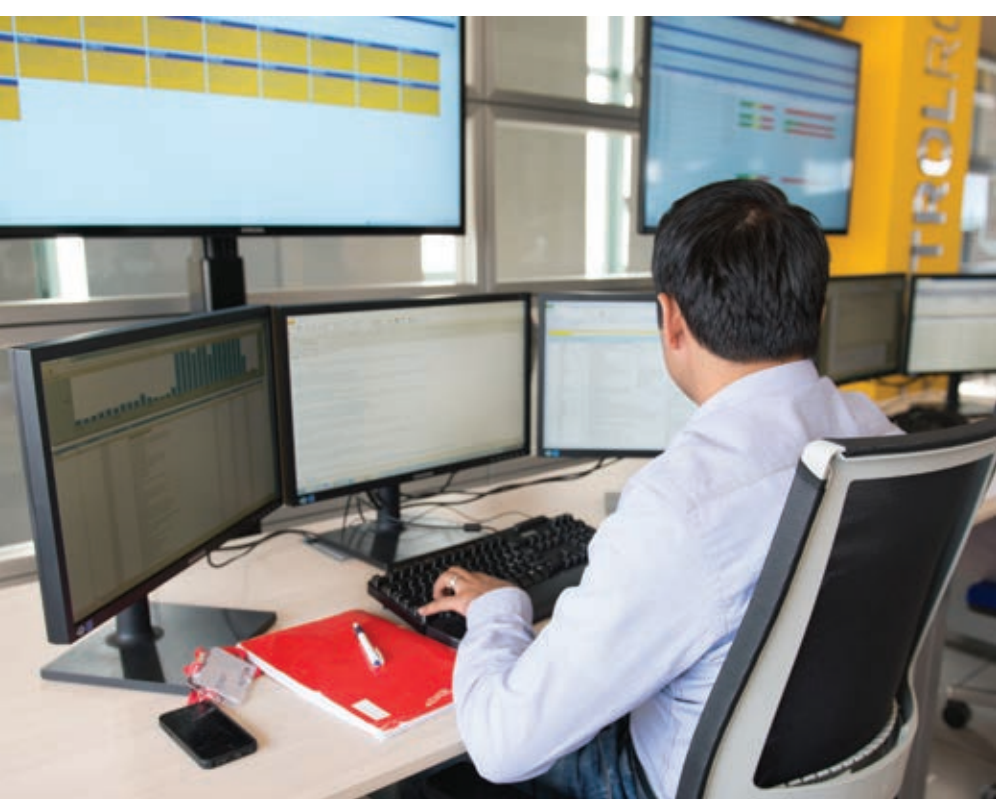


Avtor: Samo R. Zorko / Razvoj poslovnih priložnosti, ZARJA Elektronika



SISTEM VIZUALNEGA UPRAVLJANJA Z ALARMI - AMS

V primeru izrednih dogodkov, kjer potencialno lahko nastane velika materialna škoda, je minuta zelo dolga časovna enota. V takšnih primerih štejejo sekunde, saj so se z novimi materiali močno povečale požarne obremenitve prostorov. Po zaznavi enega ali več fenomenov požara, je ključen reakcijski čas, ko pride do gašenja, avtomatskega ali s pomočjo intervencijske ekipe. Podobno je tudi z ostalimi vrstami alarmov.



Vedno znova se izkaže, da se da s sliko povedati veliko več kot z besedami in da je dobra vizualna informacija v kritičnih trenutkih ključnega pomena. To je še posebej pomembno, kjer je na dvorišču več soodvisnih objektov, kjer gre za funkcijsko porazdelitev lokacij ali lokacije v različnih delih mesta, celo v različnih mestih. Kamniška cesta obstaja v Ljubljani in v Jaršah, razlika pa je tudi ali gori v Mengšu ali Lendavi. Slikovna dimenzija vsebuje veliko število informacij, za katere bi potrebovali zelo veliko besed, da bi jih opisali. Poleg tega v stanju strahu in panike na ključne informacije največkrat pozabimo, jih interpretiramo netočno, da o prenašanju govornih informacij sploh ne govorimo. Če pride do požara v velikem podjetju, z več stavbami, proizvodnimi halami, skladišči ... več uvozi, mora intervencijska ekipa jasno vedeti ali gorijo pisarniški prostori, skladišča z nevarnimi snovmi in možnostjo eksplozije, proizvodne hale .. Ugotavljanje mesta požara in možnosti dostopa na licu mesta zahteva čas, ki ga v takšnih intervencijah ni na razpolago niti sekunde.

Grafični nadzorni centri (GNC), Centralni nadzorni sistemi (CNS), AMS (»Alarm Management Systems«), BMS (»Building Management Systems«) ... so svoje pomembno mesto našli tudi v sistemih tehničnega varovanja, še posebej pa pridejo do izraza tam, kjer je vgrajenih več vrst sistemov: javljanje požara, vloma, kontrola pristopa, video-nadzorni sistem. S stališča preglednosti, upravljanja in vzdrževanja je vse podsisteme tehničnega varovanja na objektih/dvorišču/v podjetju smiselno med seboj povezati in integrirati v enoten sistem. Na večjih objektih je namreč preglednost sistemov in naprav za tehnično



varovanje slaba, upravljanje z njimi pa oteženo. Vzrok za to je lahko, kot že rečeno, več vrst sistemov ali en sistem, ki zaradi obsežnosti vsebuje več central. Vsi dogodki (alarmi, napake, izklopi, opozorila ...) se prikazujejo na zaslonu računalnika ali mobilne naprave v grafični in tekstovni, ali pa samo tekstovni obliki (3D prikaz, tloris, aksonometrični prikaz objekta ...) skupaj ali ločeno za vsako vrsto dogodkov.

Delo varnostnika oz. odgovorne osebe je na ta način zelo olajšano, preglednost nad sistemi tehnične zaščite veliko večja, možnost človeških napak pa minimalna. Ker je komunikacija dvosmerna, AMS – Alarm Management Sistem omogoča tudi krmiljenje in upravljanje s posameznimi elementi tehnične zaščite. Z enostavnim klikom na izbrani grafični element se lahko resetira centrala, izklopi opozorilni ton, vklopi/izklopi javljalnik, odklene/zaklene vrata, krmili videokamere ... Uporabnost in prednosti sistema se pokažejo v vsakdanjih praktičnih situacijah.

Ko je zaradi vročih vzdrževalnih del pričakovan pojav dima, se z enostavnimi kliki izklopi javljalnike v teh prostorih (lažni alarm). Seveda pa morajo biti vsa takšna dela pod strogim nadzorom, saj so ravno vzdrževalna dela kritična glede povzročitve požara. Zavedati se je potrebno, da ti javljalniki ne bodo reagirali tudi v primeru resničnega požara. Po zaključku del pa je potrebno te javljalnike ponovno vključiti v sistem, kar je je v primeru centralnega nadzora zelo poenostavljeno.

Če se na vhodu objekta v nočnih urah zaustavi neznan avtomobil, je zopet povsem enostavno obrniti kamero v želeno smer, približati sliko, osvetliti področje, vklopiti nočni pogled, posneti dogajanje. Pomembno je, da odgovorni osebi ni potrebno zapustiti nadzornega mesta, lokacije nadzora ampak lahko vse to opravi na daljavo. Lahko obravnava sočasen nastop izrednih dogodkov in seveda ustrezno ukrepa. V primeru odhoda na mesto dogodka to ni mogoče, številni takšni dogodki pa so nemalokrat »nastavljeni« zaradi namernega odvračanja pozornosti.

Osnova sistema AMS je SCADA

SCADA sistem ali Supervisory Control and Data Acquisition je programska in strojna oprema namenjena za nadzor in upravljanje z različnimi procesi. SCADA je kratica za programski paket in strojno opremo s katero sodeluje preko procesorske elektronske naprave (IED – »Intelligent Electronic Device« pomeni inteligentno elektronsko napravo) ali preko oddaljene terminalske enote (RTU – »Remote Terminal Unit«), kateri omogočata spremljanje in upravljanje nekega procesa. Podatki se potem prenesejo preko komunikacijskega kanala do glavne enote (MTU – »Master Terminal Unit«), kjer se obdelajo, nadzorujejo in običajno tudi arhivirajo. Obdelani podatki se običajno prikazujejo na operaterskih zaslonih, kjer je možno ukrepati v realnem času, kar daje celotnemu konceptu veliko uporabno vrednost na zelo različnih področjih.

Zgradba sistema

AMS sistem v osnovi temelji na dveh hierarhičnih ravneh. Prva raven vključuje inteligentne elektronske naprave (IED), ki so bodisi oddaljene terminalne enote (RTU) ali programrljivi logični krmilniki (PLC). Kot smo že omenili, elektronske komponente zbirajo podatke iz krmilnih naprav (ali senzorjev) na različnih lokacijah in jih pošiljajo nazaj k nadzorniku (»SCADA master«) sistema, ki predstavlja drugo stopnjo hierarhije. Nadzornik obdeluje podatke in posreduje informacije spet nazaj na prvo stopnjo. Komunikacija med inteligentnimi napravami in nadzornikom je zagotovljena z uporabo lokalnih omrežij (LAN – »Local Area Network«) ali prostranega omrežja (WAN – »Wide Area Network«), lokalnih zaščitenih povezav v lasti podjetij ali nelastniških povezav.

Sistem je sestavljen iz štirih osnovnih gradnikov: javljalniškega (detekcijskega) nivoja, oddaljenih postaj, komunikacijskega omrežja in glavne terminalske enote.

Najnižji nivo predstavljajo senzorji, ki so vezani na vmesnike ali centrale, ki jih nadzoruje sistem. Njihova glavna naloga je pretvorba fizikalnih parametrov v električni signal, ki se nato posreduje oddaljeni postaji.

Senzorji, ki so neposredno povezani s točko merjenja/zaznavanja, oddaljenim postajam posredujejo podatke, ki jih le-te nato obdelujejo in nadzorujejo. Funkcije oddaljene postaje so:

- Zbiranje podatkov iz različnih detekcijskih/merilnih naprav.
- Shranjevanje podatkov v pomnilniku in čakanje na glavno postajo, da te podatke zahteva.
- Prejemanje ukazov iz glavne postaje (MTU).

Oddaljena daljinska postaja je lahko terminalna enota ali programrljivi logični krmilnik. Terminalna enota se uporablja v primeru bolj zahtevnejših komunikacij. Ima digitalne in analogne vhode in izhode s svetlečimi LED diodami za prikaz kanala. Vgrajeni mikroprocesorji so občutno izpopolnili funkcije in procesno moč teh naprav, tako da so sposobne sprejemati samostojne odločitve in se učiti na podlagi zaznavanja informacij iz okolja (preprečevanje lažnih alarmov).

Oddaljene enote, ki so geografsko lahko na zelo različnih lokacijah, so preko komunikacijskih kanalov povezani na glavno terminalno enoto. Za povezavo uporabljamo več različnih komunikacijskih kanalov kot so radijski, internet, ethernet, optika.

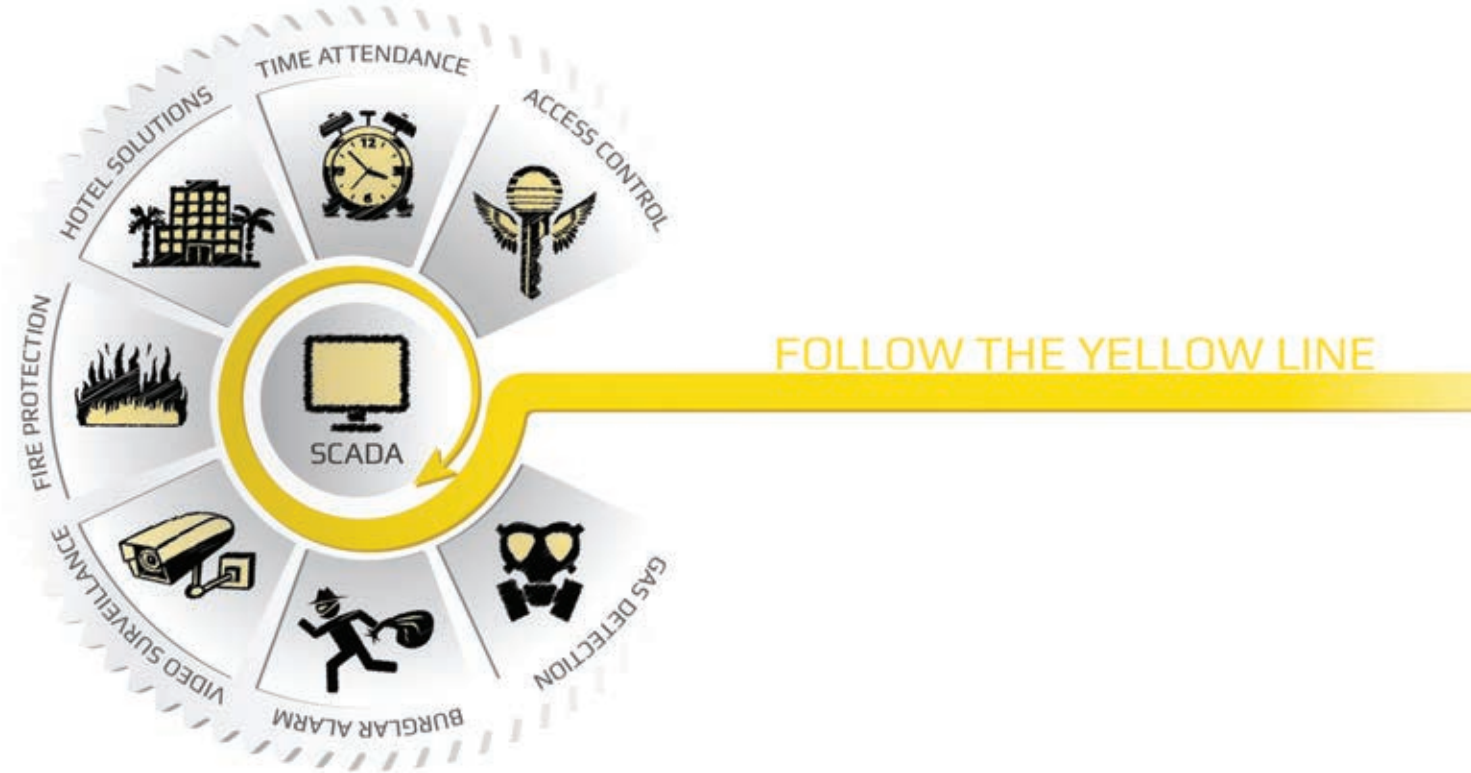
Tehnične karakteristike oddaljenih in glavne enote določajo lastnosti celotnega sistema, njegove omejitve in strošek komunikacijskih kanalov. Dizajn strojne in programske opreme mora zagotoviti, da se podatki pravilno in v realnem času prenesejo iz oddaljenih postaj do glavne enote in da naključen šum ne vpliva na komunikacijski kanal.

Konfiguracija komunikacijskega sistema je odvisna od:

- Števila in lokacij oddaljenih enot.
- Števila odjemnih mest na posamezni oddaljeni enoti.
- Razpoložljivosti komunikacij in komunikacijske opreme, objektov .

Glavna terminalska enota je osrednja kontrolna enota, centralna postaja in je nadzornik SCADA sistema. Je osrednji del sistema, ki skrbi za:





- vzpostavitev komunikacije, zbiranje podatkov, shranjevanje podatkov, pošiljanje informacij do drugih sistemov,
- obdelavo podatkov, zbranih iz oddaljenih postaj, da se izvedejo potrebne akcije in
- povezovanje z operaterji predvsem preko zaslonov in tiskalnikov

Upravljanje z alarmi

Upravljanje alarmnih sporočil temelji na preverjanjih stanj, izvedenih na podatkovnih strežnikih. Zapletenejše algoritme (z uporabo aritmetičnih ali logičnih izrazov) je mogoče definirati z kreiranjem izpeljanih parametrov. Alarmi se logično obdelujejo centralizirano; to pomeni, da informacija obstaja samo na enem mestu in vsi uporabniki vidijo enak status (npr. potrdilo). Alarm ima lahko več nivojev, glede na pomembnost in vrsto. V splošnem so omogočene več kot tri stopnje alarma. Skupinske alarme je mogoče združiti in ravnati z njimi enotno (običajno filtriranje v skupine ali potrditev vseh alarmov v skupini). Alarme se lahko tudi izniči – zavrne, bodisi posamično ali skupinsko. Obstajajo tudi različni filtri: prednostno, prostorsko, časovno ... Je pa pomembnost določenega alarma določena vnaprej in je ni možno enostavno spreminjati, kar je tudi razumljivo.

Prednosti uporabe AMS

Grafični sistem za vizualno upravljanje z alarmi (AMS – »Alarm Management System«) je enostaven za namestitev, priklop, konfiguriranje in uporabo. Prilagoditi ga je mogoče praktično vsem zahtevam in alarmnim centralam različnih vrst tehnične zaščite (lastni produkti in tuji proizvajalci). AMS je s centralami povezan preko komunikacijskega vmesnika, ki prilagodi protokol na strani strojne opreme, in preko programskih gonilnikov, ki omogočajo dvosmerno komunikacijo. Glavna postaja (centralni strežnik) AMS je z oddaljenimi enotami (delovnimi postajami) povezana s standardnim Ethernet TCP/IP omrežjem, ki pa je lahko preko preklopnika ali usmerjevalnika povezano tudi z internim računalniškim omrežjem podjetja. AMS struktura omogoča priklop večjega števila delovnih postaj različnih uporabnikov (varnostnik v recepciji, vodja izmene, direktor, gasilska služba ...). Vsak uporabnik se prijavi s svojim geslom, ki določa obseg in vrsto pooblastil. Vsi dogodki v sistemu (alarmi, izklopi, napake, stanja, obvestila) so shranjeni na datotečnem arhivskem strežniku. Operater s pooblastili lahko v vsakem trenutku te dogodke obdeluje po različnih kriterijih iskanja in prikazovanja. Alarmna in druga sporočila se lahko pošiljajo v obliki elektronske pošte, SMS ali govornih sporočil več izbranim uporabnikom. Ob nastopu izrednega dogodka se lahko na zaslonu prikažejo navodila in koraki, ki jih mora pooblaščena oseba v tem primeru izvesti, v primeru požarnih alarmov in vlomnih dogodkov, interaktivno upravljanje video-sistema in sistema pristopne kontrole. Vsi dogodki in izvršeni ukazi, operacije se arhivirajo. Med arhivirane dogodke spadajo tudi videoposnetki, ki pa so podvrženi Pravilniku o videonadzoru in Zakonu o zasebnem varovanju in je z njimi potrebno ravnati še posebej previdno, v skladu z navodili in pooblastili. ■

Avtorica: Adriana Dvoršak, magistra evropskih študij / Slovensko združenje korporativne varnosti*



VARNOSTNE RAZISKAVE IN INOVACIJE V OBZORJU 2020

Posamične stroke občasno izražajo dvom, da je pridobivanje evropskih sredstev v Sloveniji res optimalno zastavljeno. Organizacija izvajanja operativnega programa 2014-2020 na področju varnostnih raziskav in inovacij je razpršena, za učinkovit pristop je potreben osrednji koordinator in jasen znesek sredstev namenjenih nacionalni varnosti po prednostnih oseh.

Varnostne raziskave in inovacije v 7. raziskovalnem programu in v Obzorju 2020

V prejšnjem obdobju financiranja evropskih raziskav za varno družbo so v okviru sedmega okvirnega raziskovalnega programa dodelili sredstva 542 projektom v višini 1,4 milijarde evrov. Slovenski upravičenci evropskih sredstev so prihajali iz vrst raziskovalnih inštitucij, dinamičnih inovativnih podjetij ter posamičnih oddelkov javnega sektorja.

IZOBRAŽEVALNO RAZISKOVALNE INŠTITUCIJE (Univerza v Ljubljani, Institut Jožef Stefan, Mednarodna podiplomska šola Jožefa Stefana, Univerza v Mariboru),

MALA IN SREDNJA PODJETJA (XLAB, SETTCE, THYIA Tehnologije, Inštitut za fizikalno biologijo),

JAVNA UPRAVA (Informacijski pooblaščenec, Splošna bolnišnica Celje, Mestna občina Ljubljana, Policijska uprava Maribor, Ministrstvo za notranje zadeve).[1]

Udeleženci evropske kohezijske politike in tudi Obzorja 2020 pa so v prvi vrsti potencialni upravičenci, Služba vlade za razvoj in evropsko kohezijsko politiko kot glavni organ upravljanja in nadzora, ministrstva kot posredniški organi, izvajalski organi, v našem primeru gre pozornost predvsem Javni agenciji za raziskovalno dejavnost (ARRS), odbor za spremljanje uspešnosti v katerem so različni deležniki in ki poroča vladi ter Urad za nadzor proračuna kot organ, pristojen za sodelovanje z Evropskim uradom za boj proti goljufijam. Sredstva EU dodeljena Sloveniji za namen izvajanja kohezijske politike v obdobju 2014-2020 znašajo 3.255 milijarde evrov.

Evropske varnostne raziskave Obzorje 2020 v Sloveniji

Podobno strukturo upravičencev lahko pričakujemo tudi v raziskavah varnosti Obzorje 2020, čeprav bi organizacijsko veljalo imenovati nacionalnega predstavnika ali »focal point« in pripraviti informacijski dan na temo evropskih varnostnih raziskav. Poudarjamo, da nacionalni predstavnik pomaga potencialnim upravičencem pri pridobivanju evropskih sredstev iz že razpisanih področij civilne zaščite, notranje varnosti, kibernetske varnosti terorizma, medtem ko političnega odgovora na to, katere slovenske varnostne probleme naj slovenske raziskave sploh rešujejo, še nismo dosegli. Slednje je politično vprašanje, locirano v kabinetu predsednika Vlade. Priprave v ARRS obsegajo predvsem upravljanje raziskav in sodelovanje s posredniškimi telesi, ki razpisujejo ustrezne projekte v okviru kohezijskih sredstev. Trenutno sta to Ministrstvo za gospodarski razvoj in tehnologijo in Ministrstvo za notranje zadeve, medtem ko Ministrstvo za zunanje zadeve

Civilnodružbene organizacije naj bi v novem operativnem programu sodelovale kot partnerji v raziskavah in zagotovile legitimnost raziskav ter spoštovanje zasebnosti in človekovih pravic, saj je civilna sfera zaskrbljena vsled razvoja brezpilotnih letal, zbiranja biometričnih podatkov in masovnega nadzora.

*avtorica je članica Slovenskega združenja korporativne varnosti

in Ministrstvo za obrambo lahko več dosežeta v mednarodnih povezavah in s projekti, ki se nanašajo na jugovzhodno Evropo s severnim in srednjeevropskim delom, tudi z Jadransko-jonsko makroregijo in Podonavsko makroregijo. Ducat mikropodjetij iz varnostnih storitev in svetovanja, centri odličnosti in zagonska podjetja ne morejo prevzeti pobude za nacionalne raziskave varnosti. Prednostna področja skrbno preštudirajo v ustreznih ministrstvih, kompromise sklene politika in na razpise se prijavijo podjetja. Formalno je postopek sicer bolj zapleten. Civilnodružbene organizacije naj bi v novem operativnem programu sodelovale kot partnerji v raziskavah in zagotovile legitimnost raziskav ter spoštovanje zasebnosti in človekovih pravic, saj je civilna sfera zaskrbljena vsled razvoja brezpilotnih letal, zbiranja biometričnih podatkov in masovnega nadzora. Vzorci optimalne ureditve nastajajo in smiselno je, da se stabilizirajo nekje do konca leta 2015 in ne šele v letu 2020.

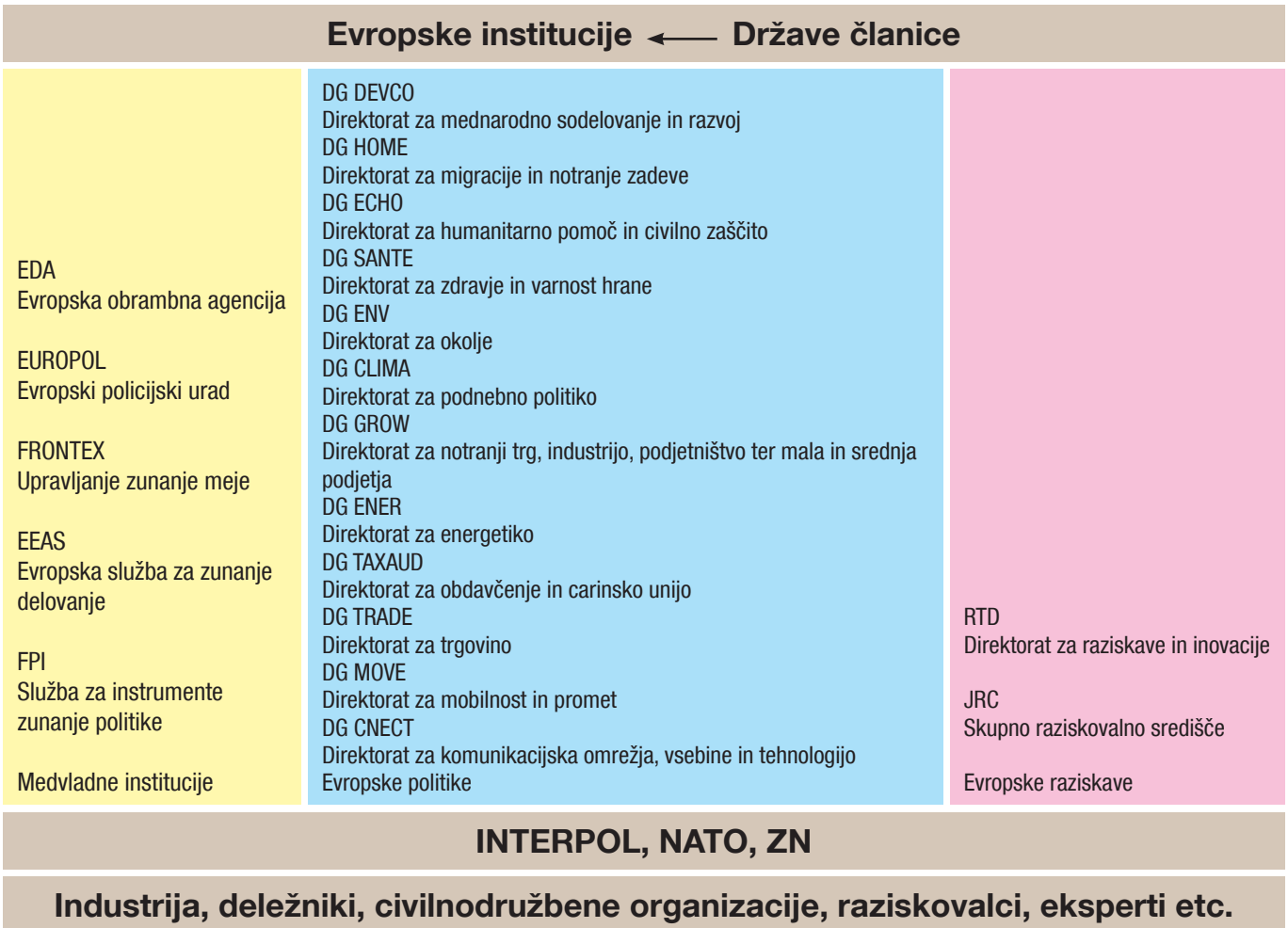
Ne le bazična znanost in aplikativne raziskave, tudi varnostne storitve in svetovanje

Bazična znanost se v državah z učinkovitimi varnostnimi raziskavami in inovacijami razvija v naravoslovnih vedah (biologija, kemija, medicina), varnostne raziskave vsekakor obsegajo tudi humanistične in družbene vede ter bolj inženirske tehnologije in materiale. Multiplikacijski sektor informacijskih in komunikacijskih tehnologij (IKT) je eden izmed ključnih za razvoj informacijske družbe, ustvarjanje delovnih mest, predstavlja pa tudi vir neprekinjenih inovacij v varnostnih raziskavah skupaj s proizvodnjo in storitvami. Slednje so zanimive za sodelovanje malih in srednjih podjetij, ki bi jih morala razpisati ministrstva. Raziskovalne organizacije in podjetja za korporativno varnost bi lahko sodelovala pri javnih razpisih raziskav v varnostnih storitvah in svetovanju, v proizvodnji, shranjevanju in razdeljevanju energije, logistiki, transportnih sistemih, satelitskih tehnologijah in raziskavah vesolja, izdelavi scenarijev, reševanju in evakuaciji, podpori odločanju in drugih. Ker vabilo na informativni dan ne bo prišlo samo od sebe, priporočamo proaktivni pristop ali da zainteresirana podjetja vsaj postavijo kakšno javno vprašanje o tem, kam plovejo naše ladje.

Čeprav Ministrstvo za obrambo, tako kot Ministrstvo za finance in zunanje zadeve v operativnem programu 2015-2020 ne morejo razpisovati projektov, je financiranje varnostnih raziskav možno v okviru drugih resorjev ali v kateri izmed enajstih prednostnih osi. Predvsem govorimo o podpori podjetništvu in malemu gospodarstvu, za katere bi razpise moralo pripraviti Ministrstvo za gospodarski razvoj in tehnologijo, pristojno za tehnologijo vključno z vedno pomembnejšo tehnologijo za dvojno rabo. Ustrezne projekte s področja notranje in korporativne varnosti bi moralo pripraviti tudi Ministrstvo za notranje zadeve in nanje se bodo prijavljala konkretna podjetja, to je upravičenci do evropskih sredstev. Vsekakor pomembne razpise pričakujemo tudi s strani Ministrstva za izobraževanje, znanost, šolstvo in šport, predvsem vse projekte s področja IKT. Pomembno ostaja vprašanje, kakšna je optimalna organizacija tega velikega števila organov, ki bi vsi lahko, v resnici pa noben ni zavezan k političnemu odgovoru na vprašanje, katere slovenske varnostne probleme naj slovenske raziskave sploh rešujejo. Kot primer kako osmisliti varnostne raziskave s poudarkom na pridobivanju kohezijskih sredstev poglejmo evropski koncept (Skica 1), v Sloveniji pa imenujmo enega nacionalnega predstavnika, po možnosti fizično osebo z imenom in priimkom iz ARRS.



Koncept varnostnih raziskav v evropskih politikah



Skica 1: The policy nexus of Security Research, (Priredila A.Dvoršak)[2]

Po drugi strani je razlog za imenovanje političnega koordinatorja dejstvo, da je medresorska Strategija pametne specializacije, ki je osnovni razvojno raziskovalni dokument, nastajala kar tri leta in je varnostne raziskave in inovacije zelo šibko in posredno umestila v področji imenovani delovno okolje in industrija. Preseči je potrebno veliko število pasivnih deležnikov v programiranju kohezijskih sredstev in odsotno politično vizijo. Ustrezno mesto je centralna pozicija v kabinetu predsednika vlade iz katere se določajo prednostne naloge s področja nacionalne varnosti ter ministrstva, ki bodo pripravila javne pozive in razpise ali neposredno potrdila operacije, za kar se bodo pač odločila kot sočasni načrtovalci nacionalnih politik in posredniški organi za kohezijska sredstva.

Civilnodružbene organizacije

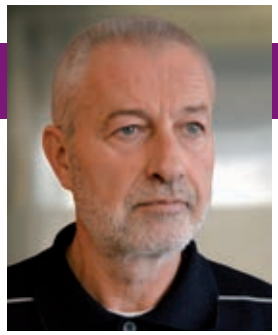
Kot novost varnostnih raziskav, v katero so že vključene slovenske nevladne organizacije, naj omenimo sodelovanje civilnodružbenih organizacij v raziskovalnih projektih Obzorje 2020. Novost je osnovana na Evropski varnostni agendi iz letošnjega aprila in praktično pomeni, da bodo v vsak evropski raziskovalni projekt financiran s strani Evropske unije, vključeni tudi predstavniki civilnodružbenih organizacij. Namen je zagotoviti legitimnost raziskav, saj so z obstoječimi zahtevami po obveščanju javnosti dosegli le informiranje, pogosto pa nikakršne legitimnosti. To velja zlasti za evropske projekte vseobsežnega nadzora v podporo zunanjim politikam Evropske unije, kot so nadzor migracij, zunanje meje in podobno. Le-ti morajo biti tudi sprejeti, da bi v družbi sploh lahko zaživeli.

O tem, kaj se uvrsti na agendo varnostnih raziskav, odločijo države članice na medvladnih dogovorih, kjer pogajanja v veliki meri potekajo pod vplivom velikih evropskih vojaških in varnostnih podjetij. Postopek bo netransparenten in zaprt, dokler ne bomo imeli evropske varnostne strategije s katero bi utemeljili investicije v proizvode in storitve, ki predstavljajo legitimne varnostne odgovore na skupne varnostne grožnje. Slovenija in ostale male države močne industrije ne premoremo, zato nas mora toliko bolj skrbeti, v katere skupne varnostne projekte investira Evropa v našem imenu.

Viri

(Endnotes)
1 Security Research Projects under the 7th Framework Programme, EU Research for Secure Society
2 Security in 2020, Meeting the challenge. ■

Avtor: Vito Murgel, univ. dipl. ekon., svetovalec direktorja, Nova Panorama d.o.o.



REPORTAŽA:
London - mednarodni sejem varnostne industrije

SEJEM IFSEC INTERNATIONAL 2015

Sejem IFSEC International 2015 je potekal od 16. do 18. junija 2015 na razstaviščnem prostoru Excel v Londonu, Anglija. Ta sejem je največji dogodek na področju varnostne industrije, na katerem se zbere velika večina proizvajalcev, distributerjev, dobaviteljev in uporabnikov ter odjemalcev vseh segmentov varnosti iz celega sveta.

Že več kot 40 let predstavlja središče dogajanja v varnostni industriji z zagotavljanjem odličnosti in inovativnosti na vseh segmentih, ki so vključeni v sejemsko prireditev. Vsako leto pritegniti več kot 24.000 obiskovalcev, več kot 650 vodilnih proizvajalcev, dobaviteljev in distributerjev iz 100 držav. Vodilni proizvajalci, distributerji in dobavitelji vsakoletno predstavljajo najnovejše tehnologije in rešitve. Sejem in obsejemske dejavnosti predstavljajo mnogo več kot le prikaz tradicionalnih varnostnih in požarnih rešitev, saj prestavitev zajema vsa področja, ki kakor koli sooblikujejo pojem varnosti.

IFSEC sestavljajo predstavitve tehnično-tehnoloških ter programskih rešitev in seminarji naslednjih produktnih področij kot so videonadzorni sistemi, sistemi pristopne kontrole, inovacije, fizično varovanje, protivlomni sistem, osebni stražarji, internetne varnost, rešitve za pametne naprave, montaža sistemov, sistemi za zgodnje odkrivanje in javljanje požara.

Akademija za izobraževanje, ki je del sejemskih dogodkov, je, z udeležbo največjih svetovnih strokovnjakov s celotnega področja varnosti, nudila brezplačne seminarje za distributerje, monterje, programerje, pa tudi uporabnike s področja vseh segmentov varnosti .

IT in internetna varnost je danes zaradi vse več internetnih groženj eden od najhitreje se razvijajočih varnostnih segmentov, vključena pa je v vse segmente varnosti, ki se kakor koli srečujejo s hrambo in prenosom podatkov, zato je bila v veliki meri vključena v predstavitev in akademijo Varna mesta.

Predstavitev in akademija Varna Mesta je že drugo leto zapored vključena v sejemske dogodke z namenom predstavitve rešitev za prihodnost v mestih, boja proti terorizmu, aplikacij in tehnologij za vzpostavljanje integralnih varnostnih sistemov, ki poleg ostalega vključujejo inteligentne stavbe, inteligentne predele mest pa tudi celotna inteligentna mesta in se osredotoča na zaščito nacionalne kritične infrastrukture ter procese, potrebne za neprekinjeno poslovanje subjektov kritične infrastrukture. Varna Mesta prikazujejo, kako se tradicionalne varnostne rešitve povezujejo z modernimi rešitvami v sisteme, ki igrajo ključno vlogo v naprednih varnostnih arhitekturah mest za zagotavljanje večje neobčutljivosti na razne varnostne grožnje, doseganje višje stopnje varnosti in varnejšo prihodnost, seveda



vse ob usklajenem delovanju vseh služb, ki so kakorkoli povezane z varnostjo, zdravjem, razvojem in podobno. Varnostno vprašanje vedno bolj postaja del našega vsakdanjega življenja in mestne oblasti se dan za dnem pod velikim pritiskom spopadajo s celo vrsto pričakovanih in nepričakovanih nevarnosti in groženj. Predvsem v tako imenovanih mega mestih lahko majhna motnja v katerem koli delu infrastrukture mesta (oskrba z energijo, pitno vodo, javni prevoz, itd.) postane dejavnik, ki vpliva na milijone ljudi in predstavlja ogromno tveganje za zmanjšanje kvalitete življenja, zmanjšanje stopnje varnosti in finančno tveganje, ne nazadnje pa predstavlja tudi oviro za nadaljni razvoj mesta.

Predvsem v tako imenovanih mega mestih lahko majhna motnja v katerem koli delu infrastrukture mesta (oskrba z energijo, pitno vodo, javni prevoz, itd.) postane dejavnik, ki vpliva na milijone ljudi in predstavlja ogromno tveganje za zmanjšanje kvalitete življenja, zmanjšanje stopnje varnosti in finančno tveganje, ne nazadnje pa predstavlja tudi oviro za nadaljni razvoj mesta.

Na področju novitet in inovacij na IFSEC 2015 je bilo predstavljena vrsta novih tehnično-tehnoloških in programskih rešitev. Naj omenimo samo nekatere:

- Face VACS Video Scan C5 je visoko specializirana IP video kamera z nameščeno programsko opremo za zaznavanje in prepoznavo obrazov in tehnologijo sledenja, ki zagotavlja optimalno kakovost slike s prepoznavanjem v realnem času tudi v težavnih pogojih, hkrati pa zahteva dokaj enostavno in cenovno ugodno strojno opremo in majhno pasovno širino za prenos podatkov,
- uvajanje nove identifikacijske tehnologije za natančno in varno identifikacijo s pomočjo »palm žil« (kot so jo poimenovali razvijalci), ki je posebej prilagojena za bančni sektor,
- Sony je predstavil novo PXW-FS7 4k XDCAM kamero, ki se lahko pohvali z Super35 CMOS senzor, ki lahko snema v 4K Quad Full HD (QFHD) in super slow-motion Full HD,
- Arecont Vision je predstavil naslednjo generacijo panoramskih kamer, to sta 5MP Surround Video z Arecont Vision in 12MP Surround Video z Arecont Vision za uporabo v šibki svetlobi z uporabo 12MP tehnologijo Surround Video, obe kameri imata nameščen sistem Wide Dynamic Range (WDR) in motorizirani leči za enostavno nastavljanje,
- zunanji PIR detektor za javljanje gibanja z vgrajeno barvno VGA kamero in močno LED osvetlitvijo, ki sproži snemanje, ko zazna gibanje, deluje na baterije, preko mobilnega omrežja 3G pa se lahko poveže na namensko



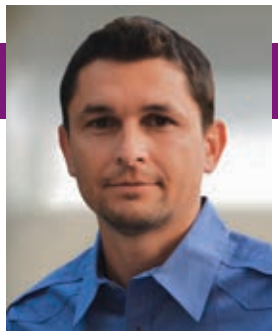


oblačno storitev, ki omogoča oddaljen dostop do posnetkov,

- Road Pixel je programska oprema za spremljanje vozil, omogočanje varnosti in pristopno kontrolo na parkiriščih, lepo oblikovana in enostavna za uporabo, omogoča pa spremljanje vseh podatkov v realnem času in oddaljeno upravljanje parkirišč za uporabniške skupine z različnimi nivoji dostopa in v različno opredeljenih časovnih okvirih, med shranjenimi podatki je omogočeno hitro iskanje preteklih dogodkov po raznih kriterijih (registrska tablica, barva vozila, oblika, znamka, itd.), omogoča pa tudi avtomatska opozorila o posebnih ali neznanih vozilih,
- TBS je predstavil biometrični sistem, ki poleg 3D biometričnega čitalca ponuja celovito programsko rešitev za vse vrste biometričnih aplikacij za nadzor dostopa in prisotnosti, saj s tridimenzionalnimi čitalci in brez dotika senzorska tehnologija zajame največjo možno količino podatkov o prstnih odtisih, kar zagotavlja bistveno večjo varnost in s tem izpolnjuje pogoje predvsem za uporabo na področjih z visokim tveganjem in v večjih uporabniških skupinah ali higiensko občutljivih aplikacijah,
- Simple Home sistem je programska oprema razvijalca Comelite za namestitev v pametni hiši, ki združuje popolno brezžično oddaljeno kontrolo in upravljanje vseh funkcij pametne hiše z vključenimi vsemi sistemi tehničnega varovanja in sistemi za zgodnje odkrivanje in javljanje požara in omogoča popolno oddaljeno kontrolo in upravljanje s pomočjo pametnih telefonov , poleg tega pa sistem omogoča nastavitev optimalne porabe električne energije vseh elementov pametne hiše,
- zanimiva je tudi programska oprema Crime Analytics Tools, ki se uporablja za analiziranje preteklih kriminalnih dogodkov in raznovrstnih groženj ter pripravo simulacij z oceno stopnje potencialnih bodočih kriminalnih dejanj in goženj s poudarkom na tihotapski dejavnosti vseh oblik in z upoštevanjem sodobne tehnološke opremljenosti tihotapskih organizacij,
- Vorty je predstavil sistem kontrole pristopa z bluetooth čitalcem kontrole pristopa, ki omogoča kontrolo in upravljanje vseh, v sistem povezanih električnih ključavnic na vratih in drugih napravah preko bluetooth prenosa signala.

Iz vsega videnega in slišanega na sejmu je dokaj težko izluščiti glavne smernice razvoja varnostnih segmentov. Celoten prikazan napredek in razvoj, tako na področju tehnično-tehnoloških rešitev in kot tudi na področju razvoja programskih rešitev, kaže na vse večjo avtomatizacijo in združevanje vseh procesov, ki kakorkoli igrajo vlogo v celovitem gledanju na življenje v določenem okolju. Okolje pa tudi ni več omejeno na lokalno skupnost, ampak se širi na področja posameznih držav oziroma celo več držav skupaj, ki se srečujejo z enakimi oziroma podobnimi varnostnimi vprašanji, tveganji oziroma grožnjami. Avtomatizacija in združevanje se tako širi na področja življenja, ki direktno niso segment varnosti, lahko pa odločilno vplivajo na varnostne razmere. ■

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



REPORTAŽA:
Mednarodna konferenca "Dnevi korporativne varnosti 2015"

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

Institut za korporativne varnostne študije (ICS) je ob soorganizaciji Slovenskega združenja korporativne varnosti in SE European Corporate Security Association (SECSA) v mesecu marcu organiziral tradicionalno mednarodno konferenco z nazivom »Dnevi korporativne varnosti«. Udeležba več kot 120 udeležencev in visokih gostov iz širšega regijskega prostora je ponovno dokazala, da je dogodek nedvomno postal najkvalitetnejši regijski dogodek na področju korporativne varnosti.

Otvoritveno slovesnost so s svojimi nagovori odprli **dr. Denis Čaleta**, predsednik Slovenskega združenja korporativne varnosti, **g. Mitja Bervar**, predsednik Državnega sveta Republike Slovenije, **mag. Tatjana Bobnar**, namestnica Generalnega direktorja policije, **dr. Dragan Trivan**, podpredsednik Gospodarske zbornice Beograd in **dr. Franc Željko Županič**, direktor Kontrole zračnega prometa Slovenije.

Odlična konferenca je v organizaciji Instituta za korporativno varnostne študije ponovno dokazala, da je vsebinsko ena od najpomembnejših v širšem regijskem prostoru. Skozi odlična predavanja in odmevno okroglo mizo so udeleženci lahko tudi sami razpravljali o dobrih praksah in najnovejših spoznanjih na področju korporativne varnosti. Letos je znotraj glavne konference z osrednjo temo »Korporativna varnost kot orodje v rokah strateškega managementa« potekala tudi konferenca z nazivom „Informacijska varnost - danes in jutri“, ki je udeležencem ponudila zelo aktualne in praktično uporabne informacije s področja obvladovanja informacijske varnosti in kibernetskih tveganj.



V zaključku prvega dneva konference je bila izvedena odmevna okrogla miza na temo »**Korporativna varnost kot orodje v rokah strateškega managementa**«. Udeleženci so bili dr. Franc Željko Županič, direktor Kontrole zračnega prometa Slovenije, mag. Danilo Burnač, direktor Mariborskega vodovoda, dr. Iztok Podbregar član uprave Aerodroma Ljubljana in g. Igor Loborec, član vodstva ELES. Na okrogli mizi sta sodelovala še dr. Dragan Trivan podpredsednik Gospodarske zbornice Beograd in dr. Denis Čaleta, predsednik Slovenskega združenja korporativne varnosti. V razpravo pa se je aktivno vključil tudi g. Zlatko Lazarevič, poslovni direktor Interne klinike UKC. Okroglo mizo je povezovala ga. Katja Fašink iz GEA Collega-Fakultete za podjetništvo. V dinamični razpravi so vsi razpravljavci poudarili pomen razvoja korporativne varnosti, kot enega od ključnih orodij oz. dejavnikov, katerega ima strateški management na voljo za učinkovito obvladovanje tveganj.

Na otvoritvi mednarodne konference je potekala tudi podelitev »**Slovenian Grand Security Award**« za leto 2014. Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje Institut za korporativne varnostne študije, ICS-Ljubljana, v sodelovanju s Slovenskim združenjem korporativne varnosti.

*avtor je član Slovenskega združenja korporativne varnosti

Nagrada je namenjena procesom dvigovanja splošnega zavedanja in varnostne kulture v širši družbeni skupnosti, ki vsebuje poslovna in druga okolja. V šestih kategorijah neodvisna komisija izbere tiste najboljše in najbolj inovativne, ki s svojim zgledom in aktivnostmi na področju zagotavljanja varnosti v svojih sredinah, predstavljajo primer dobrih praks in inovativnih rešitev. Te kvalitete nagrajujemo z uglednimi priznanji, ki so bila tokrat podeljena za dosežke na področju varnosti v letu 2014.

Nagrade so bile podeljena v vseh šestih kategorijah. Podelili so jih g. Mitja Bervar, predsednik Državnega Sveta Republike Slovenije, prof. dr. Jaka Vadnjal, Dekan GEA College-Fakulteta za podjetništvo ter mag. Miran Vršec in dr. Denis Čaleta predstavnika Instituta za korporativne varnostne študije.

- NAJBOLJ VARNO PODJETJE – Kontrola zračnega prometa Slovenije d.o.o. - nagrado je prevzel direktor dr. Franc Željko Županič



- KORPORATIVNO VARNOSTNI MANAGER LETA – g. Sašo Korenjak, Telekom Slovenije d.d. - nagrado je zaradi njegove odsotnosti prevzel g. Marko Boštjančič, svetovalec predsednika uprave



- NAJBOLJ INOVATIVNA VARNOSTNA REŠITEV – podjetje Zarja Elektronika d.o.o. - nagrado je prevzel direktor g. Boris Grivič



- NAJBOLJ VARNO MESTO - Mestna občina Ptuj - nagrado je prevzel Podžupan g. Gorazd Orešek



- NAJBOLJŠA KNJIGA S PODROČJA VARNOSTI – g. Dejan Pavlović in g. Milan Stojanović za knjigo „Ekonomska bezbednost poslovanja“ - nagrado sta prevzela avtorja

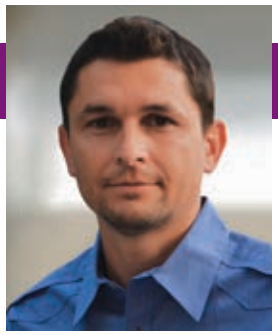


- INOVATIVNA MEDIJSKA PROMOCIJA VARNOSTI - Informativna oddaja ODMEVI, RTV Slovenija - nagrado sta v imenu ekipe, ki ustvarja oddajo, prevzela ga. Mojca Pašek in g. Igor E. Bergant.



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

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



REPORTAŽA:
Nacionalni posvet v Državnem svetu Republike Slovenije

»DILEME IN IZZIVI UPORABE BREZPILOTNIH LETALNIKOV TER NJIHOVA NORMATIVNA UREDITEV«

Aktualnost problematike uporabe brezpilotnih letalnikov (dronov) je dokazala že rahlo pretesna velika dvorana Državnega sveta, kjer se je zbralo več kot 130 udeležencev.

V veliki dvorani državnega sveta je 22. junija 2015 v so-organizaciji ICS-Ljubljana, Državnega sveta Republike Slovenije in Slovenskega združenja korporativne varnosti potekala izredno odmevna okrogla miza z naslovom »Dileme in izzivi uporabe brezpilotnih letalnikov ter njihova normativna ureditev«. Na njej so strokovnjaki predstavili različne vidike, ki neposredno in posredno vplivajo na potrebo po pripravi ustreznih normativnih aktov glede uporabe brezpilotnih letalnikov.



V uvodu sta udeležence pozdravila **g. Mitja Bervar**, predsednik Državnega sveta in **mag. Klemen Grebenšek**, državni sekretar na Ministrstvu za infrastrukturo. Poudarila sta, da so se brezpilotni letalniki pokazali kot izjemno uporabni, tako da so se iz vojaške sfere razmahnili tudi v civilno. Ne prinašajo pa samo koristi, ampak tudi možnosti zlorab in varnostnih tveganj**.** Številne države že pospešeno iščejo rešitve, kako preprečiti zlorabe brezpilotnih letalnikov in grožnje javni varnosti, še preden bi te naprave res postale nevarne.

Aktualno razpravo je odprl **dr. Denis Čaleta**, predsednik sveta Inštituta za korporativne varnostne študije, in problematiko normativne ureditve obravnavanega področja predstavil iz različnih zornih kotov. V nadaljevanju so svoja stališča predstavili vabljeni gostje okrogle mize.

Po besedah **mag. Alojza Krapeža,** vodje sektorja za letalstvo na ministrstvu za infrastrukturo, področja niso zanemarjali. Znotraj EU-ja obstaja težnja po

*avtor je član Slovenskega združenja korporativne varnosti



enotni večplastni ureditvi tega problema na ravni celotnega EU-ja, nekateri pa zagovarjajo idejo, da bi se sprejela le osnovna pravila. Normativno ureditev tega področja pa je treba zasnovati v okviru delovne skupine na ravni vlade. Informacijska pooblaščenka **ga. Mojca Prelesnik** je izpostavila vidik zasebnosti, saj se z uporabo brezpilotnih letalnikov zbirajo in obdelujejo osebni podatki. Poudarila je, da je normativno ureditev sprejelo že kar nekaj evropskih držav, lani jo je sprejela tudi Avstrija. Prav avstrijski model je zelo dober, je prepričana, z njo pa soglaša tudi namestnica generalnega direktorja policije **mag. Tatjana Bobnar**. Slovenska policija že ima delovno skupino za proučitev možnosti uporabe brezpilotnih letalnikov za potrebe policije. Policija vidi uporabnost letalnikov predvsem pri iskanju pogrešanih oseb, še posebej na težavnem terenu, kakršen je gorski svet, za oglede lokacij večjih nesreč, nadzorovanje prometa, preprečevanje nezakonitih prehodov meje in spremljanje demonstracij.

G. Sandi Knez, v. d. direktorja Agencije za civilno letalstvo, je izpostavil, da bo normativna ureditev dobra, če jo bo mogoče kakovostno izvajati in dodal, da so za to potrebni kadrovski in materialni viri.

Stališče Slovenske vojske je predstavil polkovnik **Blaž Pavlin**. Ti so se za nakup brezpilotnih letalnikov že odločili, saj jih bodo potrebovali v okviru vojaških operacij za lažje in cenejše pridobivanje informacij o terenu. Vzpostaviti nameravajo program usposabljanja za operaterje brezpilotnih sistemov, uporabljali pa jih bodo tudi v zaščitne in reševalne namene.

Strokovnjak za letalsko varnost **dr. Iztok Podbregar** in svetovalec direktorja Kontrole zračnega prometa Slovenije **dr. Tone Magister** sta se strinjala, da je treba regulacijo področja zastaviti tako, da bodo ob zagotavljanju primerne varnosti industriji vseeno omogočeni konkurenčni pogoji.

V poglobljeno razpravo so se aktivno vključili tudi udeleženci nacionalnega posveta, ki so s svojih zornih kotov poudarjali nujnost čim prejšnjega sprejema ustrezne normativne podlage za uporabo brezpilotnih letalnikov. S strani odgovornih je bilo poudarjeno, da mora biti normativna ureditev pripravljena do konca 2015 ter, da bo v pripravo ustreznih normativnih aktov povabljena tudi strokovna javnost iz vladnega in nevladnega sektorja.

Naj omenimo še, da je svečani dogodek v uvodu ponudil tudi možnost za sprejem novih članov v Slovensko združenje za korporativno varnost. V združenje so bili sprejeti g. Stanislav Veniger, ki predstavlja korporativnega člana Zavarovalnico Triglav d.d., g. Ivo Blaževič, predstavnik podjetja Elita i.b. d.o.o. ter g. Tibor Tanjšek in g. Boštjan Špehonja. ■



Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Management korporativne varnosti

Magistrski študijski program (2 letni študij)

Izredni študij



Cilj študija

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

Zakaj **Management korporativne varnosti**?

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

Komu je študij namenjen?

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



Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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



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

doc. dr. 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

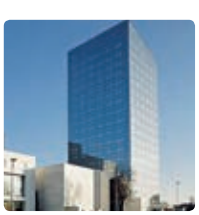
FAKULTETA ZA PODJETNIŠTVO

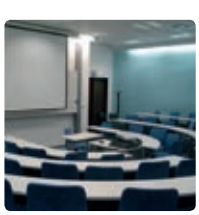
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

Varno v nov dan

