# Korporativna varnost

ICS
Institut za korporativne varnostne študije

Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha! Letnik 2015, marec • št. 9



## Kaj sploh je korporativna varnost

**dr. Milan Vršec, mag. Miran Vršec, ICS-Ljubljana**

## Magistrski program "Management korporativne varnosti"

**Fakulteta za podjetništvo - GEA College**

# 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:
dr. Denis Čaleta

Namestnik odgovornega urednika:
Andrej Kovačič

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
marec 2015

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com

ISSN 2232-6170

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

Slovenija počasi vendar nezadržno postaja del globalnega okolja, kar je na žalost mogoče zaznati tudi na področju povečevanja tveganj in groženj katerim so izpostavljene slovenske organizacije in tudi posamezniki. V družbeni skupnosti je zaznati določene premike v smeri zavedanja, da živimo v okolju, ki je postalo varnostno bolj tvegano, kot smo si bili sami pred časom pripravljeni priznati. Teroristične grožnje po Evropi so medijsko odmevale tudi v Sloveniji, še posebej po javni objavi podatkov, da se tudi slovenski državljani odhajajo boriti na območje kriznega žarišča v Iraku in Siriji. Priča smo anormnemu povečanju spletnih vdorov v informacijske sisteme podjetij in posameznikov ter druga tveganja, ki so povezana s kibernetsko kriminaliteto. Nenazadnje se je začelo tudi v Sloveniji dogajati, da v domnevno naročenem umoru ustrelijo osebo na javnem mestu, kot je bil to zadnji primer direktorja Kemijskega inštituta. To vse nam kaže, da bo v prihodnje varnost postala dobrina za katero bo potrebno poleg višjega zavedanja poskrbeti tudi skozi druge ukrepe, ki ne bodo ostali samo na plečih policije. Le ti bodo tudi v domeni vsakega posameznega subjekta pa naj si gre za podjetje s svojimi vložki v varnost ali za posameznika v svojem zasebnem okolju. Velik korak k višji stopnji varnosti pa vsekakor pomeni višje varnostno zavedanje. Odgovorni lastniki in strateški upravljalci podjetij morajo imeti še kako močan interes, da je korporativna varnost v organizacijah učinkovita do te mere, da v njihovih rokah predstavlja ustrezno orodje pri obvladovanju tveganj za nemoteno delovanje teh organizacij. Koraki na tem področju so sicer počasnejši, kot bi si jih verjetno vsi mi želeli, vendar pa je že opaziti določene pomembne premike, ki bodo dolgoročno zagotovili ustrezno delovanje korporativne varnosti v podjetjih. To spreminjanje zavedanja pri strateškem managementu se kaže tudi skozi pripravljenost strateških managerjev iz pomembnih slovenskih gospodarskih družb, da bodo na okrogli mizi, na letošnjih Dnevih korporativne varnosti, prvič v Sloveniji na tem nivoju, razpravljali o korporativni varnosti, kot njihovem orodju za obvladovanje tveganj v organizacijah katere vodijo. Seveda je k tej prepoznavnosti vsekakor pripomogla tudi nagrada »**Slovenian Grand security Award**«, ki jo tradicionalno vsako leto podeljuje Institut za korporativne varnostne študije in posebej izpostavlja podjetja, posameznike in lokalna okolja, ki so bila najbolj inovativna in so na področju zagotavljanja varnosti naredila veliko delo.

Za uveljavitev korporativne varnosti kot spoštovane profesije, pa morajo strokovnjaki s področja korporativne varnosti, največ narediti sami. Zapiranje v lastne okvirje svojega podjetja in predvsem lastno miselnost, da ni ničesar kar bi se lahko naučil od profesionalnih kolegov, pa je popolnoma zgrešena pot. Danes znanje tako hitro zastareva, da smo se že v nekaj letih popolnoma nepripravljeni in nesposobni zooperstaviti kompleksnim tveganjem in grožnjam, ki obdajajo našo organizacijo. Zaradi navedenega še posebej izpostavljam pomen stanovske organizacije kot je Slovensko združenje za korporativno varnost in okolje, ki ga le ta ponuja za aktivno izmenjavo dobrih praks, novih znanj in predvsem izkušenj. Vsak izmed nas nosi del odgovornosti za splošno stanje profesije korporativne varnosti v družbenem okolju, kjer deluje. To dejstvo jasno izraža tudi eden izmed temeljnih postulatov združenja »Ab uni bisce omnes ali po enem spoznanj vse«. Profesijo na mikro nivoju organizacije ocenjujejo in vrednotijo na podlagi uspešnosti, strokovnosti in prodornosti korporativno varnostnega managerja. Če ta ni ustrezno strokoven in prodoren, dela škodo ne samo sebi in svoji organizaciji, temveč celotni skupnosti korporativno varnostnih strokovnjakov. S tem zavedanjem na mikroravni bomo lahko zelo hitro začeli spreminjati tudi strateške poglede na potrebnost in uveljavljanje profesije korporativne varnosti. Z ugledom in strokovnostjo pa pride z roko v roki tudi ustrezen družbeni položaj in nenazadnje ustrezno plačilo, ki ga dobri korporativno varnostni manager vsekakor zasluži.

Doc. dr. Denis Čaleta
Glavni urednik



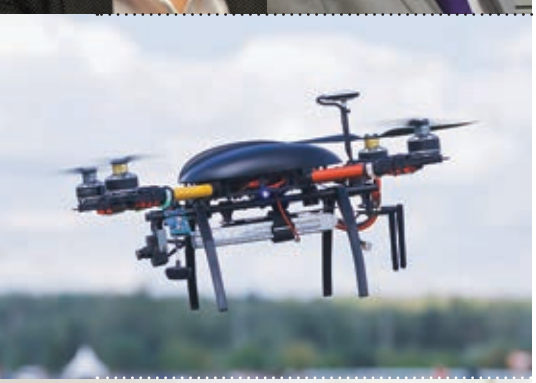
**INTERVJU**
**g. Sašo Korenjak**
Vodja službe za varnost Telekom Slovenije d.d.

KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE 10



**INTERVJU**
**ga. Barbara Černec in g. Tilen Pahor**
Studenta prve generacije magistrskega programa Management korporativne varnosti na Fakulteti za podjetništvo-GEA College

IZOBRAŽEVANJE BODOČIH STROKOVNJAKOV MANAGEMENTA KORPORATIVNE VARNOSTI KLJUČNI TEMELJ ZA PROMOCIJO PROFESIJE 19



BREZPILOTNI LETALNIKI – MED NADZOROM IN ČLOVEKOVIMI PRAVICAMI

Brezpilotniki letalniki ali (droni) si počasi utirajo pot v naš vsakdan. V nekaterih državah so že izrazito prisotni. V Franciji tako obstaja že 650 registriranih operaterjev in 42 proizvajalcev brezpilotnih letalnikov, samo lani pa naj bi prodali 500.000 enot najbolj prodajanega letalnika za domačo rabo. Z naraščanjem uporabe se pojavljajo tudi prvi primeri, ko se porajajo resna varnostna vprašanja glede njihove rabe. 24



KAKO ZMANJŠATI TVEGANJA NOTRANJIH PREVAR

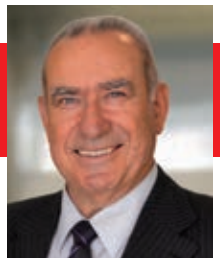
Notranje prevare niso novost ali presenečenje v vsakdanjem in v poslovnem življenju. Novost so najnovejše informacijske tehnologije, ki lahko služijo kot sredstvo za izvajanje notranjih prevar in istočasno kot zelo dobra in učinkovita orodja za preprečevanje in odkrivanje le-teh. 33



DVIG MINIMALNE PLAČE – PASTI IN PRILOŽNOSTI Z VIDIKA KORPORATIVNE VARNOSTI

V zadnjem času se s strani sindikatov pojavljajo zahteve po spremembi definicije minimalne plače. Naj svoj članek začnem z odgovorom na vprašanje: Kaj je plača? 39

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





# KAJ SPLOH JE KORPORATIVNA VARNOST

**V praksi upravljanja z varnostjo se vse bolj uveljavlja izraz korporativna varnost in upravljanje korporativne varnosti. Kljub temu pa še ni povsem jasno kaj korporativna varnost sploh je v okviru korporativnega upravljanja korporacij, koncernov, gospodarskih in drugih družb. Vendar pa je nekaj izhodišč korporativne varnosti možno videti iz najinih prispevkov v dosedanjih revijah Korporativna varnost, kjer je korporativna varnost obravnavana iz različnih zornih kotov.**

## Uvod

Tako kot vsebina dosedanjih prispevkov je tudi vsebina tega prispevka rezultat najinih projektov o vzpostavljanju integralnih varnostnih sistemov v velikih gospodarskih družbah v kritični infrastrukturi in drugih družbah. V naše gospodarske družbe, ki so sestavni del kritične infrastrukture in v drugih družbah namreč še ni dovolj močno prodrlo spoznanje o ekonomskih, poslovnih in etičnih razsežnostih korporativne varnosti. To pomeni, da pri lastnikih, upravljavcih in nadzornikih ni pravega dojemanja vloge, namena, vsebine in koristnosti vzpostavljanja integralnih varnostnih sistemov in managementa korporativne varnosti.

Zato bo v prihodnje treba z izobraževanjem in s promocijo managementa korporativne varnosti ter pridobivanjem projektov vzpostavljanja integralnih varnostnih sistemov informirati lastnike, upravljavce in nadzornike o pozitivnih premikih v procesih korporativnega upravljanja.



## Poskus definiranja korporativne varnosti

Pri pregledovanju literature na temo korporativna varnost sva se odločila, da podava vsaj tri definicije korporativne varnosti, ki so blizu najine opredelitve tega pojma.

»Korporativna varnost je po svoji definiciji integrirana in vsebuje izvajanje več različnih funkcij, ki jih je potrebno sinhronizirati. Kot taka predstavlja funkcijo korporacije, ki kontrolira in koordinira vse dejavnosti znotraj poslovnega subjekta, ki se nanašajo na varovanje, kontinuiteto in varnost. Obstoj učinkovitega sistema korporativne varnosti ščiti poslovni subjekt pred vsemi oblikami ogroženosti, vzpostavlja temelj za odločanje, zagotavlja top managementu pristop k zaupnim informacijam in oblikuje procese in procedure ki preprečujejo iznos varovanih podatkov iz korporacije«( Miloševič, M. v Trivan,D. Korporativna bezbednost 2012, str. 82).

»Korporativna varnost v najširšem pomenu besede je dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Kot taka predstavlja eno od osnovnih funkcij za delovanje podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi ključnimi funkcijami v podjetju. Procesi zagotavljanja korporativne varnosti so nedeljiva celota krovnega modela upravljanja korporacij in se izraža skozi korporativno upravljanje in korporativno družbeno odgovornost.« (Čaleta D. 2014).

»Korporativno oziroma poslovno varnost lahko opredelimo kot varnostni sistem podjetja ali sistem za zagotavljanje notranje varnosti v podjetju. Je celota pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov za ohranitev

*avtorja sta člana Slovenskega združenja korporativne varnosti

Korporativna varnost je integralni varnostni sistem z managementom korporativne varnosti, ki v korporaciji, koncernu in gospodarski družbi, predstavlja enega od varnostno, ekonomsko in poslovno pomembnih ustvarjalcev finančnega zdravja in pozitivnih poslovnih rezultatov.

reda, spoštovanja zakonov in internih predpisov ter varnosti ljudi in premoženja v podjetju.« (Gostič, Š. 2012).

Najino razmišljanje pa je naslednje. Na kratko lahko definicijo korporativne varnosti opredelimo takole: Korporativna varnost je integralni varnostni sistem z managementom korporativne varnosti, ki v korporaciji, koncernu in gospodarski družbi, predstavlja enega od varnostno, ekonomsko in poslovno pomembnih ustvarjalcev finančnega zdravja in pozitivnih poslovnih rezultatov. Vendar pa je treba za natančnejše razumevanje vloge, namena, strukture, vsebine in procesa upravljanja korporativne varnosti bolj natančno definirati njeni glavni sestavini, ki sta:

- Prvič: Integralni (celovit, vseobsežen) varnostni sistem, v katerem mora biti zagotovljena sinergija med posameznimi področji varnosti (varnost in zdravje pri delu, požarna varnost, varstvo okolja, varstvo pred naravnimi nesrečami, fizično in tehnično varovanje, varovanje informacij itd.) in sinergija varnostnega procesa z drugimi poslovnimi procesi.
- Drugič: Management korporativne varnosti, ki je ključni upravljavec korporativne varnosti na vseh organizacijskih ravneh (od najvišjega vodstva do operativnega vodenja), kjer mora biti zagotovljena sinergija med managementom korporativne varnosti in sinergija med managementom korporativne varnosti in ostalim managementom.

Oboje je deležno nekoliko širše razlage, ki je opisno in grafično predstavljena v nadaljevanju.



## Integralni varnostni sistem

Prava podoba integralnega varnostnega sistema se prikaže le v primeru, če ta sistem obravnavamo in opredelimo vsaj z dveh vidikov: z zelo širokega (nacionalnega in globalnega) prostorskega vidika (slika 1) in z vsebinskega vidika (slika 2), ki ga predstavlja arhitektura varnostnega sistema. To je potrebno zaradi tega ker grožnje, nevarnosti, tveganja in spremembe (terorizem, organizirani in gospodarski kriminal, mafije, idr.) prihajajo iz globalnih človeških in tehnično-tehnoloških virov in iz podnebnih sprememb. Znotraj integralnega varnostnega sistema pa je treba videti vse segmente, ki jih je potrebno - glede na zakonodajo, standarde in ocene ogroženosti in tveganj – opredeliti kot nujne za načrtovanje preventive (preprečevanje škod in izgub), obvladovanje izrednih dogodkov in varnostnih tveganj ter za graditev višje stopnje varnostne kulture, poslovne etike ter osebne in družbene odgovornosti.




Slika 1: Prostorski vidik integralnega varnostnega sistema

**Pri prostorskem vidiku** gre za vzpostavljanje integralnega varnostnega sistema od znotraj (varovanje prostorov) navzven (obvladovanje globalnih varnostnih groženj). Kajti najprej je treba varnostno obravnavati lastne človeške vire in lastne vrzeli v varnostnem sistemu in v poslovnih procesih, vzporedno s tem pa tudi zunanje vplivne dejavnike na poslovne procese in na korpora tivno varnost kot so: obiskovalci, stranke oziroma poslovni partnerji in pogodbeni izvajalci. Nadalje management korporativne varnosti zanima kaj se dogaja v neposredni okolici družbe, kaj v slovenskem prostoru in kaj v globalnem okolju, da bi na podlagi preteklih, aktualnih in prihodnjih dogodkov organizirali ustrezne varnostne mehanizme. Z drugimi besedami gre za umestitev konkretne korporacije, koncerna in gospodarske družbe v kompleksno prostorsko dimenzijo, ki je tu pa tam težko varnostno obvladljiva. Zato ne gre prezreti, da je vsak segment prostora od znotraj navzven ali obratno izredno pomemben. Varnostno zanemarjanje katerega od prostorskih dimenzij lahko povzroči velike vrzeli v varnostnem sistemu in s tem sistemsko tveganje, da varnostni sistem v nekaterih delih ne bo učinkovit. To pa si lastniki, poslovodstva in nadzorniki, zlasti pa management korporativne varnosti, ne smejo privoščiti.

**Pri vsebinskem vidiku** pa ne gre za enostavno temveč za dokaj zahtevno arhitekturo integralnega varnostnega sistema, ki ga upravlja management korporativne varnosti. Arhitektura v bistvu predstavlja tri varnostne stebre. Prvi (levi) steber v sliki 2 predstavlja pravno poslovno vsebino, drugi (sredinski) steber predstavlja kadrovsko organizacijsko vsebino, tretji (desni) steber pa predstavlja tehnično tehnološko in funkcionalno vsebino arhitekture integralnega varnostnega sistema. Vse tri stebre pa podpira evropska varnostna politika in pravna regulativa EU, nacionalna zakonodaja, nacionalna varnostna politika, nacionalni varnostni sistem in nacionalni nadzorni sistem. Za obvladovanje tako kompleksnega upravljanja korporativne varnosti oziroma upravljanja integralnega varnostnega sistema je potreben širok portfelj znanj in sposobnosti, poleg tega pa še primerna doza posedovanja komunikacijskih, retoričnih in etičnih vrednot managerjev korporativne varnosti. To velja zlasti za upravljanje korporativne varnosti na strateški ravni in na ravni vodenja službe za korporativno varnost.

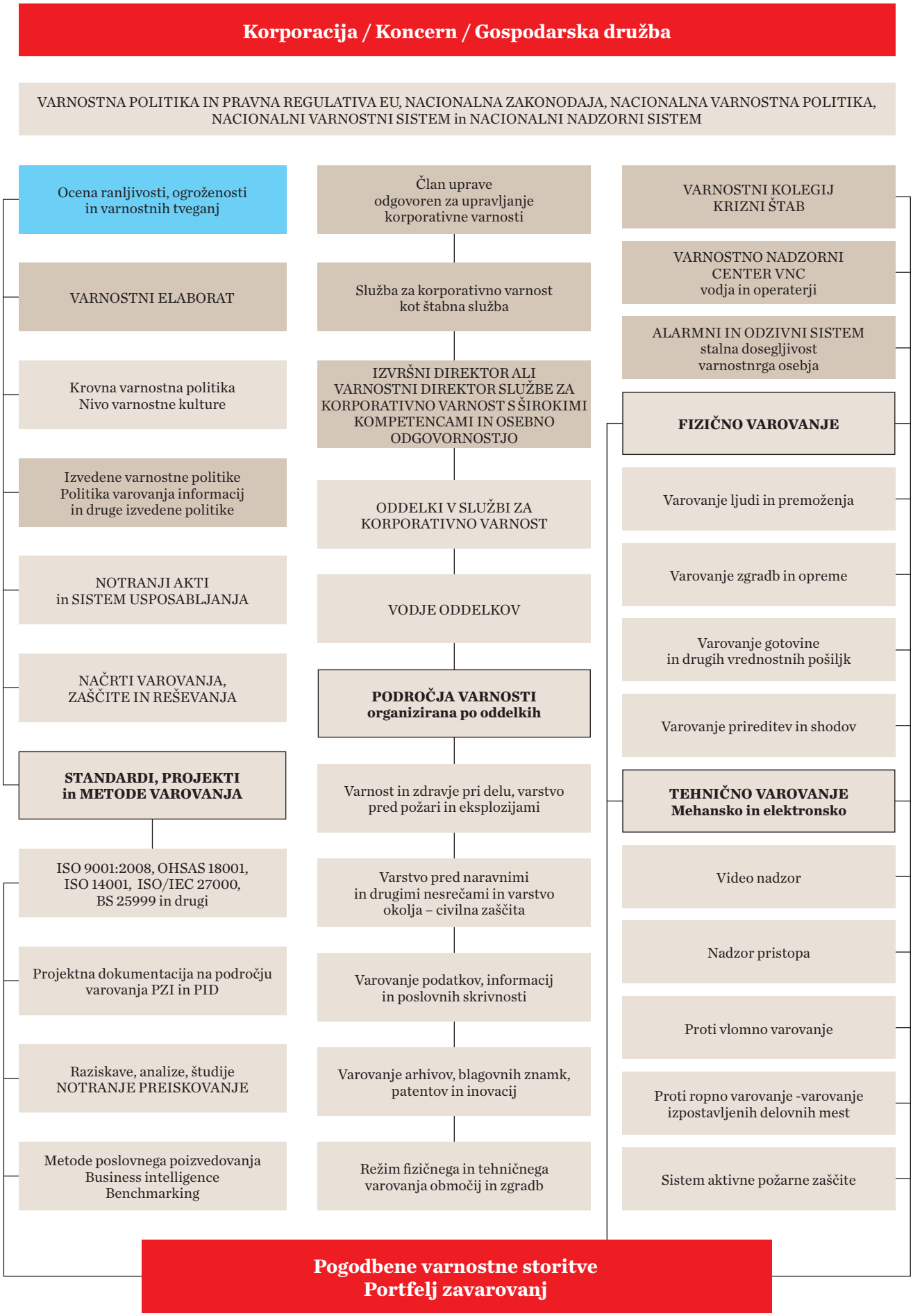
## Management korporativne varnosti

V strukturo managementa korporativne varnosti uvrščamo krovno odgovorno osebo in druge odgovorne osebe, ki upravljajo s posameznimi organizacijskimi enotami integralnega varnostnega sistema. Te odgovorne osebe so:

- Član uprave ali namestnik/pomočnik generalnega direktorja v vlogi krovne odgovorne osebe za upravljanje korporativne varnosti na strateški ravni – krovni manager korporativne varnosti (lahko tudi koordinator upravljanja korporativne varnosti);
- Izvršni direktor ali varnostni direktor službe za korporativno varnost s 4 oddelki (ko gre za korporacije, koncerne in velike gospodarske družbe);
- Vodja oddelka za informacijsko varnost, varnost elektronskih komunikacij in upravljanje neprekinjenega poslovanja ter kriznega vodenja (velika vloga informatike in sistema kriznega komuniciranja);
- Vodja oddelka za varnost in zdravje pri delu, varstvo pred požari in eksplozijami, varstvo pred naravnimi in drugimi nesrečami (zaščita in reševanje-civilna zaščita);
- Vodja oddelka za fizično in tehnično varovanje, upravljanje varnostno nadzornega centra, odzivanje na alarmna sporočila in odzivanje na varnostne grožnje;
- Vodja oddelka za varstvo osebnih in tajnih podatkov, poslovnih skrivnosti, arhivov in blagovnih znamk.
- Vodja (poveljnik) štaba CZ ali poverjenik CZ;
- Vodja kriznega štaba.

Pri managementu korporativne varnosti je treba upoštevati posamezne zakone (denimo Zakon o varnosti in zdravju pri delu, Zakon o varstvu pred požari), po katerih mora poslovodstvo imenovati ustrezno izobražene in usposobljene odgovorne osebe za posamezna področja korporativne varnosti.






Slika 2: Arhitektura integralnega varnostnega sistema, ki ga upravlja management korporativne varnosti

Osnovna oblika delovanja managementa korporativne varnosti je varnostni kolegij, ki ga sklicuje in vodi krovni manager korporativne varnosti ali izvršni direktor za korporativno varnost.

Management korporativne varnosti – v okviru svojih kompetenc in odgovornosti - izvaja zlasti naslednje naloge:

- Upravlja z implementacijo varnostne politike in varnostnega elaborata;
- Informira lastnike in top management o nastalih in potencialnih izrednih (škodnih) dogodkih in načrtovanih ter izvedenih varnostnih ukrepih;
- Zagotavlja, da je vsa varnostna dokumentacija (varnostna politika, elaborati, analize, študije, načrti, navodila, evidence) kompletirana kot celovita in pregledna varnostna dokumentacija;
- Povezuje službo za korporativno varnost z drugimi organizacijskimi enotami v podjetju, ko gre za razreševanje varnostnih vprašanj;
- Nadzira interno in eksterno varnostno usposabljanje;
- Ocenjuje/presoja nevarnosti, ogroženosti in varnostna tveganja;
- Razrešuje vse izredne (škodne) dogodke in pojave kot so nesreče, dogodki kriminalne narave in drugi izredni dogodki;
- Presoja morebitne posledice »skoraj nesreča« in skoraj »kriminalni dogodek«, do katerega še ni prišlo zaradi raznoterih okoliščin (zgodnji opozorilni sistem, pravočasni varnostni ukrepi ipd.);
- Stalno vodi izvajanje in izboljšave načrta varovanja, protipožarnega načrta, načrta evakuacije in drugih načrtov v smeri večje uporabnosti in koristnosti za poslovanje podjetja;
- Daje predloge za varnostne izboljšave v integralnem varnostnem sistemu;
- Načrtuje in pridobiva potrebna finančna sredstva za upravljanje korporativne varnosti;
- Predlaga, spremlja in nadzoruje outsourcing varovanja;
- Sodeluje z notranjo kontrolo in revizijo ter z državnimi nadzornimi institucijami.

Za izvajanje teh nalog so potrebna interdisciplinarna znanja torej znanja s področja zakonodaje, varnostne stroke, standardov kakovosti in varnostnih standardov, ocenjevanja varnostnih groženj, obvladovanja varnostnih in drugih tveganj, načrtovanja, organiziranja, izvajanja in nadziranja dela organizacijskih enot, upravljanja s človeškimi viri, poznavanja trga varnostnih storitev in druga znanja. Vsa potrebna znanja za upravljanje korporativne varnosti na strateški ravni in na ravni služb za korporativno varnost nudi magistrski program Management korporativne varnosti v GEA College Fakulteta za podjetništvo.

Kajti korporativna varnost z managementom korporativne varnosti je tukaj in zdaj ter v prihodnosti priložnost za lastnike, upravljavce in nadzornike, da si namesto razdiralne strategije ustvarijo razvojno vizijo in razvojno strategijo, ki bo s preprečevanjem škod in izgub gospodarstvo postopoma pripeljala v obdobje razcveta.

## Sklepna misel

O vlogi, pomenu in vsebini korporativne varnosti bo v prihodnje najbrž še veliko govora, razprav, debat in proučevanj. To bi bilo dobrodošlo, kajti najin prispevek v tej reviji lahko motivira marsikoga, da se bolj zavzeto posveti razmišljanju kaj sploh je korporativna varnost in v čem je njena »čarobna« moč. Vsakršno razmišljanje bo dobrodošlo za razvoj korporativne varnosti in za krepitev pomena, vloge, statusa, ugleda in dobrega imena managementa korporativne varnosti. Kajti korporativna varnost z managementom korporativne varnosti je tukaj in zdaj ter v prihodnosti priložnost za lastnike, upravljavce in nadzornike, da si namesto razdiralne strategije ustvarijo razvojno vizijo in razvojno strategijo, ki bo s preprečevanjem škod in izgub gospodarstvo postopoma pripeljala v obdobje razcveta. ■



Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*

**INTERVJU**
**g. Sašo Korenjak**
Vodja službe za varnost Telekom Slovenije d.d.

# KORPORATIVNA VARNOST POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE UČINKOVITEGA DELOVANJA ORGANIZACIJE

**V današnjem poslovnem svetu korporativna varnost odraža tudi zavedanje tveganj poslovanja, spremljanje trendov, ustrezno ureditev poslovanja, predvsem pa prinaša dodano vrednost podjetjem, v katerih ima ustrezno mesto.**

**Svoje delo izvajate kot korporativno varnostni manager oz. vodja Službe za varnost v Telekomu Slovenije. Nam lahko poveste, katera so ključna področja vaših pristojnosti?**

Glavna dejavnost Telekoma Slovenije so seveda telekomunikacije in s tem povezane dejavnosti oz. storitve, z razvojem tehnologij pa je naša družba vedno bolj prisotna tudi na trgu celovitih informacijsko-telekomunikacijskih storitev. S tem se širijo tudi aktivnosti na področju varnosti. Tako je poleg klasičnih aktivnosti s področja varovanja, kot so zagotavljanje varovanja ljudi in premoženja, zagotavljanje varnega delovnega okolja in obravnava incidentov, Služba za varnost odgovorna tudi za zagotavljanje neprekinjenega poslovanja, določanje varnostne politike ter izvajanje zakonsko določenih nalog in obveznosti do državnih organov, ob tem pa tudi za preprečevanje potencialnih zlorab in vzpostavitev sekundarnih kontrol pri obračunavanju prihodkov.

g. Sašo Korenjak je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2014«

**Telekom Slovenije predstavlja del kritične infrastrukture na področju sektorja telekomunikacij. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?**

Telekom Slovenije je s svojo dejavnostjo eden izmed nosilcev varovanja v sektorju kritične infrastrukture, ki zagotavlja informacijsko in komunikacijsko podporo. V primeru več kot 24-urnega nedelovanja strojne ali programske opreme, ki podpira ključne funkcije v državi in zagotavlja delovanje t.i. kritičnih sektorjev (kot so energetika, promet, finance...), bi to prav gotovo lahko vplivalo na delovanje države oz. družbe. Pri tem smo se v Telekomu Slovenije najprej opredelili do posameznih tveganj, kot so medsektorska tveganja (kjer npr. zaradi izpada sektorja energije ne bi mogli zagotavljati izvajanja storitev oz. procesov) in zunanji vplivi oz. zunanja tveganja (naravne nesreče, terorizem, nadomestna oprema, delovanje dobaviteljev...). Med koraki, ki smo jih sprejeli, so medsektorska soodvisnost in usklajevanje (npr: energetika - zagotavljanje

*avtor je član Slovenskega združenja korporativne varnosti

oskrbe z energijo za delovanje opreme in zagotavljanje storitev, rezervno napajanje tehničnih zmogljivosti oz. opreme), zagotavljanje georedundance ključnih sistemov za zagotavljanje razpoložljivosti storitev (obhodne poti, nameščanje sistemov na drugih geolokacijah...), usposabljanje zaposlenih, zagotavljanje opreme za osnovne intervencije pri odpravljanju posledic naravnih nesreč in zagotavljanje varovanja ključnih objektov. Izpostavil bi še aktivnosti na področju neprekinjenega poslovanja, kjer imamo vzpostavljen sistem zagotavljanja ključnih storitev družbe.

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

Zavedanje pomembnosti korporativne varnosti in učinkovitega obvladovanja tveganj v slovenskih podjetjih narašča. Vodstva večjih družb se vedno bolj zavedajo širšega pomena varnosti in na zagotavljanje varnosti ne gledajo le skozi prizmo stroškov. Zadovoljni zaposleni, varno delovno okolje in učinkovito obvladovanje tveganj so prav gotovo dejavniki, ki podjetjem prinašajo dodano vrednost in s tem konkurenčno prednost na trgu. K temu je prav gotovo pripomoglo tudi to, da ima varnost kot vrednota v družbenem okolju vedno večji pomen. Okolje, v katerem poslujejo podjetja, se ves čas spreminja, pravočasna prepoznava tveganj in izzivov pa zahteva strokovnost in izkušnje. Tako smo danes v situaciji, ko družbe iščejo strokovnjake, ki znajo prepoznati in ovrednotiti tveganja.

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

Prava in pravočasna informacija je v današnjem času, ko je v okolju ogromno informacij, zelo pomembna. Res pa je, da je z razvojem tehnologije tudi virov informacij vedno več. V Telekomu Slovenije veliko pozornosti namenjamo varnosti ključnih informacij, ki so pomembne za naše poslovanje. Zavedanje in visok nivo varnostne kulture morata biti prisotna pri vseh zaposlenih, zato redno skrbimo za njihovo osveščanje. Ne glede na to, da vedno ne razpolagamo s celotno informacijo oz. imamo le posamezne podatke, se moramo zavedati, da lahko nekdo z ustreznimi veščinami tudi delne informacije med seboj poveže in se z njimi okoristi. Zato je ključno, da se vsak zaposleni zaveda pomena zaupnosti in varovanja informacij.




NAŠE VODILO JE **ZADOVOLJEN UPORABNIK**.
JAZ SEM
Telekom Slovenije


**Kako pristopate k preprečevanju kibernetskih tveganj, ki so v vaši dejavnosti zelo izpostavljena?**

Kibernetskim tveganjem in grožnjam, ki prihajajo iz interneta, namenjamo veliko pozornosti. Pri kibernetskih grožnjah se je potrebno zavedati, da se lahko napad izvede kadarkoli in od koderkoli na svetu, okolje ni več ovira. Telekomunikacijski operaterji sodijo med »zanimivejše« tarče, saj uspešen napad na operaterja lahko pomeni tudi onesposobitev uporabnikov, ki so prek njega povezani v internet. Zato redno spremljamo dogajanja in aktivnosti na tem področju, jih analiziramo in prilagajamo obstoječe načine varovanja. Pri tem sodelujemo z

Okolje, v katerem poslujejo podjetja, se ves čas spreminja, pravočasna prepoznava tveganj in izzivov pa zahteva strokovnost in izkušnje. Tako smo danes v situaciji, ko družbe iščejo strokovnjake, ki znajo prepoznati in ovrednotiti tveganja.

Zavedanje pomembnosti korporativne varnosti in učinkovitega obvladovanja tveganj v slovenskih podjetjih narašča. Vodstva večjih družb se vedno bolj zavedajo širšega pomena varnosti in na zagotavljanje varnosti ne gledajo le skozi prizmo stroškov.

različnimi organizacijami, združenji in operaterji, si medsebojno izmenjujemo informacije in po potrebi tudi usklajujemo aktivnosti. Temu primerno imamo tudi vzpostavljeno interno organiziranost. Vsekakor je to področje, ki zaradi svoje dinamičnosti zahteva nenehno prilagajanje in odzivanje.

**Kakšno je vaše sodelovanje s tujimi operaterji na področju zagotavljanja varnosti in predvsem preprečevanju zlorab informacijskih poti?**

S tujim operaterji smo vsakodnevno v stiku, na področju preprečevanja zlorab pa sodelujemo tudi v dveh združenjih operaterjev, in sicer GSMA in FIINA. V okviru FIINA sodelujejo operaterji fiksnih in mobilnih storitev, medtem ko v združenju GSMA sodelujejo predvsem mobilni operaterji. Aktivni smo v t.i. »Fraud Forumu«, ki se je z letošnjim letom združil s skupino »Security Group«. V okviru novonastale skupine FASG (Fraud and Security Group) so vzpostavljene delovne skupine, kjer si izmenjujemo izkušnje, širijo se zavezništva, opredeljujejo značilnosti zlorab, njihovih posledic in načini ter mehanizmi za obrambo, opredeljuje se nevarnosti in ranljivosti storitev, omrežij in naprav ter iščejo rešitve za še boljšo varnost. Dodatno se spremljajo tudi delovna srečanja organizacije CAFC, ki ima sicer sedež v ZDA, vendar v njej sodelujejo tudi evropski operaterji fiksnih in mobilnih storitev. GSMA je prav gotovo eno najpomembnejših združenj in ima na mobilno panogo tudi največji vpliv.

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

Skrb za izobraževanje in strokoven razvoj zaposlenih sta izredno pomembni. Z razvojem tehnologij so vse bolj popularna e-izobraževanja, pri katerih lahko tudi z omejenimi sredstvi veliko dosežemo, predvsem pa lahko določene vsebine v podjetjih z večjim številom zaposlenih približamo prav vsem. Vlaganje v izobraževanje in osebni razvoj zaposlenih, ki se v podjetjih profesionalno ukvarjajo s področjem varnosti, je nujno in podjetjem prav gotovo prinaša prednosti.

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

Prav gotovo je to ena izmed poti. Poleg izobraževanja pa je potrebno v praksi predvsem širiti zavedanje in uveljaviti pomen ustreznega nivoja korporativne varnosti. Izobraževalni proces in magistrski program nedvoumno dajeta dodatna znanja in širino slušateljem. Menim, da bi k dodatni uveljavitvi stro-






kovnjakov in zavedanju pripomogle tudi posamezne izobraževalne vsebine, ki bi bile namenjene vodstvom v slovenskih podjetjih. Glede na dejstvo, da je skladnost poslovanja eno izmed področij, ki mu slovenska podjetja v zadnjem času namenjajo veliko pozornosti, je mogoče to trenutek, ki bi ga lahko izkoristili in dodali določene vsebine.

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

Telekom Slovenije je član združenja od aprila 2012. Združevanja oz. skupna nastopanja so potrebna in koristna, prav tako je koristna izmenjava izkušenj. Še posebej to velja za slovenski prostor, kjer se korporativna varnost še vedno razvija in postopoma uveljavlja. Združenje je torej izredno pomembno tako z vidika uveljavljanja korporativne varnosti na področju gospodarstva kot z vidika njenega razumevanja v državni upravi in sprejemanja v širši družbi. V današnjem

Telekomunikacijski operaterji sodijo med »zanimivejše« tarče, saj uspešen napad na operaterja lahko pomeni tudi onesposobitev uporabnikov, ki so prek njega povezani v internet.

poslovnem svetu korporativna varnost odraža tudi zavedanje tveganj poslovanja, spremljanje trendov, ustrezno ureditev poslovanja, predvsem pa prinaša dodano vrednost podjetjem, v katerih ima ustrezno mesto.

**Na letošnji otvoritvi mednarodnega dogodka Dnevi korporativne varnosti boste prejeli prestižno nagrado »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2014«, ki ga vsako leto podeljuje Slovensko združenje korporativne varnosti in Institut za korporativno varnostne študije-ICS. Kaj vam osebno pomeni ta laskavi naziv?**

Leto 2014 je bilo za Telekom Slovenije leto, v katerem smo izvedli številne aktivnosti, ki so in ki bodo tudi v prihodnje pomembno vplivale na poslovanje družbe. Pri vseh aktivnostih je izvajanje ustreznih ukrepov s področja varnosti dodatno okrepilo razumevanje in zavedanje o njenem pomenu. V Telekomu Slovenije se zavedamo svoje odgovornosti do uporabnikov naših storitev, do poslovnih partnerjev in do širše družbe nasploh, zato verjamemo, da je ustrezna in učinkovita ureditev korporativne varnosti naša prednost.

Osebno vidim ta laskavi naslov kot priznanje celotni družbi, njenemu poslovodstvu in vsem zaposlenim, ki smo aktivno prispevali k razvoju in uveljaviti varnosti v družbi. Priznanje je potrditev našega dosedanjega dela in je znak, da smo na pravi poti, a hkrati pomeni tudi veliko odgovornost za prihodnost. ■

# Varno v nov dan



Avtor: Samo R. Zorko / varnostni manager, Zarja Elektronika d.o.o.



# INTEGRACIJA TEHNIČNIH SISTEMOV – PRILOŽNOSTI IN IZZIVI

**Leta 1950 je ekonomist Peter Drucker, ki ga lahko štejemo za očeta sodobnega menedžmenta, dejal: »Živimo v času velikih sprememb.« Težko je primerjati spremembe leta 1950 z današnjimi, kaj šele ocenjevati katere so večje. Potem je bilo nekaj časa moderno govoriti ali imeti za podjetje slogan: »Naša edina stalnica so spremembe.« Danes tega ne počne nihče več. Očitno so postale spremembe tako same po sebi umevne.**

Osnovni namen varovanja je obvarovati in zavarovati premoženje ter varovano območje pred nedovoljenimi vstopi, posegi in odtujitvijo. Pod posegi razumemo širok spekter dejanj, ki so za lastnika škodljivi, vsiljivec pa jih opravi z določenim namenom (namestitev/podtaknitev, prikrojitev, poškodovanje ...). Iz samega namena izhaja dejstvo, da je za zagotovitev kvalitetnega varovanja potrebno skrbno in strokovno načrtovanje ter ustrezna izbira tehničnih sredstev. To od samega začetka izbire oblike varovanja vključuje tudi dobro projektiranje. Pomembna je tudi kakovost vgrajenih tehničnih sredstev v sistem varovanja, saj je tako že na začetku zmanjšana verjetnost lažnih alarmov, ki so nezaželeni, prav tako pri naročnikih kot pri dežurnih intervencijskih službah, saj po nepotrebnem angažirajo osebje in povečujejo stroške varovanja. Z vso skrbnostjo in strokovnostjo je potrebno določiti stopnjo ogroženosti človeških življenj in materialnih dobrin, najbolj verjetna mesta za poskus nepooblaščenega vstopa v objekt, pravilne lokacije javljalnikov ... Učinkovitost varovanja pa ni odvisna le od tehnike ampak tudi od hitrega odziva prejemnika sporočila o nedovoljenem vstopu (neželenem dogodku) oziroma reakcijskem času dežurne intervencijske ter servisne službe.

## Biti ali ne biti?

Ne samo biti, tudi bajti, mega in giga bajti. Podatki se prenašajo in hranijo samo še v obliki logičnih ničel (0) in enic (1). Biti (logična 1) ali ne biti (logična 0) to je zdaj vprašanje in osnova digitalne logike in današnjega digitalnega sveta nasploh. To že zelo dolgo ni več vprašanje saj je, odkar je William Shakespeare napisal svojega Hamleta, že davno. Svet se danes »vrti« digitalno in na svetu sta »10« (op. avtorja: 10 v digitalnem zapisu pomeni dve ...) vrsti ljudi. Tisti. ki razumemo digitalno/dvojiško logiko, in tisti, ki je ne. Živimo v svetu digitalnega prenosa podatkov, digitalnega bančništva, digitalne glasbe, digitalnih kinodvoran, digitalne fotografije, digitalne televizije, digitalnih slik ... Živimo v varnih in pametnih hišah s prepoznavanjem prstnih odtisov, procesorji za analizo zvoka in slik, ena naprava je bolj pametna od druge, med seboj komunicirajo, so povezane v omrežja, le-ta pa z nami. Naprave se od nas učijo in posnemajo naše navade, digitalne centrale so možgani sistema, vmesniki in izvršilni členi pa naše roke in noge. Ko nas ni doma, digitalni dom prevzame našo vlogo in na okolico dela vtis, da v hiši vendarle smo.

Pred leti je na steni največjega računalniškega sejma CeBit, v nemškem Hannovru, pisalo: »In zukunft werden wir anders einkaufen, anders verkaufen, anders arbeiten und anders leben.« Kar pomeni, da bomo v prihodnosti nakupovali, prodajali, delali in živeli drugače. Prihodnost se je že zdavnaj zgodila, stvari so se popolnoma spremenile in tudi tehnično varovanje je postalo globalni posel. Tudi varujemo danes povsem drugače. Tehnološki razvoj, predvsem razvoj na področjih elektrotehnike in računalništva, je korenito spremenil tudi področje tehničnega varovanja, varovanja na sploh. Mikroprocesorska tehnologija ima za posledico miniaturi-

Naprave se od nas učijo in posnemajo naše navade, digitalne centrale so možgani sistema, vmesniki in izvršilni členi pa naše roke in noge. Ko nas ni doma, digitalni dom prevzame našo vlogo in na okolico dela vtis, da v hiši vendarle smo.

Zanimivo je, da se vse manj uporablja besedna zveza pametna hiša (»Smart house«) oziroma hišna avtomatizacija. Nadomešča jo termin povezani dom (»Connected home«).

zacijo sistemov varovanja, njihovo programabilnost, funkcionalnost na zahtevo (»Functionality on demand«), povezljivost, interoperabilnost, možnost integracije, oddaljen dostop ... Novi materiali v senzorjih javljalniških elementov omogočajo zanesljivejše, robustnejše delovanje z manj lažnimi alarmi, predvsem pa hitrejšo odzivnost ob nastopu dogodkov v varovanih območjih, kar omogoča še hitrejše in seveda pravočasno ukrepanje. Vzporedno oziroma posledično z razvojem elektrotehnike, so se razvijale tudi telekomunikacije, kar je privedlo do neskončnih možnosti prenašanja alarmnih sporočil preko različnih medijev, kar povečuje uporabnost in prilagodljivost tehničnih sistemov.

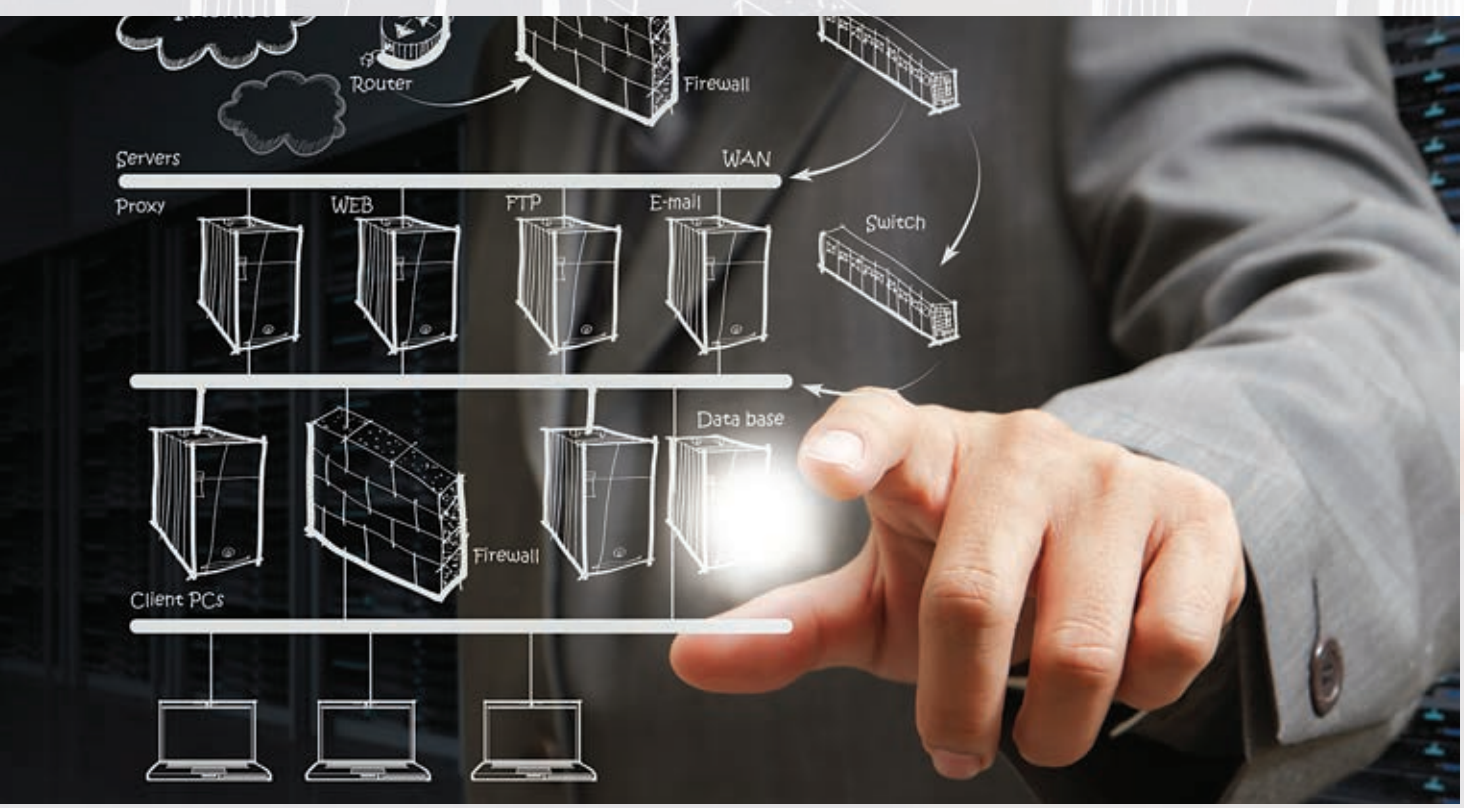
## Začetki segajo v leto 1969

Zarja Elektronika je eno vodilnih slovenskih podjetij na področju tehničnega varovanja z delovanjem v širši regiji. Podjetje je bilo ustanovljeno leta 1969, ko je majhna skupina navdušencev začela z razvojem, proizvodnjo in montažo protivlomnih sistemov. Po letu 1976 je Zarja pričela izvajati elektro inštalacije v večjih industrijskih objektih in objektih širšega družbenega pomena. Pojavljale so se že zahteve po sistemih za zgodnje odkrivanje in javljanje požara. Na tem področju je bila prisotna le Iskra z opremo Cerberus iz Švice, ki pa je imela izredno dolge dobavne roke. V letu 1978 je imela Zarja več naročil za vgradnjo avtomatskih naprav za zgodnje odkrivanje in javljanje požara s pripadajočimi elektro-inštalacijami, v objektih posebnega družbenega pomena. Takrat je bil najpomembnejši objekt nova poslovna stavba Občine Ljubljana-Bežigrad na Linhartovi cesti 13. Svečani rok za izročitev objekta namenu je bil takrat največji državni praznik 29. november 1979. Takratni dobavitelj te opreme Iskra je podala izjavo, da opreme do tega dne ne more dobaviti. Edina rešitev za pravočasno izvedbo bi bila, da Zarja pospeši lastni razvoj naprave za javljanje požara, ki je že bila v fazi preskušanja in prototip že razstavljen na sejmu Elektronike v Ljubljani, septembra 1979, na razstavnem paviljonu Elektrotehne Ljubljana, ki je pri tem poslu sodelovala z Zarjo. V oktobru 1979 je Zarja, na Elektrotehniški fakulteti v Ljubljani, pridobila pozitivni atest za novo razvito napravo za javljanje požara NJP-010, ki je bila nato vgrajena pred 29. novembrom 1979, v novo stavbo Občine LJ-Bežigrad. Avtomatske javljalnike dima RID-1 (z delovno napetostjo DC 200V) je dobavila Elektrotehna Ljubljana.

Od davnih začetkov pa do danes se je Zarja Elektronika preko vztrajnega dela, lastnega znanja in razvoja, nenehnega strokovnega izpopolnjevanja, sledenja svetovnim trendom in izvedbe tehnično najzahtevnejših projektov razvila v dinamično vodilno strukturo z več kot 50 zaposlenimi.

## Integracija osmih področij

Čeprav je podjetje Zarja Elektronika iz Kamnika najbolj prepoznavno po sistemih zaznavanja, javljanja in gašenja požara, pa je močno prisotno tudi na ostalih področjih tehničnega varovanja in zaščite: javljanja prisotnosti plina, tehničnih alarmov, odkrivanja vlomov in ropov, hotelske SOS signalizacije, kontrole prisotnosti in delovnega časa ter video nadzora. Vseh osem stebrov dejavnosti je skupaj z integracijo v en sistem in vizualizacijo predstavilo tudi na letošnjem jubilejnem sejmu Security v Essnu (Nemčija), ki je letos praznoval svojo 40-letnico.

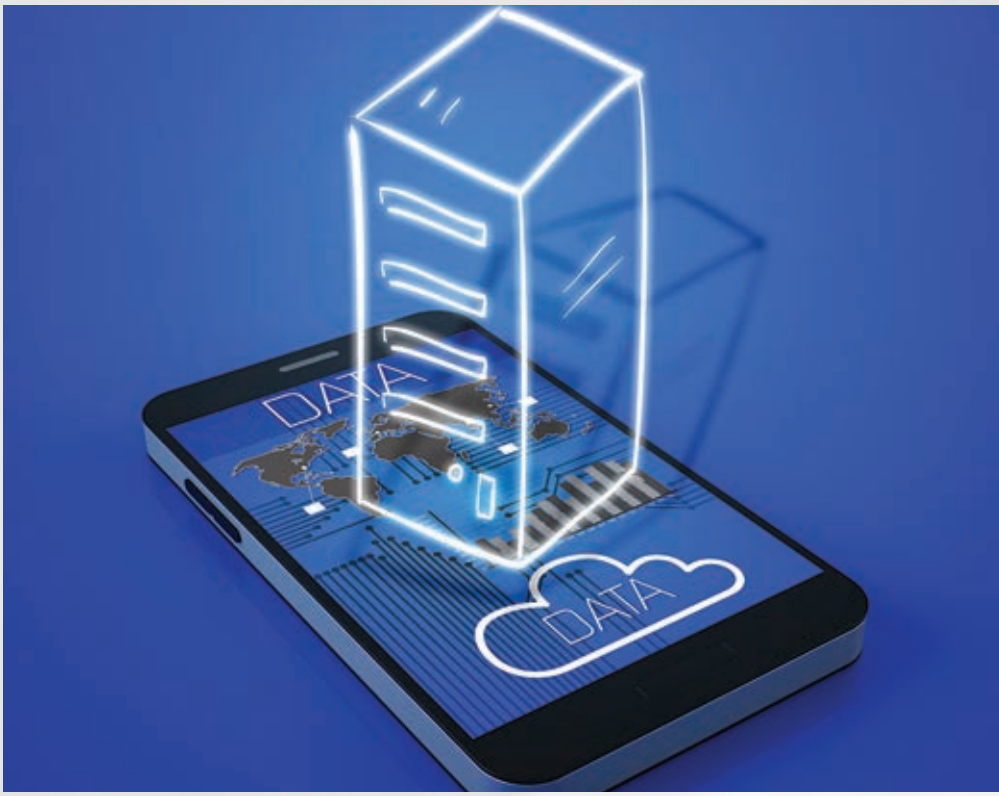


Svoje reference ima v številnih prepoznavnih slovenskih podjetjih, pa tudi v širši regiji. Eden največjih in tehnološko najzahtevnejših projektov v zadnjih letih je bil sistem gašenja z vodno meglo (angl. »water mist«) za potrebe letališča Jožeta Pučnika. Pred leti je Zarja posodobila tudi sistem tehničnega varovanja stavbe Državnega zbora. Čeprav je osnovni namen tehničnega varovanja v vseh primerih enak, pa so pristopi zelo različni, bodisi da gre za Plečnikovo hišo, otroški vrtec, nuklearko, prestižen hotel, industrijski obrat ... Potrebno je zelo veliko znanja in praktičnih izkušenj. Tehnične rešitve podjetja v takšni ali drugačni obliki uporablja že več kot 5000 naročnikov.

Trendi današnjega tehničnega varovanja so, da do škode sploh ne pride, če pa že, naj bo ta minimalna. Povedano drugače, procesi naj zaradi neljubih dogodkov ne bodo moteni. Tudi neprimerno gašenje lahko povzroči veliko škodo. Čeprav le-ta požar in širjenje ognja zaustavi, pa je škoda gašenja lahko tudi večja od škode, ki jo je povzročil požar. Čas do vzpostavitve prvotnega stanja je v tem primeru zelo dolg. Vse to pomeni motnje v poslovnih procesih in dobavnih verigah. Kupci se preusmerijo drugam, proizvodnja stoji, izdelki v skladišču so uničeni ...

Zaradi tega se vedno več uporabljajo čista, plinasta gasila (Novec, FM-200, Inergen, Argonite, ogljikov dioksid). Tudi gašenje z vodno meglo ne povzroči škode saj so kapljice tako majhne, da je z njimi mogoče gasiti tudi knjige v knjižnici. Knjige po gašenju seveda niso uničene. Čista, plinasta gasila se ne uporabljajo le v prostorih z napravami pod napetostjo, za kar so še posebej primerna, ampak tudi v drugih aplikacijah. Z njimi je mogoče pred požarom zaščititi tudi zasebne, muzejske in ostale zbirke neprecenljivih vrednosti.

Podobno je tudi pri vlomu. Vlomilec naj bo zasačen, preden je uspel priti v objekt in napraviti kakršnokoli škodo ter kaj ukrasti. Po eni strani morajo biti detektorji in javljalniki zelo občutljivi, da zaznajo vsako minimalno spremembo, po drugi strani pa dovolj robustni, da ne sporočajo lažnih alarmov. Tu tehnologija vedno išče kompromise, z različni fizikalnimi principi delovanja, ločenim zaznavanjem in zapleteno logiko, »učenjem« sistemov iz okolja, kjer so vgrajeni. Veliko se uporabljajo tudi kombinacije sistemov varovanja, na primer protivlomnega varovanja in videonadzora. Takšne pod-sisteme je potem zaradi




Eden od ključnih elementov za arhitekturo povezanega doma so rešitve, ki temeljijo na tehnologiji oblaka.

enostavnosti upravljanja in vzdrževanja zelo smiselno integrirati v celoto. Ljudje se vedno bolj zavedajo pomena varnosti, tako da se veliko tehničnih sistemov vgradi tudi v individualne hiše, stanovanja, vikende ... Nekateri se za to odločijo šele potem, ko se jim je neprijeten dogodek žal že zgodil.

## Povezani dom, internetne stvari in oblak

Področje tehnične varnosti se pospešeno digitalizira. Tudi starim dobrim alarmnim centralam v kleteh in garažah se ni uspelo skriti pred informacijskimi tehnologijami, internetom in mobilnimi aplikacijami ter komunikacijami. Evforija mobilnih telefonov in tablic je že zdavnaj zajela tudi alarmne centrale, vsak naslednji model je »in« krajši čas in je seveda boljši od predhodnika. Releji in breznapetostni kontakti so se »razklenili« v zgodovino, tipkanja na okorne tipkovnice nameščenih »škatel« je konec. No ne čisto, le oblika škatel in vloga zaslonov se je močno spremenila.

Zanimivo je, da se vse manj uporablja besedna zveza pametna hiša (»Smart house«) oziroma hišna avtomatizacija. Nadomešča jo termin povezani dom (»Connected home«). V naslednjih letih se pričakuje močna rast industrije, ki proizvaja naprave za povezane oziroma pametne domove. Po napovedih analitičnih hiš, ki napovedujejo prodajne trende (»BI Intelligence«), naj bi prodaja teh naprav presegla prodajo mobilnih telefonov in tablic. Če smo do nedavnega govorili o pametni hiši (ogrevanje/hlajenje, razsvetljava, senčila, pametno merjenje, prezračevanje ...) na eni strani in varnostnih sistemih na drugi (požarni sistem/gašenje v kuhinji, vlomni sistem, videonadzor, kontrola pristopa, nadzorni zasloni, zaznavanje strupenih plinov ...), potem koncept povezanega doma vsekakor briše meje med obema poloma naprav. Včasih se je bilo že težko opredeliti ali določen sistem (na primer odpiranje vhodnih vrat s pomočjo prstnega odtisa) spada v koncept varnosti ali pametne hiše. Težko je tudi reči kaj je bilo prej, pametna hiša ali varnost, katera tehnologija se bo sedaj prilagajala kateri, hišna avtomatizacija varnosti ali obratno. Edina logična razlaga, ki jo napovedujejo tudi prihodnji trendi, je povezan dom, kar pomeni, da bosta šli tehnologiji »z roko v roki«. Sistem povezanega doma naj bi bil toliko napreden, da



bo analiziral bivalne navade stanovalcev in jih, v primeru odsotnosti, oponašal. V večini primerov to zadostuje za odvrnitev nepovabljenih gostov.

Eden od ključnih elementov za arhitekturo povezanega doma so rešitve, ki temeljijo na tehnologiji oblaka. Ta imenovana ekonomija oblaka (»Cloud economy«), ki jo poganja zrela mrežna infrastruktura in številne mobilne aplikacije, ustvarja številne poslovne priložnosti v zvezi z upravljanjem doma. Vse to je mogoče z oddaljenih lokacij s pomočjo pametnih prenosnih naprav. Tu ne gre le za vključevanje/izključevanje luči ali termostatov ampak za popoln nadzor nad objektom (vpogled v objekt in okolico, spremljanje dogodkov v objektu, nadzor nad varnostnim sistemom ...), glede na dodeljene pravice in vgrajeno funkcionalnost. Bistvo je, da ne dostopamo do posameznih sistemov in naprav v objektu, ampak je dostop posreden, preko oblaka, ki vsebuje vse pomembne in ključne podatke za krmiljenje naprav.

„Internet stvari" bo v prihodnosti predmetom za vsakdanjo rabo, kot so pametni telefoni, pametni števci, videokamere, vse vrste central, avtomobili, gospodinjski aparati, oblačila in celo hrana ..., s pametnimi čipi omogočal brezžično povezavo z omrežjem ter zbiranje in izmenjavo podatkov. Zadevni podatki zajemajo tudi vedenjske vzorce, lokacijo in prednostne izbire uporabnikov, zato se je potrebno ves čas zavedati, da gre za zelo občutljive podatke. Povprečen človek razvitega sveta ima danes vsaj dve napravi povezani z omrežjem, do leta 2020 pa naj bi to število naraslo na sedem, kar bo na svetovni ravni pomenilo 25 milijard brezžično povezanih naprav. To pomeni, da bo v prihodnosti povezanih veliko vsakdanjih stvari. Na primer, če bi zadnji zaposleni ob odhodu iz službe pozabil vklopiti alarm, bi sistem preveril prisotnost v objektu, pregledal ustaljeno prakso (navade zaposlenih, statistiko) in samodejno vklopil alarm. Če sistem dalj časa ne bi zaznal gibanja starejše osebe, bi se opozorilno sporočilo poslalo bližnjemu sorodniku ali celo bližnjemu centru za pomoč, tako da bi lahko preverili, če je s to osebo vse v redu.

## Vse je v (pametnem) koncentratorju

Le nekaj let za industrijo električnih števcev in merjenja (»Smart metering«) je na identičen problem naletela tudi industrija tehnične varnosti. Kako pod eno streho postaviti različne modele, različne generacije izdelkov, različne proizvajalce, komunikacijske protokole ... in pričakovati, da bo delovalo? Industrija merjenja si je takrat izmislila IDIS (»Interoperable Device Interface Specification«). Pri merjenju je koncentrator v transformatorski postaji bral podatke iz dodeljenih električnih števcev, jih hranil in posredoval naprej. Kako se bo vprašanja standardizacije in interoperabilnosti lotila industrija povezanega doma? Bo ponovila napake storjene na drugih področjih? Kakorkoli obrnemo, pri integraciji ne moremo mimo standardizacije in interoperabilnosti.

Koncentrator (»gateway«, »hub«, »router«) je najpomembnejša komponenta pametnega/povezanega doma. Koncentrator rešuje »problem« povezovanja in komuniciranja naprav različnih proizvajalcev in različnih standardov. Zadnja generacija koncentratorjev (»Smart concentrator«) združuje štiri funkcije: inteligentno upravljanje s prometom, pametno nastavljanje propustnosti mreže, enostaven krmilni vmesnik in na tehnologiji oblaka temelječo nadgradnjo. Učinkovitost hišnega omrežja (»HAN – Home Area Network«) postane še posebej pomembna, ko se v sistemu nahaja več kot 20 različnih naprav, kar pa je ob današnjih trendih seveda kar hitro. Pametni koncentrator ima sposobnost, da sam nastavlja prioritete mrežnega prometa in tako optimizira propustnost mreže oziroma internetne povezave (»LAN-Local Area Network«, »WAN – Wide Area Network«).

## Varno v nov dan

Kot proizvajalci sistemov tehnične varnosti smo neprestano vpeti v trikotnik; **zadnjega stanja tehnike – kontinuiranega in hitrega tehnološkega razvoja**, **trga – naših strank** in **zakonodaje**: tehnične (standardi, smernice, priporočila, direktive) na eni strani in pravno organizacijske (ZZasV) na drugi strani. Vse to je neprestano »v gibanju«. Ves čas je potrebno slediti in razvijati vse tri osi, ki so medsebojno soodvisne in se dopolnjujejo. Opustitev katerekoli izmed omenjenih osi privede do nestabilnosti sistema/podsistema. Končni cilj pa je seveda zadovoljen uporabnik, ki bo šel **Varno v nov dan**. ■

Avtor: Andrej Kovačič / Inštitut za korporativne varnostne študije*

**INTERVJU**
**ga. Barbara Černec in g. Tilen Pahor**
Študenta prve generacije magistrskega programa Management korporativne varnosti na Fakulteti za podjetništvo-GEA College

# IZOBRAŽEVANJE BODOČIH STROKOVNJAKOV MANAGEMENTA KORPORATIVNE VARNOSTI - KLJUČNI TEMELJ ZA PROMOCIJO PROFESIJE

**Na fakulteti za podjetništvo-GEA College svoj študijski proces aktivno izvaja prva generacija bodočih strokovnjakinj in strokovnjakov s področja managementa korporativne varnosti. Z ga. Barbaro Černec in g. Tilnom Pahorjem smo se pogovarjali o njunih pričakovanjih in predvsem kvaliteti znanja, ki ga pridobivata v času študija.**

**Nam lahko v kratkem predstavite vaše trenutno delovno okolje in povezanost vašega dela s procesi korporativne varnosti.**

**(Černec)** V Banki Celje sem zaposlena že od leta 1994, vodenje delovnega področja, ki je povezano s procesom korporativne varnosti pa sem prevzela leta 2001. Danes smo, organizacijsko gledano, samostojna služba, poleg korporativne varnosti pa skrbimo tudi za nabavo materiala, investicijska vlaganja v objekte in opremo, upravljanje in vzdrževanje vseh nepremičnin, zagotavljanje požarne varnosti in varstva pri delu, vodenje elektronskega vložišča, elektronskega in papirnega arhiva in upravljanje z voznim parkom banke. Področje korporativne varnosti zahteva nenehno prilagajanje razmeram na trgu, zakonodajnim smernicam, ter nadzoru in poročanju nadzornim institucijam.

> Upravljanje s korporativno varnostjo je področje, kjer lahko, ravno zaradi hitrih sprememb v okolju, svoje znanje nenehno nadgrajuješ.

**(Pahor)** Trenutno delam kot poslovni sekretar na interni kliniki v UKC Ljubljana. Na oddelku za geriatrično medicino sem odgovoren za zagotavljanje, da organizacija izpolnjuje visoke standarde finančno-pravne prakse ter vzdržuje korporativno upravljanje. Večino časa namenim za načrtovanje, organiziranje in vodenje delovnih procesov v pisarni, priprava poslovnih analiz, nadzor nad stroški, vodenje evidenc podpisanih pogodb in priprave poročil za upravo. Neposredne povezanosti s procesi korporativne varnosti na trenutnem delovnem mestu skoraj da ni, ne le pri meni, menim, da teh procesov v UKC Ljubljana

*avtor je član Slovenskega združenja korporativne varnosti



Do sedaj so bila moja pričakovanja vsekakor dosežena, predvsem me je pozitivno presenetil način izobraževanja, odnos predavateljev in vzpodbudni pozivi po pridobivanju ustreznega multidisciplinarnega znanja.

skoraj, da ne poznamo. Imamo službo, ki naj bi se s tem ukvarjala, a kogar koli vprašam, za njih ni še nihče slišal.

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

**(Černec)** Upravljanje s korporativno varnostjo je področje kjer, lahko, ravno zaradi hitrih sprememb v okolju, svoje znanje nenehno nadgrajuješ. Že nekaj časa me je mikalo, da bi naredila korak v smeri dodatnega izobraževanja in, ko sem prejela vabilo na dogodek, ki ga je organiziral Inštitut za korporativne varnostne študije sem spoznala, da je to področje velikih dimenzij, ki ponuja ogromno priložnosti in novih strokovnih znanj. Od tu dalje je bila pot jasna.

**(Pahor)** Biti bodoči manager korporativne varnosti je v slovenskem prostoru nekaj novega. V bodoče bodo »pametna« podjetja iskala tovrsten poklic, ki je izredno odgovoren in ta oseba predstavlja v podjetju enega ključnih igralcev. Eden izmed glavnih razlogov za vpis so tudi profesorji, ki izhajajo iz velikih in uveljavljenih slovenskih podjetij in na praktičnih primerih poenostavijo, kar se je prej zdelo nerešljiv problem. Izkušnje - neprecenljive.

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

**(Černec)** Postavljeni novi cilji na poti osebne rasti, so že na samih informativnih dnevih ponudili izziv v študiju. Seveda je prvi vtis, ki ga naredi ustanova in njegovo osebje, velikega pomena. V mesecu septembru, kjer sta predsednik Slovenskega združenja za korporativno varnost dr. Čaleta in dekan Fakultete za podjetništvo Gea College dr. Vadnjal predstavila program študija, nekateri nosilci

Znanje, ki ga bom pridobila tekom študija bo zagotovo prineslo korist, tako meni osebno, kot delodajalcu. Je pa res, da je na nas samih, kako se bomo odzivali spremembam v okolju in kako bomo pridobljeno znanje znali unovčiti.

posameznih predmetov pa so podali tudi svoje izkušnje in pričakovanja, je bilo občutiti predvsem pozitivno energijo, močno strokovno podkovanost predavateljev, katerih cilj ni samo v čisto formalnem podajanju znanja, temveč oblikovanju nove oz. širše celovitosti vsakega posameznika, v smislu avtoritativnega nastopanja, zavedanja strokovne moči, poznavanja in razumevanja globalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja.

Program študija poteka že vse od meseca novembra 2014 in prvi vtisi predavanj in vsebine predmetnika so zelo pozitivni. Do sedaj so bila moja pričakovanja vsekakor dosežena, predvsem me je pozitivno presenetil način izobraževanja, odnos predavateljev in vzpodbudni pozivi po pridobivanju ustreznega multidisciplinarnega znanja. Mogoče je to še toliko bolj izraženo, ker je naša skupina manjša (šteje le 5 udeležencev), zato je vsako predavanje dosti bolj intenzivno in interaktivno, kar pa je za nas, ki smo željni novega znanja, samo pozitivno.

**(Pahor)** Prvi vtisi so odlični, več kot sem pričakoval. Povezanost med profesorji in študenti je enkratna. Neprestano nas spodbujajo in vključujejo v različne dogodke in podjetja. Teorijo enkratno povezujejo s praktičnimi primeri. Pripravljajo nas, da bomo bodoči strokovnjaki s področja korporativne varnosti, ki ima širok spekter poslovnega znanja ter razumevanja poslovnega in varnostnega okolja. Varnostni mehanizmi bodo v tem hitro se razvijajočem svetu vedno bolj pomembni, tako v gospodarstvu, kot v industriji, državnih inštitucijah itd.

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

**(Černec)** Glede na to, da se v moje delovno okolje prepleta veliko vsebine, ki jo nadgrajujem skozi študijski program managementa korporativne varnosti, mi obnova dosedanjega znanja in seveda vse to kar pridobivam pomeni možnost suverenega nastopa v delovni sredini. Ne nazadnje mi tudi možnost udeležbe na različnih dogodkih v organizaciji Slovenskega združenja za korporativno varnost in Instituta za korporativno varnostne študije, omogoča spoznati nove ljudi, izmenjati informacije, preveriti stopnjo svojega vedenja in poiskati tiste vire, ki mi bodo v pomoč pri nadaljevanju moje poti.

**(Pahor)** Definitivno. Zbrali se bodo top slovenski managerji, odlična priložnost

Pripravljajo nas, da bomo bodoči strokovnjaki s področja korporativne varnosti, ki ima širok spekter poslovnega znanja ter razumevanja poslovnega in varnostnega okolja.






za nova spoznanja in kontakte. Izmenjava mnenj in poslušanje predavanja najuspešnejših managerjev, je ena izmed dodanih vrednosti, ki jo ponuja ta magistrski študij.

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

**(Černec)** Krepitev zavedanja o potrebnosti celovitega obvladovanja tveganj in iskanje ustreznih rešitev na področju varnosti, bo zagotovo področje, ki mu bodo podjetja posvečala vedno več pozornosti. Še bolj izrazito se to kaže v bančništvu, kjer imamo nenehno opravka s tveganji. Znanje, ki ga bom pridobila tekom študija bo zagotovo prineslo korist, tako meni osebno, kot delodajalcu. Je pa res, da je na nas samih, kako se bomo odzivali spremembam v okolju in kako bomo pridobljeno znanje znali unovčiti.

**(Pahor)** Upam, da bo UKC Ljubljana prepoznal moje znanje, ker če ga ne bo, ga bo neka druga organizacija, ki bo tovrstna znanja spoštovala in izkoristila sebi v prid za boljše in varnejše poslovanje. Organizacijo je potrebno neprestano razvijati in izboljševati. Sistem, ki ga imamo trenutno v UKC Ljubljana je bil najboljši v letu 1980, piše se leto 2015 in temu se je treba tudi prilagoditi. Brez ustreznega, mladega kadra bomo to težko dosegli. Vedno se radi primerjamo z bolnico na Dunaju, pa če pustimo čakalne dobe in plače in se osredotočimo na same procese, potem vidimo kako zaostajamo. To izvem iz prvih rok; zdravnikov in sester, ki so ali trenutno tam delajo. Potrebno je še veliko sprememb in predlagam, da enkrat začnemo na vrhu, ker kadar koli začnemo na dnu, se za večino slabo konča.

Upam, da bo UKC Ljubljana prepoznal moje znanje, ker če ga ne bo, ga bo neka druga organizacija, ki bo tovrstna znanja spoštovala in izkoristila sebi v prid za boljše in varnejše poslovanje.

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

**(Černec)** Če bi me o tem vprašali pred nekaj časa, vam ne bi znala odgovoriti, saj sem si termin »korporativna varnost« predstavljala preozko. Danes lahko pritrdim, da se Slovenija počasi le prebuja in

se pomen korporativne varnosti vendarle postavlja na svoje mesto. Seveda nosijo levji delež zaslug v Organizaciji Slovenskega združenja za korporativno varnost pa tudi na Fakulteti za podjetništvo, ki z roko v roki usmerjata in skozi program managementa korporativne varnosti izobražujeta nove strokovne kadre.

Na nas pa je odpadlo poslanstvo, da postanemo ambasadorji tega študija in tako pomagamo vsem tistim, ki še iščejo svoje priložnosti za nova znanja, da mogoče del tega najdejo tudi v omenjenem študijskem programu.

In naj končam z že zapisano mislijo odličnega predstavnika in aktivnega voditelja korporativne varnosti v svetovnem merilu g. Andreja Podvršiča:

»Če smo nekoč čas merili v letih, mesecih in dnevih, ga danes merimo v urah, minutah in sekundah, saj se svet okoli nas spreminja s tako naglico, da mu enostavno ne moremo več slediti!« Seveda pa so te spremembe pozitivne, ali negativne, vse predstavljajo izzive in nam dajejo priložnosti, da pokažemo svojo moč – ZNANJE!

**(Pahor)** Upam si trditi, da ne. Korporativna varnost je pri nas še vedno potisnjena v ozadje. Menim, da slovenski direktorji premalo poznajo kako močno vlogo igra ta položaj v podjetju. Slovenska miselnost je žal še vedno taka, da je bolje tvegati naše premoženje in ključne informacije in upati, da se ne bo nič hudega zgodilo, kot pa vpeljati sistem, ki bo te informacije varoval. Dokler se ne bomo zavedali, da je varnost v podjetju eden izmed osnovnih pogojev za učinkovito delovanje organizacije, bodo podjetja lahke tarče za različne kriminalne aktivnosti in v UKC Ljubljana ni nič drugače. Informacije s katerimi razpolagajo zdravstvene ustanove so neprecenljive, pa ne mislim le datumi rojstva, domači naslovi, govorim o informacijah, ki so v zadnjih letih po svetu žal v porastu, in kjer se letno obrne 1,5 milijarde dolarjev. Govorim o trgovanju z organi. Slovenija ni imuna na tovrstno trgovanje in vse ključne informacije se lahko dobi v zdravstvenih kartonih. Prav ta osrednji informacijski sistem, ki ga UKC Ljubljana uporablja se »outsourca«, kar lahko predstavlja velik varnostni problem. Nekoga na minimalni plači ni težko prepričati, da v zameno za koristne zdravstvene informacije o neki osebi, dobi dodatni denar. ■



Avtor: mag. Andrej Tomšič / namestnik informacijske pooblaščenke,
Informacijski pooblaščenec Republike Slovenije*



# BREZPILOTNI LETALNIKI – MED NADZOROM IN ČLOVEKOVIMI PRAVICAMI

**Brezpilotniki letalniki ali "droni" si počasi utirajo pot v naš vsakdan. V nekaterih državah so že izrazito prisotni. V Franciji tako obstaja že 650 registriranih operaterjev in 42 proizvajalcev brezpilotnih letalnikov, samo lani pa naj bi prodali 500.000 enot najbolj prodajanega letalnika za domačo rabo. Z naraščanjem uporabe se pojavljajo tudi prvi primeri, ko se porajajo resna varnostna vprašanja glede njihove rabe.**

Brezpilotne letalnike so tako že zasledili nad Belo hišo, palačo francoskega predsednika in jedrskimi elektrarnami. Njihova uporaba odpira številne dileme, med njimi pa so pogoste tudi tiste, ki se nanašajo na posege v človekove pravice.

Poleg komercialne rabe imajo brezpilotniki številne možne uporabe tudi z vidika varnosti, obrambe in odkrivanja in pregona kaznivih dejanj. Organi pregona kaznivih dejanj pogosto podcenjujejo posege v človekove pravice in glede uporabe brezpilotnih letalnikov zagovarjajo stališče, da gre pač enostavno za manjše helikopterje, ki lahko učinkovito opravljajo določene naloge. Policije po svetu že vrsto let uporabljajo helikopterje za opravljanje različnih nalog in pristojnosti, zakaj bi bili potem brezpilotniki drugačni in zakaj bi zanje potrebovali posebna pooblastila, saj gre vendarle le za še eno tehnično sredstvo? Z brezpilotniki bi lahko na cenejši, bolj učinkovit in varnejši način iskali pogrešane v gorah, izvajali prikrite preiskovalne ukrepe, nadzorovali množična zborovanja in po potrebi na bolj varen način v množico odvrgli plinska sredstva.

Kako je torej z brezpilotnimi letalniki in posegi v človekove pravice, zlasti pri uporabi s strani organov pregona? Gre za eldorado nadzora ali bodo po drugi strani brezpilotni letalniki prinesli tisto kruto prebujenje, da je skrajni čas, da k varstvu temeljnih človekovih pravic pristopimo bolj zavzeto[1]? V članku poskušam odgovoriti na ta vprašanja.

Uvodoma je treba poudariti, da gre pri sistemih brezpilotnih letalnikov (Unmanned Aircraft Systems – UAV) za sistem, ki sestoji iz treh podsistemov:
- nosilec (zrakoplov),
- sistem delovanja in upravljanja,
- sistem za opravljanje nalog.

Ključna nevarnost za neupravičene posege v človekove pravice in s tem povezano tveganje je, da se celoten sistem enači samo s podsistemom nosilca (brezpilotnega letalnika), medtem ko najpomembnejša tveganja v povezavi z varovanjem človekovih pravic izvirajo predvsem iz naslova sistema za opravljanje nalog (angl. payload). Ta lahko med drugim vključuje:
- oborožitvene sisteme (plinska sredstva, oborožitveni sistemi ipd.),
- sisteme za transport in dostavo (dostava paketov, zdravil, opraševanje in škropljenje kmetijskih površin ipd....),
- sisteme za nadzor in zajem podatkov (sredstva za fotografiranje, video snemanje, naprave za nočno opazovanje, toplotne kamere...).

Podatki sistemov za nadzor in zajem podatkov se lahko shranjujejo v zrakoplovu ali pa se prenašajo v bazno postajo na tleh.

Ključno je, da se tveganja za posege v človekove pravice analizirajo glede na sisteme za opravljanje nalog, pri čemer so z

Ključno je, da se tveganja za posege v človekove pravice analizirajo glede na sisteme za opravljanje nalog, pri čemer so z vidika posegov v varstvo osebnih podatkov ključni sistemi za nadzor ter zajem podatkov in ne sistemi za oborožitev ali transport, ki pa imajo lahko posledice na druge pravice.

*avtor je član Slovenskega združenja korporativne varnosti



vidika posegov v varstvo osebnih podatkov ključni sistemi za nadzor ter zajem podatkov in ne sistemi za oborožitev ali transport, ki pa imajo lahko posledice na druge pravice. Brezpilotni letalnik kot tak, brez sistemov za opravljanje nalog, v osnovi ne predstavlja posega v temeljne človekovega pravice – podobno kot ga ne predstavlja sam helikopter kot tak[2]. Če govorimo o pravici do zasebnosti in konkretneje o pravici do informacijske zasebnosti, je treba poudariti, da imajo lahko določeni **sistemi za opravljanje nalog, nameščeni na brezpilotne letalnike** (ali na druga tehnična sredstva), kot so biometrijska prepoznava obrazov, zajem slike in videa, infrardeče, termo in UV kamere, imsi lovilci, radarji, sistemi avtomatske prepoznave registrskih tablic in merjenja hitrosti vozil, da ne govorimo o sistemih za oborožitev in pasivizacijo (solzilec ipd.), **pomembne posledice na cel spekter ustavno varovanih človekovih pravic**.

Mednje sodijo pravica do svobode gibanja (32. člen Ustave RS) splošna pravica do zasebnosti (35. člen Ustave RS), pravica do nedotakljivosti stanovanja (36. člen Ustave RS), pravica do komunikacijske zasebnosti (37. člen Ustave RS), pravica do informacijske zasebnosti (varstvo osebnih podatkov, 38. člen Ustave), pravica do svobode izražanja (39. člen Ustave RS), pravica do zbiranja in združevanja (42. člen Ustave RS)... Sistem brezpilotnih letalnikov, ki bi bil opremljen z naštetimi podsistemi za opravljanje nalog, nadzor in zajem podatkov, bi lahko posegal v vse omenjene pravice.

Obseg in intenzivnost posega v človekove pravice (s poudarkom na pravico do zasebnosti) podrobno analizira študija »*Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations*[3]«, ki jo je naročila Evropska komisija. Študija jasno izpostavlja, da so tveganja pri uporabi brezpilotnih letalnikov glede s strani organov odkrivanja in pregona kaznivih dejanj glede posegov v zasebnost visoka (»high risk«), zlasti v primerjavi z uporabo na nekaterih drugih področjih.

V študiji so dalje izpostavljena tudi etična tveganja uporabe brezpilotnih letalnikov in sicer gre za možnost:
- diskriminacije,
- učinka zastraševanja glede svobodnega uveljavljanja človekovih pravic (angl. chilling effect),
- dehumanizacije nadzorovanih,
- javnega nezadovoljstva in odpora proti nadzoru,
- pojava zlorabe za druge namene (angl function creep).

Čeprav se v trenutnem času zdi naslednji primer distopičen, gre vendarle za **tehnološko povsem realno možnost stalnega, vseprisotnega in popolnega nadzora**: roj medsebojno povezanih in težko vidnih brezpilotnih letalnikov, ki so stalno v zraku, težko zaznavni, opremljeni z visoko-zmogljivimi senzorji, ki omogočajo zajem in posredovanje širokega nabora podatkov (npr. senzorji za biometrijsko prepoznavo obrazov, zajem slike in zvoka, imsi lovilci, radarji, sistemi avtomatske prepoznave registrskih tablic in merjenja hitrosti vozil, sistemi za obvladovanje množic). In čeprav verjamemo, da takšne prihodnosti iz finančnih ali drugih vzrokov še dolgo ne bomo dočakali, je tehnološka realnost temu čedalje bližje, kot jasno kažejo primeri:
- opremljanja brezpilotnikov z elektrošokerji[4],
- sistema stalnega nadzora iz zraka (primer Dayton, Ohio[5]),
- delujočih brezpilotnih letalnikov, ki oponašajo videz živali[6] (t.i. bio-mimetični brezpilotniki).

Sistemi za zajem in obdelavo podatkov, ki se lahko namestijo (tudi) na brezpilotne letalnike omogočajo stalnost in vse-prisotnost nadzora, ki lahko zaradi nesorazmernosti povzroči

tudi ogorčene odzive javnosti. Verjetno se vsi zelo živo spomnimo poskusa merjenja hitrosti vozil v Mariboru s sistemom stalnega nadzora s strani velikega števila stacionarnih radarjev. Uvajanje sistemov za zajem in obdelavo podatkov mora zato nujno potekati dovolj transparentno, preudarno in po izvedenih analizah tveganj ter testih sorazmernosti.

Uvajanje novih pooblastil organov pregona kaznivih dejanj mora biti izvedeno ob upoštevanju načela sorazmernosti. Informacijski pooblaščenec je zato pripravil smernice **Presoje vplivov na zasebnost glede uvajanja novih policijskih pooblastil**[7]**,** ki predstavljajo metodološki okvir za preudarno, smiselno in legitimno uvajanje novih policijskih pooblastil, zlasti tistih s tehnološkim značajem, in uporaba brezpilotnih letalnikov je izrecno omenjena kot primer uporabe zadevnih smernic. Uporaba smernic je tako v javnem kot tudi v interesu policije, saj lahko z uporabo metodološkega pristopa iz smernic policija predloge za spremembe ali nova pooblastila podpre z izvedenimi analizami in izkazano nujnostjo, primernostjo in učinkovitostjo ter sorazmernostjo pooblastil in tako doseže legitimnost predlaganih ukrepov v smeri ciljev, ki jih zasleduje ter večjo transparentnost sprejemanja ukrepov, ki imajo učinek na varstvo človekovih pravic.

Pri uvajanju novih pooblastil policije, kot je recimo primer avtomatske prepoznave tablic s sistemi na brezpilotnih letalnikih, se priporoča metodološki pristop iz smernic in sicer je treba;
- natančno definirati konkretne primere uporabe[8], predvsem pa:
- sisteme za zajem podatkov, ki bodo uporabljeni v določeni situaciji,
- konkretne okoliščine, ko bo uporabljeno določeno pooblastilo;
- identificirati tveganja;
- analizirati tveganja;
- opredeliti varovalke.

Smernice podajajo tudi katalog možnih tveganj. Šele na podlagi takšne analize je namreč možno ugotavljati, ali je podana sorazmernost za uporabo določenega ukrepa in kakšne varovalke so potrebne (v katerih situacijah je npr. primerna in potrebna sodna odredba).

Informacijski pooblaščenec v svojem mnenju glede policijske rabe brezpilotnikov zastopa stališče, da lahko policija uporablja tiste sisteme za zajem in obdelavo podatkov, za katere že razpolaga z izrecno pravno podlago, tudi če so ti sistemi nameščeni na brezpilotne letalnike.

Takšni primeri so:
- uporaba sredstev za fotografiranje ter avdio in video snemanje, nameščenih na brezpilotnih letalnikih, pri spremljanju javnih zbiranj pod pogoji iz 2. odstavka 114. člena Zakona o nalogah in pooblastilih policije;
- uporaba fotografskih in snemalnih naprav pri izvajanju nalog nadzora državne meje pod pogoji iz Zakona o nadzoru državne meje;
- tajno opazovanje s pomočjo sistemov za ugotavljanje položaja in gibanja ter tehničnih naprav za prenos in snemanje glasu, fotografiranje in video snemanje, nameščenih na brezpilotnih letalnikih, pod pogoji iz 1. odstavka 149.a člena Zakona o kazenskem postopku.

Če za uporabo določenih sistemov za opravljanje nalog, ki vključujejo zajem in obdelavo osebnih podatkov, kot so npr.

Informacijski pooblaščenec v svojem mnenju glede policijske rabe brezpilotnikov zastopa stališče, da lahko policija uporablja tiste sisteme za zajem in obdelavo podatkov, za katere že razpolaga z izrecno pravno podlago, tudi če so ti sistemi nameščeni na brezpilotne letalnike.

stalni videonadzor iz zraka ali biometrijska prepoznava obrazov, policija nima pravnih podlag, potem tudi nima podlage, da bi uporabljala takšne sisteme, ki bi bili nameščeni na brezpilotnih letalnikih.

Glede na to, da ima uporaba brezpilotnih letalnikov tudi druge implikacije (npr. varnostne), bi bilo - če primerjamo pogoje za uporabo plinskih in drugih sredstev za pasivizacijo – pogoje za uporabo brezpilotnih letalnikov za določene namene, z uporabo določenih sistemov za opravljanje nalog, podrobneje urediti v zakonodaji.

Uporabi brezpilotnih letalnikov bo po vsej verjetnosti treba prilagoditi temeljni zakon o letalstvu, odlašanje z regulacijo (ta mora biti seveda preudarna) pa ni primerno, saj neregulirana raba brezpilotnih letalnikov povečuje tveganja za storitev kaznivih dejanj in posege v temeljne človekove pravice, obenem pa ovira razvoj novih storitev in delovnih mest ter povečuje varnostna tveganja. Informacijski pooblaščenec je podobno kot policija že pozval resorno ministrstvo in Javno agencijo za civilno letalstvo k pripravi potrebnih pravnih podlag, pri čemer jima je ponudil vso strokovno pomoč, ki se nanaša na vprašanja varstva osebnih podatkov[9]. Najbrž si nihče na želi ponovitve balonarske nesreče.

[1] Prof. Ryan Calo s Stanforda trdi, da bi lahko brezpilotni letalniki s svojimi neizprosnimi in očitnimi možnostmi za nadzor povzročili ravno obratne učinke, t.j. da bi prišlo do ponovnega premisleka o pomenu zasebnosti in drugih človekovih pravic ter novih okvirih za njihovo varovanje.

[2] Pri tem zanemarimo druge vplive, ki lahko izvirajo iz hrupa, ki ga povzroča ipd.

[3] Dostopno na: http://ec.europa.eu/enterprise/sectors/aerospace/uas/

[4] http://mashable.com/2014/03/09/flying-taser-drone/

[5] https://www.aclu.org/blog/technology-and-liberty-national-security/ohio-aerial-surveillance-system-moving-forward-without

[6] http://www.avinc.com/nano

[7] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf

[8] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf

[9] https://www.ip-rs.si/novice/detajl/kdaj-pravila-glede-uporabe-brezpilotnih-letalnikov-dronov/?cHash=f59466a5bdf1f3745fb3c596caeda22a ■

# 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 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;
- brezplačna naročnina na revijo Korporativna varnost;
- popusti pri oglaševanjih in postavitev logotipa na spletno stran ICS-Ljubljana
- popusti pri članarinah za strokovne člane, ki prihajajo iz vrst organizacij, katere so korporacijski člani združenja;

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

www.ics-institut.si

ELES

hse Holding Slovenske elektrarne d.o.o.

KONTROLA ZRAČNEGA PROMETA SLOVENIJE

MARIBORSKI VODOVOD

energetika ljubljana

LUKA KOPER Port of Koper

interblock LUXURY GAMING PRODUCTS

SIEMENS

MIŠKA 20 let FMC Group

Zanesljivo vsepovsod POŠTA SLOVENIJE

REISSWOLF secret. service.

TelekomSlovenije

DARS

Nova KBM PRIPRAVLJENI NA JUTRI

univerzitetni klinični center ljubljana

gorenjegroup

si·cert

INFORMACIJSKI POOBLAŠČENEC

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



**KOLUMNA**
**denis.caleta@ics-institut.si**

# JE TERORIZEM RES POSTAL DEL NAŠEGA VSAKDANA ?

**Terorizem postaja oziroma ostaja grožnja s katero bomo morali živeti v modernem varnostnem okolju. Terorizem se v svojih pojavnih oblikah pojavlja skozi vso zgodovino vse do današnjih dni.**

Vzroke za nastanek terorizma lahko najdemo v različnih družbenih dejavnikih, ki imajo versko, politično, nacionalno ali drugo opravičilo za izvajanje terorističnih dejanj. Gre pa seveda za eno od najnevarnejših groženj saj v okviru svojega delovanja, poleg žrtev, pušča predvsem brazgotine v družbeni zavesti in spominu celotne družbene skupnosti, ki je bila priča terorističnemu napadu.

V zadnjem obdobju je postal terorizem v svoji izvedbi še nevarnejši in zahtevnejši za preprečevanje. Namreč zadnje oblike terorističnih dejanj kažejo na smer, kjer teroristični storilci svoja dejanja izvedejo na skrbno izbranih ciljih, ki imajo močan simbolni, predvsem pa medijski odziv. Ta dejanja so storjena v omejenem obsegu storilcev, ki ne pripadajo neki večji organizirani teroristični skupini, temveč so radikalizirani posamezniki, ki na valu radikalnih idej in osebnih prepričanj izvedejo teroristično dejanje. Za izvedbo največkrat uporabijo lahko strelno orožje do katerega je na črnem trgu zelo lahko dostopiti. Vse to predstavlja zelo zahtevne dejavnike, ki varnostnim organom in policiji predstavljajo veliko težavo pri učinkovitem preprečevanju terorističnih napadov. Namreč v fazi priprave takega terorističnega dejanja storilci ne operirajo z večjimi količinami finančnih sredstev kateri bi postali sumljivi in bi jim varnostni organi lahko sledili. Ker ne pripadajo večji organizirani sredini in ker uporabljajo lahko strelno orožje, ki je zelo lahko dostopno, se varnostni organi zelo hitro znajdejo v situaciji, ki jim preprečuje učinkovito preventivno odkrivanje terorističnih storilcev. Naslednji dejavnik pa so moderni globalni mediji in informacijska doba v kateri danes živimo in predstavljajo enega od najpomembnejših vplivnih dejavnikov terorizma. Medijska pozornost predstavlja kisik za terorizem in prinese sporočilo, ki so ga želeli teroristi preko terorističnega dejanja sporočiti skoraj do vsakega posameznika. S tem terorizem transformira sporočilnost iz primarnega cilja terorističnega napada na celotno družbeno skupnost. Želeli si ali ne, nam mediji v naše domove in v naša organizacijska okolja, dnevno prinašajo sporočila povezana s terorizmom.

V zadnjem obdobju je postal terorizem v svoji izvedbi še nevarnejši in zahtevnejši za preprečevanje.

Medijska pozornost predstavlja kisik za terorizem in prinese sporočilo, ki so ga želeli teroristi preko terorističnega dejanja sporočiti skoraj do vsakega posameznika.

Največji problem Evrope pa v tem trenutku predstavljajo procesi radikalizacije, ki so še posebej izraženi zaradi družbenih problemov, gospodarske krize in iskanja odgovorov na procese integracije priseljencev in versko ter kulturno raznolikost evropske družbe. Predvsem mladi so tisti, ki zelo hitro prihajajo pod vpliv različnih vplivnih skupin, pridigarjev in drugih radikalno usmerjenih posameznikov, ki novačijo nove podpornike radikalnih idej povezanih s terorizmom. Ta radikalizacija je še toliko bolj izpostavljena v skupinah, ki so po svoji obliki bolj zaprte kot so to na primer okolja institucij za izvrševanje kazenskih sankcij, določena verska okolja in druge skupine, ki v svoji osnovi nastajajo na temelju nestrpnosti, popačenih resnic in pričakovanj. V zadnjem obdobju so v evropskem prostoru izražene tako grožnje terorizma, ki imajo versko konotacijo, kakor tudi terorizem in nasil-

*avtor je član Slovenskega združenja korporativne varnosti



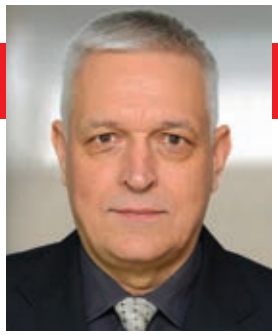

ništvo povezano s skrajno desnimi radikalnimi skupinami. V tem okviru ima internet, kot orodje za širjenje radikalnih idej, rekrutacijo in komunikacijo, izredno nevarno vlogo saj ga je zaradi obširnosti zelo težko nadzorovati. Seveda pri poskusih nadzora nad raznovrstnimi informacijskimi oblikami komunikacije hitro trčimo na področje poseganja v človekovo komunikacijsko zasebnost in človekove pravice zato morajo biti ti ukrepi še toliko bolj pretehtani in sorazmerni glede na izražena tveganja in grožnje. Res pa je, da na drugi strani terorizem, za svoje učinkovitejše delovanje, s pridom izrablja vse pridobitve demokratične družbe. Vsem tem pojavom se, tudi v Republiki Sloveniji, nikakor ne moremo izogniti. Javnost je bila šokirana ob posredovanju informacij, da je bilo nekaj posameznikov, ki so se radikalizirali do te mere, da so odšli na krizna žarišča Sirije in Iraka. Eden izmed le teh je tam izgubil tudi svoje življenje. Najbolj kar nas v tem procesu skrbi je predvsem hitrost radikalizacije, od sprejema nove vere, ki ni sicer nič spornega, pa do končanja radikalizacije, ki je bila izvedena v pičlih 6 mesecih, kar je izredno hitro glede na ostale poprej zaznane primere. Ta hitrost tega procesa je zelo zaskrbljujoča saj pred varnostne organe prinaša pomemben dejavnik časovnega pritiska, kateremu so izpostavljeni v fazi odkrivanja in preprečevanja takih dejanj, ki se lahko končajo v izvedbi terorističnega napada.

Potrebno se je ozreti tudi na naša dejanja in si realno in trezno odgovoriti ali so ukrepi, ki jih izvajamo na področju boja proti terorizmu ustrezni in predvsem ali prinašajo ustrezne rezultate. Na žalost lahko zelo hitro ugotovimo, da so ukrepi precej stihijski in odražajo predvsem odzivanje na že storjena teroristična dejanja. Ni pa politične volje in energije, da bi se spopadli s pravimi problemi in simptomi, ki bi zmanjševali možnost za razmah in nadaljnjo rast terorizma kot družbenega pojava, kateri predstavlja rakavo tkivo vsake družbe. Pri tem nerazumevanju ali nepripravljenosti učinkovitega ukrepanja imajo veliko težo tudi geopolitični interesi posameznih držav, predvsem velesil. Dejstvo pa ostaja, da predvsem Evropa, ki na dolgi rok zaradi svoje geografske izpostavljenosti, kulturne raznolikosti in energetske odvisnosti, v globalnem varnostnem okolju zaradi tega dolgoročno največ izgublja.

V vsakem primeru pa je radikalizacija tisti proces, kateremu moramo namenjati pomembno pozornost tudi v korporativno varnostnih okoljih. Radikalizirani posamezniki so ravno tako lahko del naših organizacijskih sredin, kar je še posebej tvegano v okoljih, ki obvladujejo kritično infrastrukturo.

Ne glede na precej pesimistično sliko in pričakovanja po omejevanju nadaljnje rasti dejavnikov, ki vplivajo na razmah terorizma, moramo v svojih mikro korporativno varnostnih okoljih zagotoviti, da je zavedanje o tej grožnji na zadostnem nivoju ter, da smo ustrezno pripravljeni na odzivanje v primeru pojava teroristične dejavnosti. Danes živimo v globalni vasi, kjer se, zaradi širokega poslovnega sodelovanja, naši poslovni procesi odvijajo in zaposleni gibajo praktično po vsem svetu. To namreč pred nas postavlja določena tveganja in odgovornost, da zaposlene pripravimo in jih varnostno osvestimo o nevarnostih, ki jih lahko prinese terorizem. V tem okviru so seveda pomembna tudi druga tveganja, ki trenutno v našem nacionalnem okolju mogoče niso tako izražena. V vsakem primeru pa je radikalizacija tisti proces, kateremu moramo namenjati pomembno pozornost tudi v korporativno varnostnih okoljih. Radikalizirani posamezniki so ravno tako lahko del naših organizacijskih sredin, kar je še posebej tvegano v okoljih, ki obvladujejo kritično infrastrukturo. Zaradi navedenega je tudi Institut za korporativne varnostne študije postal del evropskega projekta in mreže EU Radicalization Awareness Network (EU RAN), kjer smo kot nevladna organizacija aktivni v več skupinah, ki se ukvarjajo z ukrepi in aktivnostmi na področju preprečevanja radikalizacije. Preko tega pa omogočamo tudi vsem članom Slovenskega združenja korporativne varnosti, da v okviru te pobude dodajo tisti potreben del, ki bo omogočil varnejše okolje za delovanje in poslovanje. ■

Avtor: mag. Igor Trontel / Telekom Slovenije, d. d.*



# ZLORABE ELEKTRONSKIH KOMUNIKACIJ

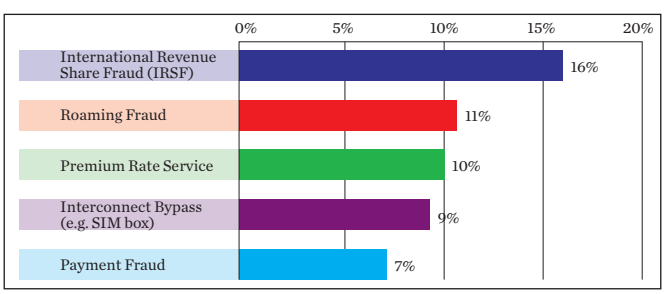
**V času medsebojno povezane in prepletene informacijske družbe se ni mogoče izogniti tveganju zlorabe elektronske komunikacije[1]. Zavedanje nevarnosti zlorab elektronskih komunikacij in možnih posledic je torej za upravljalce varnosti komunikacijskih in informacijskih sistemov ključnega pomena.**

Verjetnost napada na komunikacijsko omrežje, opremo ali storitev je velika, zloraba posameznega elementa komunikacijskega sistema, ki je v domeni upravljanja enega udeleženca[2], pa lahko vpliva na varnost komunikacijskih in informacijskih sistemov drugih udeležencev. Posledice zlorab so lahko za udeležence različne. Kažejo se v obliki negativnih finančnih učinkov (posamezni primer lahko doseže tudi več sto tisoč evrov), kršenju zasebnosti, lahko pa imajo tudi druge negativne vplive.

## Značilnosti in trendi

Zlorabe elektronskih komunikacij se odražajo v različnih oblikah, izvajajo se na različne načine in za različne namene. V okviru mednarodnih združenj za preprečevanje zlorab, v katerih sodelujemo ponudniki komunikacijskih storitev, dobavitelji komunikacijske opreme, razvijalci informacijskih rešitev, predstavniki regulatorjev ter drugi, so bile opredeljene nekatere specifične lastnosti zlorab, na tej osnovi pa opredeljene različne klasifikacije, kar predstavlja dobro osnovo za nadaljnje raziskave, obravnavo ter medsebojno izmenjavo izkušenj.

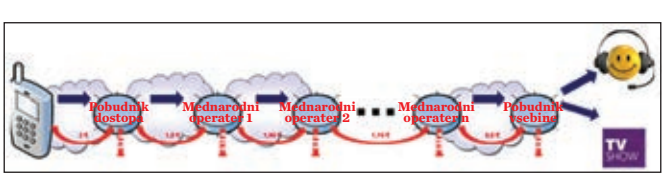
Število zlorab elektronskih komunikacij se iz leta v leto povečuje. Združenje Communication Fraud Control Association[3] je v letu 2013 med ponudniki komunikacijskih storitev[4] ponovno izvedlo raziskavo o tovrstnih zlorabah. V njej ugotavljajo, da se je število primerov, ki jih obravnavajo oddelki za preprečevanj zlorab[5], v preteklih dveh letih v povprečju povečalo za več kot 100 % in da se je zaradi intenzivnejših aktivnosti povečala tudi ocena izgub[6]. V raziskavo so bili vključeni ponudniki fiksnih, mobilnih in širokopasovnih storitev oziroma ponudniki prenosa govora, podatkov, vsebin in finančnih transakcij.




*Slika 1: Zlorabe elektronskih komunikacij, razvrščene po vrstah – TOP 5 /* Vir: CFCA, 2013.

## IRSF (International Revenue Share Fraud)

Tovrstne zlorabe so v telekomunikacijski panogi že nekaj časa zelo razširjene, storilci pa izkoriščajo poslovni model delitve dohodka med različnimi medomrežnimi ponudniki posredovanja telefonskega prometa. Finančne učinke največkrat ustvarjajo tako, da pri posameznem ponudniku generirajo telefonski promet in ga posredujejo proti številkam geografsko oddaljenega lastnika številčnega prostora[7], s katerim si delijo dohodek (sostorilec), pri tem pa izvornega prometa ne nameravajo plačati.




*Slika 2: Delitev dohodka med različnimi udeleženci elektronske komunikacije*

Pri opazovanju IRSF-zlorab je smiselno, da pozornost usmerimo na tok komunikacijskega prometa in na 'denarni' tok.

*podjetje je član Slovenskega združenja korporativne varnosti



Pri tem velja osnovni princip, da je za posredovani promet treba plačati, vendar pri tem pošiljatelj ne ve, kam je prejemnik (naslednji udeleženec v verigi) usmeril plačani promet. Posredniki zaslužijo pri marži, zadnji v verigi pa prejme plačilo za zaključevanje prometa oziroma za posredovane storitve. Sled za storilcem se izbriše, saj je v verigi običajno večje število udeležencev, na trgu pa velja konkurenca.

IRSF je torej le poslovni model - infrastruktura, ki storilcem omogoča, da pridobijo dohodek od svoje dejavnosti, za dosego cilja pa izkoriščajo 'šibke točke' drugih udeležencev. V povezavi z IRSF se pojavlja kar nekaj vrst zlorab, med katerimi so najbolj razširjene zlorabe Wangiri, zlorabe gostovanja v tujem omrežju, PBX-zlorabe, zlorabe naročniškega razmerja in druge. Tovrstne zlorabe imajo negativne posledice tako za uporabnike kot za ponudnike komunikacijskih storitev, saj so stroški posamezne zlorabe lahko precej visoki. Nemalokrat uporabijo storilci ta 'poslovni model' tudi za pranje denarja iz drugih kriminalnih dejavnosti.

Številni uporabniki mobilnih komunikacijskih storitev smo že prejeli zelo kratek klic z nepoznane številke iz tujine, na katerega nismo uspeli odgovoriti (zgrešeni klic). Osnovni cilj storilcev je dosežen, če se ne zavedamo 'grožnje' in pokličemo nazaj ter tako ustvarimo promet proti dražji, geografsko oddaljeni destinaciji.

## Wangiri

Številni uporabniki mobilnih komunikacijskih storitev smo že prejeli zelo kratek klic z nepoznane številke iz tujine, na katerega nismo uspeli odgovoriti (zgrešeni klic). Osnovni cilj storilcev je dosežen, če se ne zavedamo 'grožnje' in pokličemo nazaj ter tako ustvarimo promet proti dražji, geografsko oddaljeni destinaciji. Ko pokličemo nazaj, nas storilec s posnetim sporočilom ali lažnim zvonjenjem poskuša obdržati v komunikaciji čim dlje časa. Končni finančni 'prispevek' posameznega udeleženca k dohodku storilcev sicer ni velik, zato pa le-ti s pomočjo različnih računalniških sistemov dnevno generirajo veliko število klicev proti različnim destinacijam.

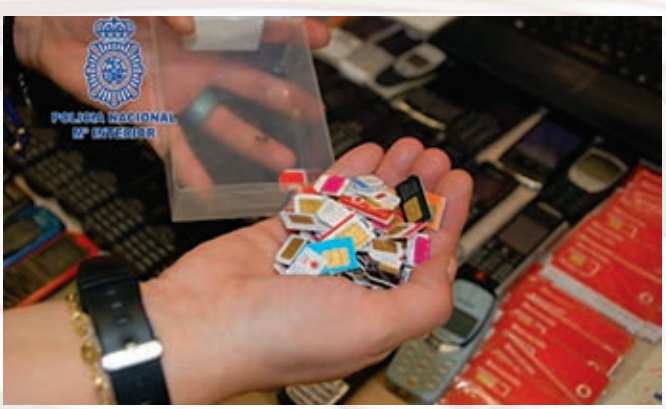
## Zlorabe gostovanja v tujem omrežju

Pri tej vrsti zlorab storilci izkoriščajo 'ranljivost', ki je že vgrajena v storitev mobilnega gostovanja - obstaja namreč določen zamik med izvajanjem komunikacijskega prometa v tujem omrežju in dostavo CDR-zapisov[8] o tem prometu domačemu operaterju[9]. V tem vmesnem času sistemi za preprečevanje zlorab oziroma za preprečevanje visokih računov, ki jih uporabljajo domači operaterji, ne morejo spremljati prometa v tujih omrežjih in reagirati na povišane vrednosti.

Za izvajanje tovrstnih zlorab so storilci običajno dobro organizirani v obliki mednarodnih kriminalnih združb in specializirani za posamezne naloge, kot so kraja mobilnih komunikacijskih naprav, prebijanje zaščitnih mehanizmov mobilnih naprav, prebijanje zaščitnih mehanizmov in kloniranje kartic SIM, generiranje prometa idr. Škoda, ki nastane pri posameznem primeru, je lahko precej visoka (tudi več kot 100.000 evrov).

Za izvajanje tovrstnih zlorab so storilci običajno dobro organizirani v obliki mednarodnih kriminalnih združb in specializirani za posamezne naloge, kot so kraja mobilnih komunikacijskih naprav, prebijanje zaščitnih mehanizmov mobilnih naprav, prebijanje zaščitnih mehanizmov in kloniranje kartic SIM, generiranje prometa idr. Škoda, ki nastane pri posameznem primeru, je lahko precej visoka (tudi več kot 100.000 evrov).

Kraja mobilnih naprav je v nekaterih državah že kar množičen pojav. Tako je španska policija v letu 2014 poročala o obsežni akciji, ko so v Barceloni aretirali več kot 10 storilcev, ob tem pa zaplenili 330 mobilnih naprav, 450 SIM-kartic in drugo opremo.




*Slika 3: Fotografija zaseženih SIM-kartic in mobilnih naprav pri policijski akciji v Španiji leta 2014*
Vir: http://www.policia.es/prensa/20140110_2.html#

## Zlorabe sistemov PBX (Private Branch Exchange)

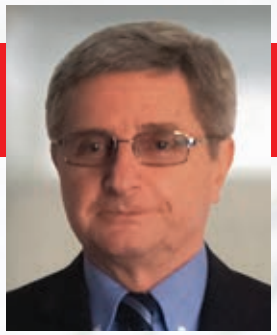
Sistem PBX[10] največkrat predstavlja t. i. most med zasebnim lokalnim omrežjem, telefonskim in internetnim priključkom. Storilci poznajo številne pomanjkljivosti upravljanja varnosti PBX-sistemov, ki so v domeni njihovih lastnikov, oziroma je upravljanje varnosti zaupano drugim izvajalcem. Ko je most med internim in telefonskim priključkom vzpostavljen in ko je zaščita prebita, imajo storilci prosto pot za posredovanje telefonskega prometa proti želenim destinacijam. Tudi pri tovrstni zlorabi je negativni finančni učinek pri posameznem primeru lahko precej visok (tudi več sto tisoč evrov).

## Zaključek

V tem prispevku je predstavljenih le nekaj značilnih pojavov zlorab elektronskih komunikacij. Pri celovitem načrtovanju oziroma upravljanju varnosti komunikacijskih in informacijskih sistemov, ki so med seboj vedno bolj prepleteni, pa velja, da je treba stalno in podrobno proučevati tako verjetnost tovrstnih pojavov kot njihov vpliv na upravljani sistem.

1 Zloraba elektronske komunikacije pomeni uporabo elektronskega komunikacijskega omrežja, opreme ali storitve z namenom pridobitve premoženjske ali druge koristi na nedovoljen način.
2 Udeleženci elektronske komunikacije (EK) – akterji in prejemniki: ponudniki dostopa oz. ponudniki EK-storitev, ponudniki EK-omrežij, ponudniki OTT-storitev, ponudniki specializiranih aplikacij in medijskih vsebin, uporabniki in drugi udeleženci.
3 CFCA – Communication Fraud Control Association ima sedež v ZDA. V združenje so vključeni tudi evropski operaterji. Rezultati raziskave so na voljo na http://www.cfca.org/fraudlosssurvey/.
4 V raziskavi je sodeloval največ predstavnikov iz Evrope in ZDA.
5 Tudi v Telekomu Slovenije varnostne incidente obravnavamo s posebno pozornostjo ter pri tem ugotavljamo povečano število poskusov zlorab.
6 Ocena je, da so izgube zaradi zlorab na globalni ravni v letu 2013 znašale 46,3 milijard USD.
7 Po raziskavi CFCA se telekomunikacijski promet največkrat zaključuje v Latviji, Gambiji, Somaliji, Republiki Sierra Leone ....
8 CDR – zapis ustvari centrala o posamičnem posredovanem klicu.
9 Po priporočilu, ki ga je objavilo mednarodno združenje GSMA in ga od 2008 dalje upošteva večina operaterjev, je maksimalni čas za dostavo t. i. NRTRDE datotek (zapisov o prometu med gostovanjem) 4 ure.
10 PBX-hišne centrale so napredne računalniško podprte centrale, ki omogočajo telefonsko podporo notranjim omrežjem poslovnih uporabnikov in so lahko povezane proti internetu in s priključkom ponudnika telefonskih storitev. Glej tudi spletno stran Agencije za komunikacijska omrežja in storitve RS: http://www.akos-rs.si/files/Koncni_uporabniki/Koristni_nasveti_in_opozorila/Smernice-pri-zasciti-PBX.pdf. ■

Avtor: mag. Janko Uratnik / PRIS, CISA, CISM, CGEIT,
sodni izvedenec in sodni cenilec za računalništvo in informatiko



# KAKO ZMANJŠATI TVEGANJA NOTRANJIH PREVAR

**Notranje prevare niso novost ali presenečenje v vsakdanjem in v poslovnem življenju. Novost so najnovejše informacijske tehnologije, ki lahko služijo kot sredstvo za izvajanje notranjih prevar in istočasno kot zelo dobra in učinkovita orodja za preprečevanje in odkrivanje le-teh.**

## Uvod

Notranja prevara v neki organizaciji predstavlja namerno zavajanje sodelavcev, izkoriščanje položaja in možnosti delovnega mesta, izkoriščanje strokovnega znanja, zloraba virov poslovanja in lastnine organizacije in njenih strank, nepošteno delovanje v organizaciji, vse to z namenom pridobitve materialne ali drugačne koristi za sebe osebno ali v povezavi s sostorilci.

Pojem notranje prevare vključuje zelo veliko različnih področij in vključuje veliko različnih načinov kako prevare izvajati in veliko orodij s katerimi si posamezniki ali prevarantske združbe pri tem pomagajo. Možnosti za prevare so brezmejne, omejene so le s človeško domišljijo.

Pomembna značilnost notranjih prevar je, da se izvajalci nahajajo »znotraj obrambnega zidu oziroma sistema« neke organizacije, ki le-to brani pred informacijskimi napadi predvsem od zunaj. Notranji izvajalci imajo veliko strokovnega znanja na svojem področju in dobro poznajo organiziranost in delovanje organizacije, imajo veljavna uporabniška imena in gesla za dostop do informacijskega sistema. Notranji prevaranti so torej popolnoma »legalni« uporabniki sistema, ki lahko izkoriščajo pomanjkljiv vodstveni nadzor, neustrezne kontrole v poslovnih in v informacijskih sistemih, neobstoječe revizijske sledi in neopredeljene politike obvladovanja notranjih prevar.

Ali in na kakšen način lahko zavarujemo podatke in informacijske sisteme pred pooblaščenimi uporabniki ?

## Zakaj se dogajajo notranje prevare

Kaj so razlogi, vzgibi, spodbude, utemeljitve za izvajanje notranjih prevar. Zakaj je J. Kerviel iz Societe Generale zaigral 4,9 mdr evro, zakaj je B. Madoff zgradil Poncijevo piramido v vrednosti 50 mrd USD, zakaj ....

Literatura o prevarah združuje razloge za izvajanje notranjih prevar v t.i. trikotnik prevar (*Fraud Triangle*), ki se je s časom razširil na kvadrat prevar (*Fraud Diamnond*). Ta vključuje vsaj naslednje razloge, vzgibe, motive:

**Potreba** (finančna, življenjski stil, pohlep, revščina),

**Priložnost** (slabe notranje kontrole, preveliko zaupanje, prevladujoč položaj),

**Prepričanje** (samozavest, narcisoidnost, pravičništvo, maščevanje),

**Zmožnost, sposobnost** (strokovnost, dokazovanje).

Tipična prevara je trajala 18 mesecev predno so jo odkrili. Največ prevar je bilo odkritih na osnovi namiga zaposlenih ali strank (40%), nato na osnovi vodstvenih kontrol (14%), notranjega revidiranja (14%), po naključju (7%), zunanjega revidiranja (3%) in IT kontrol (1%). 15% namigov o morebitnih prevarah je prišlo anonimno.




## Zgovorne številke in dejstva o prevarah

Podatke o obsegu izvajanja in o učinkih notranjih prevar sistematično zbirajo in obravnavajo različne inštitucije po svetu, med njimi tudi Association of Certified Fraud Examiners – ACFE in PWC.

Poročilo ACFE je izdelano na osnovi 1.483 analiz primerov posameznih vrst prevar v več kot 100 državah. Poročilo PWC je narejeno na osnovi 5.128 anket udeležencev iz 95 držav.

## Vrste prevar

Prevare se v osnovi delijo na tri osnovne skupine: **poneverjanje in zloraba virov**, **podkupovanje in korupcija** ter **prirejanje finančnih in računovodskih poročil**. Najbolj pogoste so zlorabe virov (85%) s povprečno škodo 130.000 USD, bolj redke so finančne prevare (9%), a imajo večje škode - povprečno 1 mio USD. Tretjina primerov prevar vključuje več oblik prevar.

Tipična prevara je trajala 18 mesecev predno so jo odkrili. Največ prevar je bilo odkritih na osnovi namiga zaposlenih ali strank (40%), nato na osnovi vodstvenih kontrol (14%), notranjega revidiranja (14%), po naključju (7%), zunanjega revidiranja (3%) in IT kontrol (1%). 15% namigov o morebitnih prevarah je prišlo anonimno.

Med tipične IT prevare in zlorabe štejejo kraja podatkov, kršitev intelektualne lastnine, nepooblaščeno razkrivanje podatkov, vdiranje v informacijske sisteme, spreminjanje parametrov delovanja v informacijskem sistemu, izvajanje nepooblaščenih transakcij, pranje denarja, kraja identitete. Vse več groženj kibernetskega kriminala ki prihaja, je notranjih.

## Učinki prevar

Tipična letna izguba zaradi notranjih prevar je v višini 5 % prihodka gospodarstva. To na svetovnem nivoju **v letu 2013 pomeni 3,7 mrd USD**.

Najbolj prizadete industrije so banke in finančne institucije (17%), vladne ustanove in javna uprava (10%), proizvodni sektor (10%) ter zdravstvo (7%). V večjih organizacijah je največje tveganje za korupcijo (35%), v manjših pa pri različnih vrstah obračunavanja (32%). Manjše organizacije namenjajo preprečevanju in odkrivanju prevar manjša sredstva, zato so bolj izpostavljene prevaram. Poleg neposredne škode izražene v denarju pa nastaja tudi posredna škoda, ki jo je težje ovrednotiti v denarju in se odraža v poslabšani morali in zaupanju zaposlenih, v omajanem ugledu organizacije v javnosti in med poslovnimi partnerji ter v povečanju dvomov o sposobnosti obvladovanja tveganj poslovanja in zato večji pozornosti pri regulatorjih.

Več kot polovica žrtev prevar ni uspela povrniti izgube zaradi prevar. Približno dve tretjini oškodovancev je oškodovanje prijavila organom pregona, a le v približno 16% primerov je prišlo do obsodbe, pri tem je 56% storilcev priznalo krivdo.

## Notranje kontrole

Prisotnost notranjih kontrol in postopkov je močno korelirana – sovpada z zmanjšanjem izgub in s trajanjem prevar. Pri preprečevanju in odkrivanju notranjih prevar so se organizacije najbolj posluževale pomembnih splošnih kontrol kot so zunanje revidiranje finančnih poročil in neodvisno revidiranje notranjih kontrol finančnega poročanja (80% prizadetih organizacij). **Zanimivo pri tem je, da so zunanji revizijski pregledi odkrili le 3% zaznanih in poročanih prevar.**

Največje učinke na zmanjšanje škode zaradi prevar imajo notranje kontrole kot so vodstveni nadzor (46% prihranek), obveščanje in podpora zaposlenim (45% prihranek), vroča linija za poročanje (44% prihranek), izobraževanje vodstvenega kadra (36% prihranek). Učinkovitost notranjih kontrol se je v obdobju do poročanja povečala za več kot polovico (PWC).

Trajanje izvajanja prevar je bilo manjše tam, kjer so bile uvedene kontrole obvezne menjave delovnih mest in obvezni dopusti (62% zmanjšanje), nagrajevanje namigovalcev (60% zmanjšanje), nenapovedani revizijski pregledi (58% zmanjšanje).

Pri analiziranju načinov izvajanja notranjih prevar so v največji meri sodelovali preiskovalci prevar (28% primerov), notranji revizorji (27% primerov) in finančni strokovnjaki (13%) primerov**. Specialisti za forenziko informacijskih sistemov so sodelovali le v 1% primerov, kar pomeni velike možnosti za izboljšave.**

Pri odkrivanju prevar se vse bolj uveljavlja način analize podatkov v informacijskih sistemih in poročanja o sumljivih transakcijah. Za analizo podatkov je potreben sistematičen pristop k zbiranju podatkov, čiščenju podatkov in standardiziranju podatkov. Sodobne tehnologije obdelave podatkov in računalniška strojna oprema omogočajo obsežne možnosti **sistematičnega analiziranja velikih količin podatkov** in s tem boljše razumevanje potencialnih tveganj za prevare. Ustrezna programska oprema za potrebe nadaljnje analize učinkovito razvrsti transakcije in ostale podatke glede na njihovo stopnjo tveganosti. To omogoča zaznavanje zakritih odnosov in povezav med transakcijami, aktivnostmi uporabnikov in med tveganimi podatki. S pomočjo statističnih podatkov, ključnih besed, brskanja po podatkih na osnovi izjem in na osnovi izdelanih profilov, takšna programska oprema odkriva nestandardne in sumljive transakcije.

U.S. Securities and Exchange Commission Office of the Whistleblower (5) je v letu 2013 namigovalcem (*whistleblower*) podelil preko 14 mio USD nagrad za njihove utemeljene namige o izvajanju prevar. Nagrade so v višini od 10% do 30% odkritega in prihranjenega zneska prevare. Med namigi je bil eden tudi iz Slovenije.

## Kdo so storilci

Storilci na višjih položajih in z večjimi pooblastili ter daljšim delovnim stažem v neki organizaciji so najbolj delovni in uspešni pri izvajanju prevar. So pa zato lastniki in izvršni vodstveni kader najbolj učinkoviti pri višini ustvarjene škode (desetkrat več kot zaposleni). Prav tako je bil čas izvajanja njihovih prevar pred odkritjem povprečno dve leti, kar je dvakrat več, kot pri zaposlenih.

V primerih, ko se pri izvajanju prevare združi več storilcev hkrati (dva ali več storilcev), so posledice za organizacijo bistveno bolj neprijetne.

Skoraj dve tretjini storilcev po spolu so moški, ki ustvarijo v povprečju dvakrat večje izgube zaradi prevar kot ženske. Večina storilcev je po starosti srednjih letih (med 31 in 45). Več kot polovica storilcev ima višjo in visoko izobrazbo. Najbolj pogosti so storilci z 1 do 5 letnim delovnim stažem, najbolj učinkoviti pa so storilci z nad 10 letnim stažem v neki organizaciji. Več kot 80% storilcev ni bilo predhodno obtoženih ali kaznovanih zaradi izvajanja prevar.

Skoraj dve tretjini storilcev po spolu so moški, ki ustvarijo v povprečju dvakrat večje izgube zaradi prevar kot ženske. Večina storilcev je po starosti srednjih letih (med 31 in 45). Več kot polovica storilcev ima višjo in visoko izobrazbo. Najbolj pogosti so storilci z 1 do 5 letnim delovnim stažem, najbolj učinkoviti pa so storilci z nad 10 letnim stažem v neki organizaciji. Več kot 80% storilcev ni bilo predhodno obtoženih ali kaznovanih zaradi izvajanja prevar.

V 92% primerov je bilo pri storilcih prevar mogoče zaslediti vsaj enega od pokazateljev za izvajanje prevar (življenje preko zmožnosti, finančne težave, pretesni odnosi s prodajalci ali strankami, pretirano zanimanje).

## Obvladovanje notranjih prevar

Pri naporih po obvladovanju notranjih prevar je potrebno in smiselno izvajati naslednje aktivnosti:

- Izvajati **preventivne** ukrepe za odvračanje morebitnih storilcev in za zmanjševanje priložnosti za izvajanje prevar,
- Izvajati ukrepe za **hitro zaznavanje, analiziranje in ukrepanje** ob prevarah. To je pogosto lahko že prepozno, saj se prevara že dogaja in zguba že nastaja.





Pri obeh načinih obvladovanja notranjih prevar je potrebno uvesti **organizacijske ukrepe** v obliki pravil poslovanja, izobraževanja in osveščanja zaposlenih ter **tehnične ukrepe** v obliki sposobnih informacijskih orodij za prepoznavanje in preprečevanje izvajanja prevar. Uvedba informacijskih orodij za odkrivanje prevar je lahko draga, a je še vedno cenejša kot so lahko morebitne neposredne in posredne izgube zaradi uspešno izvedenih prevar.

## Kako prepoznati izvajalce prevar

Večina prevarantov je motiviranih s kakršnokoli vrsto finančne stiske ali finančne potrebe. Ko nekdo začne izvajati prevaro se to zaradi stresa in strahu pred odkritjem odraža na njegovem obnašanju do sodelavcev in do okolice. Prav tako se spremeni njegov utečeni način dela, pogostost in uporaba informacijskega sistema. Takšne spremembe v obnašanju in v načinu uporabe informacijskega sistema so pomembni pokazatelji pri ustvarjanju suma in pri odkrivanju izvajanja prevar. Nekaj tipičnih pokazateljev izvajanja prevar (*Red Flags, Key Fraud Indicators*) je (1, 2) je: življenje preko zmožnosti, nepredvideni izdatki, nenavadne sorodstvene povezave, manjkajoči dokumenti, družinske težave, dominantnost, spletkarstvo, zasvojenost, daljše neizrabljanje dopusta, sledi preteklosti, ipd.

## Kako ravnati ob zaznavi notranje prevare

Vsem ukrepom za obvladovanje notranjih prevar navkljub se le-te dogajajo. V takem primeru zaznave dogajanja notranje prevare velja nekaj pravil o tem kaj se sme narediti in kaj se ne sme narediti, da s svojimi dejanji ne povzročimo dodatne škode oziroma ne onemogočimo pravilnega poteka preiskave dogajanja in morebitnega kasnejšega postopka kazenskega in sodnega pregona storilca.

V primeru odkritja prevare je potrebno čim prej vključiti strokovnjake, osumljencu odvzeti pooblastila, ohraniti in varovati dokazila, ohraniti zaupnost. Neprimerno pa je spreminjati stanje računalnikov, odkrivati podrobnosti o poteku pregleda, obtoževanje brez pravilne pravne podlage.

## Programska orodja za preprečevanje in odkrivanje notranjih prevar

Med načini za boljše obvladovanje notranjih prevar so tudi »tehnični ukrepi«, kjer so mišljena predvsem sposobna programska orodja za prepoznavanje in preprečevanje izvajanja notranjih prevar. V prejšnjih poglavjih so naštete prepoznavne lastnosti tako prevar kot storilcev prevar, ki istočasno predstavljajo osnovo za pričakovane lastnosti učinkovitih programskih orodij za preprečevanje in odkrivanje notranjih prevar.

V današnjih informacijskih sistemih se obdeluje zelo velike količine podatkov o strankah in o poslovanju, prisotni so različni viri podatkov, veliko je komunikacijskih poti in različnih baz podatkov, kar vse kliče po sposobnih orodjih za odkrivanje prevar.

V 92% primerov je bilo pri storilcih prevar mogoče zaslediti vsaj enega od pokazateljev za izvajanje prevar (življenje preko zmožnosti, finančne težave, pretesni odnosi s prodajalci ali strankami, pretirano zanimanje).

## Lastnosti programskih orodij za preprečevanje in odkrivanje notranjih prevar

Za upravljanje varnostnih informacij in dogodkov so pogosto uporabljani razni sistemi **SIEM - Security Information and Event Management.** Sistem SIEM zbira velike količine podatkov o dogodkih predvsem v sistemski opremi informacijskega sistema in jih zapisuje v dnevnike (*System-Log*) ter po potrebi proži alarme. Tak sistem lahko označimo kot »tehnični sistem«, vezan na računalniško strojno opremo in na varnostne incidente v sistemu, v nasprotju s »poslovnimi sistemi« ali »inteligentnimi sistemi«.

Druga vrsta programskih orodij za preprečevanje in odkrivanje notranjih prevar so »poslovni sistemi« ali »inteligentni sistemi« za celovit nadzor izvajanja poslovnih funkcij **ECMS - Enterprise Case Management Systems**.

Sistemi SIEM imajo v primerjavi z »inteligentnimi sistemi« vrsto pomanjkljivosti, ki izvirajo iz njihove tehnične naravnanosti, medtem ko poslovni sistemi analizirajo obnašanje uporabnikov na osnovi njihovega izvajanja poslovnih funkcij in uporabe sistema.

Sistemi za preprečevanje in odkrivanje notranjih prevar omogočajo preprečevanje odtekanja podatkov - DLP, kraje identitete, IT sabotaže, zavarovalniške goljufije, goljufije pri plačilih, nepooblaščen prevzem računov, goljufije e-banke, goljufije telefonske banke, goljufije na bankomatih – ATM, goljufije na plačilnih terminalih – POS, goljufije pri kartičnem poslovanju – PCI, goljufije pri izvajanju zdravstvenega zavarovanja in pri porabi medicinsko tehničnih pripomočkov, upravljanje operativnih tveganj – OT, spremljanje in poznavanje strank (*Know Your Customer – KYC*), spremljanje izvajanja sumljivih transakcij .

Nepooblaščeno odtekanje podatkov se lahko dogaja na treh nivojih: na aplikativnem, na mrežnem in na nivoju delovnega mesta. Standardna orodja za preprečevanje odtekanja podatkov lahko spremljajo promet z občutljivimi podatki na nivoju mreže in na nivoju delovnega mesta (e-sporočila, tiskanje, zapis na ključ USB), ne morejo pa preprečiti npr. slikanja podatkov na ekranu s pametnim telefonom in pošiljanja tretji osebi. Prav tako standardna orodja, ki analizirajo podatke poslane po mreži kot npr. številke kartic ali številke računov, ne bodo zaznala, da je v priponki k e-sporočilu priložena slika (*PrintScreen*) iskanih podatkov. Analizatorji prometa tudi ne bodo zaznali spremembe številke 1 v črko I ali številke 0 v črko O v primeru, ko je prevarant na tak način zakril pravo vsebino sporočila. Uporaba analizatorjev prometa zahteva njihovo namestitev na delovne postaje, kar je drago in zahtevno za vzdrževanje. Inteligentni sistemi zato spremljajo uporabnikov način dela in njegovo obnašanje ter na osnovi tega sklepajo na morebitno nepooblaščeno odtekanje podatkov.



## Kontrole, ki jih omogočajo sistemi ECMS

Programska orodja za preprečevanje in odkrivanje notranjih prevar s pričakovanimi lastnostmi, kot so opisane v prejšnjem poglavju, lahko izvajajo vrsto kontrol dogajanja v informacijskem sistemu in na ta način nadzirajo delo uporabnikov.

Kontrole vsebujejo med drugim na primer tudi: preverjanje pristopnih kontrol, primerjanje prijav v sistem, pooblastila izvajalcev, nenavadne aktivnosti uporabnikov, nestandardno uporabo informacijskega sistema, ocenjevanje faktorjev tveganja, zaznavanje sprememb profila uporabnika, izvajanje nestandardnega števila delovnih operacij, zaznavanje spremembe načina uporabe informacijskega sistema in vrsta drugih kontrol, zgrajenih na osnovi zaznavanja odstopanj od normalnega obnašanja uporabnikov.

## Zaključek

Prikazane številke in dejstva iz poročil o obsegu izvajanja notranjih prevar potrjujejo, da se obseg in škoda iz notranjih prevar večata, da njihovo obvladovanje postaja vse bolj zahtevno in da so storilci vse bolj iznajdljivi. Možnosti za bolj uspešno obvladovanje notranjih prevar lahko povzamemo v nekaj skupnih, osnovnih navodil o tem, kako lahko zavarujemo podatke in informacijske sisteme pred pooblaščenimi uporabniki:

- Bistveni del programa za zmanjševanje obsega notranjih prevar je dati zaposlenim možnosti in orodja za poročanje o sumljivih dogajanjih (kot npr. anonimne in zaupne vroče linije). Najbolj pogosto se notranje prevare odkrije na osnovi sporočil in namigov zaposlenih.
- Za zaposlene in za vodstvene kadre je zelo pomemben program izobraževanja in osveščanja o obvladovanju in preprečevanju notranjih prevar.
- Budno je potrebno spremljati obnašanje zaposlenih in pokazatelje za izvajanje prevar (rdeče zastave - R*ed Flags*), še posebej v povezavami z raznimi drugimi nepravilnostmi.
- Zelo učinkovito in vse bolj potrebno je uvajanje sodobnih, inteligentnih informacijskih orodij za odkrivanje notranjih prevar, ki sisteme in dogajanja v njih nadzorujejo on-line in omogočajo razne oblike analiziranja in koreliranja podatkov. ■

**V okviru otvoritve mednarodne konference**
**Dnevi korporativne varnosti bo svečana podelitev nagrad**

# Slovenian Grand Security Award 2014

ICS

Institut za korporativne varnostne študije

## Plaza hotel Ljubljana, 18. marec 2015

Slovenska velika nagrada varnosti je največja nagrada s področja varnosti v Republiki Sloveniji, ki bo podeljena izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti.

Neodvisna komisija ocenjuje in izbira kvaliteto in izvirnost prijavljenih udeležencev v naslednjih kategorijah:

**Najbolj varno mesto**
**Najbolj varno podjetje**
**Najbolj inovativna varnostna rešitev**
**Korporativno varnostni manager leta**
**Najboljša knjiga s področja varnosti**
**Inovativna medijska promocija varnosti**

www.ics-institut.si

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



# DVIG MINIMALNE PLAČE – PASTI IN PRILOŽNOSTI Z VIDIKA KORPORATIVNE VARNOSTI

**V zadnjem času se s strani sindikatov pojavljajo zahteve po spremembi definicije minimalne plače. Naj svoj članek začnem z odgovorom na vprašanje: Kaj je plača?**

Plača je izplačilo, ki ga zaposleni dobi za opravljeno delo. Lahko bi rekli, da je plača nadomestilo zaposlenemu za njegov vložen trud in mu služi kot priznanje za njegov prispevek k poslovanju organizacije. Plača je sestavljena iz fiksnega in gibljivega dela. Fiksni del tvorijo osnovna plača, ugodnosti in dodatki med katere štejemo: dodatke za posebne pogoje dela, dodatek za delovno dobo, pokojninsko, zdravstveno in socialno zavarovanje, nadomestilo za čas, ko delavec ne dela (dopust, bolezen, porodniška, očetovski dopust), plačilo (nagrade) za uspešnost, povračilo stroškov v zvezi z delom (prehrana, prevoz, službena potovanja), drugi prejemki (regres, odpravnina, solidarna pomoč) ter druge še nekatere ugodnosti. Gibljivi del plače predstavljajo predvsem nagrade za uspešnost in je odvisen predvsem od tega, kako dobro posamezni zaposleni opravlja svoje delo, lahko pa je vezan tudi na uspešnosti skupine, oddelka ali celotne organizacije. Z osnovno plačo posameznika motiviramo za napredovanje na delovna mesta, ki zahtevajo več spretnosti, znanja, odgovornosti in kompetenc, plačilo za uspešnost pa spodbuja posameznika k boljšemu in učinkovitejšemu opravljanju svojega dela in dvigovanju uspešnosti organizacije.

Izplačilo minimalne plače v Republiki Sloveniji ureja Zakon o minimalni plači, ki določa pravico do minimalne plače, njeno višino in pogoje pod katerimi se lahko izplačuje prehodni znesek minimalne plače ter način njenega določanja in objave. Gre za neko vrsto »varovalke«, ki delavcem zagotavlja, da mesečno zaslužijo vsaj za pokritje osnovnih življenjskih stroškov. Njena višina je izračunana na podlagi stroška življenjske košarice in ni odvisna od delavčeve osnovne plače, določene s pogodbo o zaposlitvi. Po omenjenem zakonu ima delavka in delavec, ki pri delodajalcu v Republiki Sloveniji dela poln delovni čas, pravico do plačila za opravljeno delo najmanj v višini minimalne plače, določene z Zakonom o minimalni plači. V minimalni plači so zajete naslednje postavke: bruto osnovna plača določena v pogodbi o zaposlitvi, dodatek na delovno dobo, dodatek za posebne pogoje dela, ki izhajajo iz razporeditve delovnega časa in sicer za nočno delo, delo v nedeljo, delo na praznik idr., dodatek za posebne pogoje dela, ki izhajajo iz posebnih obremenitev pri delu, negativnih vplivov okolja in nevarnosti pri delu, delovna uspešnost delavca in dodatek za poslovno uspešnost. Zneski, ki se po zakonu izplačujejo

Z osnovno plačo posameznika motiviramo za napredovanje na delovna mesta, ki zahtevajo več spretnosti, znanja, odgovornosti in kompetenc, plačilo za uspešnost pa spodbuja posameznika k boljšemu in učinkovitejšemu opravljanju svojega dela in dvigovanju uspešnosti organizacije.

*avtor je član Slovenskega združenja korporativne varnosti

nad zneskom minimalne plače pa so: nadurno delo in zneski za povračilo materialnih stroškov, katere je delavec imel zaradi dela (stroški prevoza na delo in z dela ter strošek prehrane na delu).

V zadnjem času se s strani sindikatov pojavljajo zahteve po spremembi definicije minimalne plače, ki gredo v smeri, da se iz minimalne plače izvzamejo naslednji dodatki: dodatek na delovno dobo in dodatki za posebne pogoje dela (nočno delo, delo v nedeljo, delo na praznik). Gospodarska zbornica Slovenije (GZS) ocenjuje, da bi omenjena sprememba definicije minimalne plače z izvzemom dodatkov povzročila težave okoli 12.500 podjetjem, kolikor jih po oceni GZS posluje na meji rentabilnosti. Ta podjetja naj bi zaposlovala okoli 100.000 ljudi in številna od teh delovnim mest bi bila v tem primeru resno ogrožena.

V čem je problem? Preprosta primerjava izračuna minimalne plače po sedanji definiciji in predlagani spremembi definicije, ki jo zagovarjajo sindikati pokaže, da se strošek minimalne plače delavca, ki opravlja delo v treh izmenah po novi definiciji poveča za nekaj manj kot 300,00 EUR mesečno. Ob upoštevanju predpostavke, da delavec opravlja delo v treh izmenah in tako v enem mesecu opravi 84 dnevnih ur, 68 nočnih ur in 24 nedeljskih ur in ima 10 let delovne dobe, znaša minimalna plača po obstoječi definiciji cca. 1.060,00 EUR, po predlagani novi definiciji pa cca. 1.360,00 EUR. Kaj hitro lahko zaključimo, da to za organizacije predstavlja skoraj 30% povečanje stroškov dela. To je še poseben problem za storitvena podjetja, katerim stroški dela v strukturi stroškov poslovanja predstavljajo pretežen del stroškov. V to skupino spadajo tudi zasebna varnostna podjetja in druga specializirana podjetja, ki v sistemu korporativne varnosti predstavljajo pomemben člen pri obvladovanju ranljivosti, ogroženosti in varnostnih tveganj na operativnem nivoju.

Prepričan sem, da obstoječ sistem izplačila plač varnostnemu osebju, ki skrbi in odgovarja za varnost ljudi in premoženja (tudi na območjih, objektih in v organizacijah, ki so posebnega pomena za državo/regijo), ne zagotavlja ustrezne socialne varnosti. Veliko njih ima blokirane račune, sodne izvršbe na izplačila plač, nekateri pa so celo v osebnem stečaju. Za uporabnike je to zadostni, če ne njuni razlog za alarm. Varnostno osebje, ki ne zasluži dovolj za osnovno preživetje predstavlja »tempirano bombo«, ki lahko v vsakem trenutku eksplodira. S tem namigujem na stopnjo izpostavljenosti varnostnega osebja kriminalni ogroženosti in izpostavljenosti skušnjavam, ki se lahko izkazuje v povezovanju varnostnega osebja s kriminalnimi združbami, izvajanju kaznivih dejanj, sprejemanju podkupnin, malomarnemu opravljanju varnostnih nalog, neizpolnjevanju pogodbenih obveznosti ipd. Iz tega vidika je sprememba plačne politike nujna in neizogibna, prizadevanja sindikatov po spremembi definicije minimalne plače, ki bi imela za posledico bistveno povišanje plače delavcem, pa razumljiva. Nerodno je namreč, če ima varnostnik, ki nadzira zaposlene naročnika, nižjo plačo od tistih, ki so podvrženi njegovemu nadzoru. Tako na področju varovanja preprosto ne gre. In tu je priložnost, da stroka pove, kako rešiti ta problem. Sam vidim kar nekaj možnosti, ki pa žal presegajo okvir tega članka.

In kje so pasti? V primeru sprejema pobude sindikatov o spremembi definicije minimalne plače, bi se stroški dela varnostnega osebja, ki v večini prejema minimalno plačo, povišali za cca. 300,00 EUR na mesec, kar predstavlja cca. 1,70 EUR več na uro dela. Zasebna varnostna podjetja tega povišanja stroška dela enostavno ne bi preživela. Logična posledica je torej dvig cen storitev, kar čez noč postane problem naročnika. Za naročnika to pri neprekinjenem 24-urnem fizičnem varovanju predstavlja cca. 1.250,00 EUR mesečnega povišanja stroškov. In spet se znajdemo v spirali, ki preko dviga stroškov dela zaradi spremembe definicije minimalne plače, predstavlja povišanje stroškov v celi verigi sodelujočih. Na koncu to, po eni strani za podjetja pomeni zniževanje konkurenčnosti, po drugi strani pa sili podjetja v zmanjševanje obsega varovanja kar ima praviloma negativen vpliv na procese obvladovanja ranljivosti, ogroženosti in varnostnih tveganj, s tem pa se povečuje ranljivost podjetij.

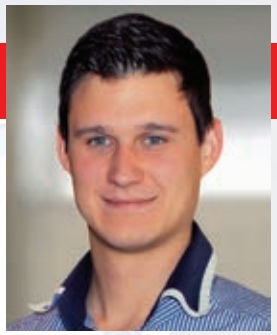
Kdo tu dobi in kdo zgubi? V bistvu so na boljšem tisti delavci, ki se jim plača dvigne in obdržijo delo, na slabšem pa so delavci, ki zaradi tega izgubijo delo in podjetja, ki zaradi dviga stroškov postajajo manj konkurenčni. Moralni zmagovalci so torej sindikati in delavci, ki obdržijo delo, realni poraženci pa delavci, ki delo izgubijo (in teh ne bi bilo malo) in podjetja, ki po eni strani zgubljajo bitko na trgu zaradi zniževanja svoje konkurenčnosti (in tudi teh ne bi bilo malo), po drugi strani pa zaradi manjših vlaganj v varnostne ukrepe povečujejo stopnjo tveganja in verjetnost nastanka škodnih dogodkov.

Menim, da bi si morali tisti, ki vneto in brez ustreznih analiz posledic, zagovarjajo spremembo definicije minimalne plače, nujno zastaviti naslednje vprašanje: Je to res edina pot?

Jaz verjamem, da ni in da obstajajo tudi druge poti (rešitve), ki prav tako omogočajo višja izplačila plač, pri tem pa povišanje stroškov poslovanja iz naslova dviga plač, ostajajo v sprejemljivih okvirih. V inštitutu za korporativne varnostne študije imamo odgovore tudi na to aktualno problematiko. ■

Varnostno osebje, ki ne zasluži dovolj za osnovno preživetje predstavlja »tempirano bombo«, ki lahko v vsakem trenutku eksplodira.

Avtor: Boštjan Špehonja / Etični hacker*



# INFORMACIJSKA VARNOST RES POSTAJA DEL NAŠEGA VSAKDANA

**Živimo v času, ko si življenja brez elektronskih naprav ne predstavljamo. Postavlja pa se nam vprašanje ali se dovolj dobro zavedamo potrebe po varnosti v informacijski družbi?**

Začetki širše uporabe računalnika segajo v devetdeseta leta prejšnjega stoletja, ko so računalniki začeli postajati dostopni širši javnosti. To je bilo za tisto obdobje revolucionarnega pomena. Od takrat naprej pa se razvoj informacijske tehnologije širi s svetlobno hitrostjo. Dokaj dobro smo se navadili na stacionarne računalnike, ko nam je industrija že ponudila prenosne računalnike, v zadnjih letih pa so nam po tiho podtaknili trend tabličnih računalnikov ter pametnih telefonov. Tudi tu se razvoj informacijske tehnologije ni ustavil, ampak se nadaljuje v smeri interneta stvari. To pomeni, da gremo v smeri, ko bodo na internet priklopljene vse mogoče stvari, žarnice, mikro valovne pečice, hladilniki, hiše, avtomobili... Vse funkcionalnosti, ki nam jih ponuja razvoj tehnologij nam precej olajšajo vsakdanje delo, vendar se s tem povečuje tudi rizik informacijske varnosti. Ko so v šestdesetih letih prejšnjega stoletja v projektu Arpanet uspešno prenesli prvi paketek po omrežju je bil to velik uspeh in nihče ni niti pomislil o varnosti. Danes so na trgu produkti vredni več sto tisoč evrov, ki so namenjeni izključno prepoznavanju napadov ter namenjeni informacijski varnosti. Iz tega je razvidno, da postaja informacijska varnost del našega vsakdana, vendar so uporabniki interneta velikokrat premalo osveščeni o varni uporabi interneta ter napravah povezanih nanj, pasti in groženj pa se niti ne zavedajo. V zadnjih letih se zelo strmo povečuje trend napadov na uporabnika, kar je razvidno tudi iz poročila o omrežni varnosti, ki ga vsako leto izda Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI CERT). Iz leta v leto opažajo porast spletnih goljufij, škodljive kode, razobličenja spletnih strani ter drugih prevar. Slabo osveščenost uporabnikov spretno izkoriščajo spletni goljufi, ki uporabljajo tako imenovano tehniko socialnega inženiringa. Gre za način prevare, kjer prevarant z izkoriščanjem človekovih lastnosti ter s pomočjo manipulacije in psiholoških učinkov, prepriča žrtev v neko dejanje, ki ga sicer običajno ne bi storila. Največkrat se začne prevara s prejetjem elektronske pošte. V roku 24-ih ur se na svetu pošlje približno 250.000.000.000 (dvesto petdeset milijard) sporočil in velika večina teh je nezelena elektronska pošta. Zato je velika verjetnost, da se takšno sporočilo kdaj znajde tudi v našem elektronskem predalu. Najpogosteje nam prevaranti obljubljajo več milijonske zneske pod pretvezo dobitka na loteriji ali odkritega starega vojnega denarja v neki oddaljeni državi. Če navežemo stik s prevarantom nam ta kmalu pove, da je potrebno plačati stroške odprtja računa, stroške zavarovanja prenosa in drugo. V kolikor opravimo transakcijo, denar posredujemo goljufu. Za njim se izgubi vsaka sled, prav tako za obljubljenimi milijoni. Zato je priporočljivo, da se na takšna elektronska sporočila ne odgovarja, še posebej, če zaznamo v njih polomljeno slovenščino, ki spominja na prevod s spletnimi orodji kot so Google, Bing in drugi. Velikokrat se zgodi, da so tarča napadov zaposleni v podjetju. Kadar gre za posebej targetirana sporočila, je pri slednjih zelo težko prepoznati, da gre za prevare. Po svoji obliki in sestavi so zelo podobna resničnemu sporočilu, vendar se pasti skrivajo v minimalnih detajlih. Preveriti je potrebno ali je bilo sporočilo poslano iz dobesedno istega naslovnika kot navadno, ali so v sporočilu nepričakovane stisnjene (zip) priponke ter povezave na druge neznane spletne strani, pri nepričakovanem elektronskem sporočilu pa se je potrebno vprašati tudi o smotrnost same vsebine sporočila. V kolikor sporočila ne pričakujemo in se v njih skrivajo priponke, sploh z izvršljivimi datotekami, jih je vsekakor nepriporočljivo odpirati saj se v njih lahko nahajajo virusi. Prav tako so lahko nevarne povezave v

V zadnjih letih se zelo strmo povečuje trend napadov na uporabnika, kar je razvidno tudi iz poročila o omrežni varnosti, ki ga vsako leto izda Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (SI CERT).

*avtor je član Slovenskega združenja korporativne varnosti

elektronskem sporočilu saj nas lahko pripeljejo do okužene spletne strani in, v kolikor naš sistem ni posodobljen, se lahko okužimo samo ob kliku na stran, brez da bi se na njej dlje časa zadrževali. Primer množičnih phishing napadov se je zgodil januarja letos, tarča pa so bile slovenske banke. Prevaranti so na več spletnih naslovov prekopirali spletno stran in postavili enako grafično podobo za prijavo v elektronsko bančništvo kot jo uporablja vaša banka. Uporabnikom so na elektronske pošte pošiljali obvestila, da njihov račun potrebuje dodatno preverjanje, zraven pa so pripeli povezavo do njihove, lažne spletne strani, ki je bila identična bančni, le na drugem naslovu. Ko je uporabnik vpisal svoje podatke, jih je s tem posredoval goljufom. Kljub temu, da se je veliko govorilo o tem, da so se zgodili napadi na slovenske banke, je bil to dejansko napad na uporabnike spletnega bančništva. Novica o vdoru v banke je v javnost prišla februarja letos, ko so strokovnjaki ugotovili, da je skupina kriminalcev uspešno odtujila okoli 300 milionov evrov v preko 100 inštitucijah v 30-ih državah sveta. Z elektronsko pošto in zgoraj omenjenimi prevarami se je po vsej verjetnosti seznanil sleherni izmed nas. Niso pa uporabnikom poznani drugi segmenti informacijske varnosti. Kot je bilo že prej omenjeno, se z vsako novo tehnologijo pojavi tudi novo tveganje in potencialna nevarnost. Pametni telefoni lahko komunicirajo kar preko 9 kanalov: Zaslon, Jack,

Etični heker se postavi v vlogo napadalca in poizkuša na različne načine priti do zasebnih podatkov v podjetju od načinov kako onemogočiti storitev ali do privilegiranega dostopa do vaših naprav.

WI-FI, 3G, 4G, LTE, bluetooth, GPS ter NFC. Vse omenjene protokole uporablja večina pametnih telefonov in vsi morajo biti za uporabnikovo varnost ustrezno zavarovani. Telefon je varen toliko, kot je varen najšibkejši kanal. Ne pomaga nam antivirusni program, če nimamo posodobljenih aplikacij oziroma, če za odklepanje telefona nimamo gesla ali kakšne druge metode varovanja. Prav tako je pomembno, da se wi-fi ter bluetooth storitev po zaključeni uporabi izklopi. Prva prednost je v tem, da bo baterija zdržala dlje časa, kot drugo pa vaš mobilni telefon v lokalnem omrežju ne bo podvržem raznim napadom. V kolikor je v telefonu vklopljena WI-FI funkcija, je mogoče iz njega prebrati vsa brezžična omrežja, v katerih ste bili že prijavljeni (SSID - je). To je uporabna informacija, ker lahko potencialni napadalec ustvari dostopno točko z istim imenom kot ga je prebral iz vašega telefona. Ta se bo v tem primeru avtomatsko, brez vaše vednosti, povezal na znano dostopno točko in tako sta z napadalcem v istem omrežju. Ta metoda napadalcu zelo olajša delo, če želi priti do podatkov na vašem telefonu. Enak scenarij pa se lahko zgodi v restavracijah, trgovskih centih, ter drugih lokacijah, kjer nudijo brezplačni brezžični internet. Na teh lokacijah velja posebej omeniti nevarnost kraje seje. Ko obiščemo kakršnokoli stran za prijavo, bodisi v spletno pošto ali socialno omrežje, je potrebno vpisati svoje uporabniško ime ter geslo. Tej podatki se po mreži pretakajo preko https povezave, kar pomeni, da je povezava kriptirana in za napadalca neberljiva. Ko je povezava vzpostavljena in se uspešno prijavimo, pa se med napravo in strežnikom vzpostavi seja. Ta pa predstavlja nevarnost saj se po mreži pretaka v berljivi obliki in z nekaterimi napadi je mogoče v lokalnem omrežju priti do te seje in s tem do profila uporabnika. Seja je veljavna toliko časa, dokler se ne odjavimo. Ko se v profil ponovno prijavimo, nam strežnik dodeli novo sejo in stara ne deluje več. Zato je priporočljivo, da se po brskanju na nezavarovanih oz. javnih omrežjih vedno odjavimo, v času brskanja po teh omrežjih pa imamo v mislih, da nam mogoče nekdo v bližini prebira naša sporočila in se sprehaja po našem






profilu. Velikokrat si ljudje mislimo, da je nemogoče, da bi se kdorkoli virtualno spravil na nas in da naši podatki za nikogar niso zanimivi. Marsikdo je prepričan, da tudi če kdo pride do njegovih podatkov, jih tako ali tako nima za kaj uporabiti, ker niso zanimivi. Tukaj bi opozoril na spletne prevarante, za katere mogoče niste zanimivi vi in vaši podatki, ampak vaš informacijski sistem, ki vključuje računalnike, telefone, usmerjevalnike, spletne strani in drugo, ki jih nato izkorišča za nadaljnje napade. Če se ujamete v past, in postane vaš računalnik okužen, je to odlično orodje za izvajanje nadaljnjih napadov bodisi ddos napada ali pošiljanje neželene elektronske pošte. To početje je kaznivo, in zato spletni goljufi iščejo ranljive naprave priklopljene v internet, ki jih nato izkoriščajo. Tako zakrijejo svojo sled, v primeru večje škode pa bo imel težave lastnik okužene naprave, tako z ponudnikom internetne storitve, kot morda tudi s policijo. Podobne stvari se dogajajo na spletnih straneh. Veliko je takšnih, ki niso vzdrževane in s časom postanejo ranljive. Ranljive zato, ker se vsak dan odkrije kakšna nova ranljivost, prej ali slej tudi pri tehnologiji ali programski opremi, iz katere je sestavljena spletna stran. Te ranljivosti prevarantje spretno izkoriščajo in lahko se zgodi, da vam razobličijo spletno stran, lahko vam na stran postavijo povezavo, ki vodi do neke druge lažne spletne trgovine, ali celo na vaši strani postavijo podstran za vpis v elektronsko bančništvo, kot se je dogajalo januarja pri napadu na slovenske banke. V vsakem primeru je lastnik spletne strani odgovoren za dogajanje na njej in, če bodo goljufi na vaši strani uspešno postavili lažno stran elektronske banke, boste nehote postali del preiskave. Zato je pomembno, da administrator spletne strani redno posodablja in vzdržuje. Za podjetja pa je smiselno, da bi se večkrat posluževala storitve etičnega hackinga. Pri tem gre za storitev, ko podjetje najame hekerja da preišče njihovo IT infrastrukturo. Ne gre za hekerja, ki bi namenoma povzročil kakršnokoli škodo, ampak etičnega hekerja, ki v točnem časovnem obdobju in z vso vednostjo zaposlenih v podjetju, preverja ranljivosti v vaši infrastrukturi. Tako spletne strani, spletne aplikacije, požarne pregrade, strežnike, kot tudi pregled internetnih iskalnikov ter arhivov, kaj se vse se o podjetju nahaja na spletu. Etični heker se postavi v vlogo napadalca in poizkuša na različne načine priti do zasebnih podatkov v podjetju od načinov kako onemogočiti storitev ali do privilegiranega dostopa do vaših naprav. Kot rezultat podjetje dobi obširno poročilo kaj vse je etični heker počel, katere metode je uporabil, pri katerih je bil uspešen, pri katerih ne, do kakšnih podatkov podjetja je lahko prišel ter priporočila za odpravo ranljivosti. Kot je bilo na začetku omenjeno, se trend tehnologij v zadnjih parih letih premika v smeri interneta stvari. To pomeni, da bo na internet priklopljenih vse več naprav, pa ne samo dosedanje komunikacijske kot smo jih vajeni, ampak bo mogoče vsako stvar preko brezžičnih povezav povezati v internet. Govorimo o televizijskih sprejemnikih, hladilnikih in drugih gospodinjskih aparatih, avtomobilih, celo oblekah, aparatih za britje in ostalo. Vsak najmanjši predmet, ki bo povezan na internet, bo postal internet stvari. Ena od prvih napovedi, ki jo je pred leti objavil Ericsson je trdila, da bo do leta 2020 v internet povezanih preko 50 milijard »stvari«. Intel pa je objavil, da bo v gospodinjstvu štiričlanske družine, ki ima danes v povprečju v internet povezanih 10 naprav, do leta 2022 že kar 50 povezanih naprav. Ob tem se poleg vprašanja zasebnosti ponovno pojavlja vprašanje varnosti. Kako se bo posodabljalo mikrovalovne pečice, če bo na njih odkrita ranljivost? Kaj, če se bo nekdo poigral z gretjem vaše hiše sredi poletja, medtem ko boste na dopustu? Posebej zanimivo pa bo po medijih poslušati informacije, da so hladilniki in mikrovalovne pečice krivec za napade na različne ustanove. ■

Ena od prvih napovedi, ki jo je pred leti objavil Ericsson je trdila, da bo do leta 2020 v internet povezanih preko 50 milijard »stvari«. Intel pa je objavil, da bo v gospodinjstvu štiričlanske družine, ki ima danes v povprečju v internet povezanih 10 naprav, do leta 2022 že kar 50 povezanih naprav.

ICS
Institute for Corporative Security Studies

## ICS PUBLIKACIJE - NOVOST

# Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection




NATO OTAN

*This workshop is supported by:* The NATO Science for Peace and Security Programme

**Editors:**
**dr. Denis Čaleta, dr. Vesela Radović**

## ICS PUBLIKACIJE - NOVOST



Papirni izdelki po meri



Dolgoletna tradicija – že od leta 1954





## *PAPIRNI IZDELKI SEDEJ*

Mivka 30, Ljubljana, T: +386 1 283 93 12, G: +386 31 353 034, sedej.sp@siol.net, www.skatla.eu



Kakovost je najpomembnejša



Avtor: Ingo Falk Pasch Wallersberg*



# EVROPSKA USKLADITEV PREVERJANJA POKLICNE USPOSOBLJENOSTI VARNOSTNIKA

**Področje zasebnega varovanja je eno izmed zelo redkih področij, na katerih pravne ureditve poklicev v tej specifični dejavnosti, še vedno niso evropsko sinhronizirane. Kvalifikacijske zahteve in poklicne možnosti za varnostno osebje so kljub sorodnim zahtevam za te poklicne profile v državah, članicah EU, urejene zelo različno.**

Minimalni pogoji za kvalifikacijske zahteve se raztezajo od tega, da je treba predložiti potrdila, s katerimi se dokazuje, da je oseba zaupanja vredna, do zahtev, da oseba opravi nekajdnevno usposabljanje, pa vse do tega, da opravi najmanj dvoletno izobraževanje. Zahteva, da se na evropski ravni opredelijo skupni minimalni poklicni standardi za varnostno osebje je odprta že več desetletij. Glede na to, da se zasebno varovanje v mnogih državah uvršča med dejavnosti z najnižjimi plačami, pa je komaj mogoče doseči, da bi se na področju izobraževanja predpisali kakovostno ustrezni strokovni pogoji in zahteve za opravljanje tega v resnici zelo občutljivega poklica. Tega niti danes v 21. stoletju še vedno ni mogoče doseči, kljub temu da postaja dejavnost varovanja – še posebej glede na čedalje večje varnostne rizike v sodobnem svetu – eden izmed najpomembnejših strokovnih izzivov prihodnosti.

Tako obstajajo v državah, članicah EU, zelo različne vsebine usposabljanja, ki jih je mogoče primerjati šele na podlagi analize izdanih certifikatov oziroma učnih vsebin. To področje je na področju EU še vedno bistveno neurejeno. Usklajen postopek preverjanja zahtev poklicnih standardov in katalogov, ki ga predvidevajo rezultati posebnega evropskega projekta v programu Leonardo da Vinci, naj bi omogočil objektivno transparentnost pri ugotavljanju in priznavanju kvalifikacij, pridobljenih v različnih državah, članicah EU. Glede na to,da so v teh državah vsebine nacionalnih poklicnih kvalifikacij (NPK) oziroma teh poklicnih profilov zelo različne, je cilj tega evropskega projekta, da se omogoči objektivna primerjava teh profilov v različnih državah na ravni EU. Na podlagi takšne primerjave pa bo možna tudi ugotovitev vsakokratnih deficitov, ki jih mora kandidat – emigrant iz ene države odpraviti z ustrezno dokvalifikacijo v drugi državi, članici EU. K temu je treba dodati, da se danes pri obstoječem formalnem primerjanju doseženih poklicnih kvalifikacij na področju zasebnega varovanja med različnimi državami, članicami EU – katerih postopki so še vedno bistveno nezadovoljivo regulirani – neformalno pridobljene kompetence in spretnosti ne obravnavajo in glede na zgolj formalno ocenjevanje in ugotavljanje zahtevnosti teh poklicnih profilov v posameznih državah ne upoštevajo pri ugotavljanju kandidatovih znanj in spretnosti.

Navedeni evropski projekt, ki je v prvi fazi potekal v koordinaciji »Deutsche Angestellten- Akademie« iz Frankfurta s sodelovanjem skupine strokovnjakov iz partnerskih združenj iz Irske, Španije, Slovenije in Nemčije od oktobra leta 2010 do oktobra 2012, je vzpostavil podlago za razvoj evropskega sistema ocenjevanja kompetenc na področju poklicev zasebnega varovanja – seveda z nujnimi omejitvami na določen poklic-

Usklajen postopek preverjanja zahtev poklicnih standardov in katalogov, ki ga predvidevajo rezultati posebnega evropskega projekta v programu Leonardo da Vinci, naj bi omogočil objektivno transparentnost pri ugotavljanju in priznavanju kvalifikacij, pridobljenih v različnih državah, članicah EU.

*avtor je član Slovenskega združenja korporativne varnosti

ni – kompetenčni profil. Ta kompetenčni profil je bil z navedenim projektom opredeljen v okviru CEMES sistema (Competence Evaluation Method for European Specialists) in pokriva kvalifikacijske stopnje 3 in 4 iz evropskega okvira kvalifikacij (primerjalno s slovenskimi NPK v pretežni meri na ravni NPK varnostnica/varnostnik) ter je v tem projektu tudi podprt z ustreznimi izpitnimi vprašanji in nalogami. Gre za poskus evropskega objektivnega merjenja strokovne oziroma poklicne usposobljenosti varnostnega osebja iz različnih držav – članic EU in s tem vzpostavitve evropske objektivne ocene o doseženem obsegu in ravni usposobljenosti konkretnega kandidata. Za takšno ocenjevanje je skupina partnerjev v tem projektu pripravila ustrezne sklope več-izbirnih in odprtih vprašanj na petih (na projektni konferenci v Ljubljani opredeljenih) tematskih kompetenčnih področjih: a) zakonodaji, b) dejavnosti zasebnega varovanja, c) postopkih, č) komunikaciji in d) nevarnostih; pri tem je (razumljivo) na prvem področju, t.j. zakonodaje, priprava navedenih vprašalnih sklopov ločena po posameznih državah. Ta izkaz je predviden kot izhodišče za ugotovitev potrebe po obsegu in vrsti nadaljnjega usposabljanja tega kandidata, ko se le-ta želi zaposliti v konkretni drugi državi, članici EU.

Ta problematika, ki je neposredno povezana z migracijo delavcev iz ene v drugo državo EU, je bila doslej zaradi jezikovnih ovir za Slovenijo manj aktualna, postaja pa sedaj s polnopravnim članstvom R Hrvatske v EU vsak dan bolj prisotna (ter se bo njen pomen s kasnejšo pridružitvijo drugih držav, osamosvojenih po razpadu nekdanje SFRJ, k EU še bistveno povečal). V tej zvezi velja na tem mestu le na kratko pripomniti, da za varnostno osebje pri nas - kljub zakonsko opredeljeni zahtevi po znanju slovenskega jezika - še vedno niso razviti niti kriteriji niti metode za ustrezno preveritev tega znanja; ta problematika je in ostaja pri nas nedopustno zanemarjena. Domnevati pa smemo, da je ta problematika pomembna v obratni smeri, t.j. glede na interes in možnosti slovenskih izvajalcev, da opravljajo varnostne storitve v drugih državah, članicah EU. V tej zvezi je – ne glede na morebitne izjeme v primerih občasnega oziroma začasnega opravljanja storitev – vendarle potrebno upoštevati temeljno pravilo o veljavi *lex loci labori*.

Glede na različne vsebine in standarde usposabljanja varnostnega osebja (oziroma celo glede na odsotnost takšnega usposabljanja) pri državah, članicah EU, je danes nedvomno odprta potreba po vzpostavitvi objektivnega in evropsko enovitega sistema strokovne preveritve in primerjave usposobljenosti kandidatov iz različnih držav, članic EU. Takoj pa je treba jasno poudariti, da je bistvo projekta izključno samo objektivna strokovna podpora pristojnim organom in inštitucijam v državah, članicah EU, pri njihovem ugotavljanju dejanskega stanja strokovne usposobljenosti posameznega kandidata iz druge države, članice EU, ko naj bi pričel delati v njihovi državi. S tem se v veliki meri zmanjšuje možnost realnega ali nestvarnega očitanja, da pristojna inštitucija države gostiteljice pristransko ocenjuje doseženo raven strokovne usposobljenosti in kompetence, ki jih je kandidat pridobil v svoji državi. Hkrati se s tem tudi sedanje popolnoma različne ravni takšnega ocenjevanja po posameznih državah privedejo na skupen (objektiven) imenovalec.




Glede na različne vsebine in standarde usposabljanja varnostnega osebja (oziroma celo glede na odsotnost takšnega usposabljanja) pri državah, članicah EU, je danes nedvomno odprta potreba po vzpostavitvi objektivnega in evropsko enovitega sistema strokovne preveritve in primerjave usposobljenosti kandidatov iz različnih držav, članic EU.

V tem projektu predvideni evropski postopek opredeljevanja kompetenc varnostnega osebja sestoji iz treh med seboj povezanih stopenj:

- računalniško podprtega MC (več-izbirnega) testa s takojšnjim ovrednotenjem, na podlagi katerega se preverja strokovno vedenje kandidata
- računalniško podprtega testa, v katerem so s strani ekspertov pripravljena kompleksno zastavljena vprašanja, s čimer se preverja kandidatovo vedenje o soodvisnostih
- testa s kompleksnimi študijami primerov, s katerimi se preverjajo kandidatove kompetence za delovanje

Na podlagi navedenih postopkov je mogoče nato izdelati oziroma ugotoviti profil kandidata.

Poudariti je treba, da naj bi se na podlagi z navedenim projektom predvidenega testiranja kandidatov (na omenjenih petih področjih njihovih strokovnih poklicnih kompetenc) ugotavljala njihova usposobljenost le na podlagi in v obsegu sporazumno (kompromisno) določenih vprašalnikov (za katere so partnerji dokončane prve faze projekta na podlagi več kot 50 specifičnih spretnosti in več kot 250 strokovnih pojmov zasnovali preko 200 odprtih in programiranih vprašanj, preverjenih glede njihove ustreznosti z vidika specifičnih pravnih ureditev v njihovih državah). Seveda pa ti vprašalniki v posameznih državah (tako zlasti tudi v Sloveniji) le delno pokrivajo zahteve njihovih opredeljenih NPK. Izvajanje testiranja in ugotavljanja usposobljenosti kandidatov na navedeni evropski, nadnacionalni ravni bo zato lahko le pripomoček za objektivno oceno njihove že dosežene usposobljenosti, kadar bodo iskali zaposlitev izven svoje matične države, t.j. na področju druge države, članice EU.

Nadaljevanje projekta je namenjeno razširitvi v predhodni fazi projekta določenih evropsko primerljivih kompetenc varnostnega osebja in vključitvi partnerjev iz dodatnih držav članic EU ter praktičnemu preizkusu testiranja kandidatov na podlagi evropsko usklajenih postopkov testiranja in harmoniziranih testnih vprašanj. V tej zvezi je predvideno tudi ustrezno usklajevanje oziroma oblikovanje projektno predvidenih nacionalnih certifikacijskih centrov. Obenem je tudi predvidena vključitev ustreznih državnih organov in inštitucij v projekt (kot svetovalcev, izvedencev ali zunanjih sodelavcev) ter ustrezna objava rezultatov projekta.

V tej zvezi so cilji predvidenega projekta KOMSI II:

- Namen je, da se vzpostavi primerjava med doseženimi specifičnimi kompetenčnimi profili v posameznih državah in s tem podlaga za neposredno primerjavo različnih nacionalnih izobraževanj. V tej zvezi bo v pomoč nacionalnim organizacijam, oblastnim organom, združenjem ali podjetjem, ki rešujejo naloge v zvezi s priseljenimi delavci iz drugih držav na področju zasebnega varovanja, mogoče določiti kompetenčne profile glede na postopke izobraževanja oziroma usposabljanja v teh partnerskih državah. Tako določeni profili bodo omogočili neposredno primerjavo formalno doseženih kvalifikacij varnostnih delavcev med udeleženimi državami.
- Primerjava nacionalnih specifično opredeljenih kompetenčnih profilov bo v okviru projekta preizkušena in evaluirana, pri čemer bo opredeljen standardiziran postopek za oceno formalnih kvalifikacij, s katerim bo omogočeno primerjalno ocenjevanje in vključitev različnih nacionalnih kvalifikacij (zaradi omejenih možnosti v okviru tega predvidenega projekta najprej samo v okviru 6 do 7 držav). Ta predvideni standardizirani postopek za ocenjevanje različnih nacionalnih kvalifikacij je namenjen za uporabo predvsem nacionalnim inštitucijam, katerih področje dela so delovni migranti z različnimi nacionalnimi kvalifikacijami na področju zasebnega varovanja, kakor tudi izvajalcem te dejavnosti.
- Nadaljnji pomembni cilj je obveščanje pristojnih inštitucij na področju zasebnega varovanja na evropski ravni kakor tudi pristojnih nacionalnih oblastnih organov držav članic EU. Predvideno je, da se obveščanje o rezultatih projekta izvede v okviru mednarodnih strokovnih posvetov kakor tudi s pomočjo neposredne vključitve evropskih socialnih partnerjev v okviru socialnega dialoga na področju zasebnega varovanja.

Na podlagi izmenjave izkušenj in razprave nacionalnih izvedencev za kvalifikacije v dejavnosti zasebnega varovanja bodo partnerji v projektu s pomočjo CEMES orodja vzpostavili postopek za ocenjevanje formalnih nacionalnih kvalifikacij na področju zasebnega varovanja. Ta postopek bo za izbrane nacionalne kvalifikacije na področju zasebnega varovanja v udeleženih državah preizkušen, evaluiran in obdelan ter pri uspešni realizaciji predlagan evropski strokovni javnosti kot standardni postopek ocenjevanja.

Rezultati projekta na področju ocenjevanja in neposredne primerjave formalnih kvalifikacij v dejavnosti zasebnega varovanja med udeleženimi državami bodo neposredno na razpolago nacionalnim izvajalcem v tej dejavnosti. ■



Avtorici: Milka Pungartnik, magistrica ekonomskih in poslovnih ved /
Sanja Androić, magistrica managementa* / Mariborski vodovod**





# SISTEMSKA KORUPCIJA IN KORPORATIVNA VARNOST

**V prispevku bomo najprej definirali korupcijo in korporativno varnost, nato pa poskušali prikazati kako koruptivna dejanja vplivajo na korporativno varnost.**

Po najenostavnejši razlagi izpeljani iz zakonske definicije je korupcija vsaka kršitev dolžnega ravnanja z namenom pridobiti korist zase ali za koga drugega. (KPK, b.l.) Vrst in oblik korupcije je veliko, a se bomo v nadaljevanju osredotočili samo na sistemsko korupcijo in posredno tudi na ujetje države, ki sta medsebojno povezani.

Ujetje države pomeni podkupovanje poslancev in funkcionarjev ter javnih uslužbencev v obliki netransparentnih plačil s ciljem spodbuditi jih, da sprejmejo takšne zakone, pravila, uredbe in predpise, od katerih bodo imeli podkupovalci določeno korist (Bursač, 2006, str. 11). Opredelitev sistemske korupcije pojmuje ta pojav širše in ga členi v različne prvine kriminalnega prevzema države. Caiden in Caiden (1977, str. 301 – 309) definirata sistemsko korupcijo kot stanje, ko hudodelstvo postane norma in ko standardno pričakovano vedenje, nujno za doseganje ciljev organizacije, skladno s predstavo o javni odgovornosti in zaupanju, postane izjema in ne pravilo. V takem stanju korupcija postane tako običajna in institucionalizirana, da organizacijska podpora ščiti hudodelstvo in dejansko kaznuje tiste, ki delujejo skladno s starimi normami. Takšno razumevanje sistemske korupcije precej upošteva KPK (2011), ki sistemsko korupcijo opredeljuje kot:

- vsako doseganje ali ustvarjanje normativnih institucionalnih, statusnih ali postopkovnih pogojev oziroma okoliščin zaradi omogočanja ali pridobivanja koristi uradnim in drugim fizičnim ali pravnim osebam v škodo javnih sredstev;
- vsako drugo obliko izkoriščanja normativnih, institucionalnih, statusnih ali postopkovnih pristojnosti, pomanjkljivosti, nekonsistentnosti ali neusklajenosti, vključno z neupoštevanjem ali neodzivanjem na uradne ugotovitve in pozive pristojnih nadzorstvenih organov;
- vsako ponavljajoče se ali trajajoče opuščanje uporabe nadzorstvenih in samoregulativnih postopkov ter ukrepov zaradi omogočanja ali pridobivanja koristi zase ali za druge osebe v škodo javnih sredstev ali javnega interesa.

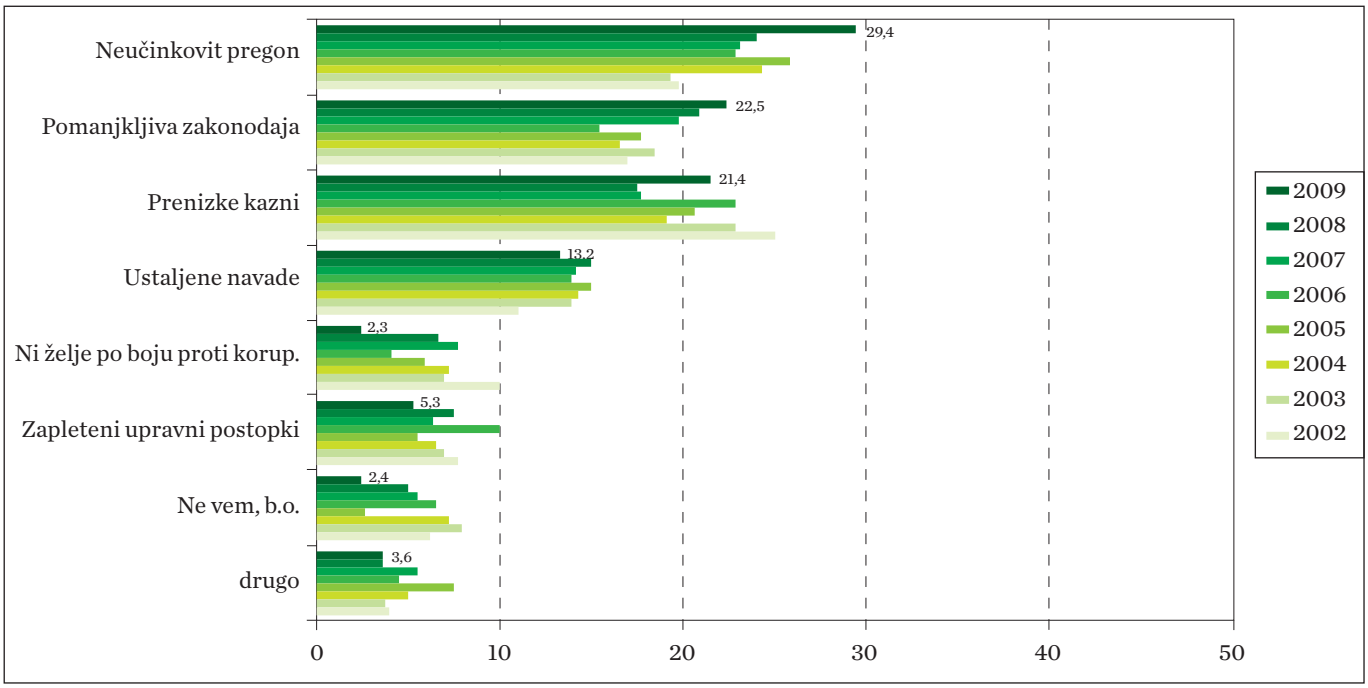
Leta 2013 se KPK definiciji sistemske korupcije še bolj približa. Gre za oceno stanja korupcije v Sloveniji leta 2013. Izpostavi kriminalni prevzem države oziroma ujetje kot prilagojeno zakonodajo, ujetje javnih naročil, denarnega toka ter ključnih sektorjev gospodarstva; koruptivno dejavnost kot model organiziranega kriminala, ki je vzpostavljen od zgoraj navzdol, ter relativno trajnost tovrstnega delovanja. Lahko rečemo, da je za sistemsko korupcijo značilna močnejša navezava na procese znotraj države oziroma vladnih institucij.(KPK, 2013)

Najbolj pogosta opredelitev sistemske korupcije je zloraba javne funkcije za pridobitev osebnih koristi, ki vključuje tako malo kot veliko korupcijo. Mala korupcija zajema delovanje javnih uslužbencev na "ulični" ravni – od uradnikov za okencem v lokalnih upravnih organizacijah, pa do medicinskih sester in prometnih policistov. Velika korupcija vključuje odločitve elit o avtoritativni alokaciji družbenih virov. Posledično lahko odločitve elit služijo skupnemu dobremu le ob doslednem ločevanju "kovčkov" kralja od "kovčkov" države. Natančneje, ključni problem "velike" korupcije je (ne) razlikovanje med javnim in zasebnim, saj je zabrisovanje teh meja pravzaprav pot v korupcijo. Poglavitno spodbudo za sistemsko korupcijo predstavlja (neo)korporativna tradicija vključno z ohranitvijo neposredne vpletenosti države v produkcijski proces skozi lastniške deleže. Največjo oviro za njo pa predstavljajo odnosi z Evropsko unijo in drugimi mednarodnimi organizacijami ter napori nacionalnih neodvisnih nadzornih institucij (protikorupcijskih organov). (Krašovec, Johannsen, Pedersen Hilmer in Deželan, 2014, str. 207-220).

Najbolj pogosta opredelitev sistemske korupcije je zloraba javne funkcije za pridobitev osebnih koristi, ki vključuje tako malo kot veliko korupcijo.

*avtorica je članica Slovenskega združenja korporativne varnosti
**podjetje je član Slovenskega združenja korporativne varnosti

Na sliki 1 vidimo kakšno mnenje ima reprezentativen vzorec slovenskih državljanov glede najpogostejših vzrokov za korupcijo. Vidimo, da so največji problem zakonodaja in neproduktivni državni organi pregona.




Slika 1: Najpomembnejši vzroki za korupcijo v Sloveniji / Vir: KPK (2009)

V nadaljevanju želimo prikazati še korporativno varnost za katero avtor Čaleta (2011, str. 40–41) podaja naslednjo definicijo: "Korporativna varnost je v najširšem pomenu besede tako dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Zato je ena od osnovnih funkcij za delovanje podjetja in se nujno izvaja v tesnem sodelovanju z vsemi drugimi ključnimi funkcijami v podjetju. Celostno področje korporativne varnosti za ustrezno obvladovanje varnostnih tveganj nujno vključuje področje varnosti, procesa neprekinjenega poslovanja in varnosti pri delu."

Korporativna varnost je vključena v vsakodnevno poslovanje in delovanje podjetij in organov javne uprave (v nadaljevanju organizacij) v obliki zagotavljanja normalnega poteka poslovnih procesov, ustvarjanja varnih delovnih pogojev, odpravljanja morebitnih težav z varnostjo, itd. (Trivan, 2013, str. 61–62). V času gospodarske krize je izredno pomembno, da se del denarnih sredstev nameni za izboljšanje področja korporativne varnosti, ki zagotavlja veliko podporo uspešnosti organizacij. Urejeno področje korporativne varnosti pa je tudi strateškega pomena za varovanje kritične infrastrukture, ki je bistvenega pomena za delovanje družbe in gospodarstva. Organizacije, ki upravljajo s kritično infrastrukturo morajo imeti izdelane ocene tveganja, pripravljene ukrepe za odpravo tveganj in vzpostavljeno neprekinjeno poslovanje. Predvsem pa morajo imeti poskrbljeno za dobro fizično in tehnično varovanje ter dobro informacijsko varnost. Menimo, da je izrednega pomena, da se vodstva in lastniki organizacij zavedajo pomena kritične infrastrukture, tveganj in potrebe, da del finančnih sredstev vložijo v preventivne ukrepe in izobraževanje zaposlenih. Zadnji večji primer, ko smo se vsi državljani Slovenije zavedli pomembnosti kritične infrastrukture je bil žled, saj smo takrat ugotovili kaj nam pomenijo elektrika, voda, cestne ali železniške povezave, informacijska tehnologija, itd. Nekatere organizacije, ki skrbijo za kritično infrastrukturo niso predvidele možnosti takšne razsežnosti katastrofe zato npr. elektro podjetja niso imela zadostnega števila agregatov, Luka Koper je imela težave z neprekinjenim poslovanjem zaradi onemogočenega železniškega prometa po določenih trasah, itd.

"Korporativna varnost je v najširšem pomenu besede tako dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Zato je ena od osnovnih funkcij za delovanje podjetja in se nujno izvaja v tesnem sodelovanju z vsemi drugimi ključnimi funkcijami v podjetju.

Če povežemo korporativno varnost s sistemskimi korupcijskimi dejanji lahko vidimo naslednje vplive:

- Korupcijska dejanja, ki povzročajo neenakost državljanov in organizacij pred zakonom in pri upravnih postopkih v javni upravi, vplivajo na njihov občutek varnosti in jim, če želijo kaj doseči, povzročajo dodatne stroške. Neenakost pred zakonom privede tudi do nezadovoljstva zaposlenih in vodstev, ki posredno vplivajo na varnost organizacije s svojo nepazljivostjo ali pa se celo sami pričnejo posluževati korupcijskih ravnanj (npr. zloraba poslovnih informacij za lastno korist, podkupovanje, itd.).

- Nestransparentnost financiranja političnih strank posredno vpliva na področje korporativne varnosti, saj imajo tiste organizacije, ki so finančno na skrivaj podprle vladajoče politične stranke privilegije in lahko vplivajo na zakonodajo in postopke v svojo korist in tudi na drugi strani v škodo drugim organizacijam, kar lahko celo vpliva na njihovo varnost in preživetje.
- Vpliv posameznih lobijev in interesnih skupin lahko privede do sprejetja takšne zakonodaje, ki bi bila veliko organizacijam v škodo in bi vplivala na njihovo varnost. Kot primer lahko damo zakon o javnih naročilih, ki je tako zapisan, da nekaterim omogoča izrabo ''lukenj''. Po drugi strani pa zakon določa naročnikom objavo vseh razpisnih pogojev zaradi transparentnosti, kar lahko na področju naročanja varnostnih storitev kot so npr. tehnično in fizično varovanje zlonamernim osebam razkrije varnostno organiziranost organizacije-naročnika, ki tako postane ranljiv za zunanje vdore oz. škodljiva dejanja.
- Neučinkovit pregon in prenizke kazni za kriminalna in koruptivna dejanja vplivajo na samo varnost organizacije saj, če ni sankcij škodna dejanja povečajo.
- Naročanje nekvalitetno izvedenih storitev in gradenj je nato potencialna nevarnost v varnostnem in finančnem vidiku za organizacijo, ki je naročnik storitev. (npr. Onkološki inštitut – sporna in zdravju nevarna vodovodna napeljava, ki je naročniku-organizaciji prinesel dodatne stroške, zaposleni so bili v nevarnosti na delovnem mestu, nevarnost je bila tudi za paciente, itd.)
- Zaposlitev nestrokovnega ali premalo strokovnega kadra po zvezah in poznanstvih na ključnih področjih ali področju korporativne varnosti v posamezni organizaciji poveča ranljivost organizacije.

Po vsem navedenem lahko zaključimo, da je sistemska korupcija močno zakoreninjena v slovenski politični kulturi, družbi in upravnih razmerjih. Stari vzorci družbenega delovanja iz Jugoslavije se niso spremenili z neodvisnostjo Slovenije ter njenim prehodom v demokracijo in tržno gospodarstvo. Bistveni problem v Sloveniji je, da obstaja veliko sumov za sistemsko korupcijo in skoraj nič obtožnic. Nezaupanje državljanov je veliko, saj si glede na sistem skoraj ''čuden'', če ne uporabljaš vez in poznanstev ter celo morebiti manjše korupcije pri vsakodnevnem urejanju raznih upravnih in podobnih zadev (npr. preskok čakalne vrste pri zdravnikih specialistih, itd.). O velikih sistemskih korupcijah se skoraj ne govori in tudi ne raziskuje, saj vse bolj temelji na izmenjevanju uslug. Višja kot je stopnja korupcije višje je tveganje na področju korporativne varnosti. Za nadaljnje raziskovanje se nam postavlja naslednje vprašanje: Kje, pri vsem navedenem, najdemo osebno integriteto in pripadnost skupnim vrednotam?

## Viri in literatura


- Krašovec, A., K., Johannsen, L., J., Pedersen Hilmer, K. in Deželan, T. (2014). Nevarnost sistemske korupcije v Sloveniji: spodbude in ovire. *Revija za kriminalistiko in kriminologijo, 65*(3), 207–220.
- Bursač, S. (2006). Razvoj protikorupcijskega boja v Sloveniji. Diplomsko delo, str. 11.
- Caiden, G. E. in Caiden, N. J. (1977). Administrative corruption. Public Administration Review, 37 (3), 301–309.
- Čaleta, D. (2011). Varnost mojega podjetja. *Podjetnik, 11*(10), 40–41.
- Ministrstvo za obrambo RS (b.l.). Pridobljeno na http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/
- MMC RTV SLO/STA (2014). *Raziskava društva Integriteta potrdila obstoj sistemske korupcije v Sloveniji.* Pridobljeno na http://www.rtvslo.si/slovenija/raziskava-drustva-integriteta-potrdila-obstoj-sistemske-korupcije-v-sloveniji/277788
- Komisija za preprečevanje korupcije [KPK]. (b.l.). Pridobljeno na https://www.kpk-rs.si/sl/korupcija-integriteta-in-etika
- Komisija za preprečevanje korupcije [KPK]. (2013). *Ocena stanja*. Pridobljeno na https://www.kpk rs.si/upload/t_datoteke/Ocena_stanja_korupcije_v_RS.pdf
- Komisija za preprečevanje korupcije [KPK]. (2011*). Ocena stanja korupcije v Republiki Sloveniji: redno letno poročilo*. Ljubljana: Komisija za preprečevanje korupcije.
- Komisija za preprečevanje korupcije [KPK]. (2009). *Stališča o korupciji 2009.* Ljubljana: Univerza v Ljubljani, Center za raziskovanje javnega mnenja in množičnih komunikacij [izdelava].
- Trivan, D. (2013). Corporate security in the Southeast European countries under conditions of global economic crisis. V D.Čaleta in M. Vršec (ed.), *Management of Corporate Security – New Approaches and Future Challenges* (str. 51–62). Ljubljana: Institute for Corporative Security Studies. ■




Avtorica: Nina Jeznik / iSON



# INFORMACIJSKA VARNOST V ENERGETIKI

**Infrastruktura v energetiki spada med kritično infrastrukturo Slovenije. Sistemski operaterji omrežij za prenos, distributerji in proizvajalci električne energije so dobro pripravljeni na naravne nesreče in možne kibernetske napade.**

Slovenski elektroenergetski sistem postaja in je vedno bolj odvisen od informacijske - komunikacijske tehnologije. Podjetja imajo uvedene sisteme daljinskega odčitavanja merilnih mest ter elektrarne vodijo brez posadke. Uporaba informacijske - komunikacijske tehnologije in pametnih omrežij v prenosnem in distribucijskem delu elektroenergetskega sistema vodi v tveganja za oškodovanje kritične infrastrukture. Zaradi podnebnih sprememb prihaja do vedno več naravnih katastrof, kot so žled in poplave. Storilci, ki načrtujejo kibernetske napade lahko samo še izkoristijo nepredvidljivo okolje naravnih nesreč in napredne tehnologije. Ozaveščenost na področju informacijske varnosti je v današnjem svetu neprecenljiva in lahko privarčuje ogromno denarja.

Brez elektrike si ljudje ne znamo več predstavljati našega obstoja. Vsa proizvodno usmerjena podjetja, ki delajo neprekinjeno dan in noč, potrebujejo za delovanje neprekinjeno električno energijo. Neprekinjena proizvodnja, distribucija in prodaja električne energije je pomembna za delovanje države in državnih podsistemov v kriznih razmerah, zakonodaja iz civilne obrambe tako nalaga osnovne obveznosti distributerjem električne energije. Sistemski operater prenosnega elektroenergetskega omrežja (v nadaljevanju ELES) mora po obrambnem načrtu zagotoviti delovanje storitev tudi v kriznih razmerah. Prav zaradi pomembne funkcije delovanja področja energetike za državo je zavedanje na področju informacijske varnosti še toliko večje.




Osnovne karakteristike informacijske varnosti so zaupnost, celovitost ter razpoložljivost. Pri vsem tem napredku nove tehnologije pa se včasih pozabi identificirati ranljivosti, ki lahko nastanejo z modernizacijo opreme.



Zimski izpad električne energije zaradi žledu nas je opomnil, kako ranljiv je elektroenergetski sistem in kako zelo smo od njega odvisni.

Izdelan načrt zaščite in reševanja v ELE-Su omogoča, da se čimprej vzpostavi normalno delovanje v primeru naravnih ali drugih nesreč kot so terorizem, nasilje, motnje dobave, opustitev dejavnosti, naravni požar, nevihtna neurja, obilne snežne padavine, potres, viharni vetrovi, visoke vode, plazovi, usadi in podori ter žled (Cerk & Loborec, 2013).

Zimski izpad električne energije zaradi žledu nas je opomnil, kako ranljiv je elektroenergetski sistem in kako zelo smo od njega odvisni. Del Slovenije je bil brez električne energije skoraj dva tedna. Mnogi so bili brez gretja in komunikacijsko odrezani. Gospodarska škoda na kritični elektroenergetski in prometni infrastrukturi presega škodo za sto dvajset milijonov evrov. Popolna obnova bo trajala več let. Zaradi izpada električne energije je milijonsko škodo utrpelo tudi gospodarstvo na prizadetih območjih (ProMonitor, 2015).

V Podravju so novembra leta 2012 utrpeli ogromno škodo zaradi poplav na celotnem toku reke Drave na ozemlju Slovenije, od Dravograda do državne meje s Hrvaško. Visokovodni val je poplavil stanovanjske zaselke, kmetijska zemljišča ter cestno in vodno infrastrukturo ter poplavil HE Formin (Klaneček, 2012).

Pri prepoznavanju informacijskih tveganj v družbah se osredotočamo na sredstva, ki morajo delovati, da lahko proces oziroma družba sploh deluje. Osnovne karakteristike informacijske varnosti so zaupnost, celovitost ter razpoložljivost. Pri vsem tem napredku nove tehnologije pa se včasih pozabi identificirati ranljivosti, ki lahko nastanejo z modernizacijo opreme.

Kljub vsej tehnologiji tehnološke sisteme še vedno upravlja človek. Za primer človeške napake navajam primer, ki se je zgodil avgusta leta 2009 v največji Ruski hidroelektrarni – Sayano Shushenskaya na reki Yenisei. Ob 8:13 uri po lokalnem času je 17. avgusta 2009 hidroelektrarna utrpela katastrofalno »povečanje pritiska« v turbini, znano kot kladivo vode. Nenadno povečanje pritiska vode je povzročilo izmet turbine 2, z vso opremo, skupna teža je bila nekaj več kot 900 ton. Zasilna vrata se v tistem trenutku niso zaprla, izstopna vrata pa so zaprli ročno potapljači. Na voljo ni bilo električne energije, niti zasilne električne energije ni bilo. Ker zasilna razsvetljava ni delovala so želeli uporabljali žepne svetilke, vendar tudi teh ni bilo na voljo. Vodja za krizno upravljanje je zapustil elektrarno, novice v zvezi z incidentom pa so poročali šele 3 ure po incidentu tako, da zaposleni sploh niso imeli jasnih navodil za usmerjanje ljudi na varna mesta, saj niso imeli postopkov za krizno upravljanje. Nesreča je prizadela vseh 7 turbin, nekatere so bile v celoti poškodovane, nekatere poplavljene z napakami na električnem napajanju, umrlo pa je 75 ljudi, škode je bilo za 440 milijonov evrov. Po nesreči so ugotovili , da bi lahko bila turbina 2 zaustavljena že v aprilu ali maju pred nesrečo zaradi vibracij. Vibracije bi morale biti največ 38% od omejitve, po vzdrževanju 2009 so bile 93% čez omejitve. Turbina 2 pa je bila na koncu svoje življenjske dobe (29 let in 10 mesecev), celotna življenjska doba je bila 30 let (Palsit d.o.o., 2014).

Pomanjkljivosti v varnostnem sistemu lahko izkoristijo sumljivi storilci zato morajo biti zaposleni ozaveščeni na področju neprekinjenega poslovanja in

informacijske varnosti, da se lahko čimprej vzpostavi normalno delovanje, se prepreči tatvine, nepooblaščene dostope ali odnašanje opreme. Kljub poostrenim varnostnih mehanizmom, pa se nepredvidljivi storilci vedno bolj osredotočajo na uporabnika, ki bi ga prelisičili preko elektronske pošte s pripeto sumljivo priponko ali pa mu ukradli geslo preko spletnega bančništva ali socialnega omrežja, zato je v zadnjem letu največji poudarek na ozaveščenosti zaposlenih.

114 kontrolnih točk standarda ISO 27001:2013, ki podaja dobre prakse in smernice iz sistema upravljanja varovanja informacij, so v podjetju ELES in DEM dodobra preučili in jih implementirali v svoje poslovanje ter tako zmanjšali tveganja. Vzpostavili so skrbnika sistema upravljanja varovanja informacij ter člane tima za varovanje informacij, ki se odzivajo in ukrepajo v primeru incidentov. Zapisani so upravljalski postopki za reševanje, zaposleni pa so ozaveščeni v primeru kršitev informacijske varnosti ter z načinom dela, ki je sprejemljiv za odgovorno ravnanje z informacijami. Sredstva organizacije so zaščitena pred krajo, saj imajo v obeh družbah zaposlene varnostnike, ki so odgovorni, da vzpostavijo ločnico med obiskovalci in zaposlenimi. Kartični dostopi v prostore z višjim tveganjem zagotavljajo, da lahko samo pooblaščene osebe prihajajo v stik z informacijami ali sredstvi, katerim odobri dostop nadrejena oseba. Definiranje odgovornosti za posamezno sredstvo je vzpostavilo zavedanje, da je vsak skrbnik sredstva odgovoren za njegovo ravnanje, hrambo, pošiljanje in razpečevanje. Ker sta podjetji vzpostavili klasifikacijo informacij, zaposleni ločujejo med javnimi, internimi, zaupnimi ali tajnimi informacijami. Za posamezne klasifikacije so zapisana pravila, tajne informacije ali poslovne skrivnosti v elektronski obliki pa se morajo kriptirati v primeru, da se pošiljajo v elektronski obliki. V informatiki se vsakoletno izvajajo penetracijski testi, s katerimi se ugotavlja odstopanje od željenega stanja ali pomanjkljivosti v primeru varnosti informacij. Tudi dobavitelji in naročniki so zavezani k molčečnosti ter k prijavi incidentov v primeru sumov na varnostni incident. Ustrezno prepoznavanje incidentov, pa vodi v hitro in odločno reševanje incidentov, brez da bi prišlo do večje škode. Kljub dobrim praksam standarda, družbi upoštevata tudi zakonodajo na tem področju. Vsakoletno presojanje sistema pa sledi k njihovem izboljševanju.

Stalno izobraževanje in ozaveščanje zaposlenih v energetiki, pripomore k zagotavljanju visoke stopnje varnosti in zanesljivosti sistemov informacijske infrastrukture, centra vodenja, številčnih sistemov ter drugih sistemov povezanih s proizvodnjo, vodenjem električne energije ter distribucijo električne energije.

Ozaveščenost zaposlenih na področju informacijske varnosti je bistveno, saj je človek najšibkejši člen v varnostni verigi in ga je potrebno izobraževati. S svojim znanjem in ozaveščenostjo o nevarnostih, lahko prav zaposleni preprečijo namerno vdiranje v informacijske sisteme, saj v nekaterih primerih ne delujejo klasična orodja varovanja (Jeznik, 2011).

Suhoparno napisane varnostne politike na belem papirju z enakimi črnimi črkami ne pritegnejo nobene pozornosti zaposlenih, po katerih bi se morali ravnati za izboljšanje informacijske varnosti. V Dravskih elektrarnah Maribor so izdali knjižico za zaposlene Informacijska varnost. Od ideje natisa stripa do izdaje knjižice so izpilili varnostne politike ter jih zapisali na prijazen način s slikicami, ki prikazujejo ravnanje z informacijami na hudomušen način. Priročnik na enostaven način prikazuje logično in pričakovano obnašanje vsakega zaposlenega v določeni situaciji, ki se nam kdaj dozdeva, da je samoumevno, pa temu ni tako. Knjižica je zanimiva in prijazna tako za branje tistim, ki imajo veliko računalniškega znanja in tudi tistim, ki takšnega znanja nimajo. Zaposleni so spoznali skozi knjižico kakšno je dobro geslo, kaj je politika čiste mize in praznega zaslona, kaj pomeni klasifikacija informacij, kam in kako morajo javljati varnostne incidente. Povečali so celovitost, razpoložljivost ter zaupnost informacij ter zaupanje zaposlenih v napredno tehnologijo in v splošno varnost v podjetju.

Tako v Dravskih elektrarnah Maribor, kot v ELESu so skrbniki sistema upra-





vljanja varovanja informacij izvedli podrobno izobraževanje za vse zaposlene. Organizacijski in logistični problem izobraževanja za vse zaposlene so premagali z idejo, da so izvedli e-izobraževanje. Vsebine s področja informacijske varnosti so naložili na spletno e-učilnico, kjer so vsi zaposleni morali opraviti e-izobraževanje ter se testirati. Natisnjeno potrdilo o izobraževanju sedaj najdemo na stenah zaposlenih, ki prenašajo sporočila med seboj, da gesel ne rabijo hraniti pod tipkovnicami, če si le znajo ustvariti kvalitetno in dobro geslo za dostope, kar pa so se naučili skozi e-izobraževanje. Vsi zaposleni sedaj razumejo celovit koncept informacijske varnosti ter lažje sodelujejo pri notranjih in zunanjih presojah, predvsem pa se lažje odločajo, ko morajo hitro reagirati v primeru varnostnih incidentov.

Po anketi je bilo ugotovljeno, da je najboljša kombinacija klasično in elektronsko izobraževanje. Pozitiven odnos zaposlenih do e-učenja in pripravljenost na e-vsebine in e-testiranja tudi na drugih področjih je pokazal, da lahko e-izobraževanje prinese podjetju prihranek denarja, zaposlenim pa prihranek časa, enostavnost, dostop kjerkoli in kadarkoli ter lastno prilagajanje tempa učenja.

Povezovanje družb in skupno učenje iz incidentov bi lahko pripeljalo do zmanjšanja incidentov na področju informacijske varnosti. Pretok informacij in znanj med družbami bi pripomoglo k trdnejšim temeljem na področju varnosti.

Podjetja, ki se nevarnosti kibernetskih napadov v elektroenergetskem sistemu zavedajo, se najpogosteje zatekajo k nakupu strojne in programske opreme ali najemu svetovalcev. A ranljivosti v sistemih ostajajo. Prav tako ne moremo odstraniti vseh groženj kibernetskih napadov. Podjetja lahko iščejo nove načine za preprečevanje napadov in odzivanje na napade. Pomembna sta sodelovanje in izmenjava informacij med podjetji in s pristojnimi državnimi organi (ProMonitor, 2015).

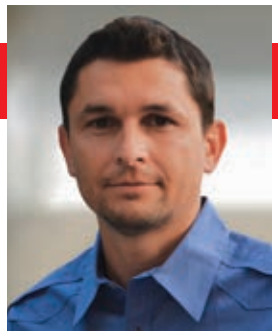



Slika 1: Arhiv Dravskih elektrarn Maribor

## Viri:


- Cerk, J. & Loborec, I., 2013. *Načrt zaščite in reševanje.* Interni dokument ured. Ljubljana: ELES.
- Fekonja, S., 2011. *SUVI v DEM,* Maribor: DEM.
- Jeznik, N., 2011. Implementacija sistema upravljanja varovanj informacij v DEM, Ekonomska fakulteta Maribor: Diplomsko delo.
- Klaneček, M., 2012. *Poplave 5. novembra 2012 v porečju Drave.* [Elektronski] Available at: http://www.sos112.si/slo/tdocs/ujma/2013/052.pdf [Poskus dostopa 2 17 2015].
- Palsit d.o.o., 2014. *Neprekinjeno poslovanje.* Nova Gorica, s.n.
- ProMonitor, 2015. *Competitive Analysis & Foresight.* [Elektronski] Available at: http://blog.caf.si/2014/08/informacijska-varnost-kriticne-infrastrukture.html [Poskus dostopa 17 2 2015]. ■

Avtor: Aljoša Kandžič / Inštitut za korporativne varnostne študije*



# RADICALISATION AWARENESS NETWORK – RAN

**Boj proti terorizmu in nasilnemu ekstremizmu ni le vprašanje povezano z izvajanjem varnostnih ukrepov temveč se je potrebno problema lotiti pri koreninah njegovega pojavljanja.**

Najboljša preventiva je preprečiti ljudem, da bi se vpletli v nasilne ekstremistične ali teroristične aktivnosti, oziroma jih prepričati, da se ne zatekajo k takim idejam in metodam. Ta zahtevna naloga ne more biti prepuščena majhnemu številu organov in akterjev, ki se ukvarjajo s to tematiko. Narava tega pojava zahteva, da se v aktivnosti preprečevanja vplete široko paleto partnerjev oziroma deležnikov. To je zelo pomembno za boljše razumevanje vedenja o problemu radikalizacije in široko izvajanje ukrepov za njeno preprečevanje.

Za reševanje pojava radikalizacije so v najboljšem položaju tako imenovani »first-liners« - ljudje, ki so v neposrednem stiku s ciljno usmerjenimi posamezniki ali ranljivimi skupinami prebivalstva. Praktiki, raziskovalci in nevladne organizacije imajo veliko znanja o tem, kako ravnati s tem vprašanjem v problematičnih okoljih. V ta namen je bila s strani Evropske komisije ustanovljena mreža »The Radicalisation Awareness Network (RAN)«, ki predstavlja vseevropsko krovno združenje (dežnik). Njen namen je povezovanje strokovnjakov, praktikov in lokalnih akterjev pri preprečevanju radikalizacije, terorizma in nasilnega ekstremizma. Znotraj RAN-a delujejo različne delovne skupine, kjer si lahko udeleženci oziroma člani izmenjujejo ideje, znanje, izkušnje in dobre prakse s področij pomembnih za boj proti radikalizaciji in nasilnemu ekstremizmu. RAN povezuje predstavnike različnih skupnosti, strokovnjake na terenu, socialne delavce, učitelje, nevladne organizacije, organizacije civilne družbe, skupine žrtev, lokalne organe, organe pregona, predstavnike vladnih organizacij in svetovalnih podjetij.

RAN je sestavljena iz osmih tematskih delovnih skupin, ki jih podpira in usmerja odbor (RAN Sekretariat): (1) RAN POL - delovna skupina policistov in uradnikov kazenskega pregona; (2) RAN DERAD - delovna skupina za odpravo radikalizacije in ukrepov izstopanja iz teh skupin; (3) RAN VVT - delovna skupina za glasove žrtev terorizma; (4) RAN @ - delovna skupina na področju interneta in socialnih medijev; (5) RAN PREVENT - delovna skupina za zgodnje ukrepanje in preprečevanje radikalizacije; (6) RAN INT/EXT delovne skupine notranjih/zunanjih dejavnikov, kot so tuji borci in ogrožene skupnosti; (7) RAN P&P - delovna skupina, ki se ukvarja z zapori in pogojnem izpustu; (8) RAN HEALTH - delovna skupina zdravstvenih delavcev.

RAN je razvil zbirko pristopov, spoznanj in praks ter tesnejše delo s partnerskimi državami za preprečevanje in boj proti radikalizaciji znotraj in zunaj EU. V ta namen je v mesecu februarju na povabilo slovenske vlade izvedel usposabljanje »Train-the-trainer Awareness and Actions« v Ljubljani. Namenjena je bila izobraževanju strokovnjakov, ki bodo v prihodnje prenesli znanje, izkušnje, dobre prakse in zavedanje na lokalne deležnike na področju radikalizacije in nasilnega ekstremizma v Sloveniji. Med udeleženci je bil tudi g. Aljoša Kandžič, kot predstavnik Instituta za korporativne varnostne študije (ICS), ki je zastopal nevladne organizacije v tem projektu.

ICS-Ljubljana je v okviru omenjenega projekta dejaven skozi različne aktivnosti. Ena od takih je tudi vzpostavitev mreže strokovnjakov v okviru nastajajočega EU RAN Center of Excellence. Pridobitev ustrezne licence za usposabljanje je drugi korak, ki pomeni možnost, da navedeni projekt razširimo skozi organizacije nevladnega sektorja v Republiki Sloveniji. V tem okviru bo sodelovanje razširjeno na nevladne organizacije, ki bodo s svojo dejavnostjo pripomogle k ustreznim ukrepom za preprečevanje radikalizacije posameznikov na področjih kjer delujejo. Posebej je v tem okviru potrebno izpostaviti pomen javno-zasebnega partnerstva in sodelovanja, ki je nujen za uspešno izvajanje programa. ■

*avtor je član Slovenskega združenja korporativne varnosti

geacollege
Fakulteta za podjetništvo

Prva generacija študentov že aktivno nabira novo znanje.



# MANAGEMENT KORPORATIVNE VARNOSTI

Magistrski program

# Magistrski program **Management korporativne varnosti**

**Magistrski program Management korporativne varnosti je namenjen izobraževanju ter usposabljanju podjetnikov in managerjev za obvladovanje poslovno varnostnih mehanizmov in upravljanje varnostnih tveganj v gospodarstvu, industriji, državnih institucijah in civilni družbi.**

**Z magistrskim študijem Management korporativne varnosti omogočamo študentom poglobljeno podiplomsko izobraževanje, v katerem pridobijo teoretična in aplikativna znanja s področja poslovno varnostnega managementa, s kompetencami za upravljanje korporativne varnosti. Poudarek je na: geostrateških in političnih vidikih varnostnih tveganj, varnostnih standardih v poslovnih procesih, prepoznavanju in analiziranju ranljivosti, ogroženosti in varnostnih tveganj, upravljanju varnostnih tveganj, informacijski in komunikacijski varnosti, načrtovanju in razvoju korporativne varnosti, procesih nadzora, zavarovalništvu, financah, gospodarskem poizvedovanju, ekoloških vidikih in varnemu delovnemu ter poslovnemu okolju.**

### RAZPISANE SMERI

- Korporativni varnostni manager
- Korporativni varnostni manager – podjetnik

### TRAJANJE ŠTUDIJA IN STROKOVNI NASLOV

- 2 leti
- magister/magistrica managementa korporativne varnosti

## Kaj omogoča študij Managementa korporativne varnosti



Pridobiti ustrezna multidisciplinarna znanja, ki temeljijo na znanstveno raziskovalnem delu in praktičnih izkušnjah ter dobrih praksah v nacionalnem in mednarodnem korporativnem okolju. Študentje bodo pridobili znanja za upravljanje z varnostnimi tveganji in vodenje organizacijskih struktur na področju korporativne varnosti v javnem in gospodarskem okolju ter mednarodnih korporacijah. Poseben poudarek je na varnostnih mehanizmih v organizacijah, ki upravljajo s kritično infrastrukturo (energetika, telekomunikacije, informatika, transport, finančne institucije, prehrambena industrija idr.). Bodoči magistri bodo v času študija pridobili vsa potrebna znanja in kompetence, ki so potrebne za delovanje v podjetniškem okolju tudi kot samostojni podjetniki, ki bodo drugim organizacijam nudili (tržili) tovrstne strokovne storitve s področja načrtovanja, izvajanja in upravljanja korporativne varnosti.

### PARTNERJI PROGRAMA

- ICS – Inštitut za korporativne varnostne študije
- Slovensko združenje korporativne varnosti (SZKV)
- Mednarodna asociacija SE European Corporate Security Association (SECSA)

ICS
Inštitut za korporativne varnostne študije

SECSA
SE Europe Corporate Security Association

»Varnost je pojem, s katerim se srečamo že v naših rosnih letih in ima velik pomen za uspešno rast, razvoj in delovanje vsakega posameznika v vseh obdobjih njegovega življenja in ustvarjanja. Korporativna varnost pa je, podobno kot varnost pri posameznikih, za razvoj in uspešno delovanje pomembna predvsem v organizacijah. Kakršnihkoli – v velikih ali malih, pri globalnih mednarodnih korporacijah ali zgolj lokalnem samostojnem podjetniku, in sicer ne glede na to, na katerem področju ustvarja in razvija svoje ideje oziroma poslovne rešitve. Pri tem je pomembno, da se ne omejimo zgolj na osnovno varnost ljudi, premoženja ali informacijsko varnost, saj je izrednega pomena, da znamo pravočasno in pravilno prepoznati vsa možna dejanska in potencialna tveganja ter nevarnosti, ki lahko nastopijo v kateremkoli procesu delovanja naše organizacije. V današnjem hitro razvijajočem, naprednem in hkrati zelo konkurenčnem okolju so pravilna strateška usmeritev korporativne varnosti, njena učinkovita preventivna dejavnost ter strokovno načrtovano ukrepanje in delovanje ključnega pomena za uspešnost organizacije. Našteto lahko dosežemo le prek ustreznega strokovnega izobraževanja, ki bo pripomoglo k dvigu omenjene stroke in zadovoljilo vse bolj naraščajoče potrebe po znanjih s tega področja. Slednja so namreč izrazitega pomena za učinkovitejše obvladovanje varnostnih tveganj v organizacijskih okoljih.«



**mag. Boris Novak, generalni direktor Pošte Slovenije**

# Vpisni pogoji

## V 1. LETNIK SE LAHKO VPIŠE:

- kdor je končal študijski program prve stopnje z ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...) z najmanj 180 kreditnimi točkam po ECTS,
- kdor je končal študijski program za pridobitev visoke strokovne izobrazbe z ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), sprejet od 1. 1. 1994 do 11. 6. 2004,
- kdor je končal študijski program prve stopnje ali za pridobitev visoke izobrazbe, sprejetim od 1. 1. 1994 do 11. 6. 2004 drugih strokovnih področij, vendar pa morajo pred vpisom opraviti diferencialne izpite do 24 kreditnih točk, ki jih glede na strokovno področje predhodnega študija določi pristojna komisija GEA College - Fakultete za podjetništvo na podlagi individualne vloge kandidata.

## PO MERILIH ZA PREHODE SE V 2. LETNIK LAHKO VPIŠEJO:

- diplomanti študijskega programa za pridobitev univerzitetne izobrazbe, sprejetega pred 11. 6. 2004, iz sorodnih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki se jim praviloma priznajo študijske obveznosti v obsegu do 40 KT,
- diplomanti študijskega programa za pridobitev univerzitetne izobrazbe, sprejetega pred 11. 6. 2004, drugih strokovnih področij, ki se jim praviloma priznajo študijske obveznosti v obsegu do 30 KT,
- diplomanti specialističnega študija podjetništva GEA College - Fakultete za podjetništvo, ki se jim prizna 60 KT,
- diplomanti specialističnega študija sorodnih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki se jim praviloma priznajo študijske obveznosti v obsegu do 40 KT,
- diplomanti specialističnega študija drugih strokovnih področij, ki se jim praviloma priznajo študijske obveznosti v obsegu do 30 KT,
- študent drugostopenjskega študijskega programa ustreznih strokovnih področij (družbene vede, poslovne in upravne vede, varstvoslovje in obramboslovje ...), ki izpolnjuje pogoje za vpis v višji letnik (40 KT ali več).

# Predmetnik

| Obvezni skupni predmeti |
|---|
| **PREDMET** |
| Management korporativne varnosti – obvezni predmet |
| Geostrateški in politični vidiki varnostnih tveganj v mednarodnem poslovnem okolju – obvezni predmet |
| Pravni vidiki korporativne varnosti – obvezni predmet |
| Ekonomika obvladovanja tveganj v poslovnem okolju |

| Obvezni usmeritveni predmeti |
|---|
| **SMER - Korporativni varnostni manager** |
| Varnostni standardi v poslovnih procesih |
| Upravljanje varnostnih tveganj |
| Načrtovanje in razvoj korporativne varnosti |

| Obvezni usmeritveni predmeti |
|---|
| **SMER - Korporativni varnostni manager - podjetnik** |
| Varnostni standardi v poslovnih procesih |
| Upravljanje varnostnih tveganj |
| Načrtovanje in razvoj korporativne varnosti |

| Izbirni predmeti (študent izbere dva) |
|---|
| **PREDMET** |
| 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 v 1. in 2. letniku |
|---|

| Magistrsko delo |
|---|

»Če smo nekoč čas merili v letih, mesecih in dnevih, ga danes merimo v urah, minutah in sekundah, saj se svet okoli nas spreminja s tako naglico, da mu enostavno ne moremo več slediti! Seveda so te spremembe tako pozitivne kakor negativne narave, ki se lahko pojavijo tudi v obliki varnostnih tveganj in izzivov. Samo holistično izobražen korporativno varnostni manager, ki bo svoje teoretično pridobljeno znanje lahko oplemenitil z ustrezno prakso pod skrbnim mentorstvom izkušenih korporativnih varnostnih managerjev, se bo lahko uspešno kosal s tovrstnimi izzivi! Magistrski študij "Management korporativne varnosti" predstavlja pomemben mejnik v izobraževanju in usposabljanju korporativno varnostnih managerjev, saj zajema tako teorijo kakor tudi prakso!«

**Andrej Podvršič, EMEA Director of Security**
**DuPont de Nemours International Sárl**



## CILJI ŠTUDIJA

Ključni cilj programa je izobraziti in usposobiti strokovnjake, ki imajo poslovna, pravna, tehnična in druga znanja ter dobro poznavanje in razumevanje globalnega ter nacionalnega poslovnega, informacijsko-komunikacijskega in varnostnega okolja, za celovito upravljanje korporativne varnosti v različnih organizacijah.

V programu bodo diplomanti pridobili naslednje kompetence:

- Znanje s področja globalnih družbenih, ekonomskih, političnih in varnostnih vidikov.
- Razumevanje, oblikovanje in uvajanje varnostnih politik in varnostnih strategij v kontekstu družbenega in gospodarskega razvoja ter poslovne uspešnosti.
- Sposobnost proučevanja varnostnih pojavov, izdelava varnostnih elaboratov ter analiziranje in ocenjevanje ranljivosti, ogroženosti in tveganj.
- Zmožnost uvajanje celovitih (integralnih) varnostnih sistemov, ki obsegajo varovanje ljudi in premoženja, informacij in poslovnih skrivnosti, poslovno poizvedovanje, okoljske vidike, obvladovanje izrednih dogodkov, neprekinjeno delovanje vitalnih poslovnih funkcij in procesov v izrednih okoliščinah.
- Prepoznavanje koristnosti uvajanja varnostnih standardov v sklopu sistemov vodenja kakovosti proizvodnje, logistike in trženja.
- Poznavanje metodologij za upravljanje procesov korporacijske varnosti v smislu poslovnih funkcij, načrtovanja investicij v varnostne izboljšave, zavarovanja tveganj in razumevanja postopkov (javnega) naročanja storitev korporacijske varnosti.

# Magistrski program **Management korporativne varnosti**



»Ko smo pred časom skupaj s partnerji – Inštitutom za korporativno varnost začeli pripravljati magistrski program Management korporativne varnosti, smo se zavedali, da orjemo ledino. Sestavili smo kakovosten program, ki je unikaten pri nas in tudi v Evropi. Tudi drugod po svetu je zelo malo študijskih programov ali smeri, ki bi bile vsaj podobne, če že niso popolnoma primerljive. Program izobražuje za nov poklic. Verjamemo, da je to eden od poklicev prihodnosti. Lastna varnost vse bolj postaja odgovornost posameznikov in organizacij. V tehnološko vse bolj zapletenem svetu, v katerem vzporedno potekajo tudi nagle spremembe v družbi in okolju, je celostno obvladovanje varnostnih procesov izziv, ki terja za to posebej usposobljene strokovnjake. Z ustreznim predznanjem in delovnimi izkušnjami z različnih področij širšega obvladovanja varnostnih procesov in tveganj bodo študentje magistrskega programa znali nadgrajena znanja predvsem povezovati v zaključene celote. Študentje bodo kasneje prevzeli najodgovornejša mesta v podjetjih, kjer se bodo ukvarjali z integralnimi varnostnimi procesi. V večjih podjetjih bodo ti strokovnjaki našli zaposlitev (managerji), v manjših pa bodo lahko nudili svoje storitve (podjetniki).«

**izr. prof. dr. Jaka Vadnjal, dekan fakultete**



»Podiplomski študij managementa korporativne varnosti je pri nas, pa tudi širše v kontinentalni Evropi, popolnoma nova smer izobraževanja, ki je prilagojena stalno spreminjajočemu se okolju in s tem najnovejšim kočljivim situacijam v podjetjih, institucijah ne glede na njihovo lastništvo. Te situacije so precej bolj tvegane in kompleksne, kot so bile pred leti. Opravka imamo s celo paleto različnih tveganj, katerim smo danes izpostavljeni praktično vsi. Ozrite se okrog sebe in opazujte, kaj se dogaja. Varovanje v svojem klasičnem smislu fizičnega varovanja predstavlja danes v podjetjih in institucijah samo majhen del vsega ščitenja, če uporabim kar ta izraz, ki ga posameznik, podjetje, institucija mora imeti oz. si ga organizirati. Magister managementa korporativne varnosti bo ta oseba, ki bo v podjetjih, institucijah organizirala in vodila službo oz. organizacijsko enoto, ki bo pokrivala to integralno in izjemno pomembno področje ščitenja pred različnimi tveganji v najširšem smislu v teh turbulentnih in nevarnih časih. V sodobneje organiziranih in nekoliko večjih pravnih osebah pa bo ta oseba kar član uprave za to integralno področje.«

**doc. dr. Draško Veselinovič, direktor in predavatelj**



»Živimo v dinamičnem gospodarskem okolju, kjer je varnost postala dobrina, ki ni več samo po sebi umevno dejstvo. Informacijska globalna družba pred nas postavlja veliko priložnosti, odpira pa tudi tveganja, katerih se je potrebno v podjetjih in drugih organizacijskih sredinah zavedati in jih tudi ustrezno obvladovati. V tem okviru posebej izpostavljam organizacije, ki obvladujejo kritično infrastrukturo, katera je nujno potrebna za delovanje širše družbene skupnosti. Ker popolne varnosti ni možno zagotoviti, je znanje korporativno varnostnih managerjev tista dodana in primerjalna vrednost, ki na strateškem nivoju bistveno vpliva na učinkovitost in kakovost obvladovanja tveganj v podjetjih. To so znanja, ki so in bodo v slovenskem in širšem regijskem prostoru v naslednjih letih izredno iskana. S temi znanji in dobrimi praksami ter najnovejšimi spoznanji vas bomo "oborožili", ko boste stopili na trg polno priložnosti za vaše uveljavljanje. Najboljšim študentom pa bo skozi povezave Slovenskega združenja za korporativno varnost in mednarodne asociacije SE European Corporate Security Association (SECSA) tudi omogočena priložnost za pridobivanje izkušenj v neposrednem organizacijskem okolju.«

**doc. dr. Denis Čaleta, predsednik Slovenskega združenja za korporativno varnost**



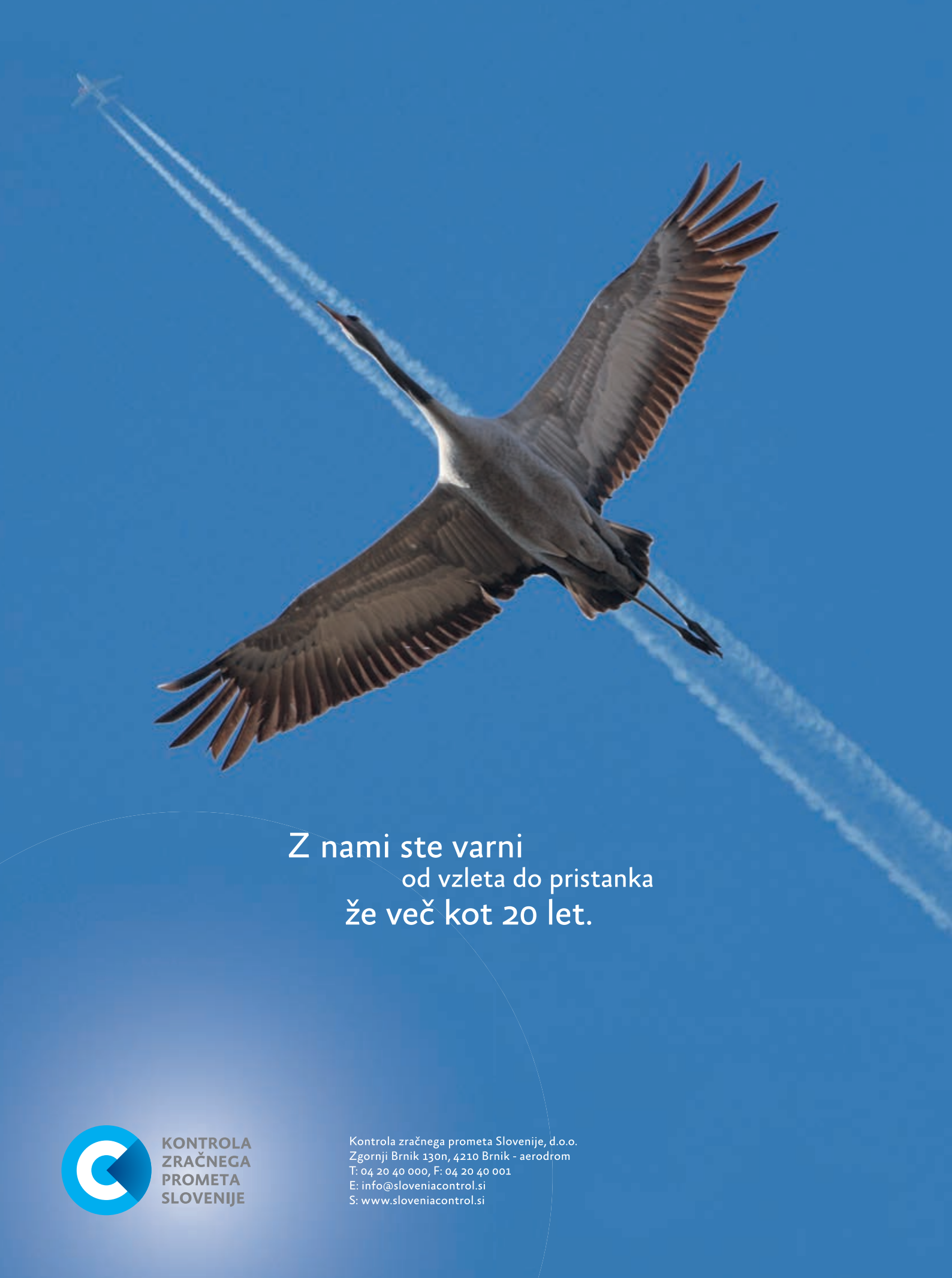
»Krizne razmere, vsesplošna ogroženost, varnostna tveganja ter pomanjkljivi varnostni in nadzorni mehanizmi že kar nekaj časa kličejo po dvigu kakovosti tistega dela managementa v gospodarskih in drugih subjektih, ki upravljajo z varnostjo ljudi, procesov in premoženja. Izhajamo tudi iz premise, da le profesionalni in celovit varnostni sistem odločilno prispeva k preprečevanju škod in izgub, k bogatenju poslovnih izidov ter k dvigu kulture, ugleda in konkurenčnih prednosti. Gre za fenomen sinergije poslovnih in varnostnih procesov ter intelektualnega kapitala, da složno in pregledno upravljajo z določeno družbo. To pomeni, da obstoječi in novi management korporativne varnosti potrebuje nova znanja, ki zagotavljajo učinkovito upravljanje varnosti ter dvig statusa in ugleda posameznih managerjev korporativne varnosti zlasti v konici korporativnega upravljanja. Inovativni magistrski program, ki je pred vami, daje lastnikom, upravljavcem in nadzornikom ter zainteresiranim posameznikom možnost in priložnost, da ustvarijo nekaj več za varnost zaposlenih, poslovnih procesov, kapitala in razvoja.«

**doc. dr. Milan Vršec**

# Kontakt

Dodatne informacije so vam na voljo na naši spletni strani **www.gea-college.si**, veseli pa bomo vašega klica na telefonski številki **01 588 13 00** ali e-pošte na **korpo@gea-college.si**.

GEA College – Fakulteta za podjetništvo, Dunajska 156 (stolpnica WTC), 1000 Ljubljana




KONTROLA ZRAČNEGA PROMETA SLOVENIJE

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