Korporativna varnost

ICS
Institut za korporativne varnostne študije

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

Letnik 2017, december • št. 15

Mednarodna konferenca "Dnevi korporativne varnosti 2018" Ljubljana - Kristalna palača, 14-15. marec 2018

Pošta Slovenije pripravljena na nove izzive prihodnosti

mag. Boris Novak, generalni direktor, Pošta Slovenije

ELES

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.

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

Več kot 2550 km
prenosnega omrežja

Več kot 550
zaposlenih

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

www.eles.si

Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
Evrografis d.o.o.

Datum izida
december 2017

Izvod revije je brezplačen

Naslovnica in slike:
© Dreamstime.com
Arhiv ICS

ISSN 2232-6170

Revija Korporativna varnost postaja redni spremljevalec vseh, ki so željni doseganja aktualnih informcij na področju obvladovanja varnostnih tveganj. Najbolj nas veseli, da so vsebino revije, poleg strokovne javnosti, začeli prepoznavati tudi predstavniki strateškega managementa. Pomembno mesto, v trendu vedno večjega povpraševanja po sami strokovni reviji, pa vsekakor predstavlja tudi kontinuiranost izhajanja in visoka strokovnost vsebin, saj smo tokrat že pri izidu 15. številke.

Tudi tokratno obdobje izzida in priprave nove številke Korporativne varnosti je postreglo s celim nizom izrednih dogodkov, ki so močno razburkali naš vsakdanjik. Strokovnjaki s področja obvladovanja tveganj pa mrzlično iščejo odgovore na pojave novih groženj, ki jih v preteklosti ni bilo možno zaznati v takem obsegu, kot smo jim priča danes. Posebej so izpostavljeni primeri celega niza AMOK situacij, ki vedno bolj postajajo stalnica modernih zahodnih družb. Ob nenehnem pojavljanju terorističnih dejanj, kibernetskih groženj in nezmanjšanem obsegu delovanja organiziranega kriminala, se varnostni izivi, ki smo jim bili priča v navalu migracij na meje Evrope, zdijo kot daljni odsev problema, kateri je na žalost prešel samo v latentno fazo in se je kot tak umaknil s prvih strani medijev. Vendar raznovrstni varnostni problemi ostajajo in jih moramo ob nenehnem spremljanju aktivno analizirati. Zaposleni v naših organizacijah v zadnjem obdobju predstavljajo pomemben vir tveganja, ki se ga vse premalokrat zavedamo. Odtekanje ključnih informacij iz organizacij je za podjetja, ki tem problemom ne posvečajo ustrezne pozornosti, lahko usodno. Vse to pred strokovnjake s področja korporativne varnosti postavlja dileme, kako biti pri vodenju razvejanih organizacij v takih razmerah, učinkovito orodje v rokah strateškega managementa. Ravno pri strateškem managementu se varnostno zavedanje o pomenu korporativne varnosti, in varnosti nasploh, počasi dviguje in prihaja v ospredje. Vendar se vse prevečkrat dogaja, da strokovno znanje in sposobnost korporativno varnostnega managementa v organizacijah, ni na ustreznem nivoju, da bi lahko izkoristil ta »zvezdniški trenutek« in se v določenih situacijah izkazal kot učinkovit mehanizem za ustrezno obvladovanje tveganj. Zaradi navedenega je potrebno, bolj kot kadarkoli do zdaj, vlagati v izobraževanje in dograjevanje svojih znanj ter veščin.

Tudi tokrat nam vsebina 15. številke prinaša veliko aktualnih tem, ki odpirajo najbolj izpostavljene dogodke zadnjega časa. Skozi odmevne intervjuje, reportaže iz vsebinsko odličnih dogodkov, pa vse do strokovnih člankov, ki pred nas postavljajo zadnja spoznanja iz aktualnih področij, se bo našlo dovolj raznovrstne vsebine, ki vam bo omogočila pridobiti dovolj odgovorov in dobrih praks za vaše uspešno poslovanje.

V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji. Glede na to, da je to zadnja letošnja številka, vam v uredništvu želimo veliko uspešnih trenutkov v novem letu in predvsem, da bo prihajajoče leto srečno, varno ter poslovno uspešno!

izr. prof. dr. Denis Čaleta
Glavni urednik

INTERVJU
dr. Jaka Vadnjal, predsednik uprave Lon d.d.

KRIPTOVALUTE POČASI A VZTRAJNO PRODIRAJO TUDI V BANČNI SEKTOR

KOLUMNA
miran.vrsec@ics-institut.si

SO SLOVENSKE BANKE (NE)VARNE?

NASILJE NA DELOVNEM MESTU IN AMOK SITUACIJE

Nasilje na delovnem mestu je zapleten in širok pojav, ki je v zadnjih letih pritegnil pozornost organov pregona, inštitucij za duševno zdravje in strokovnjakov za človeške vire.

VARNOST NA SPLETU JE V PODJETJIH ŠE POSEBEJ POMEMBNA

Z uporabo interneta je vsak posameznik in sleherno podjetje potencialna tarča spletnih kriminalcev, zato se je potrebno zavedati, da lahko napadalci “udarijo” tudi vas. Največ, kar lahko storimo je, da se tega zavedamo, ter seveda, da smo seznanjeni z vrstami groženj, ter predvsem kako se pred njimi ubraniti.

GAŠENJE Z VODNO MEGLO

Voda je najstarejše in najbolj univerzalno gasilno sredstvo. Je učinkovita, poceni, na voljo je v velikih količinah. Lahko pa z njo naredimo tudi več škode kot koristi oziroma uničimo še tisto, čemur požar prizanese.

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

INTERVJU
mag. Boris Novak, generalni direktor, Pošta Slovenije*

POŠTA SLOVENIJE PRIPRAVLJENA NA NOVE IZZIVE PRIHODNOSTI

Pošta Slovenije na temelju tradicije smelo koraka v smeri novih izzivov in poslovnih priložnosti. O ključnih težiščih obvladovanja tveganj, ki jih za poslovanje Pošte Slovenije prinaša dinamično varnostno okolje, smo se pogovarjali z mag. Borisom Novakom.

Lastnik vam je preko nadzornega sveta podelil nov mandat na čelu Pošte Slovenije. Kje vidite glavne izzive razvoja za državo tako pomembnega podjetja?

Na glavne izzive razvoja Pošte Slovenije in njenih odvisnih družb odgovarja novi Strateški razvojni program Skupine Pošta Slovenije 2017 – 2022, ki smo ga pripravili in h kateremu je nadzorni svet Pošte Slovenije podal pozitivno mnenje. Pričakujemo, da ga bo v kratkem potrdil še SDH.

Dejstvo je, da Pošta Slovenije ni več zgolj ponudnik klasičnih poštnih storitev, pač pa je razvojno usmerjen poštno-logistični operater in ponudnik IT storitev. Zaradi upada klasičnih poštnih storitev in substitucije z elektronskimi načini komuniciranja ter posledično spremenjenih navad uporabnikov se vse bolj usmerja v razvoj in nadgradnjo inovativnih in konkurenčnih storitev ter sledi strategiji rasti na področju paketnih, logističnih in informacijskih storitev. Zaradi tega smo oblikovali celotno Skupino Pošta Slovenije, ki jo poleg Pošte Slovenije sestavlja tudi sedem odvisnih družb, v paketno-logistično in IT podjetje, ki nastopa na domačem in tujem trgu. Glede na trende rasti paketnih storitev bodo strateški projekti usmerjeni v širitev kapacitet poštno-logističnih centrov, izgradnjo dodatnih skladiščnih kapacitet, modernizacijo strojnega usmerjanja paketnih in pisemskih pošiljk, optimizacijo omrežja kontaktnih točk in optimizacijo informacijske podpore. Nadaljevali bomo s prostorsko in storitveno optimizacijo ponudbe pošt, ki je na dolgi rok ključnega pomena za ugled blagovne znamke in uspešno poslovanje.

> Tehnologija prinaša prednosti, hkrati pa tudi popolnoma nova tveganja, ki v povezavi z izzivi, ki jih prinaša novodobno varnostno okolje, predstavlja tudi svojevrstni izziv za kakovostno in nemoteno zagotavljanje informacijskih storitev našim strankam.

V skladu z našo strategijo, bomo osredotočeni na nekaj ključnih ciljev: ustvarjali bomo inovativne produkte in rešitve po meri posamezne stranke, v treh ključnih stebrih: prenosu sporočil in paketov, logističnih storitvah in i-storitvah. Rast bomo dosegali tudi skozi širitev na tuje trge v širši regiji, prav tako pa skozi akvizicije družb s kompatibilno/dopolnilno dejavnostjo. V okviru Skupine Pošta Slovenije bomo vstopili na mednarodni trg na področju logističnih storitev, IT storitev, spletne prodaje in na področju t. i. hibridne pošte.

Vodite izredno kompleksno in razvejano organizacijo, ki je že zaradi svojih osnovnih procesov zelo izpostavljena celemu nizu tveganj. Kako se s stališča strateškega managerja spopadate z uravnoteženjem razmerja med zagotavljanjem ustreznega nivoja obvladovanja tveganj in nemotenim delovanjem osnovnih procesov Pošte Slovenije?

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Od Področja korporativne varnosti in nadzora se zato pričakuje, da bo zmožno odgovarjati izzivom sodobnega varnostnega okolja, pri čemer bo z izbranimi ukrepi za obvladovanje varnostnih tveganj pomembno in učinkovito prispevalo k varnosti ljudi, premoženja, ugleda podjetja ter navsezadnje tudi uspešnosti procesov, ki se odvijajo v Pošti Slovenije oz. v povezavi z njo.

Zavedamo se, da je v hitro spreminjajočem se in negotovem okolju prepoznavanje in obvladovanje tveganj pomemben dejavnik poslovnega uspeha družbe, zato ga obvladujemo v sklopu celovitega sistema korporativnega upravljanja s tveganji. Sistem stalno preverjamo in dopolnjujemo, da bi bila ključna tveganja, ki jim je Skupina Pošta Slovenije izpostavljena, pravočasno prepoznana, ovrednotena in ustrezno obvladovana. V ta namen smo v družbi sprejeli tudi Politiko upravljanja neprekinjenega poslovanja, ki je krovni dokument Sistema upravljanja neprekinjenega poslovanja Pošte Slovenije. Pošta Slovenije namreč zagotavlja storitve za prebivalstvo in poslovne partnerje na celotnem območju Republike Slovenije vse delovne dni v tednu. Z vzpostavljenim Sistemom upravljanja neprekinjenega poslovanja lahko Pošta Slovenije v primeru motenj poslovanja deluje in zagotavlja ključne storitve za stranke, ne glede na to ali gre za dogodke v okolju poslovanja ali interne dogodke.

Vedno več storitev izvajate v tesni povezavi z informacijsko komunikacijsko tehnologijo. Kako se lotevate obvladovanja tveganj, ki jih prinaša moderno varnostno okolje?

Tehnologija prinaša prednosti, hkrati pa tudi popolnoma nova tveganja, ki v povezavi z izzivi, ki jih prinaša novodobno varnostno okolje, predstavlja tudi svojevrstni izziv za kakovostno in nemoteno zagotavljanje informacijskih storitev našim strankam. V Pošti Slovenije se vsega tega zelo dobro zavedamo, zato informacijsko varnost jemljemo resno in se izzivov, ki so povezani z obvladovanjem tovrstnih tveganj, lotevamo sistematično. Zavedamo se, da informacijska varnost ne sestavlja samo tehnološka zaščita okolja, ampak tudi urejeni procesi ter v prvi vrsti ustrezno ozaveščen in usposobljen kader. Sledimo usmeritvi, da poskušamo obvladovati tveganja, pri čemer se tudi zavedamo, da vseh tveganj ni mogoče v celoti obvladati in preprečiti njihovih negativnih posledic, zaradi česar imamo tudi vzpostavljen načrt neprekinjenega poslovanja za primer izrednih dogodkov.

Poudaril bi tudi, da so nekatere naše storitve redno presojane s strani pristojnih organov in revizorjev (eArhiv, PoštarCA). Redno se izvaja tudi t. i. penetracijske teste, tako na nivoju storitev, kot na nivoju infrastrukture, kar pomeni, da strokovnjaki poskušajo zaobiti postavljene zaščite. V primeru,

da se ugotovijo ranljivosti, jih lahko še pravočasno odpravimo.

Kot eden večjih ponudnikov informacijskih storitev v državi smo v tem trenutku tudi v fazi certificiranja našega sistem upravljanja z informacijsko varnostjo po standardu ISO 27001 za segment storitev, ki jih ponujamo našim strankam. Pričakujemo, da bomo certifikat pridobili do konca letošnjega leta.

V Slovenskem okolju ste bili še do nedavnega ena redkih organizacij, ki je imela že v svoji organizacijski strukturi opredeljeno Službo za korporativno varnost in nadzor ter postavljenega direktorja korporativne varnosti. Kaj so tiste ključne strateške stvari, ki jih pričakujete od omenjene službe, kot vaše podaljšane roke za obvladovanje določenih varnostnih tveganj v vaši organizaciji?

Pravilno ste ugotovili, da smo v Pošti Slovenije kot ena prvih organizacij v Sloveniji pristopili k vzpostavitvi in organizaciji Področja korporativne varnosti in nadzora, znotraj katerega smo pod eno streho združili različne vidike obvladovanja varnostnih izzivov, s katerimi se vsakodnevno srečujemo. V to so nas vodila lastna spoznanja in izkušnje, da je podjetje lahko uspešno pri obvladovanju varnostnih izzivov, če se o vprašanjih, povezanih z varnostjo podjetja, razpravlja na enem mestu in v povezavi z najvišjimi nivoji, pri čemer je nujno, da ima podjetje za to tudi ustrezno usposobljen kader in zagotovljena določena finančna sredstva. Moja pričakovanja in zahteve do tega področja so v osnovi enaka kot do vseh ostalih področij in služb, ki delujejo v okviru Pošte Slovenije – to pa je profesionalno in strokovno delo, vključno s pogledom na prihodnost in razvojne izzive, ki jim je vsaka sodobna organizacija nenehno podvržena. Od Področja korporativne varnosti in nadzora se zato pričakuje, da bo zmožno odgovarjati izzivom sodobnega varnostnega okolja, pri čemer bo z izbranimi ukrepi za obvladovanje varnostnih tveganj pomembno in učinkovito prispevalo k varnosti ljudi, premoženja, ugleda podjetja ter navsezadnje tudi uspešnosti procesov, ki se odvijajo v Pošti Slovenije oz. v povezavi z njo. Področje si mora prizadevati za aktivno vlogo pri vprašanjih, ki se nanašajo na trenutno delovanje in obstoj podjetja, kot tudi pri vprašanjih razvoja in delovanja Pošte Slovenije v prihodnosti.

> Še tako sofisticirani in moderni sistemi tehničnega varovanja so neučinkoviti in neuspešni, če pri zaposlenih ni prisoten ustrezen nivo varnostne kulture in zavesti.

Ali Pošta Slovenije zaradi svoje pomembnosti poslovnih procesov in infrastrukture za državo predstavlja tako pomemben segment, ki vas v enem delu uvršča med upravljalce kritične infrastrukture?

Glede na predlog Zakona o informacijski varnosti, ki je v javni obravnavi, poštne storitve niso opredeljene kot bistvene storitve, zato glede na ta segment storitev Pošta Slovenije zaenkrat ne spada med zavezance oz. upravljalce kritične infrastrukture. Kljub temu, da še niso določena merila, na podlagi katerih bo pristojni organ določil izvajalce bistvenih storitev, pa menimo, da bo Pošta Slovenije, kot eden večjih ponudnikov digitalnih storitev, ki jih med drugim uporabljajo tudi državni organi, uvrščena na seznam izvajalcev bistvenih storitev.

Kripto valute vedno bolj prodirajo v plačilne sisteme moderne družbe. Kakšno politiko nameravate do tega plačilnega sredstva zavzemati na Pošti Slovenije?

Kriptovalute še niso uradno plačilno sredstvo in jih še ne uvajamo, vsekakor pa nove trende na področju plačilnih sredstev pozorno spremljamo.

Varnostna kultura in visoko varnostno zavedanje zaposlenih ločuje uspešne organizacije od slabše uspešnih. Kako v tem hitrem dinamičnem okolju, kjer je mobilnost kadrovskega potenciala zelo visoka, zagotavljate osnovne varnostne vrednote in standarde varnostne kulture?

Zagotavljanje in izvajanje varnostne kulture ter visoke stopnje varnostne zavesti je zagotovo neprekinjeni in stalni proces, ki je hkrati tudi nujen pogoj za zagotavljanje čim boljše varnosti podjetja in njegove uspešnosti. Še tako sofisticirani in moderni sistemi tehničnega varovanja so neučinkoviti in neuspešni, če pri zaposlenih ni prisoten ustrezen nivo varnostne kulture in zavesti. V Pošti Slovenije smo se zato odločili, da bomo k oblikovanju, zagotavljanju in izvajanju varnostne kulture in varnostne zavesti pristopili sistematično, na osnovi integriranega varnostnega sistema podjetja in uporabe široke palete ukrepov; od ukrepov povezanih z zagotovitvijo ustreznega nivoja varnosti z uporabo ukrepov fizičnega, tehničnega in mehanskega varovanja, do organizacijskih in kadrovskih ukrepov. V tem okviru pomembno skrb posvečamo usposabljanju zaposlenih ter njihovemu osveščanju o vprašanjih varnosti, s katerimi se vsakodnevno tudi srečujejo. Pomemben element izgradnje varnostne kulture in zavesti pri zaposlenih pa zagotovo predstavljajo tudi testi integritete in varnostno preverjanje z uporabo poligrafske metode, ukrepa, ki smo ju v Pošti Slovenije uspešno vpeljali v sklopu celovite izgradnje varnostnega sistema pri zagotavljanju varnosti ljudi in premoženja.

Nezadovoljni zaposleni lahko hitro postanejo tudi varnostni problem. Kako nameravate v prihodnje upravljati ta pričakovanja zaposlenih in vedno večji pritisk lastnikov na zmanjšanje stroškov dela?

Pošta Slovenije se sooča z velikimi strukturnimi spremembami na trgu poštnih storitev zaradi e-substitucije in sodobnih tehnologij. Še vedno je podjetje v 100-odstotni državni lasti, ki opravlja del nalog gospodarske javne službe v delu univerzalne storitve, hkrati pa posluje v pogojih tržne konkurence. Na eni strani naš lastnik oziroma SDH kot predstavnik lastnika pričakuje čim višji dobiček, zaposleni pa čim boljše pogoje dela in plače, potem pa so tu še pričakovanja lokalnih skupnosti po čim boljšem »javnem servisu poštnih storitev«.

Na Pošti Slovenije pričakujemo, da bo tudi naš lastnik svoja pričakovanja glede dobička ustrezno prilagodil tako trendom na poštno-logističnem področju in razmeram, v katerih Pošta Slovenije posluje, kot tudi ciljem, ki jim Pošta Slovenije sledi glede na zapisano v strateškem razvojnem programu. Glede zaposlenih, ki pričakujejo čim boljše pogoje dela in plače pa naj dodam, da smo z večinskim sindikatom v podjetju, Sindikatom delavcev prometa in zvez pri ZSSS, v mesecu maju, dosegli dogovor glede ureditve odprtih vprašanj v podjetju, socialni dialog s sindikati glede nekaterih vprašanj pa še poteka. Razumemo tudi pričakovanja lokalnih skupnosti, vendar se mora tudi Pošta Slovenije prilagajati spremenjenim okoliščinam poslovanja. Optimizacija in modernizacija poštnega omrežja sta pomembni smernici delovanja in poslovanja tudi vseh ostalih poštnih operaterjev v Evropi.

Dejstvo pa je, da zaradi zmanjševanja obsega tradicionalnih poštnih storitev število zaposlenih že nekaj let zapored znižujemo na določenih segmentih dela, in sicer s konstantno optimizacijo, centralizacijo posameznih ključnih funkcij in procesov (naravna fluktuacija, premestitev zaposlenih med področji dela in delovnimi mesti, prenehanje pogodb o zaposlitvi za določen čas, dokup delovne dobe...). V letošnjem letu se je število zaposlenih povečalo večinoma na področju dela dostave in predelave pošiljk ter logističnih in paketnih pošiljk. Tudi v naslednjih letih pričakujemo trend rasti zaposlovanja na teh področjih, medtem ko na določenih segmentih dela načrtujemo zmanjšanje.

Rast in razvoj Skupine Pošta Slovenije je naš odgovor na globalne poštno-logistične trende, na pričakovanja lastnika, na upadanje klasičnih poštnih storitev ter na sledenje naši strategiji rasti na področju paketnih, logističnih in informacijskih storitev. Okoliščinam se prilagajamo s posodobitvami in prenovo obstoječih storitev, predvsem pa z razvojem novih storitev in vpeljevanjem novih tehnoloških, strojnih in informacijskih rešitev v poslovanje. Pri vsem tem pa pomembno težo dajemo vzdrževanju in nenehnim izboljšavam standardov kvalitete in zanesljivosti izvajanja storitev za vsako stranko. Razvoj usmerjamo v napredne informacijske tehnologije in sodobne digitalne rešitve, ki lahko bistveno olajšajo življenje in poslovanje naših strank.

Pošta Slovenije je bila v preteklosti ena izmed prejemnic prestižnega priznanja »Slovenian Grand Secu-

Skratka, združenje je prineslo velike spremembe na področju korporativne varnosti in verjamem, da bo tudi v prihodnje zmožno odgovoriti na vse izzive, ki se bodo v modernem okolju pojavljali, za kar ima tudi ustrezne predispozicije v obliki strokovnega znanja, izkušenj in dobrih praks njegovih rednih in korporativnih članov.

rity Award« v kategoriji »najbolj varna organizacija«. Menite, da je ta nagrada lahko tudi za druge organizacije, v okolju, kjer deluje Pošta Slovenije, motivacija za bolj sistemske pristope na področju zagotavljanja varnosti?

Prepričan sem, da takšna nagrada predstavlja pravšnji motiv in cilj za vse tiste gospodarske družbe, ki so se ali se bodo odločile, da se bodo z vprašanji varnosti začele ukvarjati sistematično. Za Pošto Slovenije ta nagrada predstavlja potrditev, da je pot, ki smo jo pri tem ubrali pravilna ter kot takšna tudi prepoznana v širšem okolju in strokovni javnosti. Je pa hkrati takšna nagrada tudi velika obveza za prihodnost, saj je prejemnik neprestano opazovan in ocenjevan iz prizme takšne nagrade oz. so pričakovanja do prejemnikov takšne nagrade drugačna in večja kot do ostalih subjektov.

Kako vidite vlogo Slovenskega združenja za korporativno varnost katerega korporativni člani ste? Menite, da je to združenje v Sloveniji prineslo pozitivne spremembe na področju korporativne varnosti?

Od samih začetkov združenja dalje podrobno spremljamo njegov razvoj in vpliv na dogajanja v okolju. Ponosni smo, da smo prepoznali strokovno vrednost združenja in se vanj tudi včlanili ter tako tudi z lastno udeležbo in izkušnjami prispevali k širši prepoznavnosti združenja. Združenje je zagotovo pomembno prispevalo k prepoznavi pojmovanja korporativne varnosti in z njo povezanih tveganj v Republiki Sloveniji in v tujini. Pošta Slovenije kot korporativni član združenja prepoznava dodano vrednost združenja v povezovanju različnih deležnikov na področju korporativne varnosti in gospodarstva kot celote, izmenjavi izkušenj in dobrih praks ter izobraževanju, pri čemer pozdravljamo usmeritev, da poudarek na izobraževanju ni podan samo na nosilcih in odgovornih osebah v podjetjih za korporativno varnost, ampak tudi na najvišjem managementu v podjetjih. Skratka, združenje je prineslo velike spremembe na področju korporativne varnosti in verjamem, da bo tudi v prihodnje zmožno odgovoriti na vse izzive, ki se bodo v modernem okolju pojavljali, za kar ima tudi ustrezne predispozicije v obliki strokovnega znanja, izkušenj in dobrih praks njegovih rednih in korporativnih članov. ■

Slovensko združenje korporativne varnosti

Slovensko združenje korporativne varnosti združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij.

»Ab uno disce omnes (po enem spoznaj vse)«
»Ustvarjamo vezi, ki bogatijo
ter tako gradimo pot do uspeha!«

Namen združenja je uresničevanje interesov članstva, ki so:

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

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

www.ics-institut.si

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

INTERVJU
dr. Jaka Vadnjal, predsednik uprave Lon d.d.

KRIPTOVALUTE POČASI A VZTRAJNO PRODIRAJO TUDI V BANČNI SEKTOR

Lon d.d. je prva finančna institucija, ki v svoje finančne produkte uvaja tudi kriptovalute. O priložnostih in tudi varnostnih izzivih smo se pogovarjali z dr. Jako Vadnjalom.

Pred časom je v javnosti močno odmevala novica, da ste postali prva finančna institucija, ki na bankomatih ponujate dvig bitcoinov. Nam lahko zaupate na čem temelji vaša odločitev?

Odločitev temelji na več dejavnikih. Najpomembnejše je zagotovo zavedanje, da bomo v prihodnosti brez inovativnih pristopov težko preživeli. Pomemben del inovativnosti je vsekakor na področju digitalizacije, tehnološkega razvoja in partnerstev s tretjimi ponudniki. Hkrati potekajo stalni interni procesi iskanja neučinkovitosti našega poslovanja. Lep primer tega je bankomat, ki je relativno drag kos opreme, ki ga kot uporabniki štejemo kot nujno infrastrukturo, za banko pa večinoma pomeni neekonomično investicijo, ki se redko povrne. Bankomati so hkrati slabo izkoriščeni z vidika tehničnih možnosti, vendar doslej ni nihče dosti razmišljal, kako bi jih še uporabil, razen za dvigovanje denarja in v manjšem obsegu polaganja gotovine, plačila položnic in nakupov vrednotnic za predplačniško mobilno telefonijo. V našem intenzivnem razmišljanju in v strokovnih debatah z zunanjimi deležniki se je rodila ideja, ki je v približno šestih mesecih ugledala luč sveta. V tem

*avtor je član Slovenskega združenja korporativne varnosti

času je bilo opravljenega veliko dela in tehnično povezovanje bankomata z infrastrukturo za prodajo kuponov je bil zgolj delček v mozaiku vsega, kar smo morali postoriti. Veliko smo se tudi naučili, med drugim partnerskega sodelovanja z drugimi podjetji, pri katerem sta bila ključni podjetji Keas iz Ljubljane in Bitins iz Londona.

Na bankomatu stranka dobi vavčer o količini vzdignjenih sredstev. Kako pride neposredno do lastništva bitcoinov?

Na bankomatu stranka kupi vavčer, ki ga na spletni strani partnerskega podjetja BitIns zamenja v valuti Bitcoin ali Ethereum. To lahko stranka naredi v roku 12 mesecev od nakupa vavčerja, ki je nominiran v evrih in se zamenja v kriptovaluto po trenutno veljavnem tečaju, pri čemer se znesek zmanjša za 4% nakupne provizije. Sredstva se neposredno naložijo v elektronsko denarnico, ki jo ima stranka odprto pri kateremkoli ponudniku. Na bankomatu se lahko storitev nakupa plača z bančno kartico, na izbranih bankomatih pa tudi z gotovino. Stranka torej postane lastnik bitcoinov šele v trenutku, ko vavčer zamenja zanje. Transakcija zamenjave traja nekaj sekund.

Kriptovalute na eni strani odpirajo novo revolucijo na finančnem področju, na drugi strani pa predstavljajo resno tveganje za pranje denarja in izvajanje nelegalnih transakcij, skozi katere se financira tudi terorizem. Ste se pred izvedbo tega koraka posvetovali z institucijami, ki skrbijo za preprečevanje pranja denarja?

Kot finančna inštitucija smo zavezani najstrožjim standardom s področja preprečevanja pranja denarja in financiranja terorizma. Z vsemi organi korektno in zelo tvorno sodelujemo. Pri omenjeni storitvi prodaje vavčerjev za nakup kriptovalut smo delovali tudi preventivno, predvsem z omejevanjem gotovinskih nakupov, saj so kartični nakupi izsledljivi in zato niso toliko problematični. Redno tudi spremljamo transakcije in v enem mesecu, kolikor storitev deluje, je bilo zgolj nekaj takih, ki so bile reda velikosti enega bitcoina torej nekaj tisoč evrov. Morebitno pranje denarja torej spremljamo predvsem z vidika velikosti transakcij, ki so med seboj lahko tudi povezane. Na kakšne načine to počnemo seveda ne bi bilo smiselno javno razkrivati. Osebno sicer menim, da se kriptovalutam dela krivica s pretiravanjem glede možnosti pranja denarja. Njihova celotna kapitalizacija morda ta trenutek dosega 1% vsega svetovnega denarnega prometa. Po drugi strani pa obstajajo ocene, da je celo v razvitih ekonomijah 20% in več sive ekonomije. Veliko denarja se torej opere z »normalnimi« valutami. Potrebno je povedati, da vsi resni ponudniki elektronskih denarnic danes izvajajo zelo rigorozno politiko za preprečevanje pranja denarja, saj svojo priložnost vidijo v inovativnih storitvah in ne v »temačnih« priložnostih. Nenazadnje, dva največja svetovna ponudnika plačilnih kartic Mastercard in Visa že nekaj časa ponujata tudi predplačniške oziroma debetne kartice s kritjem v bitcoinih.

Ali kot finančni strokovnjak menite, da lahko v prihodnosti kriptovalute resno zamajejo monopol držav nad finančnimi tokovi ali gre v tem primeru za komplementarni proces, ki se bo dopolnjeval z obstoječimi finančnimi instrumenti?

Kriptovalute so doslej najbolj konkretna implikacija blockchain tehnologije, ki prinaša neslutene možnosti razvoja novih poslovnih modelov na mnogih področjih. Ne samo na finančnem, ki je ta trenutek sicer najbolj medijsko izpostavljen, zaradi vrtoglavega naraščanja menjalnih tečajev, na relaciji predvsem bitcoin proti različnim denarnim valutam (ang. fiat money). Ekonomsko gledano so kriptovalute pravzaprav fenomen, saj njihovi nasprotniki pravijo, da jih ni, ker niso definirane. Hkrati se je, predvsem z večjimi kriptovalutami, ustvaril skoraj popoln trg: vsi deležniki so lahko popolnoma informirani glede cen in količin, v vsakem trenutku je dovolj povpraševanja in ponudbe, da transakcije potekajo in to na novih omrežjih, ki so bistveno bolj učinkovita od ustaljenih, ki potekajo predvsem v zavetju bank. Če povem

samo primer: z bitcoini poteka na minuto trikrat več transakcij kot z največjo svetovno kreditno kratico. Pri tem so provizije za transakcije s kriptovalutami do 20x nižje in za enak red velikosti hitrejše. Rekel bi, da gre za tržni spopad starih tehnologij, ki so monopolizirane in slabše učinkovite in tehnoloških inovacij, ki že po definiciji motijo in razbijajo ustaljene trge. To se v življenju ves čas dogaja. Kdo bi si pred desetimi leti drznil napovedati, da bodo države začele omejevati dizelske in bencinske motorje in da bodo na tako obsežnem pohodu električni avtomobili. Če se vrnem na finančni sistem: kratkoročno si velikih sprememb ne obetam, v nekaj letih se bo pokazalo, kam vodi razvoj.

Veliko je bilo napisanega o transformaciji vaše hranilnice v banko. V kakšni fazi se trenutno nahaja ta proces?

Formalna zakonska zahteva, da se transformirano v banko, je minimalno 5 milijonov evrov osnovnega kapitala in to izpolnjujemo od začetka letošnjega leta. Sicer moramo kot hranilnica izpolnjevati popolnoma vse regulatorne zahteve, tako da bo šlo pravzaprav samo za tehnično ureditev imena. Sicer smo pred nekaj tedni uvedli novo celostno grafično podobo in navzven nastopamo samo s skrajšano firmo LON, tako kot to počnejo mnoge druge banke doma in po svetu. Banke smo in bomo šle skozi obdobja velikih sprememb in banka čez deset let zagotovo ne bo taka, kot je danes. Tudi to sporočilo vsebuje naše novo medijsko pojavljanje: nova celostna grafična podoba in slogani, ki privabljajo mlajšo populacijo, kjer so naši ciljni komitenti.

Ste na področju obvladovanja tveganj, ne samo finančnih, temveč tudi tveganj, ki jih prinaša varnostno okolje, pripravljeni na rast svojega poslovanja in širjenje mreže poslovalnic?

Obvladovanje tveganj je hrbtenica bančnega posla, saj poslujemo z denarjem, ki ni naš, hkrati pa moramo z njim upravljati, da bi dosegali vsaj minimalne donose. Sistemsko obvladovanje tveganj imamo umeščeno v več službah in delovnih področjih. Tako je na oddelku na področju upravljanja s tveganji posebna skupina za operativna tveganja, ki deluje tako preventivno kot kurativno. Imamo tudi službo skladnosti poslovanja, ki skrbi, da je vse kar počnemo v skladu z aktualnimi in prihajajočimi predpisi. Število naših poslovalnic se v prihodnosti ne bo drastično povečalo. V strategiji imamo do leta 2020 načrtovano povečanje s 15 na 20 poslovalnic. Hkrati poteka proces zmanjševanja gotovine v obtoku in prav zaradi gotovine so poslovalnice tradicionalno najbolj na udaru. Zavedamo pa se, da je tudi kriminal inovativen in se razvija hitreje, kot si želimo. Ocenjujemo, da je v prihodnosti več nevarnosti v kibernetskih tveganjih. Integralno področje obvladovanja tveganj je tudi predmet stalnega monitoringa nadzornega sveta in regulatorja.

Kako imate v podjetju urejen proces korporativne varnosti in ali je le ta komplementaren s ključnimi procesi, kot so informacijska varnost, fizična in tehnična varnost poslovalnic in zaposlenih?

Korporativna varnost, z vidika ključnih procesov, se pri nas deli na dva ključna stebra, tako imenovani »front-office«, torej komercialne dejavnosti, ki večinoma potekajo preko poslovalnic in

Obvladovanje tveganj je hrbtenica bančnega posla, saj poslujemo z denarjem, ki ni naš, hkrati pa moramo z njim upravljati, da bi dosegali vsaj minimalne donose.

Ocenil bi, da je korporativna varnost izredno pomembno orodje, vendar mora delovati z roko v roki z obvladovanjem finančnih tveganj, kar je jedrni proces našega poslovanja.

»back-office«, ki predstavlja vse zaledne procese, ki se večinoma dogajajo na sedežu banke v Kranju. Mnoge ključne elemente korporativne varnosti nam opredeljuje že bančna zakonodaja in podrejeni dokumenti, ki jih predpisuje nacionalni regulator in so usklajeni z evropskimi direktivami. Zunanja ogroženost poslovnih enot je osredotočena predvsem na ključne procese v povezavi z manipulacijo gotovine, ki morebitne nepridiprave, logično, tudi najbolj zanima. Sem sodijo procesi, ki predstavljajo preventivo pred ropi, unovčevanjem ponaredkov, goljufijami, pranjem denarja. Vsi postopki so predpisani in jih v največji možni meri spoštujemo. Seveda prihaja do odklonov, ki jih sproti analiziramo in sistem izboljšujemo. V centrali vse ključne procese koordiniramo in izvajamo njihov razvoj. Na tem mestu bi predvsem izpostavil področje informacijskih tehnologij, ki po eni strani podpirajo ključne procese, po drugi strani pa so zaradi povezanosti v medmrežje ti sistemi tudi najbolj ranljivi zaradi morebitnih vdorov in poskusov zlorab finančnih podatkov, osebnih podatkov in poslovnih podatkov. Za primere različnih dogodkov, ki jih ne moremo predvideti (npr. naravne nesreče, letalske nesrečezaradi bližine letališča, politične krize in nemiri itd.), imamo pripravljen tudi Načrt neprekinjenega delovanja, ki med drugim vsebuje tudi izračune potrebnih količin gotovine, s katero bi lahko nekaj dni zagotavljali nemoteno dobavo našim komitentom. Kot banka se zavedamo, da smo pomemben del kritične infrastrukture in se moramo ustrezno obnašati.

Ali smatrate, da je korporativna varnost lahko orodje v vaših rokah za učinkovitejše obvladovanje varnostnih tveganj v Hranilnici Lon?

Kot sam ravnokar skušal pojasniti, gre za kompleksen sistem medsebojno povezanih tveganj, ki jim moramo posvečati enakovredno pozornost. Ocenil bi, da je korporativna varnost izredno pomembno orodje, vendar mora delovati z roko v roki z obvladovanjem finančnih tveganj, kar je jedrni proces našega poslovanja. Zavedamo pa se, da je to »živa stvar«, sistem, za katerega nikoli ne morem reči, da je dovolj dober, da se ga ne bi dalo še izboljšati. Poznamo mnoge zgodbe s področja korporativne varnosti, kjer je pred škodnim dogodkom izgledalo, da je poskrbljeno za vsak še tako neverjeten scenarij, vendar so se hkrati zgodile kombinacije neželenih scenarijev, za katere bi ocenili, da je verjetnost, da se lahko zgodijo, ena proti milijon, a so se vendarle zgodili. Zavedamo se, da nas na tem področju čaka še veliko dela.

Zaposleni so največkrat tisti dejavnik, na katerega pozabljamo, ko govorimo o učinkoviti varnosti. Kako pristopate k izobraževanju zaposlenih, skozi katerega dvigujete njihovo varnostno kulturo?

Tako kot pri večini ključnih procesov, so ljudje najpomembnejši. Z njihovim usposabljanjem se zelo veliko ukvarjamo in prav na področju korporativne varnosti razumemo, da je treba zagotoviti vse tri komponente izobraževanja odraslih: odnos, veščine in znanje. Mnogih postopkov se morajo zaposleni enostavno naučiti, kako ravnati v skladu s predpisanimi procedurami. Nekatere procese morajo tudi razumeti, zakaj so potrebni. Dober primer je preprečevanje pranja denarja, kjer morajo naši zaposleni opravljati stvari, ki jih stranke razumejo kot nepotrebno birokracijo in celo nediskretno vmešavanje v zasebnost. Kako bo naš uslužbenec stranki razložil, da so nekateri postopki obvezni zaradi preventive, je odvisno predvsem od njegovega znanja in razumevanja tega občutljivega področja. Posebna zgodba je odnos do varnosti, ki lahko izhaja iz neznanja. Pred časom se je zgodilo, da je v času praznikov v poslovni enoti ostala sodelavka, ki ni dolgo z nami, sama. V poslovni enoti so sicer redno zaposleni trije, vendar je en sodelavec zbolel, drugi pa je že nekaj dni prej odšel na dopust. Sodelavka, ki je sicer zelo vestna, se je odločila »da ne bo komplicirala, ker tako in tako zaradi praznikov skoraj ni bilo ljudi«. Dogodek smo obravnavali v skladu z notranjimi akti, po drugi strani pa smo ga izkoristili, da predvidene postopke dopolnimo tudi z jasnimi navodili za take primere: če se zgodi, da nekdo ostane v enoti sam in ne more dobiti pomoči, mora poslovalnico za tisti dan zapreti.

Že dalj časa se nahajate nekje na vhodnih vratih Slovenskega združenja za korporativno varnost, ki predstavlja pomembno strokovno asociacijo v Republiki Sloveniji. Menite, da je na tej fazi razvoja prišel čas za vašo včlanitev v omenjeno asociacijo?

Najbrž. Moral se bom posvetovati s sodelavci. Pri stanovskem Združenju bank so precej aktivni v več delovnih skupinah za varnost bank, za varnost kartičnega poslovanja, na varnostnem forumu za IT in še nekaterih drugih. Želim si, da bi sami prepoznali dodano vrednost združenja za njihovo delo. ■

Slika je simbolična. Summit motors Ljubljana, d. o. o., Flajšmanova 3, 1000 Ljubljana. Uradna poraba goriva: 4,4-7,4 l/100 km. Uradne emisije CO_2: 115-172 g/km. Emisijska stopnja: Euro 6b. Uradne emisije NOx: 0,0405-0,0725 g/km. Specifične emisije trdih delcev: 0,0003-0,000416 g/km. Število delcev: 0,0405-0,0725 x 10^{11}. Ogljikov dioksid (CO_2) je najpomembnejši toplogredni plin, ki povzroča globalno segrevanje. Emisije onesnaževal zunanjega zraka iz prometa pomembno prispevajo k poslabšanju kakovosti zunanjega zraka. Prispevajo zlasti k čezmerno povišanim koncentracijam prizemnega ozona, delcev PM_{10} in $PM_{2,5}$ ter dušikovih oksidov. Navedena cena velja za vozilo Kuga Trend 1.5 TDCi 88 kW (120 KM), 6-stopenjski ročni menjalnik, na dan 1.9.2017.

Ford
Go Further

SUMMIT AVTO d.o.o., Flajšmanova 3, 1000 Ljubljana
Telefon: 01 25 25 125, e-pošta: prodaja@summitavto.si

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

KOLUMNA
miran.vrsec@ics-institut.si

SO SLOVENSKE BANKE (NE)VARNE?

Iz Letnega poročila o delu policije za leto 2016 lahko razberemo, da je bilo v letu 2016 v Sloveniji izvedenih 226 ropov (2,6% manj kot v letu 2015) ter 260 napadov na informacijski sistem (60,5% več kot v letu 2015). Omenjeni kaznivi dejanji sta le dve od množice kaznivih dejanj, ki jih storilci izvajajo na področjih in območjih delovanja bank. Iz omenjene statistike sicer ni možno točno razbrati, koliko od omenjenih kaznivih dejanj je bilo dejansko izvršenih v bančnem sistemu, pa vendar številke nazorno kažejo na nujnost sistemskega obvladovanja kriminalne ogroženosti na vseh nivojih upravljanja in delovanja bank.

V Sloveniji smo imeli do nedavnega vzpostavljen sistem nadzora nad ugotavljanjem ustreznosti organiziranosti področja varovanja bank. Vsaka banka je morala imeti izdelan Elaborat o varovanju premoženja banke iz katerega je morala biti prepoznana ustreznost varovanja banke, na področju varovanja premoženja banke, prevoza in varovanja denarja ter drugih vrednostnih pošiljk banke, upravljanja z varnostno-nadzornim centrom in načrtovanja in izvajanja varnostnih sistemov banke. Omenjeni elaborat je moral vsebovati analizo tveganj banke na zgoraj navedenih področjih in načrt varovanja banke, ki je temeljil na omenjeni analizi tveganj banke. Povzetek navedenih dokumentov so banke morale posredovati Banki Slovenije. Banke so morale najmanj enkrat v dveh letih (po potrebi pa tudi večkrat) z neodvisno tretjo osebo, ki je bila ustrezno usposobljena za nadzor nad izvajanjem zasebnega varovanja, skleniti pogodbo za nadzor nad izvajanjem zasebnega varovanja v banki. Neodvisna tretja oseba je morala za izvršitev nadzora, predhodno s strani takratne Zbornice RS za zasebno varovanje, sedaj Zbornice RS za razvoj slovenskega zasebnega varovanja, pridobiti ustrezno pooblastilo oziroma ustrezno mnenje o strokovni usposobljenosti. S spremembo bančne zakonodaje in preklicem sklepa Sveta Banke Slovenije o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice, ki je med drugim določal zgoraj navedena pogoja za izvajanje nadzora varovanja v bankah, banke niso več zavezane k izvajanju tovrstnega nadzora. Nekatere banke, ki imajo višjo varnostno zavest tovrstni nadzor izvajajo tudi sedaj, za tiste druge, katerim pa je bilo izvajanje tovrstnega nadzora »nujno zlo«, pa je bila očitno ukinitev tovrstnega nadzora dobrodošla.

Po ukinitvi prej opisanega in predpisanega sistema nadzora varovanja bank, je na področju nadzorovanja varovanja bank s strani Banke Slovenije nastala praznina.

Takratni sistem ni bil optimalen, saj ni bilo izdelane metodologije, na podlagi katere bi nadzorniki, ki so pridobili »pooblastilo« za izvajanje nadzorov, poenoteno izvajali svoje nadzore. Ker sem imel tudi sam omenjeno »pooblastilo« in sem se zavedal omenjene pomanjkljivosti, sem takratni Zbornici RS za zasebno varovanje pripravil pisne predloge enotne metodologije za izvajanje nadzorov varovanja bank, ki pa iz meni neznanih razlogov žal ni ugledala luč sveta. Prav tako v takratnem sistemu ni bila ustrezna rešitev podeljevanja »pooblastil« posameznikom, saj je bila za podeljevanje pooblastil pristojna takratna Zbornica RS za zasebno varovanje, ki kot taka ni zagotavljala neodvisnosti in nepristranskosti pode-

*avtor je član Slovenskega združenja korporativne varnosti

ljevanja »pooblastil« posameznikom, obenem pa so pridobili »pooblastila« posamezniki, ki iz vidika zakonodaje, s področja zasebnega varovanja, niso izpolnjevali pogojev za izvajanje omenjenih nadzorov. Ne glede na navedeno, pa lahko ugotovimo, da je takratni sistem nadzora (ob izključitvi navedenih pomanjkljivosti) kljub temu ob korektni, nepristranski in strokovni izvedbi bankam zagotavljal pridobivanje podatkov o stanju varovanja in potrebnih posodobitvah le-tega.

Zakon o Banki Slovenije v deveti točki 12. člena, ki navaja druge naloge Banke Slovenije določa, da Banka Slovenije oblikuje, uveljavlja in nadzoruje sistem pravil za varno in skrbno poslovanje bank in hranilnic. V 23. členu, ki opredeljuje nadzor nad poslovanjem bank in hranilnic je navedeno, da Banka Slovenije opravlja nadzor nad bankami, hranilnicami in drugimi osebami na podlagi zakona, ki ureja bančništvo in na tej podlagi oblikuje, uveljavlja in nadzoruje sistem pravil, ki zagotavljajo standarde varnega poslovanja bank in hranilnic. Prav tako je navedeno, da Banka Slovenije pri oblikovanju sistema pravil, uresničevanju nadzora in pri ukrepanju upošteva standarde in priporočila, ki jih v ta namen oblikujejo pristojne domače in mednarodne institucije. Iz navedenega torej izhaja, da je dolžnost Banke Slovenije, da nadzoruje tudi varnost poslovanja bank in hranilnic.

Po ukinitvi prej opisanega in predpisanega sistema nadzora varovanja bank, je na področju nadzorovanja varovanja bank s strani Banke Slovenije nastala praznina. Na to sem že pred časom opozoril odgovorne v Banki Slovenije. Obstoječa zakonodaja, ki ureja področje zasebnega varovanja sicer ureja izvajanje internega nadzora nad izvajanem zasebnega varovanja, ki pa nima neposredne zveze z nadzorom, ki bi ga morala nad izvajanjem varovanja bank vzpostaviti Banka Slovenije.

Na področju zasebnega varovanja, ki je tesno povezano z zagotavljanjem varnosti bank, bo v prihodnje kar nekaj izzivov, tako z vidika novo nastajajočih varnostnih tveganj, kot tudi z vidika regulatornih sprememb. V polno veljavo bo v letu 2018 stopila Splošna uredba o varstvu osebnih podatkov (GDPR). V fazi sprejemanja je tudi zakonodaja na področju kritične infrastrukture in informacijske varnosti, zakonodaja s področja zasebnega varovanja pa postaja vse bolj zastarela in tudi že kliče po prenovi. Fizična varnost ljudi in premoženja

Na področju zasebnega varovanja, ki je tesno povezano z zagotavljanjem varnosti bank, bo v prihodnje kar nekaj izzivov, tako z vidika novo nastajajočih varnostnih tveganj, kot tudi z vidika regulatornih sprememb.

in informacijska varnost postajata zaradi novih varnostnih izzivov vse bolj neločljivo povezani, kar narekuje spremembo pristopa k obvladovanju in upravljanju varnostnih in informacijskih tveganj. V tej smeri se kaže tudi vse bolj tesna povezava med strateškim in operativnim nivojem upravljanja z omenjenimi tveganji, saj nevarnost preži na vseh nivojih delovanja in upravljanja.

Omenjene spremembe same po sebi kličejo po ponovni ureditvi področja nadzora varovanja bank, katere predstavljajo pomemben steber za zagotavljanje nemotenega in neodvisnega delovanja države tudi v kriznih razmerah. V Inštitutu za korporativne varnostne študije imamo izdelan koncept na podlagi katerega se lahko ponovno vzpostavi sistem nadzora nad varnostjo bank z izključitvijo vseh navedenih pomanjkljivosti, ki so bile prisotne v prejšnjem sistemu nadzora varnosti bank. V tem kontekstu se samoumevno kaže prvi korak Banke Slovenije, ki od bank zahteva revizijo obstoječih varnostnih sistemov s ciljem prevetritve fizičnega in tehničnega varovanja, informacijske in komunikacijske varnosti ter drugih področij varnosti. Gre torej za inovativni pristop k prepoznavanju ranljivosti bank in k obvladovanju varnostnih tveganj. Kajti bančni sistem je sestavni del kritične infrastrukture, ki mora delovati tudi v kriznih razmerah.

Bistvo pri vsem tem je, da se Banka Slovenije kot krovna bančna inštitucija zave, da je z vidika zakonodaje to njena obveza, s strokovnega vidika pa nuja. Pa se odgovorni v Banki Slovenije zavedajo tega dejstva? Verjamem, do bo to kmalu pokazal čas. ■

Avtorja: mag. Danilo Burnač, dr. Milka Pungartnik /
Mariborski vodovod, javno podjetje d.d.*

PODLAGE IN RAZLOGI, ZAKAJ BI MORALA BITI VODNA INFRASTRUKTURA V SLOVENIJI VKLJUČENA MED KRITIČNO INFRASTRUKTURO DRŽAVNEGA POMENA

V našem vsakdanu ravno voda predstavlja nekaj samoumevnega, da kar pozabimo, kje se nahaja, koliko je imamo, kako pridemo do nje in kako jo varujemo. Kar je bilo glede vode včasih samoumevno, postaja danes predmet mednacionalnih, kulturnih, okoljskih in etičnih sporov.

Uvod

Voda ima v vseh kulturah in religijah, že iz zgodovinskih pogledov in virov, vrsto pomenov. Voda pomeni hrano in življenje. Pri mnogih ljudstvih je voda osnova vsega, je prasnov in jo zato imenujemo "Prima materia" vsega bivanja. Nenazadnje je voda izvirna človekova pravica. Voda vsem živim bitjem vzdržuje zdravje in jim daje energijo. Je strateškega pomena tako za kmetijstvo, promet, industrijo kakor tudi za vse ostale gospodarske panoge. Voda je z zakonom o zdravstveni ustreznosti živil in izdelkov opredeljena kot živilo[1] zato je potrebno neprekinjeno omogočati tok vode kot splošne dobrine[2].

Odkar so okoljevarstveni delavci po svetu začeli širili zgodbo o minljivosti vodnih resursov, je voda postala poleg energije geopolitično najpomembnejša surovina za življenje, delo in obstoj sodobne civilizacije. Postavlja se temeljno vprašanje: Kaj če nam zmanjka vode? Kaj narediti, da do tega ne pride? V zahodnem svetu so se z dvigom okoljske kulture, zmanjšala okoljevarnostna tveganja. Okoljevarnostna tveganja glede vode so ostala predvsem v tretjem svetu, kjer zelo hitro narašča število prebivalcev in močna industrializacija teh območij. V spremenjenih varnostnih razmerah po svetu, pa je voda postala morda najbolj pomembno varnostno vprašanje sodobnega sveta. Zato se moramo kot sodobna družba vprašati, kaj vse moramo ukreniti, da se zavaruje vodne vire pred terorističnimi in okoljskimi nevarnostmi ter varnostnimi tveganji.

Pravne podlage

Republika Slovenija je z vstopom v EU, sprejela zavezo po implementaciji direktiv Sveta Evrope. Samega pomena zdrave in varne oskrbe s pitno vodo se zaveda tudi Evropska komisija. Svet EU je leta 1998 sprejel Direktivo o kakovosti vode[3], namenjene za prehrano ljudi, ki določa cilje varovanja zdravja ljudi pred škodljivimi vplivi vsakršnega onesnaženja vode, namenjene za prehrano ljudi. Država Republika Slovenija je sprejela vrsto zakonskih in podzakonskih predpisov, kjer ureja vse v zvezi z vodami. Iz Zakona o varstvu okolja[4] je oskrba s pitno vodo opredeljena

Preko ozemlja Republike Slovenije se letno pretoči neverjetnih 34 milijard m^3 vseh vrst voda. Iz tega izhaja, da je naša država med najbolj bogatimi deželami z vodnimi viri v Evropi.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

kot obvezna občinska gospodarska javna služba varstva okolja. Občina mora zagotoviti izvajanje javne službe oskrbe s pitno vodo skladno s predpisi vlade, ki so navedeni v tem odstavku in s predpisi, ki urejajo gospodarske javne službe. V Zakonu o vodah[5] država določa pogoje glede vodovarstvenih območij in pridobivanja vodnih pravic v primeru rabe vode. Izvajalec obvezne lokalne javne službe oskrbe s pitno vodo označi območje zajetja pitne vode. Vodno pravico je mogoče pridobiti na podlagi vodnega dovoljenja ali koncesije. V Uredbi o oskrbi s pitno vodo[6], kot izvedbenem aktu, so določene vrste nalog, ki se izvajajo v okviru storitev obvezne občinske gospodarske javne službe oskrbe s pitno vodo, in nekatere pogoje za oskrbo s pitno vodo, ki se izvaja kot javna služba, ter za lastno oskrbo s pitno vodo. V Pravilniku o pitni vodi[7] so določene zahteve, ki jih mora izpolnjevati pitna voda, z namenom varovanja zdravja ljudi pred škodljivimi učinki zaradi kakršnegakoli onesnaženja pitne vode. Na podlagi druge Direktive SE o ugotavljanju in določanju evropske kritične infrastrukture[8] v Sloveniji, se določa postopek za ugotavljanje in določanje evropske kritične infrastrukture v Republiki Sloveniji. Zato je naša država sprejela Uredbo o evropski kritični infrastrukturi[9], s katero se ureja evropska kritična infrastruktura na vrsti sektorjev in podsektorjev.

Vodovodna infrastruktura kot kritična infrastruktura

Preko ozemlja Republike Slovenije se letno pretoči neverjetnih 34 milijard m^3 vseh vrst voda. Iz tega izhaja, da je naša država med najbolj bogatimi deželami z vodnimi viri v Evropi. Z Avstrijo in z Madžarsko ni ne prodaje ne nakupa vode, medtem ko s Hrvaško in Italijo poteka tako nakup, kot prodaja manjših količin vode. V Republiki Sloveniji se oskrbuje s pitno vodo iz javnih vodovodnih sistemov 1,8 milijona prebivalcev oziroma kar 88 % vsega prebivalstva v skupaj 2718 naseljih. Po uradnih podatkih je dolžina vsega vodovodnega omrežja v letu 2012 znašala 21.757 kilometrov. Od tega je okrog 2000 km cevovodov starejših od 50 let. V tem letu je bilo na območju Republike Slovenije načrpanih 169 milijonov m^3 vode, od katerih je bilo 123 milijonov m^3 načrpanih iz podzemnih virov, 38 milijonov iz tekočih voda in skoraj 8 milijonov m^3 iz drugih virov. Število javnih vodnih zajetij na podlagi izdanih vodnih dovoljenj je 1726. Na tej podlagi je dovoljeno na leto odvzeti do 470 milijonov m3 oziroma 12.440 litrov vode na sekundo. Povprečna poraba vode na prebivalca znaša 91 m3 vode na leto oziroma 249 litrov vode na dan. Od tega so vsa gospodinjstva porabila 85 milijonov m^3 vse načrpane pitne vode, na eno odjemno mesto pa je evidentiranih 3,74 prebivalca. Oskrbovanih je okrog 490.000 odjemnih mest. Na območju države se manj kot 50% prebivalstva oskrbuje iz javnega vodovodnega omrežja. Na območju 18 občin, pa se vsi prebivalci oskrbujejo iz javnega vodovodnega omrežja. V letu 2012 pa je bilo kemijskemu oziroma mikrobiološkemu onesnaženju izpostavljeno še zmeraj okrog 390.000 prebivalcev. Ob tem je bilo izven nadzora izvajalcev javnih služb, še zmeraj 234.000 vseh prebivalcev Slovenije. Z lastno oskrbo izven vodovodnih omrežij se v Sloveniji oskrbuje 163.000 prebivalcev. Cilj državnega operativnega programa oskrbe s pitno vodo je bil le še 50.000 prebivalcev. V državi še danes evidentiramo 20.469 zasebnih vodnih zajetij, kjer je dopusten odjem 7,5 milijona m^3 vode na letnem nivoju. V letu 2014 je bilo v državi 317 zasebnih vodovodov, kjer se je izvajala oskrba za več kot 50 ljudi in 878 lokalnih vodovodnih sistemov, kjer se je oskrbovalo manj kot 50 prebivalcev z manj kot 10 m^3 oskrbe vode.

Sistem vodovodnega omrežja z objekti in napravami v upravljanju Mariborskega vodovoda je največji enovit vodooskrbni sistem v državi. Mariborski vodovod je v lasti 19 lokalnih skupnosti in v 16 izvaja javno službo distribucije in oskrbe s pitno vodo. V upravljanju je 1607 kilometrov vodovodnega omrežja, s 302 objekti in napravami ter 7450 hidranti, za zagotavljanje osnovne požarne varnosti. Mariborski vodovod kot izvajalec javne službe načrpa 13 milijonov m^3 pitne vode. Oskrba se izvaja za dobrih 200.000 prebivalcev v 212 naseljih, kjer na letnem nivoju distribuiramo, do končnih uporabnikov, na 50.000 odjemnih mestih, 10 milijonov m^3 pitne vode. Na sis-

Problematika pri upravljanju z infrastrukturo posebnega družbenega in državnega pomena je, da Mariborski vodovod kot največji regionalni vodovod v državi ni vključen v EU in državne načrte varovanja vodovodne infrastrukture, kot del kritične infrastrukture posebnega družbenega pomena.

Večje varnostno tveganje je v večjih urbanih središčih, ki so zelo bogato opremljeni s komunalno infrastrukturo in s tem z vodovodno infrastrukturo. Zaradi razpršenosti javnega omrežja, objektov in naprav za distribucijo vode, pa so ti objekti praviloma fizično in tehnično nezavarovani.

tem daljinskega odčitavanja je priključenih 129 objektov. Celotna vrednost opreme in objektov znaša 1.584.000 €, stroški amortizacije znašajo 205.884 €, stroški varovanja pa znašajo 10% amortizacije in so v višini zgolj 20.558 €. Vsi stroški za varovanja na sedežu podjetja znašajo 58.351 €.

Problematika pri upravljanju z infrastrukturo posebnega družbenega in državnega pomena je, da Mariborski vodovod kot največji regionalni vodovod v državi ni vključen v EU in državne načrte varovanja vodovodne infrastrukture, kot del kritične infrastrukture posebnega družbenega pomena. Na drugi strani lokalne skupnosti kot lastniki vodovodne infrastrukture, namenjajo zelo malo sredstev v samo vzdrževanje infrastrukture. Najmanj sredstev pa skozi proračunska sredstva namenijo varovanju in zaščiti lastnega premoženja vodovodne infrastrukture. Mariborski vodovod ima sprejete vse potrebne dokumente za varovanje in delovanje v primeru izrednih razmer in neskladnosti delovanje sistema. Vrste nalog, ki jih Mariborski vodovod kot izvajalec zagotavlja in izvaja, občine niso pripravljene plačevati. Kot izvajalec zagotavljamo notranji nadzor HACCP, stalno nadgrajujemo „Načrt zaščite in reševanja oziroma delovanja v primeru izrednih razmer in neskladnosti“. Izdelano imamo „Navodilo za ravnanje v izrednih razmerah“, kjer so opredeljeni namen, odgovornosti, način dela in prepoznavanje nevarnosti. Izdelan imamo tudi „Varnostni načrt upravljalca“, izvedbeno „Navodilo za izvajanje fizičnega varovanja premoženja družbe“, „Sistem upravljanja varovanja informacij - SUVI“. V podjetju Mariborski vodovod v celoti obvladujemo poslovna in okoljska tveganja kot tudi varnostno politiko. Imamo definirano ciljno vodenje in permanentno zagotavljamo primerno stopnjo varnostne kulture. Sama korporativna varnost v našem podjetju presega fizično in tehnično varnost, saj redno izvajamo neprekinjeno delovanje z vso potrebno informacijsko varnostjo. Varujemo poslovne skrivnosti in izvajamo politiko integriranega sistema.

Vsi navedeni empirični podatki za količine načrpane vode, odjemna mesta, javnih in lokalnih vodovodnih sistemov in rabo vode, pričajo o tem, da je Republika Slovenija zelo bogata z vodnimi viri. Iz dolžine javnega vodovodnega omrežja, ki je v upravljanju izvajalcev, lahko rečemo, da je tudi izgrajeni sistem oskrbe s pitno vodo, zelo dobro razvit. Gledano iz varnostnega vidika je večje število javnih in nejavnih vodooskrbnih sistemov manj izpostavljeno varnostnim tveganjem. Večje varnostno tveganje je v večjih urbanih središčih, ki so zelo bogato opremljeni s komunalno infrastrukturo in s tem z vodovodno infrastrukturo. Zaradi razpršenosti javnega omrežja, objektov in naprav za distribucijo vode, pa so ti objekti praviloma fizično in tehnično nezavarovani. Občine kot lastniki, namreč nimajo in niso pripravljene, zagotoviti dovolj sredstev za zagotovitev vsaj minimalnih varnostnih standardov.

Razlaga za in proti umestitvi vodovodne infrastrukture med kritično infrastrukturo

V luči varnostno političnih in kulturnih sprememb v EU, je ranljivost vodovodne infrastrukture Mariborskega vodovoda izpostavljena tveganjem državnega, čezmejnega, regionalnega in lokalnega pomena. Mariborski vodovod je v svojih dokumentih določil ogroženost in ranljivost vodovodnega sistema v upravljanju, javnega podjetja za izvajanje gospodarske javne službe oskrbe s pitno vodo. V tem delu zagotavljamo obvladovanje vseh vrst tveganj, ki bi lahko nastale v Mariborskem vodovodu. Ločimo posredni in tudi neposredni vpliv na samo vodovodno infrastrukturo. Kot izvajalec, moramo prednostno zagotavljati neprekinjeno štiriindvajseturno oskrbo vsega prebivalstva. Danes smo izvajalci javne oskrbe s pitno vodo v Slovenji le najemniki vodovodne infrastrukture. Na podlagi državnih predpisov, nakazujemo najemnino v proračune lokalnih skupnosti. S prenosom vse amortizacije leta 2010 na občine, se je začelo obdobje bistveno premajhnih vlaganj v objekte, naprave in vodovodno omrežje. Najmanj ali nič so občine kot lastniki pripravljene vlagati v varnostni vidik oskrbe s pitno vodo. Zavedanje resnosti groženj v luči migracij in terorizma zagotovo pri obči-

nah narašča, vendar je neodgovorno zavedanje, da se to pri nas ne more zgoditi. Fizična in tehnična varnost vodovodne infrastrukture je eden ključnih temeljev za delovanje vodovodnega sistema. V Mariborskem vodovodu namenjamo posebno pozornost ogroženosti in ranljivosti vodovodne infrastrukture. Pri tem so ključni elementi ogrožanja zaznani v primeru naravnih nesreč, onesnaženju vode z industrijskimi nesrečami, terorizmu, kibernetskemu terorizmu in vojnim razmeram v naši bližini, ekološki kriminaliteti ter kaznivim dejanjem in vrsti drugih malomarnih dejanj internega značaja.

Varnost oskrbe s pitno vodo zahteva celovit pristop zagotavljanja zadostnih količin vode, upravljanja s prispevnimi površinami ter ustrezno upravljanje z vodovodnim sistemom, od vira do uporabnika. Za zagotavljanje ustrezne kakovosti pitne vode je potrebno dosledno izvajanje in zagotavljanje vodovarstvenih režimov na prispevni površini, ustrezno čiščenje vode na vstopu v vodovodni sistem ter ohranjanje kvalitete vode do uporabnika. Varnost oskrbe s pitno vodo, tako kakovosti kot količin, se zagotovi tudi z izgradnjo rezervnih virov. Ob tem je potrebno varovati pitno vodo pred vsemi vrstami onesnaženja. To se zagotavlja s splošnim pravnim ukrepom za varstvo zajetij pitne vode in uveljavljanje vodovarstvenih območij (VVO) na prispevni površini zajetja. V zajetjih za pitno vodo je potrebno zagotoviti zdravstveno ustrezno pitno vodo in s tem povečati varnost oskrbe s pitno vodo na območjih javnih vodovodov.

vajalci oskrbe s pitno vodo odvedejo 56 mio € vodnega povračila državi za vsak načrpan m3 vode, ki naj bi služil investicijam in investicijskemu vzdrževanju objektov. Država nalaga lokalnim skupnostim za 281 mio € stroškov za doseganje ciljev iz tega programa in izvedbo ukrepov.

Republika Slovenija je na podlagi Direktive SE o ugotavljanju in določanju evropske kritične infrastrukture leta 2014 sprejela veljavni kriterij kritičnosti državnega pomena in po opredeljenih sektorjih spada voda šele pod četrti sektor kritične infrastrukture. Mnenja smo, da bi morali biti objekti, naprave in vodovodna omrežja infrastruktura posebnega družbenega pomena, navedena kot kritična infrastruktura.

Za delovanje vodovodnega sistema je fizična in tehnična varnost vodovodne infrastrukture eden od ključnih temeljev. Skrajno neodgovorno je zavedanje lastnikov infrastrukture – lokalnih skupnosti, da smo varni pred grožnajmi s strani migracij in terorizma. Menimo, da se moramo začeti zavedati te nevarnosti in ukrepati preden bo prepozno.

Najmanj ali nič so občine kot lastniki pripravljeni vlagati v varnostni vidik oskrbe s pitno vodo. Zavedanje resnosti groženj v luči migracij in terorizma zagotovo pri občinah narašča, vendar je neodgovorno zavedanje, da se to pri nas ne more zgoditi.

Zaključek

Do leta 2020 bi morali po operativnem programu oskrbe zamenjati 36% vsega vodovodnega omrežja v ocenjeni vrednosti 1183 mio €. Vse sanacije in investicije v vodovodno infrastrukturo bi po tem operativnem programu morale zagotoviti izključno občine. Prav tako so stroški iskanja novih vodnih virov prenešeni izključno na občine, čeprav izvajalci oskrbe s pitno vodo odvedejo 56 mio € vodnega povračila državi za vsak načrpan m3 vode, ki naj bi služil investicijam in investicijskemu vzdrževanju objektov. Država nalaga lokalnim skupnostim za 281 mio € stroškov za doseganje ciljev iz tega programa in izvedbo ukrepov.

[1] Canned tomatoes are considered adulterated, in accordance with section 402(b)(4) of the Federal Food, Drug, and Cosmetic Act, if they bear any added water.

[2] Zakon o zdravstveni ustreznosti živil in izdelkov ter snovi, ki prihajajo v stik z živili (Ur. List RS, št. 52/00, 42/02 in 47/04-ZdZPZ).

[3] Direktiva Sveta EU o kakovosti vode 98/83/ES z dne 3.11.1998 (UL L 330, 5.12.1998).

[4] Zakon o varstvu okolja (ZVO-1, Ur. list RS, št. 41/04, 17/06-ORZVO187, 20/06, 28/06-Skl. US, 49/06-ZMetD, 66/06-Odl. US, 33/07-ZPNačrt, 57/08-ZFO-1A, 70/08, 108/09, 48/12, 57/12, 92/13, 38/14).

[5] Zakon o vodah (ZV-1, Ur. list RS, št. 67/02, 110/02-ZGO-1, 2/04-ZZdrI-A, 10/04-Odl. US, 41/04-ZVO-1, 57/08, 57/12, 100/13, 40/14, 56/15).

[6] Uredba o oskrbi s pitno vodo (Ur. list RS, št. 88/12).

[7] Pravilnik o pitni vodi (Ur. list RS, št. 19/04, 35/04, 26/06, 92/06, 25/09).

[8] Direktiva Sveta (ES) št. 114/2008 z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite (UL L št. 345/75 z dne 23. 12. 2008, str. 77.

[9] Uredba o evropski kritični infrastrukturi (Ur. List RS, št. 35/11). ■

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

KRITIČNA INFRASTRUKTURA ELEKTRO-ENERGETSKEGA SEKTORJA IN POMEN OCENJEVANJA GROŽENJ

Dejstvo, da je moderna družba danes v celoti odvisna od delovanja tehnologije, to družbo z varnostnega stališča dela še bolj ranljivo. Določeni segmenti infrastrukture, zlasti sektor električne energije, so tako pomembni za delovanje družbe, da bi njihovo nedelovanje ali omejeno delovanje lahko imelo resne posledice ali povzročalo resne težave za to družbo.

Varnost je za razvoj posameznika in družbe nujno potrebna dobrina. Globalizacija sveta in s tem posredno globalizacija varnosti, moderno družbo postavlja pred zahtevne dileme in sicer kako še naprej svoj razvoj temeljiti na osnovnih postulatih prostega pretoka blaga, storitev, financ in ljudi. Na drugi strani pa se pojavlja potreba kako grožnje obvladovati na sprejemljivem nivoju tveganja. Pojav asimetričnih oblik ogrožanja nacionalne in mednarodne varnosti izhaja iz popolnoma drugih predpostavk in dojemanj osnovnih konceptov zagotavljanja varnosti. Spreminjajoče družbene razmere in napetosti, ki jih je prinašal nagel tehnološki razvoj, so posamezna družbena okolja in sredine našle popolnoma nepripravljene na soočanje z novo globalno varnostno situacijo in predvsem z na novo porajajočimi kompleksnimi varnostnimi grožnjami. Dinamične spremembe in nesluten tehnološki razvoj sta tej dimenziji dodala še kompleksnejšo obliko.[1]

Električno omrežje se z razvojem tehnologije pametnih in mikro omrežij, povečano uporabo obnovljivih virov energije ter porazdeljene proizvodnje električne energije, zelo hitro spreminja. Informatizacija prinaša možnost za izgradnjo varnejšega, bolj prožnega in učinkovitejšega omrežja. Hkrati pa je vedno bolj pomemben proces zaznavanja specifik pri zapletenem delovanju teh sistemov. Zaradi razpršene narave omrežja je le ta postal občutljiv na cel niz fizičnih, kibernetskih in tudi drugih groženj, ki jih pred nas postavlja okolje. Poleg tega ta mrežna povezanost in soodvisnost pri delovanju sistema pomeni, da lahko že majhen in dobro izbran napad ali varnostni incident povzroči kaskadno reakcijo in posledično razpad tega sistema. Vendar pa nam na drugi strani ravno ta medsebojna povezanost omrežja omogoča, da se ob ustreznih ukrepih zagotavlja tudi ustrezna stopnja odpornosti tega sistema.[2]

Električno omrežje se z razvojem tehnologije pametnih in mikro omrežij, povečano uporabo obnovljivih virov energije ter porazdeljene proizvodnje električne energije zelo hitro spreminja.

Zapletenost globalnega varnostnega okolja prinaša tudi vrsto tveganj in groženj, ki jim je izpostavljen današnji elektroenergetski sektor. Sposobnost odzivanja na razvijajoče se grožnje, ki vplivajo na okolje električne kritične infrastrukture, mora biti ravno zaradi tega stalno potekajoč proces. Nemogoče je pričakovati, da bomo z določenimi ukrepi v celoti odpravili grožnje in tveganja za delovanje te kritične infrastrukture. Zaradi navedenega je ključno pravilno razumevanje in stalno ocenjevanje groženj in tveganj, ki jih za neprekinjeno delovanje električne kritične infrastrukture predstavljajo subjekti ogrožanja. Temu procesu se mora posvetiti celotna strokovna javnost, tako tista, ki je od-

*avtor je član Slovenskega združenja korporativne varnosti

govorna neposredno za delovanje posamezne kritične infrastrukture, kakor tudi širša javnost, ki v družbenem okolju zagotavlja ustrezne predpogoje za varno delovanje družbe kot celote.

Trenutno v Evropski uniji poteka pomemben raziskovalni projekt s področja zaščite električne kritične infrastrukture, ki je financiran v okviru raziskovalnega mehanizma HORIZONT H2020. Naziv projekta je »Defending the European Energy Critical Infrastructure« ali krajše DEFENDER.[3] V konzorciju partnerjev sodelujejo Francija, Grčija, Italija, Izrael, Nemčija, Portugalska, Romunija, Velika Britanija in Slovenija. Med partnerji iz Slovenije poleg Instituta za korporativne varnostne študije sodelujeta še Institut Jozef Stefan in ELES d.o.o.

Kako pomembno je razumevanje dinamičnega varnostnega okolja za nemoteno delovanje energetske kritične infrastrukture kaže tudi dejstvo, da bi bila za temelj nadaljevanja projekta izdelana celovita študija z oceno obstoječih groženj in tveganj, ki vplivajo in bodo tudi v prihodnje imele pomemben vpliv na delovanje te infrastrukture.

Konzorcij DEFENDER se je osredotočil na celoten spekter groženj, ki jih ni analiziral izolirano v smeri vpliva samo na energetsko kritično inftrastrukturo. Kompleksna analiza je bila usmerjena v raziskavo, kako določene grožnje vplivajo na posamezne domene znotraj proizvodnje, prenosa, distribucije in uporabe električne energije ter kakšen vpliv imajo le te v procesu soodvisnosti delovanja med sektorji različne kritične infrastrukture. Glede na dejstvo, da ima sektor električne energije centralno težišče pri vplivu na delovanje ostalih podsektorjev kritične infrastrukture, je bil ta proces izrednega pomena za ustrezno razumevanje delovanja celovitega sistema.

Naslednjim tveganjem projekt namenja še posebno pozornost:
- tveganja fizični varnosti in odpornosti;
- tveganja, ki jih prinašajo naravne nesreče in odpornost proti podnebnim spremembam;
- tveganja, ki izhajajo iz staranja infrastrukture in tveganja nizkih naložb v infrastrukturo;
- tveganja kibernetski varnosti;
- tveganja, ki jih v predikcijah prinaša vrzel pri razvoju strokovne delovne sile.

Nemogoče je pričakovati, da bomo z določenimi ukrepi v celoti odpravili grožnje in tveganja za delovanje te kritične infrastrukture. Zaradi navedenega je ključno pravilno razumevanje in stalno ocenjevanje groženj in tveganj, ki jih za neprekinjeno delovanje električne kritične infrastrukture predstavljajo subjekti ogrožanja.

Sistemi za proizvodnjo električne energije, prenos in distribucijo so dovzetni za fizične napade. Na drugi strani je tveganje za storilce takih dejanj relativno majhno. Posebne točke ranljivosti ob fizičnih ali terorističnih napadih je mogoče bolje razumeti z upoštevanjem vsakega pomembnejšega elementa energetskih sistemov: generatorjev, postaj, prenosnih stolpov, cevi zemeljskega plina, komponent distribucije in centrov za nadzor sistema. Dogodki, povezani z vremenom, vključno s strelami pri nevihti, so bili v preteklosti največja grožnja za nemoteno delovanje električnega sistema. Naravne nesreče, kot so poplave, potresi, gozdni požari in drugi, lahko pomembno vplivajo na prenosno in distribucijsko omrežje ter zanesljivost elektroenergetskih omrežij. Čeprav so sistemi za proizvodnjo, prenos in distribucijo energije zasnovani tako, da se odzivajo na variabilnost vremenskih razmer, kot so dnevne spremembe temperature, je električna infrastruktura še kako izpostavljena neposrednim vplivom hudih vremenskih dogodkov in ekstremnih naravnih nesreč. Številna kritična infrastrukturna sredstva v evropskih državah so dosegla ali se približujejo koncu načrtovanega življenjskega obdobja. Zlasti v primeru prenosnih in distribucijskih omrežij električne energije so nove investicije in prenova zelo drage, običajno zahtevajo dolgo dobo načrtovanja in vključujejo vplive vseh zainteresiranih strani, javno politiko in težave v zvezi z gradnjo. Kibernetske grožnje energetski infrastrukturi predstavljajo vse večji varnostni izziv, ki lahko vpliva na evropsko varnost. Kibernetske grožnje razumemo kot možnost zlonamernega poskusa poškodovanja ali prekinitve informacijskih omrežij ali sistemov. Zasebni sektor ima v lasti in upravljanju večino sredstev in omrežij

energetske infrastrukture, vlade pa so na drugi strani odgovorne za nacionalno varnost. To pomeni, da je preprečevanje groženj skupna odgovornost javnega in zasebnega sektorja, kar pa je mogoče samo ob vzpostavitvi trdnega in dobro delujočega javno-zasebnega partnerstva. Kadrovski potencial je pomembna grožnja nemotenemu delovanju te infrastrukture. Tveganja se pojavljajo tako zaradi neučinkovitosti, malomarnosti ali namernih dejanj, kakor tudi pomanjkanja usposobljenega kadrovskega potenciala. Večjo vrzel razpoložljivega kadra v energetskem sektorju predstavljajo upokojitve delovne sile, ki je že nekaj časa zaskrbljujoča. Predvideva se, da bo velik odstotek strokovnjakov v naslednjih nekaj letih upravičen do upokojitve. Ravno ta zamenjava generacij in prenosa strokovnih izkušenj, ter znanj, na nove generacije kvalificiranih delavcev bo izziv, na katerega prepogosto pozabljamo.

Vse to so izzivi, s katerimi se bo potrebno na področju celovitega obvladovanja tveganj, za nemoteno delovanje energetske kritične infrastrukture, v prihodnosti aktivno spopasti in jih upoštevati pri nadaljnjem razvoju. Rezultati projekta DEFENDER bodo vsekakor odločevalcem in strokovni javnosti v pomembno pomoč.

[1] Čaleta, D. (2011). A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership. In: Čaleta, D. & Paul Shemella (Eds.). Counter terrorism challenges regarding the process of Critical Infrastructure Protection (pp. 15-26). Ljubljana, Monterey: ICS, Centre for Civil Military Relations.

[2] CSPC (2014). Project-Securing the U.S. Electrical Grid, https://www.thepresidency.org/sites/default/files/Final%20Grid%20Report_0.pdf, accessed, 5 July 2017, str. 60.

[3] Več informacij o projektu DEFENDER na www.defender-project.eu. ■

POSVET

NADZOR NA DELOVNEM MESTU

26. september 2018, Ljubljana

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

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

www.planetgv.si

www.ics-institut.si

ORGANIZATORJA POSVETA

PLANET GV

ICS
Institut za korporativne varnostne študije

BREZPLAČNA ŠTEVILKA
080 33 44

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Dušan Sofrič, Vodja službe za varnost in zaščito v družbi Fraport Slovenija

VARNOSTI LETALIŠČ POSVEČENA POSEBNA POZORNOST

Letališče Jožeta Pučnika je naše največje in najpomembnejše letališče. O varnostnih izzivih obvladovanja tveganj v tako zahtevnem okolju smo se pogovarjali z g. Dušanom Sofričem.

Korporativna varnost na letališčih je zelo pomembna nit vaše poslovne kariere. Nam lahko poveste katera so ključna področja pristojnosti, ki ste jih v svoji bogati karieri konkretno izvajali?

V osnovi lahko rečem, da sem z varnostjo in letalstvom povezan praktično že od samega pričetka svoje kariere. V tem času sem bil ali pa sem še vedno odgovoren za velik del varnostnih funkcij. Moje sedanje odgovornosti oz. pristojnosti bi najlažje razdelil na aktivnosti povezane s področjem varovanja civilnega letalstva in varovanjem *(Security),* s področjem varnosti *(Safety),* ki jo v letalstvu ločujemo od varovanja, s področjem protipožarne varnosti, s področjem obrambnega načrtovanja in varovanja tajnih podatkov, s področjem varstva pred sevanji ter načrtovanje postopkov v sili. V preteklosti pa sem bil pristojen tudi za področje varstva osebnih podatkov, za področje varstva in zdravja pri delu, zaščite letališča pred pticami in še kaj bi se našlo.

Varnost letališč, kot zelo pomemben del transportne infrastrukture, je bila vseskozi še dodatno regulirana. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Če pogledamo samo dobre pol stoletja nazaj, lahko ugotovimo, da varnost letališč oz. civilnega letalstva sploh ni bila posebej regulirana. Na mednarodni ravni se je to pričelo dogajati v šestdesetih in sedemdesetih letih prejšnjega stoletja v okviru mednarodne organizacije za civilno letalstvo s sprejetjem Tokijske, Haške in Montrealske konvencije ter aneksom 17 k Čikaški konvenciji. Dodatna regulacija je bila odziv na naraščajoči trend ugrabitev letal in drugih terorističnih dejanj zoper civilno letalstvo. Danes je slika popolnoma drugačna, še posebej po terorističnih napadih 11. septembra 2001, v katerih so bila letala

*avtor je član Slovenskega združenja korporativne varnosti

prvič uporabljena kot orožje za množično uničenje. Upam si trditi, da je letalski promet danes eden bolj reguliranih in nadzorovanih gospodarskih sektorjev, posledično je tako regulirano tudi varovanje civilnega letalstva.

V tem kontekstu je potrebno gledati tudi na obvladovanje tveganj, ki je nemalokrat upoštevano že v samih predpisih, seveda pa je zaradi posebnosti posameznega letališča ter ogroženosti posameznih držav potrebno upoštevati tudi druge varnostne grožnje in jih vključiti v ustrezne načrte za obvladovanje tveganj. Družba kot taka, pa ni izpostavljena samo varnostnim tveganjem. Tveganj, katerim je neka organizacija izpostavljena, je precej več, zato smo v družbi že pred leti izdelali matriko tveganj za vsa področja poslovanja ter opredelili ukrepe za zagotovitev neprekinjenega poslovanja.

Se je s spremembo lastništva našega največjega letališča in prihodom novega lastnika ta raven pomena zagotavljanja varnosti kaj spremenila?

Novi lastnik je seveda prinesel določene spremembe tako v organiziranosti kot poslovanju, spremenil je status družbe, prilagodil nekatere poslovne procese, predvsem tiste povezane s finančnim področjem, implementiral svojo politiko skladnosti poslovanja in obvladovanja tveganj. Določene prilagoditve še vedno potekajo, kar pa zadeva zagotavljanje varnosti lahko rečem, da se njen pomen ni prav nič zmanjšal, prej nasprotno. Matična družba Fraport AG je eden največjih upravljavcev letališč na svetu in letališče Ljubljana je tako dobilo strateškega lastnika, kateremu je upravljanje letališč osnovna dejavnost. Novi lastnik je tako dodobra seznanjen s kompleksnostjo varovanja letališč in civilnega letalstva in veseli nas, da so znanje in izkušnje zbrane znotraj skupine dosegljive in na razpolago tudi nam. Morda na tem mestu ni odveč omeniti, da smo v družbi Fraport Slovenija, zagotavljanje učinkovitega in varnega obratovanja največjega slovenskega letališča zapisali tudi v naše poslanstvo.

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

Če pustimo ob strani vse strokovne izzive, je to na poslovni ravni verjetno eden težjih izzivov, s katerim se soočamo varnostni menedžerji. V letalstvu smo,

za razliko od nekaterih drugih dejavnosti, morda v rahli prednosti, kar zadeva našo »izhodiščno pogajalsko pozicijo«. Kot sem že poprej omenil, gre za zelo regulirano dejavnost, tako je npr. služba varovanja kot ena izmed obveznih letaliških služb, predpisana že v Zakonu o letalstvu. S tega vidika lahko rečem, da so nam nacionalni in mednarodni predpisi v veliko oporo. Pa tudi, če odmislimo zakonodajne predpise, lahko rečem, da se poslovodstvo družbe zaveda pomembnosti potrebnih sistemskih ukrepov za obvladovanje varnostnih tveganj in posledično temu tudi namenja in zagotavlja potrebna finančna sredstva.

Pri svojem delovanju imate pomembne specifike, ki jih je potrebno ves čas usklajevati z različnimi deležniki, ki nastopajo v zagotavljanju nacionalne in mednarodne varnosti. Kakšne izkušnje imate s pripravljenostjo partnerjev kot so Policija, Slovenska vojska in drugi pri sodelovanju zagotavljanja varnosti na Letališču Brnik.

Lepo in prijetno je delati v okolju, kjer se odgovorni zavedajo svoje vloge in se vključujejo ter sooblikujejo varnostno politiko. Kaj sem s tem mislil, najbolje ponazorim, če rečem, da smo vsi pomembnejši subjekti, ki pokrivamo posamezna področja in varnostna tveganja na letališču, člani letališkega sveta za varovanje civilnega letalstva, kjer celovito obravnavamo aktualno varnostno problematiko, se seznanjamo z oceno ogroženosti letališča, novostmi, trendi itd. Člani sveta prihajajo iz vrst Postaje letališke policije Brnik, FURS Sektor za carine - letališče Brnik, varnostne službe, Slovenske vojske, Kontrole zračnega prometa Slovenije, letalskega prevoznika Adrie Airways, dobavitelja letalskih goriv Petrola in ARSO sektorja za operativne meteorološke napovedi. Svet se sestaja najmanj enkrat letno, po potrebi tudi večkrat. Svet je za razreševanje posameznih strokovnih vprašanj imenoval stalno komisijo za varnost, ki se ukvarja izključno z izzivi, ki neposredno vplivajo na varnost civilnega letalstva. Varnostna komisija se sestaja pogosteje in jo sestavlja ožji krog prej omenjenih članov Sveta. Torej izkušnje so dobre in ob tej priložnosti vsem našim partnerjem lahko za dosedanje sodelovanje izrečem le veliko zahvalo.

Letalski sektor je po vseh podatkih v stalni ekspanziji glede števila potnikov in je vedno bolj odvisen od varnosti. Ali bi lahko ocenili, da bo v prihodnje zagotavljanje učinkovite varnosti postalo konkurenčna prednost posameznih letališč in posledično tudi turističnih destinacij?

Načeloma imate prav, ko pravite, da je letalstvo vedno bolj odvisno od varnosti, vendar pa pri tej odvisnosti ne gre primarno za varnost samih letališč, gre bolj za varnost celotne regije ali pa države, v kateri se samo letališče nahaja. Npr. v Evropi imamo na področju varovanja civilnega letalstva minimalne standarde, ki pa so, gledano na svetovni ravni, zelo visoki in so tudi strogo nadzorovani s strani številnih institucij in organizacij. Takšen sistem nam omogoča, da po vseh letališčih, ki izpolnjujejo zahtevane standarde, velja koncept »One Stop *Security*«, ki potnikom, kateri potujejo znotraj EU ali pa tudi širše, ponuja bolj prijazno potovalno izkušnjo. V praksi to pomeni, da če potujete iz kateregakoli letališča v EU in morate do končne destinacije prestopati, vam na nobenem transfernem letališču ne bo več potrebno opraviti ponovnega varnostnega pregleda, kar pomeni manj čakanja, manj izgubljenega časa, možnost hitrejšega prestopanja, itd. Seveda takšen sistem prinaša prednosti tudi letalskim družbam in letališčem, saj nam omogoča boljšo in hitrejšo povezljivost letalskih linij.

Kaj v praksi lahko pomeni (ne)učinkovita varnost na letališčih oz. regiji in kakšen uničujoč učinek ima lahko le ta na turistično dejavnost, pa je eden bolj nazornih primerov Egipt in resort Sharm El Sheikh. Njihova atraktivnost, kot turistična destinacija, je po terorističnem napadu na letalo ruske letalske družbe Metrojet, drastično padla. Številne države, kot npr Rusija in Velika Britanija so prepovedale lete v to regijo, številne letalske družbe pa so ukinile lete na letališče Sharam El Sheikh. Dogodek, ki se je zgodil pred dobrima dvema letoma, je imel in še vedno ima strahovite posledice za celoten turizem v tej regiji in posledično tudi za samo letališče. Število potnikov na letališču je v letu 2016 upadlo za skoraj 70% v primerjavi z letom poprej, nekdaj živahno letovišče pa je danes videti bolj kot mesto duhov.

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?

Odvisno od tega, kako široko gledamo in katera podjetja imamo v mislih. Razlike med tistimi z zavedanjem in brez, so namreč velike. Velika večina družb v tuji lasti, vsekakor pa ne vse, ki delujejo v Sloveniji, imajo to rešeno že sistemsko. Družbe posebnega pomena za državo, ki so bile kot take opredeljene s sklepom Vlade RS ali pa so del kritične infrastrukture, po mojem vedenju tako ali drugače zagotavljajo potrebne kadrovske in finančne resurse ter ustrezno obvladujejo tveganja, saj jih v to nemalokrat silijo že predpisi. Potem pa imamo nekaj podjetij, ki ne spadajo v prvi dve skupini, vendar je zavedanje pomembnosti korporativne varnosti in njihovo obvladovanje tveganj na zelo visokem nivoju. Za to skupino podjetij velja, da največkrat nastopajo na globalnem trgu. V zadnjo skupino pa bi lahko uvrstili vsa ostala podjetja izven tega kroga. Nekatera se sicer zavedajo, da obvladovanje varnostnih tveganj zahteva posebno pozornost in to poskušajo reševati z nesistemskimi pristopi. Največkrat to rešujejo s pomočjo zasebnih varnostnih služb in tem ne zaupajo le operativnih nalog, temveč tudi tiste, ki sodijo v domeno korporativne varnosti. Pri tem pa ne bi smeli pozabiti, da zasebne varnostne službe tekmujejo na trgu in jih tako kot ostale poslovne subjekte vodi skrb za lastni dobiček.

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

Verjamem, da so izobraženi, sposobni in motivirani kadri gonilo in prihodnost vsakega podjetja. V naši družbi področju internega usposabljanja namenjamo veliko pozornost. V to nas nenazadnje silijo že predpisi, standardi in sistemi kakovosti, katere smo tekom let vpeljali v družbi. Da bi lahko zadostili vsem zahtevam in bili kar najbolj učinkoviti, smo že pred leti ustanovili lastno letalsko šolo, ki je pridobila vse ustrezne certifikate in licence in v kateri sedaj skrbimo za usposabljanje tako lastnih zaposlenih kot zunanjih kadrov. Načrtujemo tudi vzpostavitev lastne letalske akademije, ki bo svoje storitve ponujala na globalni ravni.

Kar zadeva področje varnostnega zavedanja in nivo varnostne kulture lahko rečem, da praktično vsi, ki delajo na letališču in imajo dostop do t.i. varovanih območij, morajo opraviti usposabljanje na področju varnosti v letalskem prometu. Zaposleni v družbi pa so deležni tudi drugih usposabljanj, ki so tako ali drugače povezana z varnostjo npr. varnost in zdravje pri delu, protipožarna varnost, informacijska varnost, itd. Seveda vsega tega ne bi počeli, v kolikor ne bi verjeli, da je to dodana vrednost, ki ločuje uspešne od povprečnih. ■

Avtorica: mag. Sandra Avsec*

VARNOSTNA TVEGANJA IN ČLOVEŠKI FAKTOR V KEMIJSKI INDUSTRIJI

Sistem obvladovanja varnosti zagotavlja sistematično prepoznavanje nesreč, ki bi se lahko zgodile, ocena njihove verjetnosti in možnih škodljivih posledic pa zmanjšuje tveganje za njihov nastanek ter omogoča hitro ukrepanje pri prepoznavi in aktivno vključuje zaposlene v podjetju, pogodbene izvajalce, dobavitelje in ostale deležnike. V procesni industriji je znan rek, ki pravi: »Če mislite, da je varnost draga, pomislite na nesrečo!«

Na nastanek, razvoj in učinek vsakega nastalega tveganja vpliva posredno ali neposredno človek, največkrat zaposleni. Za varnejšo in zanesljivejšo prihodnost kemijskih industrij ter obratov skladiščenja nevarnih snovi in/ali nevarnih odpadkov, je v prvi vrsti potrebno, v varnostne sisteme vpeljati celostno obravnavo vseh tveganj in dejavnikov tveganj ter poudariti vlogo človeškega faktorja kot ključnega akterja v prepoznavi, obvladovanju in ukrepanju pri morebitnih nastalih tveganjih.

V kemijsko industrijo uvrščamo proizvodnjo in predelavo kemikalij, kemičnih izdelkov in umetnih vlaken, farmacevtskih izdelkov ter izdelkov iz plastike in gume.

Sem uvrščamo dejavnosti, ki slonijo na kemijskih procesih in tehnologijah, kjer gre za predelavo snovi s posebnimi lastnostmi in pri katerih lahko nenadzorovan, nezaželen in nenapovedan proces, kot sta npr. izpust ali izliv, povzroči tehnološko, ekonomsko, okoljsko in človeško škodo.

V Sloveniji je kemijska industrija relativno majhna in razdrobljena, vendar pa se v večini primerov nahaja na poseljenih območjih, kar povečuje tveganja kvalitetnega bivanja, predvsem z vidika varnosti za človeka in za okolje.

Ranljivost kemijske industrije je predvsem v grožnjah, ki se nanašajo na tehnične napake, človeške napake, kriminalna dejanja, vplive okolja, nesreče in izgube ključnega osebja, stavke, tožbe odgovornosti za proizvod, sovražne prevzeme, inflacijo, spremembe v ceni energije (Einarsson in Rausand, 1998).

Zaradi številnih zakonsko predpisanih zaščitnih ukrepov, standardov vodenja in nadzorov številnih inštitucij, okoljskih organizacij ter v zadnjem času tudi javnosti, je odkrivanje in

V Sloveniji je kemijska industrija relativno majhna in razdrobljena, vendar pa se v večini primerov nahaja na poseljenih območjih, kar povečuje tveganja kvalitetnega bivanja, predvsem z vidika varnosti za človeka in za okolje.

preprečevanje nesreč, povezanih s kemičnimi procesi, omejeno in v veliki večini primerov uspešno.

Večina na slovenskem trgu prisotnih kemijskih družb ima varnostne komponente in celostno obvladovanje tveganj sistemsko implementirane v svoje procese, kar zagotavlja varno in stabilno poslovanje.

Velja, da so večje nesreče povezane z dogodki nizke pogostosti, vendar praviloma s težjimi posledicami. Obseg škode je relativen pojem, posploševanja ni. Dejavniki, ki vplivajo na obseg nevarnega dogodka, so: čas, masa snovi, energija, razdalja, ravnanje v sili, človeški faktor in velikost zaloge nevarnih snovi.

V aktivnosti zmanjševanja verjetnosti pojave tveganj se, poleg managementa, vključujejo tudi zaposleni, ki poznajo procese dela in načine preprečevanja nevarnosti pri določenih delovnih procesih. Aktivnosti potekajo v smeri izogibanja tveganjem, programov za preverjanja neskladij, pogodbenih dogovarjanj, upoštevanja konstrukcijskih posebnosti in omejitev, formalnih pregledov, inšpekcijskih in procesnih, tehničnih,

*avtorica je članica Slovenskega združenja korporativne varnosti

in / ali splošnih nadzorov, načrtovanja nadzora nad goljufijami, raziskav in tehnološkega razvoja, izobraževanj, preizkušanj, organizacijskih ukrepov, preventivnega vzdrževanja, zagotavljanja kakovosti, ločevanja in preselitve aktivnosti ter virov v varnejše okolje, odprte notranje komunikacije in odnosov z javnostmi. Pomembna je celovita izmenjava informacij znotraj podjetja, za kar mora biti vzpostavljen učinkovit sistem notranjega informiranja skladno s kompetencami zaposlenih udeležencev. Zaposleni morajo biti usposobljeni za ukrepanje ob nastanku škodljivega dogodka, tako s strani omejitve ali odstranitve nevarnosti, kot evakuacije in preprečitve še večje škode, obvezno pa mora biti zagotovljena tudi pravočasna odzivnost vodstva na nastalo situacijo.

Upravitelji industrijskih objektov, v katerih so prisotne večje količine nevarnih snovi, so zakonsko in moralno zavezani dokazati, da delajo dovolj varno.

Za kakovostno in učinkovito vpeljavo sistema obvladovanja tveganj ter uporabo na vseh procesnih linijah je treba odgovoriti na naslednja ključna vprašanja:

- Ali smo prepoznali vsa tveganja?
- Kako so tveganja klasificirana?
- Ali smo vsa prepoznana tveganja tudi ocenili?
- Imamo opredeljene vse potrebne preventivne aktivnosti nadzora?
- Ali lahko dokažemo, da so aktivnosti nadzora usmerjene in zagotavljajo določeno varnost?
- Ali so stroški spremljanja in analiziranja tveganj manjši od potencialnih izgub?

Dodana vrednost zaposlenih, zaznana v prepoznavi anomalij proizvodnih procesov, dejavnikov tveganj in samih tveganj, se meri v učinkih preprečenih nevarnosti in škod. Le ti so ključni in realni informator v podjetju. Vsi namreč sodelujejo pri razumevanju, sprejemanju, izvajanju procesov upravljanja s tveganji, poročanju o neučinkovitih, nepotrebnih in nedelujočih nadzorih, o škodnih in »skoraj« dogodkih, pri preiskavah zapletov. V primeru neupoštevanja zakonskih in internih predpisov, navodil in/ali postopkov varnega dela, so podjetja dolžna, skladno z zakonodajo, sprejeti ustrezne sankcije proti kršitelju.

Zaposlene je potrebno ozaveščati o razumevanju varnega dela in stalnem zavedanju, kaj gre lahko narobe, kar se kaže v kulturi organizacije, ki vpliva na vedenje, varnost, zanesljivost in pripadnost podjetju. Spodbujati jih je potrebno k opazovanju delovnih procesov ter čimprejšnjemu opozarjanju na napake in morebitne težave, da jih čimprej odpravimo oziroma omejimo. K pozitivnemu pristopu pripomore uvedba sistema nagrajevanja zaposlenih za izvajanje aktivnosti glede zagotavljanja varnosti in skrbi za okolje.

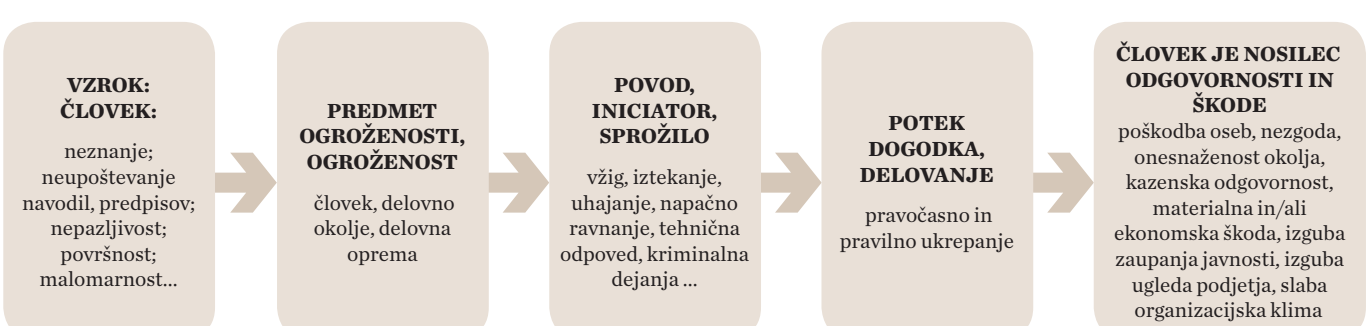
Zaposleni morajo biti usposobljeni za ukrepanje ob nastanku škodljivega dogodka, tako s strani omejitve ali odstranitve nevarnosti, kot evakuacije in preprečitve še večje škode, obvezno pa mora biti zagotovljena tudi pravočasna odzivnost vodstva na nastalo situacijo.

Odgovornost zaposlenih je odvisna predvsem od sistemizacije delovnih mest, pridobljene stopnje usposobljenosti, značajskih lastnosti posameznika, natančno določene linije odgovornosti, zadolžitev in opisa delovnih mest ter njegove pripadnosti podjetju. Do težav prihaja, če zaposleni niso primerno ali zadostno usposobljeni in nimajo ustreznih izkušenj, če je nizka stopnja pripadnosti podjetju ter če aktivnosti in procesi niso natančno določeni in opredeljeni, spremljanje pa je pomanjkljivo ali ni ažurno.

Podjetja, ki se zavedajo pomena rednih usposabljanj, znanj in sposobnosti posameznika, vloge motivacije zaposlenih, tako skrbijo za strokovna izpopolnjevanja s področij potrebnih znanj kakor tudi upoštevajo utemeljena strokovna mnenja zaposlenih ter so naklonjena izmenjavi izkušenj in praks znotraj in zunaj organizacije.

Primeri dobrih praks podjetij se pri obvladovanju varnosti ne osredotočajo samo na zaposlene, ampak tudi na usposabljanja in ozaveščanja pogodbenih izvajalcev, večjih kupcev, dobaviteljev ter lokalne skupnosti.

Pomembne elemente sistema obvladovanja varnosti predstavljajo tudi določanje, uvajanje in vzdrževanje postopkov in navodil za obratovanje brez nevarnih dogodkov, pripravljenost za ukrepanje ob nenadzorovanih dogodkih, sistematična izdelava, pregledovanje in preizkušanje notranjih varnostnih načrtov, sistematično in načrtno ocenjevanje, pregledovanje in noveliranje dokumentov in sistema obvladovanja tveganj in nevarnosti ter redna obveščenost in osveščenost zaposlenih, ki zagotavljajo podjetju kontinuiteto poslovanja in rasti ter zadovoljstvo zaposlenih.

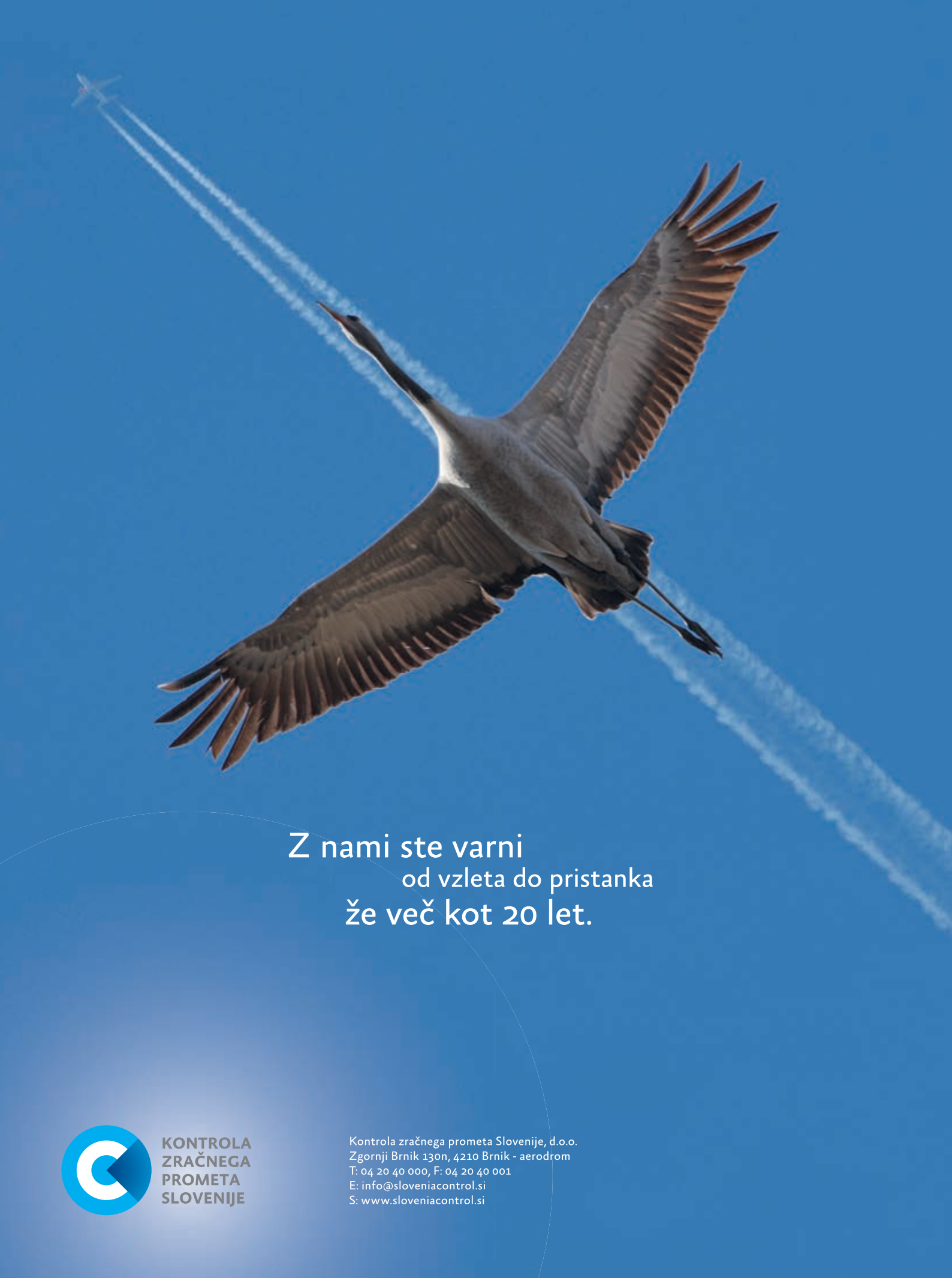


Slika: Vpliv zaposlenega - od vzroka nevarnosti do posledic

Preglednica: Ukrepi za obvladovanje ugotovljenih tveganj in nevarnosti

Ukrep	Aktivnosti
Izločanje nevarnosti v fazi načrtovanja	- sodelovanje čim večjega števila kompetentnih zaposlenih pri opredeljevanju tveganj in nevarnosti že v fazi načrtovanja aktivnosti in delovnih procesov - redno seznanjanje zaposlenih z možnimi viri ogrožanja in nevarnostmi - predvidevanje čim večjega števila dogodkov, ki bi lahko povzročili motnje v delovanju sistema in oblikovanje različnih možnih scenarijev
Zamenjava z manj nevarnimi procesi/snovmi	- preverjanje (sami ali s pomočjo strokovnjakov za določeno področje), možnosti sprememb tehnoloških procesov ali zamenjave snovi - upoštevanje vseh prednosti in slabosti vpeljanih sprememb, kakor tudi zakonodajo, čas uvajanja, čas in sposobnost zaposlenih, morebitni izpad dohodka in porast reklamacij v času prehoda
Zniževanje nevarnosti ob uporabi tehničnih ukrepov	- ločevanje nevarnih procesov od ostalih in vidno označevanje le teh - skrb za varno skladiščenje nevarnih odpadkov - uporaba ustreznega orodja - strogo upoštevanje navodil za delo v eksplozivnih območjih
Administrativna omejitev dostopa do nevarnih območij, izdelava delovnih navodil, usposabljanje zaposlenih	- uporabnikom razumljiva navodila za varno delo, tehnična dokumentacija, varnostni listi - priprava kratkih, uporabnikom razumljivih postopkovnikov za posamezna varnostno kritična delovna mesta - redna specifična usposabljanja zaposlenih - vidno postavljeni varnostni znaki in opozorila - skrb za čistočo in red na delovnem mestu
Načrtovanje ukrepov za primer nesreče in varovanje življenj	- jasna navodila za ravnanje v primeru nezgode - pripraviti interventno mapo postopkov za tipizirane izredne dogodke - označitev nevarnih območij - zagotovitev prve pomoči, vaj evakuacije - jasna navodila za izpostavljene v okolici objekta in za zavarovanje vodotokov ter podtalnice - seznanjanje intervencijskih ekip o naši dejavnosti in zagotovitev potrebnih informacij glede interventnih poti, hidrantnega omrežja .... , posredovanje tehnično kemijskih podatkov o nevarnih kemikalijah, ki jih uporabljamo - omogočanje zainteresirani javnosti spoznavanje naše dejavnosti in možnih nevarnosti ter ukrepanj v primeru nezgode
Uporaba osebne varovalne opreme	- uporaba osebne varovalne opreme, skladno z oceno tveganja za posamezno delovno mesto

Če strnimo: organizacije, ki se zavedajo svojega potenciala v znanju, usposobljenosti ter pripadnosti vseh zaposlenih in ostalih deležnikov, bodo gradile in nadgrajevale poslovno uspešnost varneje, bolj kvalitetno in hitreje za vse nas in naše naslednike.
»NI DOVOLJ DATI VSE OD SEBE; NAJPREJ MORATE VEDETI, KAJ POČETI, IN POTEM DATI VSE OD SEBE.«
(W. Edwards Deming) ■



KONTROLA ZRAČNEGA PROMETA SLOVENIJE

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

Avtor: pred. mag. Marko Potokar / Lek d.d.*

NASILJE NA DELOVNEM MESTU IN AMOK SITUACIJE

Nasilje na delovnem mestu je zapleten in širok pojav, ki je v zadnjih letih pritegnil pozornost organov pregona, inštitucij za duševno zdravje in strokovnjakov za človeške vire. Poročila o nezadovoljnih zaposlenih ali nekdanjih zaposlenih, ki se vračajo na kraj zaposlitve z orožjem in ubijejo nekdanje sodelavce, je ena oblika nasilja na delovnem mestu. Druga vrsta, ki predstavlja približno četrtino nasilja na delovnem mestu, je povezana z osebnimi odnosi, kjer posameznik pridobi dostop do delovnega mesta in izvrši kaznivo dejanje nad zaposlenim, ki je njegov sedanji ali nekdanji intimni partner. Najhujša oblika pa je izbruh nekontroliranega besa, poznan pod imenom AMOK situacija.

Nasilje na delovnem mestu

Nasilje na delovnem mestu se lahko kaže na več načinov. Raznolikost negativnega obnašanja, zajetega v splošnem pojmu nasilja na delovnem mestu, je tako velika in raznovrstna, da otežuje sprejetje enotnega in celovitega pristopa, ki obravnava vse oblike nasilja na delovnem mestu (Eurofound, 2013). Mednarodna organizacija za delo (International Labour Organisation) opredeljuje nasilje na delovnem mestu kot pripetljaje, v katerih so zaposleni ogroženi, napadeni ali žaljeni v delovnem okolju ali na poti na ali z dela in vključujejo jasno ali prikrito grožnjo njihovi varnosti, dobrobiti ali zdravju. Inštitut za dostojanstvo na delovnem mestu (Workplace Dignity Institute) pa omenjeni pojav obravnava kot enega ali več pripetljajev, v katerem/katerih je delavec fizično napaden, čustveno zlorabljen, potisnjen v stisko, vznemirjan, mučen ali se mu grozi (javno, »na štiri oči«, neposredno in posredno) z neupoštevanjem in namernim rušenjem njegove pravice do dostojanstva, do telesne in čustvene varnosti, do njegove dobrobiti, do izpolnjevanja delovnih nalog in do njegovega socialnega razvoja. Ključne ugotovitve raziskave, ki jo je izvedla organizacija Eurofound, so naslednje (Eurofound, 2013):

- Nasilje na delovnem mestu je družbeni pojav določenega obsega. Na splošno, približno 6 % evropskih delavcev poroča, da je doživelo neko obliko nasilja (fizično ali psihično) na delovnem mestu v zadnjih 12 mesecih. O nefizičnih oblikah nasilja na delovnem mestu, kot so verbalne zlorabe, grožnje fizičnega nasilja in neželene spolne pozornosti v preteklem mesecu, je poročalo 12 % delavcev.
- Na splošno je stopnja prijavljenega psihološkega nasilja višja od stopnje fizičnega nasilja. Od različnih vrst psihološkega nasilja je ustrahovanje ali splošno nadlegovanje bolj razširjeno kot spolno nadlegovanje.
- Obstajajo razlike pri izpostavljanju nasilju na delovnem mestu med evropskimi državami. Na splošno je izpostavljenost ustrahovanju ali nadlegovanju razmeroma večja v Franciji in državah Beneluksa, medtem ko so v južni in vzhodni Evropi nižje stopnje poročanja. Spremembe v poročanju posameznih držav lahko odražajo različne ravni zavedanja o tem vprašanju in pripravljenost za poročanje o dejanskem pojavljanju.

Vzroki za nasilje na delovnem mestu so različni; lahko gre za slabo vodenje in organizacijo, osebnostne značilnosti zaposlenih, večkulturnost in razlike v rasni in etični pripadnosti, spodletele osebne in službene odnose, pritiske na delovnem mest ipd.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

- Med sektorji so očitne velike razlike v pojavnosti nasilja na delovnem mestu. Izpostavljenost vsem oblikam nasilja je usmerjena v sektorje z nadpovprečnim stikom z javnostjo. Stopnja fizičnega in psihičnega nasilja je še posebej visoka v zdravstvenem sektorju in sektorju socialnega dela ter v javni upravi.
- Ženske, zlasti mlajše ženske, so bolj izpostavljene spolnemu nadlegovanju na delovnem mestu kot moški.
- Tako telesno kot psihično nasilje ima resne posledice za zdravje in dobro počutje delavcev. Delavci, ki so izpostavljeni psihosocialnim tveganjem, poročajo o bistveno višjih stopnjah slabega zdravja, povezanega z delom, od tistih, ki niso. Najpogostejši simptomi so stres, težave s spanjem, utrujenost in depresija.
- Dejavniki delovnega okolja prispevajo k pojavu nasilja na delovnem mestu. Na primer delovna mesta z višjim obsegom delovne intenzivnosti (kratki roki, hiter tempo), velikim številom omejitev delovnih časov in pogostim stikom s strankami so povezani z večjo verjetnostjo zlorabljanja.

AMOK situacija opisuje dejanje, ko eden ali več storilcev, navidez brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer je očitno, da s to aktivnostjo ne bo prenehal.

Vzroki za nasilje na delovnem mestu so različni; lahko gre za slabo vodenje in organizacijo, osebnostne značilnosti zaposlenih, večkulturnost in razlike v rasni in etični pripadnosti, spodletele osebne in službene odnose, pritiske na delovnem mest ipd.

Ena izmed kategorizacij določa štiri vrste nasilja na delovnem mestu, glede na odnos med žrtvami, storilci in delovnimi mesti:

- Incidenti tipa I vključujejo storilce kaznivih dejanj, ki nimajo nobene zveze z žrtvami ali delovnimi mesti.
- Incidenti tipa II vključujejo storilce kaznivih dejanj, ki so prejemniki storitev organizacije.
- Incidenti tipa III vključujejo sedanje ali nekdanje zaposlene, ki delujejo proti svojim sedanjim ali preteklim sodelavcem oziroma delovnim mestom.
- Incidenti tipa IV vključujejo domače spore med zaposlenimi in storilcem, ki se prelivajo na delovna mesta.
- Nasilje na delovnem mestu se giblje od žaljivk in groženj do umora. Vključuje lahko nasilje v družini, spolno nasilje, vključno s spolnim nadlegovanjem ali spolnim napadom, nasiljem na zmenku in zalezovanje. Nasilje na delovnem mestu pogosto povzroči resne poškodbe, ki lahko povzročijo invalidnost, ki zahteva stalno nego, lahko pa tudi življenjsko ogrožajoče poškodbe in celo smrt. Najhujše oblike nasilja na delovnem mestu so t.i. AMOK situacije.

Amok situacija

Izraz *amok* (tudi *mengamuk*, *pengamok*) označuje primere izbruha neobvladljivega besa, v katerih posamezniki brez vidnega razloga ali opozorilnih znakov, ubijajo in pohabljajo ljudi in živali. Leta 1849 je bil *amok* na podlagi številnih poročil in študij primerov, ki so pokazali, da je bila večina posameznikov, ki so zagrešili *amok*, duševno bolnih, uvrščen med psihične motnje. Tako Diagnostični in statistični priročnik duševnih motenj, ki ga je izdalo ameriško psihiatrično združenje, razvršča *amok* na dve uradni kategoriji: *amok* in *beramok*. *Amok* je redkejša oblika pojava in izvira iz besa, užaljenosti ali maščevanja proti posamezniku ali družbi in je tesneje povezan s psihozo, osebnostnimi motnjami, bipolarno motnjo in blodnjami. *Beramok*, ki je pogostejši, je povezan z depresijo in žalostjo, ki izhajata iz izgube, kot je smrt zakonca ali ljubljene osebe, ločitev, izguba delovnega mesta, denarja, moči itd. Povezan je z duševnimi težavami zaradi hude depresije ali druge motnje razpoloženja.

Simptomi, ki so navedeni v večini kliničnih opisov *amoka*, vključujejo:

- začetno obdobje umika iz družbe, ki traja več ur ali dni;
- nenadno, neizzvano nasilje, usmerjeno na vsakogar na dosegu roke, pa naj bodo to družinski člani, prijatelji ali pa popolni neznanci;
- napadi se nadaljujejo in lahko trajajo več minut, ur ali celo dni, dokler storilec ni ubit ali kako drugače onesposobljen;
- v primerih, ko storilec preživi, običajno pade v globok spanec ali zamaknjenost, ki lahko traja več dni;
- ko se storilec prebudi, je še naprej odmaknjen in nekomunikativen in se ne more spomniti, kaj se je zgodilo.

AMOK situacija opisuje dejanje, ko eden ali več storilcev, navidez brez motiva, poškoduje ali ubije eno ali več oseb, pri čemer

je očitno, da s to aktivnostjo ne bo prenehal. Uporablja se tudi izraz *aktivna strelska situacija*, ki označuje množični umor, pri katerem storilec uporabi strelno orožje. Za *množični umor* gre, ko je v krajšem času na omejenem geografskem območju ubitih večje število ljudi. Navedene situacije se pojmujejo pod skupnim izrazom *aktivne življenju nevarne situacije*.

V angloameriški literaturi se za tovrstne primere uporabljajo tudi naslednji pojmi (Potokar, 2017):

- MASS MURDERS: enkraten dogodek z več hkratnimi umori.
- SPREE KILLING: več umorov na dveh ali več lokacijah, med katerimi skoraj ni prekinitve.
- MASS SHOOTING: incident z več žrtvami, povzročen s strelnim orožjem.
- GOING POSTAL: izbruh ekstremnega in nekontroliranega besa, ponavadi v delovnem okolju.
- SCHOOL SHOOTING: napadi s strelnim orožjem na šolah in fakultetah.

Značilnost strelskih pohodov je ta, da gre za dejanja, ki so neposredno usmerjena proti življenju posameznikov, storilec pa se ne oziroma se ni pripravljen pogajati, ampak izvaja pomor. Za razumevanje te ekstremne oblike nasilja obstajajo številni različni pristopi, razviti s strani sociologije, psihologije, psihiatrije pa tudi kriminologije in medicine. Tako posamezne vede pogosto uporabljajo različne definicije tega pojava in postavljajo svoje specifične vidike, kot so socio-kulturni vplivi, institucionalni dejavniki, patološke strukture osebnosti itd. Prav zaradi tako razcepljenega in nepovezanega pogleda je področje proučevanja omenjenega pojava in vzrokov zanj necelovito obravnavano. Primere strelskih pohodov je potrebno gledati celovito, kot skupek različnih vzrokov, ki stoječ sami zase ne zadostujejo za razlago samega pojava. Obstaja več definicij strelskih pohodov, za vse pa so značilne naslednje karakteristike:

- lokacija nasilnega dogodka je organizacija (podjetje, šola, državna inštitucija ipd.);
- storilec je trenutni ali bivši zaposleni v tej organizaciji;
- uporabljeno je smrtonosno orožje (strelno orožje, nož, eksploziv itd.) z namenom poškodovanja ali ubitja več kot ene osebe (bistven kriterij je namen, ne dejansko število žrtev);
- napad se zgodi v prostorih organizacije, v času dela, praviloma v pričo zaposlenih;
- storilec izbira žrtve na podlagi predhodnih konfliktnih odnosov ali naključno ali pa na podlagi njihovega statusa v delovnem okolju.

Slovenski pravni vidik zagotavljanja varnosti zaposlenih

Krovni predpis na področju varnosti in zdravja pri delu je Zakon o varnosti in zdravju pri delu (v nadaljevanju ZVZD-1). Prenovljen je bil leta 2011 in delodajalcem nalaga veliko nalog in odgovornosti. Med njimi sta tudi dve, ki se neposredno dotikata nasilja na delovnem mestu. Prva določa, da mora delodajalec zagotoviti potrebno ureditev in opremo na delovnih mestih, kjer obstaja nevarnost za nasilje tretjih oseb (23. člen ZVZD-1), druga pa pravi, da je potrebno sprejeti ukrepe za preprečevanje, odpravljanje in obvladovanje primerov nasilja, trpinčenja, nadlegovanja in drugih oblik psihosocialnega tveganja na delovnih mestih, ki lahko ogrozijo zdravje delavcev (24. člen ZVZD-1).

ZVZD-1 kot krovni predpis na področju varnosti in zdravja pri delu določa pravice in dolžnosti delodajalcev in delavcev v zvezi z varnim in zdravim delom ter ukrepi za zagotavljanje varnosti in zdravja pri delu. Določbe tega zakona se uporabljajo v vseh dejavnostih za vse osebe, ki so navzoče v delov-

nem procesu. Z vidika zagotavljanja osebne varnosti zaposlenih sta pomembni dve določbi. Prva je ta, da mora delodajalec načrtovati postopke za zmanjšanje nevarnosti za nasilje tretjih oseb. V prvem odstavku 23. člena ZVZD-1 je namreč opredeljeno, da mora delodajalec na delovnih mestih, kjer obstaja večja nevarnost za nasilje tretjih oseb, poskrbeti za tako ureditev delovnega mesta in opremo, ki tveganje za nasilje zmanjšata in ki omogočata dostop pomoči na ogroženo delovno mesto. Nadalje je v tem členu določeno tudi, da mora delodajalec načrtovati postopke za primere nasilja iz prvega odstavka tega člena in seznaniti z njimi delavce, ki na takih delovnih mestih delajo. Delodajalec mora tako že v oceni tveganja opredeliti tista delovna mesta, na katerih obstaja večja možnost za nasilje s strani tretjih oseb.

Druga določba zadeva nasilje, trpinčenje, nadlegovanje in psihosocialno tveganje. Tako je za zagotovitev upoštevanja določb 24. člena ZVZD-1 delodajalec v primerih nasilja, trpinčenja, nadlegovanja in psihosocialnih tveganj na delovnih mestih (mobing) dolžan sprejeti ukrepe za preprečevanje, odpravljanje in obvladovanje primerov mobinga, ki lahko ogrozijo zdravje delavcev. Glede na to, da je določba o mobingu vključena v ta zakon, lahko inšpektorji za delo nadzorujejo izvajanje te določbe s strani delodajalcev in v primeru kršitev ukrepajo z izdajo ureditvenih odločb.

Varovanje ljudi in premoženja je urejeno tudi z Zakonom o zasebnem varovanju (ZzasV-1), ki v 1. členu med drugim določa zasebno varovanje, oblike varovanja, pristojnosti, pogoje za opravljanje zasebnega varovanja, standarde, strokovno usposabljanje in izpopolnjevanje, ukrepe in dolžnosti varnostnika itd. Varnostniki so tako najpomembnejši člen za preprečevanje neprimernih in nezakonitih aktivnosti v organizacijah, kjer opravljajo svoje delo. Poleg vprašanja, ali so usposobljeni in primerno opremljeni tudi za ravnanje v izjemno nasilnih situacijah, obstaja tudi omejitev njihovih pooblastil. Podlaga za delovanje in ukrepanje varnostnika je ZZasV-1, vendar ta ne vsebuje določil o ravnanju varnostnika v izrednih situacijah in ga k temu tudi ne zavezuje. Seveda mora varnostnik svojo službo opravljati vestno in pozorno spremljati okolico in dogajanje na varnostnem območju, preverjati prisotnost sumljivih predmetov in oseb ter ves svoj delovni čas preventivno delovati. Je dovolj, da v primeru hujših oblik nasilja ‚samo' pokliče policijo ali pa intervencijsko službo, ki jo opravljajo njegovi kolegi? V takih primerih je na preizkušnji ustrezna usposobljenost, vključujoč znanje, izkušnje in izurjenost ter ustrezna opremljenost.

Dejstvo je, da imamo človeška bitja nasilje v sebi. Kdaj in na kakšen način bo do izbruha nasilja prišlo, je odvisno od več dejavnikov, med drugim od vzgoje, čustvenega stanja, situacije in občutka ogroženosti ter samokontrole.

Zaključek

Dejstvo je, da imamo človeška bitja nasilje v sebi. Kdaj in na kakšen način bo do izbruha nasilja prišlo, je odvisno od več dejavnikov, med drugim od vzgoje, čustvenega stanja, situacije in občutka ogroženosti ter samokontrole. V družbi bi se zato moralo poudariti širjenje znanja in zavedanja o varnostni kulturi ter vzgoji za nenasilje, ki je eden od mehanizmov, s katerim bi lahko povečali varnost. Usposabljanje posameznikov s področja osebne varnosti je eno izmed ključnih dejavnikov pri zagotavljanju varnosti in dvigovanja varnostne kulture. Zagotavljanje varnega delovnega okolja bi moral biti eden izmed glavnih ciljev vsake organizacije. Zavedati se moramo, da samo določbe v zakonih in sprejeti notranji organizacijski pravilniki še niso dovolj. Spremeniti je potrebno organizacijsko kulturo in sistem vrednot zaposlenih, kar lahko dosežemo le z iskreno podporo in zgledi najvišjega vodstva. Ključno za zvišanje nivoja varnosti je ustrezno usposabljanje zaposlenih za samozaščitno ravnanje.

Zavedati pa se moramo, da sta najboljša zaščita in obramba preprečevanje ter lastna ozaveščenost in skrb za varnost. Za lastno varnost smo namreč v prvi vrsti odgovorni sami.

Viri

- Eurofound (2013). *Physical and psychological violence at the workplace*. Publications Office of the European Union, Luxembourg.
- Potokar, M. (2017). *Pripravljenost varnostnih in vodstvenih struktur na AMOK situacijo*. Revija korporativna varnost, ICS.
- Threat Assessment in Virginia Public Schools: Model Policies, Procedures, and Guidelines. (2016). Virginia Department of Criminal Justice Services.
- Zakon o zasebnem varovanju (ZZasV-1). (2011). Uradni list RS, št. 17/2011.
- Zakon o varnosti in zdravju pri delu (ZVZD-1). (2011). Uradni list RS, št. 43/2011. ■

VEDNO IZPOLNIJO PRAVO ŽELJO

*Nakup na **www.btc-city.com/darilniboni***
*in na **Info točki** v **Dvorani A**.*

TRGOVINE V BTC CITY LJUBLJANA SO V DECEMBRU
ODPRTE TUDI OB **NEDELJAH** OD **9.00** DO **15.00**

BTC CITY

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

VARNOST NA SPLETU JE V PODJETJIH ŠE POSEBEJ POMEMBNA

Z uporabo interneta je vsak posameznik in sleherno podjetje potencialna tarča spletnih kriminalcev, zato se je potrebno zavedati, da lahko napadalci "udarijo" tudi vas. Največ, kar lahko storimo je, da se tega zavedamo, ter seveda, da smo seznanjeni z vrstami groženj ter predvsem kako se pred njimi ubraniti.

Ne glede na funkcijo, ki jo ima oseba v podjetju, je vsak na svoj način lahko tarča različnih groženj, ki prežijo na nas v delovnem okolju. Goljufi si izmišljajo raznovrstne načine, kako bi prevarali in ogoljufali podjetja, pa naj si bodo mala ali velika. V imenu direktorjev pošiljajo lažna elektronska sporočila in prosijo za nujno nakazilo večje vsote denarja v tujino. Poskušajo z zlorabo elektronskega predala in vrivanjem v komunikacijo, kjer goljuf podjetju sporoči, da je prišlo do zamenjave transakcijskega računa v podjetju s katerim poslujejo in tako poskušajo podjetje prepričati v nakazilo na bančni račun goljufa. Prav tako so podjetja deležna ponudb za raznovrstne lažne kredite, ki naj bi jim pomagali prebroditi finančno težke čase. Ne pozabimo pa tudi na izsiljevalske viruse, ki resno zmotijo poslovanje, ali pa povzročijo zelo hude težave.

Na spletnem portalu Varni na internetu (https://www.varninainternetu.si/nocnamora/) so na voljo izobraževalna gradiva in preizkus znanja za vodstvene delavce, zaposlene in računovodje, kjer smo pripravili tudi priročnik Kažipot varnosti za mala podjetja. Prav tako si lahko naročite brezplačni plakat, ki ga lahko obesite na vidno mesto v podjetju, ter tako dodatno opozarjajte zaposlene na previdnost.

Previdno pri elektronski pošti

Elektronska pošta je najbolj priljubljeno orodje goljufov, s pomočjo katere vas poskušajo s phishing napadom prepričati, da jim zaupate vaše uporabniško ime in geslo. Prav tako se večina izsiljevalskih virusov širi ravno prek elektronske pošte v raznovrstnih priponkah.

Zato je pri uporabi elektronske pošte pametno upoštevati nekaj naslednjih nasvetov:

- Nikoli ne odpirajte priponke neznanih pošiljateljev.
- Če se vam pošiljatelj zdi znan, potem preverite ime pripete datoteke (primer: Rechung_906631.doc - takšna priponka že zna biti sumljiva, če ne poslujete z nemškimi partnerji, zato le-te raje ne odpirajte in pri pošiljatelju preverite, če vam je priponko res poslal on).
- Če prejmete elektronsko pošto, ki vas preko povezave vodi na spletno stran, kjer vas le-ta poziva, da vpišete vaše uporabniško ime in geslo, tega nikoli ne vpisujte.
- Če prejmete .doc ali .xls dokument, ki od vas zahteva vklop makrov, tega nikoli ne storite. Izjema so seveda interne datoteke med sode-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

lavci (vendar še takrat rajši preverite, če vam jo je res poslal sodelavec, predno makro vklopite).

- Vsako priponko lahko pred odpiranjem zelo hitro in enostavno pregledate s spletnim orodjem VirusTotal. Prejeto priponko shranite na vaš računalnik ter odprete spletni naslov https://www.virustotal.com. Kliknite gumb »Upload and scan file« ter izberite priponko, ki ste jo shranili na vaš računalnik. VirusTotal bo priponko pregledal in vas opozoril v primeru, da le-ta nakazuje na zlonamerno datoteko, ki je protivirusnim programom že znana.

Raznovrstna in močna gesla

Če spletni kriminalci poznajo vaše geslo za dostop do različnih storitev, potem so jim vrata za različne zlorabe na široko odprta. Zato bodite pozorni na:

- Gesla naj bodo za vsako storitev ločena (primer: geslo za vpis v računalnik naj bo svoje, geslo za dostop do elektronske pošte naj bo spet drugačno...).
- Gesla raje ne zapisujte na listek. Če to vseeno storite, poskrbite, da ne bo shranjen v bližini računalnika ter prosto dostopen in brez nadzora. Ne pustite ga recimo pod tipkovnico, ali še slabše, nalepite na ekran.
- Geslo naj bo po možnosti kompleksno in predvsem dolgo, ter takšno, da ga ni enostavno uganiti. Sestavite več besed, vsebujejo naj velike in male črke, številke in ločila.
- Za hrambo in ustvarjanje številnih gesel za vse storitve lahko uporabite namenski program (upravljalec gesel ali „password manager“).

Varna uporaba spletne banke

Spletno bančništvo predstavlja enostavno obliko finančnega poslovanja. Vendar pa lahko hitro pride do neželenih zlorab, če uporabnik pri uporabi ni previden, zato lahko sami uporabniki naredimo največ za samo zaščito bančnega računa:

- Certifikat za dostop do spletne banke naj bo vedno na zunanjem mediju (pametni usb ključ ali pametna kartica).
- Ko končate z delom usb ključ ali pametno kartico vedno odstranite iz računalnika.
- Bančnih storitev nikoli ne opravljajte na računalniku, ki je namenjen uporabi širšemu krogu ljudi.
- V primeru, da vaš poslovni partner sporoči, da je spremenil številko poslovnega bančnega računa, to vedno osebno preverite pri njemu in ne zaupanje zgolj elektronskemu sporočilu.
- Ko nakupujete prek spleta, če le imate možnost, vedno rajši izberite plačilo preko zaupanja vrednih posrednikov (na primer PayPal).
- Če se vaš računalnik okuži z virusom, vam lahko ukradejo avtentikacijske podatke za dostop do spletne banke. Zato redno posodabljajte vso programsko opremo.

Varnost spletne strani

Spletna stran predstavlja zrcalo vašega podjetja in je običajno prvi stik kupca z vami. Zato je pomembno, da je spletna stran enostavna in kupcu v največ treh klikih prikaže informacije, ki jih išče. A pomembna nista le videz in vsebina, temveč je potrebno poskrbeti tudi za varnost:

- Spletna stran naj ima nameščeno digitalno potrdilo (certifikat), da bo dosegljiva prek varne povezave (prepoznamo jo po »https« v URL naslovu spletne strani).
- Skrb za redno posodabljanje spletnega mesta, še posebej če uporabljate odprtokodne sisteme za urejanje vsebine (Joomla, Wordpress, Typo3, Drupal, Magento, OpenCart, Prestashop...)

- Za izdelavo in postavitev spletnega mesta izberite zaupanja vrednega ponudnika gostovanja, ter izvajalca za izvedbo, ki ne bo ravno »vaš sosed«, saj v primeru, ko sami ne znate vzdrževati postavljenega spletnega mesta, »vaš sosed« pa se odseli, hitro pride do takšnega ali drugačnega zapleta.
- Skrbite za domeno in bodite pozorni na njen datum izteka. Če jo pozabite podaljšati, jo lahko en mesec po preteku kupi nekdo drug.
- Spletna stran naj vsebuje le osnovne informacije o podjetju ter samo splošen elektronski naslov, na katerega lahko pišejo vsi. Podatke o zaposlenih pa objavljajte le v skladu s politiko vašega podjetja, saj lahko le-te goljufi izkoristijo pri prevarah.

Vodnik ABC varnosti za lastnike spletnih strani si lahko brezplačno prenesete na: https://vni.si/www

Varnostno kopiranje

Backup, backup in še enkrat backup! V primeru, da pride do kakršnih koli nezaželenih dogodkov (vdor v sistem, šifrirane datoteke zaradi virusa, okvara trdega diska...) je backup edina zanesljiva stvar, ki se je lahko oprimete, da ne ostanete brez vseh pomembnih podatkov. A tudi redno varnostno kopiranje se lahko izjalovi, zato upoštevajte:

- Varnostne kopije naj bodo obvezno na zunanjem mediju (zunanji disk - NAS) do katerega nimajo vsi dostopa, najboljše v omari, ki je pod ključem.
- Varnostne kopije lahko shranjujete tudi v oblak, vendar pri tem izberite zaupanja vrednega ponudnika (primer Amazon Drive, Google Cloud), ki omogočajo dvostopenjsko avtentikacijo pri prijavi.
- Varnostne kopije ustvarjajte dosledno in vedno na vsaj dveh različnih lokacijah (ena lokacija naj bo v službi, druga pa na primer doma).
- Ko je varnostna kopija narejena, vedno preverite ali je le-ta bila uspešno narejena, saj med samim kopiranjem lahko pride do napake in v tem primeru so podatki neuporabni

Previdna uporaba službene opreme

Če svojim zaposlenim nudite službeni prenosnik ali telefon, potem je pri tem potrebno upoštevati pametno uporabo:

- Ne nameščajte aplikacij ali nelicenčnih programov, ki niso namenjene službeni uporabi.
- Vedno nameščajte aplikacije samo iz uradne tržnice (Google Play, App Store).
- Uporabljajte šifriranje diska (primer BitLocker..), kar lahko koristi, če služben računalnik ukradejo.

VARNO DELO OD DOMA

Če zaposleni delajo od doma, poskrbite za varnost:

- Za dostop do službenega omrežja naj zaposleni uporabljajo VPN povezavo.
- Dostop od doma naj bo omejen zgolj na določene uporabnike, le tiste, ki to zares potrebujejo.
- Oddaljen dostop do službenega omrežja naj bo dobro zaščiten, tudi s požarnim zidom. Za dostop uporabljajte močno geslo in večstopenjsko avtentikacijo.

Ustrezna zaščita brezžičnega omrežja

Brezžična povezava predstavlja enostavno in hitro povezovanje v omrežje, saj se danes že skoraj vsaka naprava povezuje na Wi-Fi, zato je pomembno, da je brezžično omrežje ustrezno zaščiteno:

- Kompleksno geslo za dostop do brezžičnega omrežja.
- Uporabite šifriranje (WPA2, AES).
- Spremenite privzete (tovarniške) nastavitve na brezžičnem usmerjevalniku.
- Skrite ime brezžičnega omrežja, tako da se le-ta ne prikaže na seznamu razpoložljivih omrežij (skriti SSID).
- Ločite omrežje Wi-Fi za zaposlene in obiskovalce, pri tem slednjim onemogočite dostop do službenega omrežja.
- Skrbite za redne varnostne posodobitve vašega usmerjevalnika.

Več o zaščiti Wi-FI omrežja si lahko preberete na: https://www.varninainternetu.si/2017/kaj-moram-vedeti-o-wpa2-ranljivosti-v-wi-fi-omrezjih/

Star pregovor pravi, da je veriga toliko močna, kot je močan njen najšibkejši člen in to še kako drži na področju informacijske varnosti. Miselnost, da se nam ne more zgoditi je žal prevečkrat zgrešena, zato poskrbite za večjo ozaveščenost vseh zaposlenih, pa četudi na jutranji kavici temu namenite 10 minut sestanka kolektiva, povabite strokovnjake... Poskrbite tudi za upoštevanje osnovnih premis informacijske varnosti; zaupnost, neokrnjenost in razpoložljivost. ■

9. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 14.—15. MAREC 2018

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

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

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

Avtor: Boštjan Špehonja / Etični hacker*

NAJPOGOSTEJŠE RANLJIVOSTI SLOVENSKIH PODJETIJ

Ko govorimo o najpogostejših ranljivostih slovenskih podjetij imejmo v mislih ranljivosti, ki se nanašajo na Informacijsko Komunikacijsko Tehnologijo (IKT). Skozi leta izkušenj pri izvajanju varnostnih pregledov v najrazličnejših okoljih lahko povzamem, da se ranljivosti v podjetjih pogosto ponavljajo.

Ranljivosti v slovenskih podjetjih se pojavljajo ne glede na okolje, ali gre za bančni ali zavarovalniški sektor, ministrstva, podjetja s kritično infrastrukturo ali druga podjetja – tako manjša, srednja kot velika. Vse opisane ugotovitve so bile pridobljene skozi izvedbo varnostnih pregledov, ki so del storitev s katerimi se ukvarjamo v podjetju Unistar LC in pri katerih izvedemo samo tiste napade, ki so predhodno dogovorjeni in odobreni s strani naročnika.

V grobem lahko ranljivosti klasificiramo na dve kategoriji. Pod prvo spadajo tiste, ki jih odkrijemo pri zunanjem varnostnem pregledu. To pomeni, da je ranljivost dostopna iz interneta, in jo lahko potencialno izrabi vsak, ki ranljivost odkrije. V drugo kategorijo pa spadajo tiste ranljivosti, ki jih odkrijemo na lokaciji organizacije/podjetja pri izvajanju notranjega varnostnega pregleda. Predpogoj za izrabo takšnih ranljivosti je dostop do elektronske naprave, ki je avtenticirana v lokalno omrežje podjetja ali organizacije.

Kot prvo in najpogostejšo ranljivost, ki se pojavlja v obeh kategorijah, bi izpostavil **privzeta uporabniška imena in gesla** ter šibka gesla. Velikokrat se zgodi, da pri varnostnem pregledu pridobimo administratorski dostop do naprave s privzetimi nastavitvami, kot je primer uporabniško ime »admin« in geslo »admin«. Gre za tovarniško nastavitev, ki ob namestitvi naprave ni bila spremenjena in predstavlja kritično varnostno tveganje. Pri takšni ranljivosti napadalec ne potrebuje tehničnega znanja, le nekaj iznajdljivosti. Pridobi pa lahko popoln nadzor nad napravo. Zato se vedno priporoča, da se privzeta gesla čim prej spremeni, prav tako se priporoča uporabo varnih gesel, ki vsebujejo velike in male črke, posebne znake ter številke. Na tem mestu bi posebej izpostavil previdnost pri zunanjih izvajalcih. Zelo pogosto opažamo, da prav slednji puščajo odprta vrata v marsikatero podjetje. Zato svetujemo, da se pri vsaki novi, namenski napravi, ki se avtenticira v omrežje podjetja, preveri osnovne nastavitve in tako prepreči morebitne ranljivosti iz tega naslova.

Kot drugo, prav tako zelo visoko ranljivost bi izpostavil **ne posodobljene elektronske naprave**. Odkrivamo tako zastarele operacijske sisteme, kot tudi vse ostale storitve, ki tečejo na njih. V kolikor se v internetu pojavi naprava, ki nima nameščenih varnostnih popravkov, lahko ta za organizacijo predstavlja visoko tveganje. Zato se vedno priporoča redno nameščanje varnostnih popravkov ter ostalih posodobitev. Pri nekaterih IKT sistemih se to zaradi narave delovanja aplikacij izkaže kot težje izvedljivo. V takšnih primerih je strežnike ter aplikacije potrebno varovati z drugimi varnostnimi mehanizmi. Kljub temu, da je bilo o tem že veliko napisanega, je to še vedno rak rana skoraj vsake organizacije. V zadnjem letu smo prejeli veliko klicev organizacij, ki so bile okužene z izsiljevalskim virusom (Ransomware), brez da bi imel uporabnik interakcijo z elektronsko napravo. Izkazalo se je, da je šlo za izkoriščanje ne posodobljenih strežnikov, ki so bili dostopni na internetu. V protokolih za oddaljen dostop ter deljenje datotek (RDP ter SMB) je bila odkrita kritična varnostna ranljivost, ki je napadalcem omogočala izvrševanje kode na daljavo. Na tak način so napadalci iskali ne posodobljene elektronske naprave in okuževali sisteme. V kolikor bi se želeli prepričati, da je internet nevaren prostor, lahko računalnik z operacijskim sistemom Windows ter omogočenim protokolom SMBv1 priklopite pred vse varnostne mehanizme, direktno na javni IP naslov. Ne bo potrebno dolgo čakati, da se bo na ekranu pojavil izpis »your files has been encrypted« - in to brez kakršne koli vaše interakcije z napravo.

Pri izvajanju zunanjih varnostnih pregledov se vedno osredotočamo na pregled vseh javno dostopnih informacij o podjetju. Od IP naslovnega prostora, domen, poddomen, poindeksirane vsebine podjetja na spletnih iskalnikih, pa tudi spletnih arhivov. Kot izvajalci pregleda smo vedno nagrajeni, ko ugotovimo kje se nahajajo **testna okolja.** Ta velikokrat vsebujejo informacije, ki pripomorejo k planiranju nadaljnjega napada na organi-

*avtor je član Slovenskega združenja korporativne varnosti

zacijo. Na tem mestu bi želel opozoriti, da se pogled napadalca na IKT okolje razlikuje od pogleda skrbnika sistemov. V takšnih okoljih razvijalci velikokrat puščajo datoteke, za katere mislijo, da so varno shranjene ali skrite. Z izvedbo določenih napadov je mogoče iz takšnih okolij pridobiti vsebino, ki razkriva občutljive podatke podjetja. Zato se priporoča, da so testna okolja posebej izolirana.

Ko izvajamo notranje varnostne preglede je pogoj za izvedbo pregleda ta, da avtenticiramo svojo elektronsko napravo v lokalno omrežje podjetja. Uspešen **priklop naprave v omrežje** brez varnostnih mehanizmov že predstavlja varnostno tveganje. Priporoča se vpeljava mehanizmov, ki neznanim napravam onemogočajo priklop v omrežje. V drugem koraku notranjega pregleda preiščemo dostopne elektronske naprave. Tukaj se pojavi drugo tveganje, saj nekatere organizacije nimajo **segmentacije omrežja.** To pomeni, da so v istem segmentu tako uporabniki, kot strežniki, multifunkcijske naprave, kamere idr. V kolikor pa podjetje ima segmentacijo, se velikokrat zgodi, da nepravilno **omejuje dostope iz segmenta** v segment (prehodi med vlani). To v praksi pomeni, da lahko uporabnik, ki se z računalnikom priklopi v lokalno omrežje podjetja, dostopa do vseh naprav in vseh storitev v drugih segmentih, tudi strežniških. Odprt dostop do naprav in storitev predstavlja varnostno tveganje, saj dopušča napadalcu iskanje ranljivosti in dostop do ključnih strežnikov v podjetju. Zato se priporoča, da je omrežje vedno ustrezno segmentirano, dostopi med njimi pa skrbno načrtovani.

Ko je napadalec priklopljen v notranje omrežje podjetja, lahko z izvedbo nekaterih napadov prestreza promet, ki se prenaša iz strani odjemalcev do strežnikov in obratno. Podjetja imajo še vedno nekatere ključne storitve na **nešifriranih protokolih.** Primer takšne storitve je intranet portal na nevarnem http protokolu. To pomeni, da je mogoče prestrezati promet, ki se po mreži pretaka med odjemalcem in strežnikom v čistopisu. V kolikor tak napad izvajamo v času, ko se uporabnik z domenskim uporabniškim imenom in geslom prijavi v storitev na nešifriranem protokolu, lahko prestrežemo geslo in mu tako ukrademo digitalno identiteto. Ko v notranjem omrežju pridobimo veljavno domensko uporabniško ime in geslo, pa se nam odpre nov nabor napadov, ki bi bili brez tega neuspešni. Poleg tega se lahko prijavimo v vse storitve podjetja, do katerih ima uporabnik dostop in tako pridobivamo občutljive informacije.

Posebno poglavje so brezžična oziroma **wireless omrežja**. V kolikor so ta varovana samo z geslom, se vedno priporoča, da so povsem ločena od notranjega omrežja podjetja. V kar nekaj primerih je bilo pri pregledih brezžičnega omrežja ugotovljeno, da je mogoče iz omrežja za goste dostopati do notranjega omrežja organizacije. Tega si zagotovo nihče ne želi, da bi poslovni partner po sestanku v vaši organizaciji odšel v bližnji lokal ter se virtualno sprehajal po vašem omrežju in iskal potencialno občutljive informacije na strežnikih in med uporabniki.

Posebno pozornost pa zahtevajo aktualni napadi, ki se ne osredotočajo v tehnične izrabe ranljivosti, ampak masovno targetirajo **neukega končnega uporabnika** Spletni prevaranti so ugotovili, da je časovno in tehnično precej lažje izrabiti neukega uporabnika, kot izvajati dovršene tehnične napade. Prav zato se v zadnjih nekaj letih povečujejo napadi preko tehnik socialnega inženiringa. Posebej na udaru je neželena elektronska pošta, ki vsebuje povezavo na zlonamerno spletno stran ali priponko. Potrebno je poudariti, da je okužba ne-posodobljene elektronske naprave možna že s klikom na povezavo. Ta vas odpelje na okuženo spletno stran, ki izkorišča ne posodobljen brskalnik/vtičnik, in preko tega na računalnik naloži zlonamerno kodo. V organizacijah so domenski računalniki načeloma redno posodobljeni, predstavlja pa okužena spletna stran tveganje okužbe z mimohodom na domačih elektronskih napravah. Še nekoliko višje tveganje pa predstavlja elektronska pošta neznanih pošiljateljev, ki vsebujejo priponko, največkrat wordov ali excellov dokument, te pa od nas zahtevajo zagon programske kode ali »makrojev«. Ko uporabnik omogoči makroje, pomeni, da zažene programsko kodo v dokumentu. Ta je navadno tako napisana, da se poveže na oddaljen strežnik, in iz njega na elektronsko napravo naloži in zažene virus. Zato se priporoča, da se makrojev v neznanih dokumentih nikoli ne zaganja. Poleg tega je vedno potrebno preverit smiselnost elektronske pošte ter pošiljatelja. Radovednost na internetu je lahko usodna, zato previdnost ni odveč. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

VARNOST IN RAZNOLIKOST V EVROPI "SAFETY AND DIVERSITY IN EUROPE"

ICS-Ljubljana z mednarodnimi partnerji aktivno sodeluje pri projektu ERASMUS+, ki predstavlja enega izmed ključnih korakov na področju prepoznavanja in izvajanja sistemskih ukrepov za preprečevanje ekstremizma.

Institut za korporativno varnostne študije, ICS-Ljubljana, je postal del konzorcija v okviru programa ERASMUS+, kjer z mednarodnimi partnerji sodeluje na projektu „**Safety and diversity in Europe - efficient training modules for prevention of extremism by trainees and staff of private security services in Europe**“ oziroma v prevodu „Varnost in raznolikost v Evropi - učinkoviti moduli usposabljanja za preprečevanje ekstremizma oz. radikalizacije za inštruktorje in osebje zasebnih varnostnih služb v Evropi“. V projektu sodelujejo predstavniki kar sedmih evropskih držav. Poleg Slovenije (ICS Ljubljana) so tu še Nemčija, Irska, Španija, Estonija, Poljska in Romunija.

Omenjeni projekt bo poskušal v obdobju dveh let razviti ustrezne programske vsebine in izdelavo priročnika za »trenerje«, ki bo omogočil učinkovito usposabljanje predstavnikov organizacij na področju zasebne varnosti o pojavu, vzrokih in predvsem ukrepih za preprečevanje ekstremizma in radikalizacije. Trendi v varnostnem okolju namreč kažejo, da bo omenjena problematika v naslednjem obdobju zelo izpostavljena in bo pred zasebno varnostne subjekte postavila pomembne izzive in dileme za učinkovito izvajanje svojega poslanstva ter nalog.

Potreba po tej vrsti izobraževanj se je pokazala z množičnim prihodom beguncev v Evropo v začetku leta 2016. V prenekaterih državah za obvladovanje varnostnih razmer policija ni uspela zagotoviti dovolj velikega števila osebja, zato so si pomagali z zasebnimi varnostnimi službami, katere so tako prihajale v stik z begunci in različnimi kulturami. Zasebne varnostne organizacije žal niso usposobljene za tovrstno delo in prihajalo je (oziroma prihaja) do prenekaterih konfliktov, ki so bazirali na nepoznavanju medkulturnih razlik, predsodkov in podobno. Kot primer lahko navedemo Nemčijo, ki ima po zadnjih podatkih več kot milijon beguncev nastanjenih v zbirnih centrih, ki jih varujejo zasebne varnostne organizacije. V izogib nepotrebnim konfliktom se je pojavila ideja o izobraževanju tovrstnega kadra.

Trendi v varnostnem okolju namreč kažejo, da bo omenjena problematika v naslednjem obdobju zelo izpostavljena in bo pred zasebno varnostne subjekte postavila pomembne izzive in dileme za učinkovito izvajanje svojega poslanstva ter nalog.

V teh dveh letih, kot traja projekt, se bo poskušalo pripraviti module za inštruktorje, ki bodo lahko v naslednji fazi izobraževali osebje zasebnih varnostnih organizacij. Omenjena vsebina bo izšla v priročniku, ki bo obsegal naslednje vsebine:

- Stereotipi, predsodki in socialna diskriminacija (razložena s praktičnimi študijami primerov, ki jih lahko trener uporabi tudi za svoje usposabljanje).
- Usposabljanje, kako se zavedati, prepoznati oz. odpraviti predsodke (praktične vaje za uresničevanje in odražanje lastnih stereotipov).
- Preprečevanje radikalizacije z medkulturnimi komunikacijskimi treningi.
- Medkulturno usposabljanje (kaj je kultura?, vrste kultur, simulacijske igre, kritični incidenti).
- Komunikacija s travmatiziranimi begunci.
- Kako graditi kontakt v skupini: Kako ustvariti sodelovanje v različnih in večkulturnih skupinah.

*avtor je član Slovenskega združenja korporativne varnosti

- Preprečevanje radikalizacije (učenje na primerih)
- Glavne oblike radikalizacije - osnovno znanje za učitelje (rasizem in desničarski ekstremizem, salafizem, diaspora-nacionalizem, turški nacionalizem v Evropi, antisemitizem ...)
- Pregled, katere module lahko trener kombinira med seboj.

Priročnik bo ugledal luč sveta v avgustu 2018. V ta namen se v teh dveh letih dogajajo različne aktivnosti in konference na katerih sodelujejo tudi predstavniki ICS Ljubljana in nekateri vidni člani Slovenskega združenja korporativne varnosti.

V mesecu juliju je mag. Miran Vršec mednarodnim partnerjem predstavil trenutno stanje na področju delovanja in organiziranosti zasebno varnostnih podjetij v Sloveniji ter v kratkem tudi zakonodajo na tem področju. V mesecu septembru so nekateri predstavniki sodelovali na programu »train the trainers« v Estoniji, kjer se je poskušalo pripraviti nekatere podlage za trenerje/inštruktorje, ki bodo v kasnejši fazi izobraževali osebje zasebnih varnostnih organizacij po posameznih državah. Z omenjenim projektom se bo nadaljevalo v mesecu aprilu 2018 na Irskem.

Zasebne varnostne organizacije žal niso usposobljene za tovrstno delo in prihajalo je (oziroma prihaja) do prenekaterih konfliktov, ki so bazirali na nepoznavanju medkulturnih razlik, predsodkov in podobno.

Po izdelavi ustreznega programa usposabljanja so v državah EU načrtovane izvedbe ustreznih izobraževalnih delavnic. Omenjena delavnica bo izvedena tudi v Republiki Sloveniji.

Naj za konec omenimo, da se omenjeni ERASMUS+ projekt lepo dopolnjuje z evropskim projektom RAN oz. RAN Centre of Excellence, ki ga je ustanovila Evropska komisija. To je vseevropska krovna mreža praktikov za ozaveščanje o radikalizaciji (RAN), ki ima namen preprečevati radikalizacijo in nasilni ekstremizem. Center odličnosti (RAN CoE) deluje kot vozlišče pri povezovanju, razvoju in razširjanju strokovnega znanja. To vključuje spodbujanje dialoga med praktiki, oblikovalci politik in akademiki na vključujoč način.

V omenjeni organizaciji oz. projektu tvorno sodeluje tudi Institut za korporativne varnostne študije, na nivoju nacionalne sheme RAN Slovenija. ■

Erasmus+

Avtor: mag. Miran Novak, univ dipl inž rač. in inf., Informatika d.d.*

ALI PRIDOBITEV CERTIFIKATA ISO/IEC 27001 ZAGOTAVLJA INFORMACIJSKO VARNOST?

V praksi si organizacije velikokrat postavljajo vprašanje ali standardizacija procesov in pridobitev certifikata skladnosti zagotavlja informacijsko varnost, ki jo v podjetju potrebujejo. Celoviti pristop do obvladovanja varnostnih in s tem tudi informacijskih tveganj je nemogoče zagotoviti samo skozi golo uvajanje posameznih standardov v organizacijo.

Da bi organizacija pridobila certifikat ISO/IEC 27001, mora zadostiti velikemu številu organizacijskih, kadrovskih, varnostnih, poslovnih in drugih zahtev, ki jih certifikacijski organi pred podelitvijo na presojah preverijo. Nato mora organizacija na letnih presojah dokazati, da uspešno vzdržuje doseženo raven, oziroma, da jo stalno izboljšuje. Na prvi pogled bi lahko rekli, da izpolnjevanje zahtev standarda in aktivnosti vzdrževanja certifikata zadoščajo za »mirno spanje«. V prispevku bomo pokazali, da je pridobitev certifikata dobra osnova za doseganje primerne ravni informacijske varnosti, da pa je sama po sebi še ne zagotavlja. Razlogov za to je več, v glavnem pa lahko govorimo o naslednjih:

- **Metoda standardizacije.** Standardi družine ISO/IEC in podobni, so nastali kot skupek dobrih praks odpravljanja pomanjkljivosti, ki so v preteklosti pripeljali do odstopanj, incidentov ali celo katastrof. Po analizi vzrokov in posledic so se poiskale poti, kaj bi bilo potrebno storiti, da bi se v bodoče takšnim dogodkom lahko izognili. Zbiranje dopolnitev standarda tako traja praviloma več let, preden se koristnih dopolnitev ne nabere dovolj, da je upravičena nova izdaja. Pred izdajo so dopolnitve podvržene razgrnitvi in zbiranju pripomb, šele po obsežnem preverjanju na več ravneh, je nova izdaja zrela za objavo in veljavnost. Področje informatike pa se zaradi svojega izjemno hitrega razvoja spreminja tako hitro, da nove izdaje standardov ne morejo dovolj hitro dohitevati novih izzivov, ki jih pred informatike dnevno postavljajo bodisi malopridneži, bodisi nove smeri razvoja stroke.
- **Presoje z metodo vzorčenja.** Certifikacijski organi doseganje ravni skladnosti s standardi presojajo z metodo naključnega vzorčenja, kjer ne pregledajo celotnega obsega poslovanja, za katerega se organizacija certificira, temveč le naključno izbrane segmente. Zato dejstvo, da presoja ni ugotovila neskladnosti in odstopanj, še ne pomeni, da le-teh v presojanem sistemu dejansko ni, ampak lahko skrite pred presojevalci in vzdrževalci čakajo kot čeri plitvo pod gladino, dokler slučajno ne naletimo nanje takrat, ko je najmanj potrebno, pogosto z usodnimi posledicami. Izvajanje presoj na drugačen način bi postopek certifikacije podražilo preko meja vzdržnosti in v bistvu pokopalo samo sebe s tem, da bi svojo klientelo odvrnilo od uvajanja standarda.

Na prvi pogled bi lahko rekli, da izpolnjevanje zahtev standarda in aktivnosti vzdrževanja certifikata zadoščajo za »mirno spanje«. V prispevku bomo pokazali, da je pridobitev certifikata dobra osnova za doseganje primerne ravni informacijske varnosti, da pa je sama po sebi še ne zagotavlja.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

- **Odnos do sistema.** Organizacije pogosto pristopajo k implementaciji elementov standarda in certifikaciji iz nepravih vzgibov. Namesto da bi se potrudile, da bi uvedeni sistemi dihali in živeli s poslovanjem, skušajo s čim manjšim denarnim/kadrovskim/organizacijskim vložkom pridobiti certifikat, ki nato obešen na zidu za čast in slavo, oziroma zaradi prijav na razpise, životari iz leta v leto, dokler presojevalci ne zmorejo poguma bobu reči bob in obelodaniti neskladnosti, z grožnjo odvzema certifikata. Na tak način pridobljen in vzdrževan certifikat seveda zagotavlja temu primerno raven varnosti.

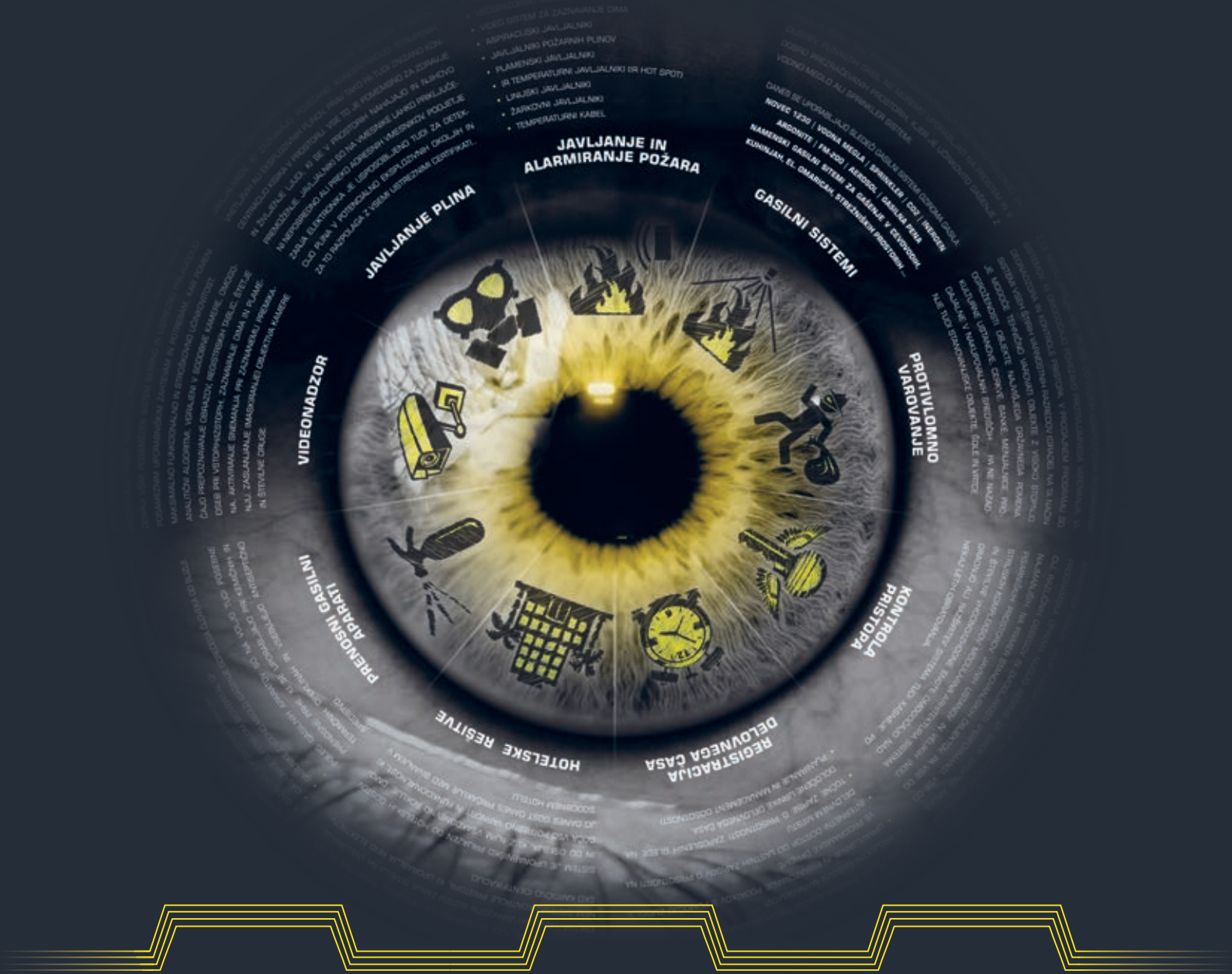
- **Togost.** Predvsem mala in srednja podjetja so bolj izpostavljena delovanju trga in se morajo za razliko od velikanov, ki razmere kreirajo, nastalim razmeram prilagajati. Pravočasne organizacijske spremembe, prilagoditev trženja in poslovanja, fleksibilnost pri upravljanju z viri, uvajanje novih izdelkov in podobni ukrepi pogosto predstavljajo ločnico med preživetjem ali propadom podjetja. Včasih se morajo te spremembe zgoditi zelo hitro, v nekaj tednih, ali celo nekaj dneh! Vzpostavitev standarda in certifikacija še ne zagotavlja, da bo sistem vodenja kakovosti omenjenim hitrim spremembam lahko sledil. Tako se lahko ustvarijo luknje, ki ostanejo nepokrite vse do naslednje presoje, v vmesnem času pa je organizacija izpostavljena nepotrebnim tveganjem.

- **Specifičnost.** Med pridobivanjem, ali pa že po pridobitvi certifikata se lahko izkaže, da je poslovanje organizacije tolikanj specifično, da »pade« izven standardov in samo doseganje zahtev standarda pusti nekatere segmente poslovanja nepokrite. Že samo ime »standard« nakazuje, da gre za splošna priporočila in »nestandardni« deli poslovanja tako lahko predstavljajo huda tveganja.

S poglobljenim študijem bi brez večjih težav lahko našteli še več razlogov, zakaj certifikat še ne pomeni zagotovljene varnosti. Na tej točki bi se marsikdo upravičeno vprašal, čemu potem sploh vlagati sredstva, trud in energijo v uvajanje standardov, certifikacijo in vzdrževanje. Izkaže se, da je večino navedenih pomanjkljivosti z malo dodatnega truda moč zaobiti in s tem zagotoviti višjo raven varovanja.

Vendar pa tudi s tem še nismo dobili zagotovila, da smo na varni strani. Poleg vzdrževanja standarda, ki predstavlja temelj, oziroma osnovo za gradnjo informacijske varnosti, je od primera do primera, od organizacije do organizacije potrebno študirati posebnosti, vlagati v izobraževanje in razvoj kadrov, ki za to skrbijo, sproti identificirati, vrednotiti in obvladovati tveganja, pogosto pa se celo poslužiti storitev zunanjih, vrhunskih strokovnjakov, ki si jih znotraj organizacije enostavno ne moremo privoščiti. Zavedati se moramo, da tudi na »temni strani« delujejo izjemni umi, ki žal svoje sposobnosti zlorabljajo v slabe in kriminalne namene. Za boj z njimi so potrebni enakovredni specialisti.

Za zaključek torej povzamemo, da je pridobitev certifikata šele prvi korak k celovitemu obvladovanju informacijske varnosti. Koristen je zato, ker dobro pokrije večino kritičnih področij, ker vzpostavi zavedanje in osnovna orodja, ker prisili organizacijo k neprekinjenemu razvijanju varnostnih sistemov, ker pripravi organizacijo na posledice morebitnih incidentov ali katastrof in ponudi splošne rešitve, ki organizaciji v takšnih primerih omogočijo preživetje. Potrebni pa so stalni napori in ukrepi za varno hojo po »noževi konici«, kar vsakdanje poslovanje v oceanu svetovnega spleta, polnega morskih psov, vsekakor predstavlja. Pri tem lahko veliko pomagajo specializirana podjetja, ki pokrpajo še preostale luknje, ki zevajo tudi še po uspešni pridobitvi certifikata. ■



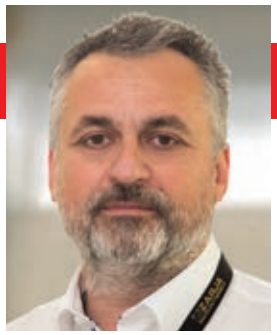
Varno v nov dan

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

www.zarja.com

ZARJA ELEKTRONIKA

Avtor: mag. Samo R. Zorko, univ.dipl.el.inž, varnostni menedžer / Zarja Elektronika d.o.o.*



GAŠENJE Z VODNO MEGLO

Voda je najstarejše in najbolj univerzalno gasilno sredstvo. Je učinkovita, poceni, na voljo je v velikih količinah. Lahko pa z njo naredimo tudi več škode kot koristi oziroma uničimo še tisto, čemur požar prizanese. Z vodo lahko požar tudi pospešimo, oziroma v primeru naprav pod napetostjo, ogrozimo življenja gasilcev in ljudi v neposredni bližini. Toda kljub vsemu povedanemu, je z vodo dovoljeno gasiti vse, kar se z vodo ne sme gasiti. Z vodo malo drugače ali s čisto majčkeno vodo ...

Lastnosti vode

Voda je z nekaterimi izjemami najbolj razširjeno in najcenejše sredstvo za gašenje. Ima ledišče pod 0°C in vrelišče nad 100°C, kar je ugodno za enostavno uporabo. Ima veliko specifično toploto in izparilno toploto. Specifična toplota vode je 4200 J/kgK, izparilna toplota vode pa znaša 2.26 MJ/kg. Učinek gašenja z vodo je predvsem hlajenje, oziroma kombinacija fizikalnih mehanizmov ohlajevanja trdne ali tekoče gorljive snovi, ohlajevanje plamena in ustvarjanje pare, ki onemogoča dostop kisika in zmanjšuje prenos toplotnega sevanja. Vodna para, ki pri tem nastaja, sicer zmanjšuje koncentracijo kisika, vendar je lažja od zraka, se hitro dviguje in premalo časa ostane v plamenu ali ob žareči površini.

Prednost vode je tudi, da je čisto gasilo, ni nevarna za zdravje ljudi ali okolje, je dokaj enostavna za skladiščenje in transport na večje razdalje (pretakanje po ceveh). Uporabiti jo je mogoče v različnih oblikah, kot curek, prho ali vodno meglo (ljudje lahko ostanejo v prostoru med gašenjem). Pri gašenju z vodnim curkom, le ta lahko prodre v notranjost žarečih snovi, kar pa, kot že rečeno, ni vedno zaželeno.

Med slabe lastnosti vode spada zmrzovanje pri nizkih temperaturah (ledišče),

razpad vode na vodik in kisik pri 1200°C, električna prevodnost (gašenje naprav pod napetostjo) in možnost reakcije pri stiku vode z drugimi snovmi (na primer alkalijske kovine). Lahko se pojavijo tudi opekline dihalnih poti, kar se zgodi pri vdihavanju zraka nad 60°C, nasičenega z vodnimi hlapi.

Običajni sprinklerski sistemi

Ti so v uporabi že zelo dolgo in so izredno zanesljivi, ne prožijo se po nepotrebnem – lažni alarmi. Ob povišani temperaturi zaradi požara se ampula v sprinklerski glavi razpoči in odpre ventil, voda začne brizgati iz šobe, dokler gasilci ne zaprejo glavnega ventila. Njihova prednost je omejitev gašenja, saj se sprožijo le šobe nad mestom požara. Voda je zaradi svoje velike uparjalne energije zelo učinkovito gasilo, vendar pri običajnih sprinklerskih sistemih večina vode odteče neuporabljene.

Zaradi velike porabe vode so cevi gasilnega sistema velikih premerov in potreben je velik rezervoar za gasilno vodo. Uporabljajo se običajne cevi, ki sčasoma v notranjosti korodirajo, zato ob gašenju priteka iz sistema nečista voda, kar do-

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

datno poveča škodo, ki je posledica gašenja. Slaba stran je tudi počasnost delovanja (dolg reakcijski čas), saj se ampula na temperaturo sproženja sistema segreje šele potem, ko je požar že kar obsežen.

Nekateri projektanti in investitorji zmotno mislijo, da jih lahko običajni sprinklerski sistem obvaruje pred večjo škodo na objektu. Zaščita pred večjo škodo pa je možna samo s kombinacijo sistema gašenja in zelo učinkovitega sistema za zgodnje odkrivanje požara (javljanje požara).

Voda kot megla

Voda je zaradi svoje velike uparjalne energije zelo učinkovito gasilo. Vendar pa je učinkovitost uporabe v klasičnih oblikah gašenja s cevmi in topovi ter običajni sprinklerski in njim podobni sistemi, zelo majhna. Velika večina vode ne opravi svoje naloge in ostane neuporabljena, samo majhen del se je dejansko porabi za gašenje – odvzemanje energije požaru. Posledice so očitne – poplavljeni objekti zaradi gašenja in škoda zaradi poplavne vode, ki je lahko celo večja od škode zaradi požara. Poznano je tudi, da se ob evakuaciji ljudje zelo neradi gibljejo skozi področje, kjer se je aktiviral sprinklerski sistem in prši voda.

Z razlogom povečanja učinkovitosti vode kot gasilnega sredstva in zmanjšanja posledic gašenja z vodo, je bil razvit sistem gašenja z vodno meglo (Water-mist: HiFog, FogTEC, FlexiFOG ...). Začetki teh gasilnih sistemov segajo v leto 1985, do nedavnega pa so se uporabljali le kot vgrajeni – stabilni sistemi za gašenje. Glede na njihov obratovalni tlak jih ločimo v nizkotlačne sisteme (do 16 barov), srednjetlačne sisteme (od 16 do 60 barov) in visokotlačne sisteme (nad 60 barov).

Sistem gašenja z visokotlačno meglo deluje podobno kot običajni sprinkler, a ima zaradi razpršitve vode v mikroskopske kapljice celo vrsto prednosti, saj je poraba vode minimalna, do 10-krat

manjša, gašenje pa poteka z ohlajevanjem, blokiranjem sevanja ter lokalnim zmanjševanjem koncentracije kisika.

Kapljice dobro prodirajo na območje požara, ljudje so lahko v prostoru tudi med gašenjem, škoda po požaru je minimalna, kar pomeni, da lahko delo skoraj nemoteno poteka naprej, saj se izpirajo tudi dim in drugi produkti gorenja. Sistem v celoti je zelo zanesljiv in zavzame manj prostora, saj je cevovod izdelan iz nerjavnih cevi majhnih premerov, ki se stikajo brez varjenja.

Področja uporabe

Na prvi pogled bi v mnogih aplikacijah, kjer se uporablja gašenje z vodno meglo, vodo kot gasilo povsem prepovedali, pa vendar ...

Ker je volumen vode minimalen, večina vode pri gašenju izpari, sekundarne škode pa praktično ni, je sistem vodne megle primeren celo za gašenje v galerijah umetnostnih slik neprecenljive vrednosti in v računskih centrih, kar večina ljudi težko verjame. Kot protipožarna zaščita se uporablja tudi na vseh luksuznih turističnih križarkah, v večini potniških ladij in na ladjah za vojaško uporabo. Prav tako številne kot ladijske so tudi zelo raznolike kopenske aplikacije: hoteli, bolnice, domovi za ostarele, letališča, pisarne, stanovanjski prostori, računalniški in telekomunikacijski centri, muzeji in stavbe kulturne dediščine, cerkve in katedrale, nebotičniki, kabelski tuneli, cestni in železniški tuneli, letališki hangarji in industrija vseh vrst. Od več tisoč objektov z vgrajenimi sistemi vodne megle jih navajamo le nekaj:

- National Gallery of Art, Washington D.C.,
- National Portrait Gallery, London,
- University Hospital, Münster Nemčija,
- Marriott Park Hotel, Rim,
- Scala, Milano,
- nadstropni cestni tunel v Parizu,
- podzemna železnica v Madridu,
- plinske turbine podjetja BASF v Ludwigshafnu,
- proizvodnja Airbus-a v Angliji ...

Za prostore z elektronskimi napravami je sistem vodne megle še dodatno dodelan in izpopolnjen. Generator megle v tem primeru proizvaja tako imenovano »suho« meglo, ki vse večje kapljice zajame in odvede v poseben rezervoar še preden jih vpiha v prostor, istočasno pa sesalni cevovod na nasprotni strani pro-

Kapljice dobro prodirajo na območje požara, ljudje so lahko v prostoru tudi med gašenjem, škoda po požaru je minimalna, kar pomeni, da lahko delo skoraj nemoteno poteka naprej, saj se izpirajo tudi dim in drugi produkti gorenja.

Ker je volumen vode minimalen, večina vode pri gašenju izpari, sekundarne škode pa praktično ni, je sistem vodne megle primeren celo za gašenje v galerijah umetnostnih slik neprecenljive vrednosti in v računskih centrih, kar večina ljudi težko verjame.

stora odsesa preostanke vodne megle, skupaj z dimom in produkti gorenja. Na ta način se takoj močno zmanjša temperatura v prostoru in koncentracija škodljivih in agresivnih snovi v zraku, ki so posledica požara. Številne demonstracije sistema, in pa predvsem praktična uporaba je prepričala vodilna računalniška podjetja (IBM, Western Digital, CISCO, Apple ...), da svoje podatkovne farme in postroje ščitijo enostavno z vodo.

Kot že omenjeno v prvi letošnji številki, je sistem vodne megle (Marioff HiFOG) instaliran v novem T-2 terminalu letališča Jožeta Pučnika, pri Inženirski Zbornici Slovenije (IZS) pa je izpostavljen kot primer dobre prakse. Potencialni objekti, kjer bi bil pri nas tudi primeren sistem gašenja z vodno meglo pa so še novi NUK, Potniški center Ljubljana, novi Kolizej, Prirodoslovni muzej, Fakulteta za kemijo in kemijsko tehnologijo, Fakulteta za računalništvo, Opera in balet SNG, Narodna galerija, farmacevtska industrija, hoteli, igralnice ...

Primerjava vodne megle s plinskimi sistemi gašenja

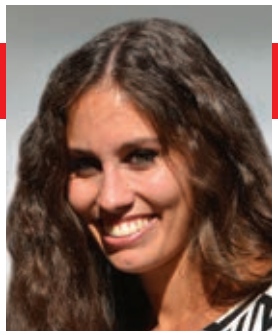
Sistemi gašenja s plini Novec, FM-200, Argon, Argonite, Inergen in drugi zahtevajo popolno tesnost prostora (zaprta okna, vrata, odprtine) in zadrževanje gasila še 10 minut po končanju gašenja, zato pa je gašenje zelo hitro (pri FM-200 in Novec 10 sekund, inertni plini pa 60 sekund po aktiviranju). Klima se mora izklopiti, zapreti se morajo vsi kanali (lopute) za prezračevanje. Za vse vrste plinastih gasil velja, da morajo ljudje pred aktiviranjem zapustiti prostor (ISO 14520-1 obravnava plinasta gasila v splošnem, različni deli pa se potem osredotočajo na uporabo posameznih plinov). Po končanem gašenju in pred vstopom nezaščitenih ljudi je potrebno prostor temeljito prezračiti.

Instalacijska cena plinskih sistemov je za majhne sisteme nižja od cene sistema z visokotlačno meglo, vendar pa se cena sistemov z vodno meglo postopoma niža zaradi vse več proizvajalcev tovrstnih sistemov in pogostejše uporabe. Sistemi z visokotlačno meglo ne potrebujejo tesnih prostorov, ljudje lahko ostanejo v prostoru tudi med gašenjem, čas gašenja je daljši (od nekaj deset sekund do nekaj minut), instalacijska cena pa je pri velikih sistemih nižja. Pri obeh sistemih je škoda povzročena zaradi gašenja minimalna, minimalen je tudi čas izpada delovnega ali drugega procesa.

Gašenje z vodno meglo ima številne prednosti:

- odlične lastnosti omejevanja požara oziroma gašenja in obvladovanja temperature,
- hitro delujoče razpršilne šobe (RTI ima vrednost 22),
- absorpcija dima in izpiranje dimnih delcev,
- minimalna poraba vode,
- majhna strojnica za vgradnjo vodnih rezervoarjev in opreme,
- nerjaveče jeklene cevi omogočajo preskušanje brez nevarnosti, da bi iztekala od rje umazana voda,
- enostavna in prilagodljiva instalacija brez varjenja z uporabo spojk,
- gasilo je čista voda, neškodljiva za ljudi in okolje,
- naključna neželena aktivacija ne povzroči škode, ne zahteva drage ponovne vzpostavitve sistema (ponovno polnjenje plinov) in povzroči minimalne zakasnitve v procesih. ■

Avtorica: Elena Blaževič, dipl.ekon. in absolventka mag. študija managementa korporativne varnosti



VARNOST IN OBVLADOVANJE TVEGANJ V INTERCONTINENTAL HOTELU LJUBLJANA

InterContinental Hotel Ljubljana (v nadaljevanju IC hotel), hotel svetovno znane verige IHG – InterContinental Hotels Group, je prvi pet zvezdični hotel v Ljubljani in se nahaja v samem središču mesta, na stičišču Tivolske, Dunajske in Slovenske ceste. Hotel je bil uradno odprt 27. septembra in ima 20 nadstropij, kjer se nahaja 165 sob.

Blagovne znamke so odvisne od njihovega ugleda. Da ustvariš dober ugled potrebuješ leta in leta, vendar se ta lahko uniči le v nekaj minutah. Eden izmed načinov, kako se ugled lahko izgubi, je nepravilno ravnanje ob incidentih in kritičnih varnostnih trenutkih. Tako je za svetovno znano verigo IHG primerna vzpostavitev varnostnega sistema ključnega pomena. Krizno upravljanje mora biti osrednja naloga vsakega organizacijskega sistema. Vsak hotel omenjene verige ima svoj tako imenovani »Crisis Manual« – krizni načrt, v katerem so opisana vsa morebitna tveganja in obvladovanje le-teh.

Hotel IC Ljubljana z visoko stopnjo organiziranosti in opremljenosti, s sposobnim vodstvom, s celovito hotelsko ponudbo, z izobraženimi, usposobljenimi in motiviranimi človeškimi viri ter z visoko stopnjo varnosti izraža razkošnost bivanja, zadovoljstvo gostov, poslovnost na ravni »deluxe« ter vtkanost vidne in nevidne varnosti v vse pore poslovnih procesov.

Hotel ima v svoj sistem varovanja uvedene ključne varnostne IHG standarde in sicer na področju tehničnega varovanja ter drugih varnostnih področij. To zagotavlja ustrezno podlago za celovito obvladovanje varnostnih groženj in tveganj ter omogoča hiter strokovni odziv na varnostne incidente, ki se pripetijo v kompleksu hotela. Varnostni standardi na področju tehničnega varovanja so dodana vrednost v varnostni arhitekturi hotela in v konkurenčni prednosti hotelskih storitev. Poleg tega uvedeni varnostni standardi prispevajo tudi k temu, da hotelski menedžment bolj učinkovito uresničuje načrt neprekinjenega poslovanja. Kajti poslanstvo, vizijo, poslovno strategijo ter tekoče poslovanje hotela lahko – poleg poslovnih težav – ovirajo tudi varnostni incidenti.

Varnostni incidenti lahko povzročijo škodo in izgubo premoženja in negativno vplivajo na varnost človeških virov, tako zaposlenih, kakor tudi gostov. Naloga in skrb vodstva hotela in vseh vpletenih v verigo odgovornosti za varnost je, da vzpostavijo in zagotavljajo učinkovit varnostni sistem, ki bo na eni strani preventivno zagotavljal minimiziranje varnostnih tveganj (preprečevanje varnostnih incidentov), na

drugi strani pa se hitro in strokovno odzival na nastale varnostne incidente.

Kakšna so morebitna tveganja, ki stojijo pred varnostjo v hotelski dejavnosti in kako jih obvladovati?

- **Tveganja človeških virov** – poznavanje zaposlenih in gostov je z vidika varnosti izredno pomemben segment varnostnega sistema. Človeški viri lahko predstavljajo resno varnostno tveganje. Lastni človeški viri (zaposleni), ki so usposobljeni in motivirani za doseganje visoke stopnje organizacijske in varnostne kulture, so garant, da se taka tveganja zmanjšajo na najmanjšo možno mero.

- **Tveganja kompleksa hotela** – ocena ogroženosti mora izpostaviti varnostno vitalne točke v zgradbi hotela in na zunanjem kompleksu hotela. IC Hotel za učinkovito in uspešno obvladovanje tovrstnih tveganj 24 ur na dan, vse leto, spremlja stanje varnostnega okolja s sodobnim video nadzornim sistemom in ustrezno opremo za analiziranje varnostnih incidentov. Videonadzor se opravlja z različnimi kamerami, katerih nadzor se izvaja iz nadzorno varnostnega centra. Vsi posnetki se hranijo in uporabljajo v skladu z določili veljavne zakonske podlage.

Zagotovljeno je vsakodnevno kakovostno spremljanje in analiziranje video nadzornih posnetkov, pri čemer varnostno osebje ugotavlja morebitne namene povzročanja varnostnih incidentov, ali druge kritične situacije na katere se je treba takoj odzvati.

Tako kot v vseh hotelih so tudi v IC hotelu vse sobe varovane z elektronskimi ključavnicami, za katere se za odpiranje uporabljajo elektronske kartice. V vsaki sobi se na podlagi sprejetega požarnega reda nahaja evakuacijski načrt. Poleg tega je v sobah sef, kjer gost shrani vrednejše stvari.
Poleg gostov imajo tudi vsi zaposleni svojo identifikacijsko kartico za vstop/izstop v službene prostore. S kartico ne samo dostopajo do prostorov, temveč z njo tudi beležijo svoj delovni čas.

- **Tveganja zunanjih pogodbenih izvajalcev** fizičnega in tehničnega varovanja, varovanja informacij in drugih izvajalcev varovanja. IC hotel ima sklenjeno pogodbo z zunanjim izvajalcem za tehnično in fizično varovanje. Zagotovljena sta kakovost, odzivnost in usposobljenost izvajalcev, nad katerimi se izvaja tudi ustrezno načrtovan nadzor kvalitete izvajanja storitev. Poleg teh pa ima hotel za izvajanje raznih del tudi druge zanesljive zunanje pogodbene izvajalce.

Da ustvariš dober ugled potrebuješ leta in leta, vendar se ta lahko uniči le v nekaj minutah. Eden izmed načinov, kako se ugled lahko izgubi je nepravilno ravnanje ob incidentih in kritičnih varnostnih trenutkih.

V turizmu se v ospredje vrednotenja turistične destinacije vztrajno prebija varnost bivanja, gibanja in koriščenja turističnih storitev.

- **Tveganja vgrajene varnostne opreme**. Hotel take kategorije se izkazuje s sodobno opremo tehničnega varovanja, kjer so upoštevani tudi vsi zgoraj opredeljeni varnostni standardi.

- **Globalna varnostna tveganja – tveganja terorizma**. Za obvladovanje tovrstnih tveganj je hotel konstrukcijsko zasnovan na osnovi predpisanih standardov, ki predstavljajo učinkovit mehanizem za obvladovanje navedenih tveganj. Poleg upoštevanja konstrukcijskih rešitev pa je bila pozornost usmerjena tudi v zagotavljanje nadzora nad človeškimi viri na segmentu gostov, zunanjih izvajalcev, obiskovalcev in drugih, ki se nahajajo v kompleksu hotela in bi lahko bili posredno in neposredno povezani z grožnjami terorizma.

- **Tveganja »obiskovalcev«, kateri to niso.** Gre za osebe z določenim negativnim namenom in sicer povzročitve varnostnega incidenta in za druge osebe, kot so prodajalci raznih izdelkov, monterji reklamnih letakov, brezdomci, iskalci informacij in druge osebe. Varnostnik take osebe opozori v okviru svojih pooblastil in primerno ukrepa, ob kritični situaciji pa pokliče policijo. Če ugotovi, da ima oseba namen povzročiti varnostni incident sproži načrtovano akcijo lastnega ukrepanja in ukrepanja varnostno nadzornega centra, ki po svojem načrtu sproži policijsko intervencijo. Sledi tudi analiza video nadzornih posnetkov.

Iz načinov obvladovanja tveganj je razvidno, da gre za preventivno vlogo varnostnega sistema. Če je zagotovljena preventivna vloga varnostnega sistema se lahko pričakuje veliko manj varnostnih incidentov in s tem minimiziranje škod in izgub.
Vodstvo hotela ima mesečne sestanke na temo varnosti hotela in hotelskih gostov, požarne varnosti, vključno s požarnimi vajami, sistemi evakuacije in drugo varnostjo. Tesno sodeluje s predstavniki policije in varnostnimi službami predvsem zaradi obiskov višjih domačih in tujih političnih in drugih predstavnikov.
Hotel IC obvladuje varnostna tveganja s preventivnim delovanjem, analizo in prepoznavanjem tveganj. V sistem varovanja hotela, hotelskih dejavnosti, hotelsko logistiko in spremljanje dogajanj v okolici kompleksa hotela, ima hotel poleg že omenjenih IHG standardov uvedene sledeče standarde: požarno varnostne standarde in standarde protivlomnega varovanja, videonadzora in kontrolo pristopa, standarde varnosti in zdravja pri delu in druge. Nekateri izmed standardov so bili uvedeni s pomočjo zunanjih certificiranih izvajalcev.
Hotel ima za upravljanje sistema varovanja izdelane določene varnostne dokumente. Požarni red in podrejeni dokumenti, izjava o varnosti z oceno tveganj na področju varnosti in zdravja pri delu, evakuacijski načrt, načrt videonadzora, varnostna navodila, načrt usposabljanja zaposlenih, načrt varovanja z varnostniki, načrt varovanja informacij, načrt delovanja recepcije, načrt protivlomnega varovanja, načrt varovanja poslovnih skrivnosti in druge.

Naj naštejem nekaj izmed IHG standardov, ki jih hotel upošteva:
RM02-01 - Vsi hoteli si prizadevajo zmanjšati vpliv kriz ali incidentov na zaposlene, goste, obiskovalce z opredelitvijo verjetnih tveganj, oblikovanjem načrtov in postopkov za njihovo obravnavo ter njihovim rednim testiranjem in pregledom.
RM02-02 - Vsi hoteli morajo razviti in preizkusiti splošni načrt za krizno upravljanje, ki ga je treba po potrebi posodobiti. Ta načrt mora vključevati kontaktne podatke in odgovornosti skupine za krizno upravljanje in ene ali več skupin za odzivanje v izrednih razmerah. Vsak hotel mora razviti in preizkusiti posebne načrte odziva za vrsto predvidljivih kriz in incidentov.
RM02-03 - Zaposleni morajo biti poučeni in usposobljeni za njihove dolžnosti, kot je opisano v načrtu za krizno upravljanje.
RM02-05 - Vsi hoteli si prizadevajo zmanjšati tveganje za poškodbe zaposlenih, gostov, povabljenih in druge „zainteresirane strani“ z ugotavljanjem verjetnih nevarnosti pri zaključku ocen tveganja, oblikovanjem in izvajanjem zaščitnih ukrepov in sistemov ter za redno testiranje in pregled teh ukrepov.

Hoteli v verigi IHG, kot tudi ostali, se najbolj soočajo s tveganji, kot so delovne nesreče in kriminalna dejanja. Želijo si tudi izboljšanja obvladovanja tveganj. V hotelski dejavnosti, logistiki in hotelskih storitvah se velikokrat zgodijo škodni pojavi. Največ je notranjih tatvin in delovnih nesreč. Veliko je nekontroliranih gibanj oseb, ki bi morale biti deležne varnostne pozornosti. Pojavijo se lahko škode kot so vdori v informacijski sistem, zloraba osebnih podatkov, uhajanje zaupnih podatkov ter kraja dokumentov.

Sklepna misel

V turizmu se v ospredje vrednotenja turistične destinacije vztrajno prebija varnost bivanja, gibanja in koriščenja turističnih storitev. Hotel IC Ljubljana lahko izkoristi dve konkurenčni prednosti. Prva je (še vedno in dokaj) varna Slovenija, kar pa sploh ni več samoumevno; in drugo, celovit varnostni sistem, ki gosta prepriča, da je prišel v hotel sproščenosti, zadovoljstva in varnosti s pridihom vračanja na isto destinacijo. InterContinental Hotels Group je največja svetovna veriga hotelov. Trdimo lahko, da so ocene ogroženosti in varnostnih tveganj ter standardi varovanja in varnostni menedžment InterContinental Hotela na najvišji ravni. Iz tega izhaja, da so storitve IC Hotela na turističnem trgu konkurenčne tudi z vidika zagotavljanja varnosti. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Andreja Marinčič, magistrica korporativne varnosti, druga diplomantka magistrskega programa »Upravljanja tveganj in korporativne varnosti«

MANAGEMENT KORPORATIVNE VARNOSTI POMEMBEN POKLICNI PROFIL PRIHODNOSTI

Pogovarjali smo se z drugo diplomantko magistrskega študija »Upravljanje tveganj in korporativne varnosti«, ki se izvaja na GEA College/Fakulteti za podjetništvo. Kot ena izmed prvih diplomantk vsekakor pušča neizbrisen pečat vezan na uveljavljanje nove profesije v Republiki Sloveniji.

Ste druga diplomantka podiplomskega magistrskega programa Upravljanje tveganj in korporativna varnost«. Kako se počutite kot ena od prvih diplomantk tega programa?

Spoznala sem, da mi je moj uspeh prinesel še večjo odgovornost do sebe, družine in do mednarodnega okolja, ki mu pripadam. Namreč vsak uspeh me še bolj obogati, vsaka izkušnja nagradi in moje poslanstvo je, da to delim v širšem mednarodnem okolju . Torej občutki so vsekakor izjemni, a ko sem magistrirala, sem se že naslednji dan s posebnim zadovoljstvom usedla na letalo in odšla novim poslovnim uspehom naproti, misleč: *‚memores acti prudentes futuri‘*.

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

Za študij sem se odločila zaradi zagotavljanja dodatne storitve našemu drugo žinskemu podjetju. Ob teoretičnem in aplikativnem znanju na področju NATO vojaških vaj ter kriznega odzivanja, sem svoje znanje želela nadgraditi in obogatiti z znanjem korporativne varnosti, skozi celotni spektrum socialnih dimenzij. Pričakovanja so bila presežena, kajti soočena sem bila z nenehnimi aplikativnimi izzivi študijskega procesa.

> Prednost današnjega informacijskega časa je, da lahko svoje znanje in izkušnje nadgrajujemo v vsakem danem času, kjer smo priča tudi vedno večjem številu spletnih študijskih izobraževanj.

Katere so tiste ključne ugotovitve in napotila, ki jih lahko posredujete mlajšim generacijam ob razmišljanju za vpis na študij Managementa korporativne varnosti?

Spomnim se svojih prvih vstopnih korakov v študijskih svet, ki me še dandanes popelje v čisto poseben svet, ki je lahko samo moj ali/in ga delim z ostalimi. Skozi leta lahko svoje male korake samo stopnjuješ in nikoli ne zmanjka tistih zmagovalnih stopnic do uspeha. Prednost današnjega informacijskega časa je, da lahko svoje znanje in izkušnje nadgrajujemo v vsakem danem času, kjer smo priča tudi vedno večjem številu spletnih študijskih izobraževanj. Ob prvem koraku se mora posameznik vprašati, kaj je namen njegovega študija in če je to tisto, s čimer bi se želel do potankosti soočiti. Ne samo mladi, vsi, ki so ali se bodo soočili s holističnimi te-

*avtor je član Slovenskega združenja korporativne varnosti

žnjami po kriznem odzivanju v mednarodnem in domačem poslovnem okolju, ex animi, morajo poznati principe tovrstnega kompleksnega vodenja. Iz tega izhaja dejstvo, da je študij Upravljanja tveganj in korporativne varnosti na Gea College, eden od redkih magistrskih študijev evropskega merila, ki to kompleksnost pokriva in zagotavlja.

Sam študij je bil prepleten z različnimi dopolnilnimi možnostmi za izpopolnjevanje in preverjanje teoretičnih spoznanj v neposrednih praktičnih okoljih. Vam je ta možnost omogočila pridobitev ustrezne širine znanja, ki je aplikativen v realnem okolju?

Nedvomno največja izkušnja študija izhaja iz udeležbe na različnih srečanjih in delavnicah, na katerem je imel aktivno vlogo tudi Inštitut za korporativno varnost. Študentje smo se mnogokrat soočili z mnogoterimi poslovnimi in varnostnimi dilemami, ki se pojavljajo znotraj različnih podjetij in korporacij. Izjemno se mi je vtisnila tudi mini-vaja, kjer smo študentje morali simulirati vloge Top managementa, ki se je v danih kriznih situacijah preoblikoval v krizni štab s svojim kriznim procesom odločanja. Bila je neprecenljiva izkušnja, katero bom nedvomno v prihodnje izkoristila za trženje storitev našega podjetja.

Vaš naslov magistrskega dela je bil posvečen področju kritične infrastrukture. Kakšne so ključne ugotovitve vaših raziskav na omenjenem področju?

Področje zaščite kritične infrastrukture me spremlja že od študija obramboslovja na FDV-ju. Področje zaščite kritične infrastrukture je področje, katerega se tako posamezne države kot tudi podjetja vedno bolj zavedajo. Potrebno je bilo kar nekaj časa, da je Slovenija prišla do stopnje, kjer imamo Predlog zakona o zaščiti kritične infrastrukture. Pozitivno spoznanje je, da se bo tudi pri nas področje kritične infrastrukture pravno-formalno uredilo. S tem se bodo zadovoljili pogoji EU in vzpostavil se bo vsaj začetni sistem celotnega kriznega odzivanja za zagotavljanje nenehnih vitalnih poslovnih procesov in družbene kontinuitete. Kljub pozitivnemu razmišljanju moramo vedeti, da, ko govorimo o zaščiti kritične infrastrukture, se velikokrat ne zavedamo kako je pravzaprav to področje kompleksno. Od analize tveganj in vplivov, inter- in intra- povezanosti posameznih sistemov, do preproste zadolžitve odgovornosti posameznikov. Ključ mojih ugotovitev je, da ima kritična infrastruktura v Sloveniji izjemen potencial in da bo v prihodnje razvila svoj enovit proces zagotavljanja poslovne kontinuitete. S tem bomo dvignili raven nacionalne/regionalne varnosti in zaščite vitalnih delov družbe, kakor tudi prispevali kot članica EU.

Trenutno nadaljujete svojo pot v družinskem podjetju Dr DM, kjer se težiščno ukvarjate z različnimi računalniškimi simulacijami in organizacijo računalniško podprtih vaj. Bodo ugotovitve in znanje, ki ste jih pridobili skozi študij aplikativno uporabne pri delu na tem področju?

Naš direktor podjetja, dr.Dušan Marinčič, je pionir na področju kriznih simulacij v svetovnem merilu, ki je tudi ena od storitev podjetja Dr DM. S študijem Managementa korporativne varnosti, smo v podjetju Dr DM razširili ponudbo izde-

lave scenarijev in načrtovanja kriznega procesa odločanja tudi za podjetja. Pridobljena znanja študija managementa korporativne varnosti ter poslovne dolgoletne izkušnje s področja strateško operativnega okolja NATO vojaških vaj, nam je omogočilo razširiti krog potencialnih strank. S tem pa so se izpolnila vsa pričakovanja vloženega časa in truda tekom študijskega procesa.

Veliko projektov izvajate za NATO. Kako v tem okolju prepoznajo tveganja, ki jih prinaša neustrezno upravljanje kritične infrastrukture?

Skozi vsa ta poslovna leta ostaja naša zvesta stranka NATO organizacija, ki je v prvi vrsti politična entiteta, z velikimi vojaškimi mehanizmi, ki so ji vseskozi na voljo. Letošnje in naslednje leto sva oba z direktorjem vpeta v izdelavo realističnega scenarija, ki ga bodo NATO članice uporabljale še v prihodnje. Gre za izredno realističen scenarij, z realnimi varnostnimi grožnjami, ki s celostnimi hibridnimi aktivnostmi negativno vplivajo na NATO in EU članice. Iz tega izhaja, da se vse bolj upošteva in uveljavlja ne samo politično in vojaško, temveč tudi ekonomsko, socialno, infomacijsko in infrastrukturno področje vpliva, znotraj NATA. Na tem mestu se vse bolj pojavlja in upošteva beseda ¨resilience¨, ki poudarja pomen celovite zaščite družbe in njenih vitalnih delov, vsake članice NATA. S tem se tudi v našem scenariju pojavlja zaščita kritične infrastrukture, ki je velikokrat tarča različnih in oddaljenih oblik ¨cyber-napadov¨. Iz tega izhaja zavedanje NATA, da je prav vsaka članica primorana zagotoviti nacionalno zaščito kritične infrastrukture, a vendar obstajajo in so na voljo mehanizmi ter sredstva, kjer NATO lahko in bo prispeval za dobrobit vseh članic.

> Ključ mojih ugotovitev je, da ima kritična infrastruktura v Sloveniji izjemen potencial in da bo v prihodnje razvila svoj enovit proces zagotavljanja poslovne kontinuitete.

Ocenjujete, da se lahko slovensko znanje na področju korporativne varnosti uveljavlja tudi v širšem mednarodnem okolju v katerem trenutno zelo aktivno delujete?

Vsekakor da! Premalokrat se zavedamo, kako proaktivni in kreativni smo kot narod. Temu pričajo tudi današnji mladi slovenski podjetniki in njihovi uspešni start-up projekti. Samo poglejte moj primer, sem mati dveh izjemnih deklic, nenehno potujem in se izobražujem ter služim svoj kruh izključno z mednarodnimi projekti. Do sedaj kot podjetje nismo veliko poslovali v slovenskem okolju. V tujini nas cenijo, kajti pripravljeni smo delati, smo disciplinirani, izjemno kreativni in razvijamo projekte v skladu z zahtevami stranke ter naših strokovnih predlogov. Povejte mi, kdo si ne bi želel delati z vrhunskimi strokovnjaki, ki ponujajo inovativne rešitve in tlakujejo nove poslovne priložnosti. Slovensko znanje je izjemno in kot pravi Shakespeare, `the world is your oyster`, kar pomeni, da lahko počnemo vse in kjerkoli, z znanjem pa še toliko uspešnejše. ■

Študijski program 2. stopnje

geacollege
fakulteta za podjetništvo

Management korporativne varnosti

Magistrski študijski program (2 letni študij)

Izredni študij

Cilj študija

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

Zakaj **Management korporativne varnosti**?

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

Komu je študij namenjen?

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

Management korporativne varnosti

Magistrski študijski program

Študijski program in način študija

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

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

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

Predmetnik

I. LETNIK

Skupni obvezni predmeti

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

I. in II. LETNIK

Obvezni smerni predmeti

Smer Korporativni varnostni manager

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

Smer Korporativni varnostni manager – podjetnik

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

Izbirni predmeti (študent izbere dva):

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

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

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

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

CENTER VIŠJIH ŠOL

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

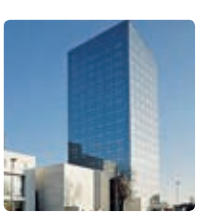
FAKULTETA ZA PODJETNIŠTVO

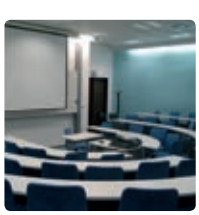
Dodiplomski programi
(3 letni študij):
- Podjetništvo
- Premoženjsko svetovanje

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

POSLOVNO-IZOBRAŽEVALNI CENTER

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





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

BREZPLAČNA ŠTEVILKA
080 11 20

geacollege
fakulteta za podjetništvo

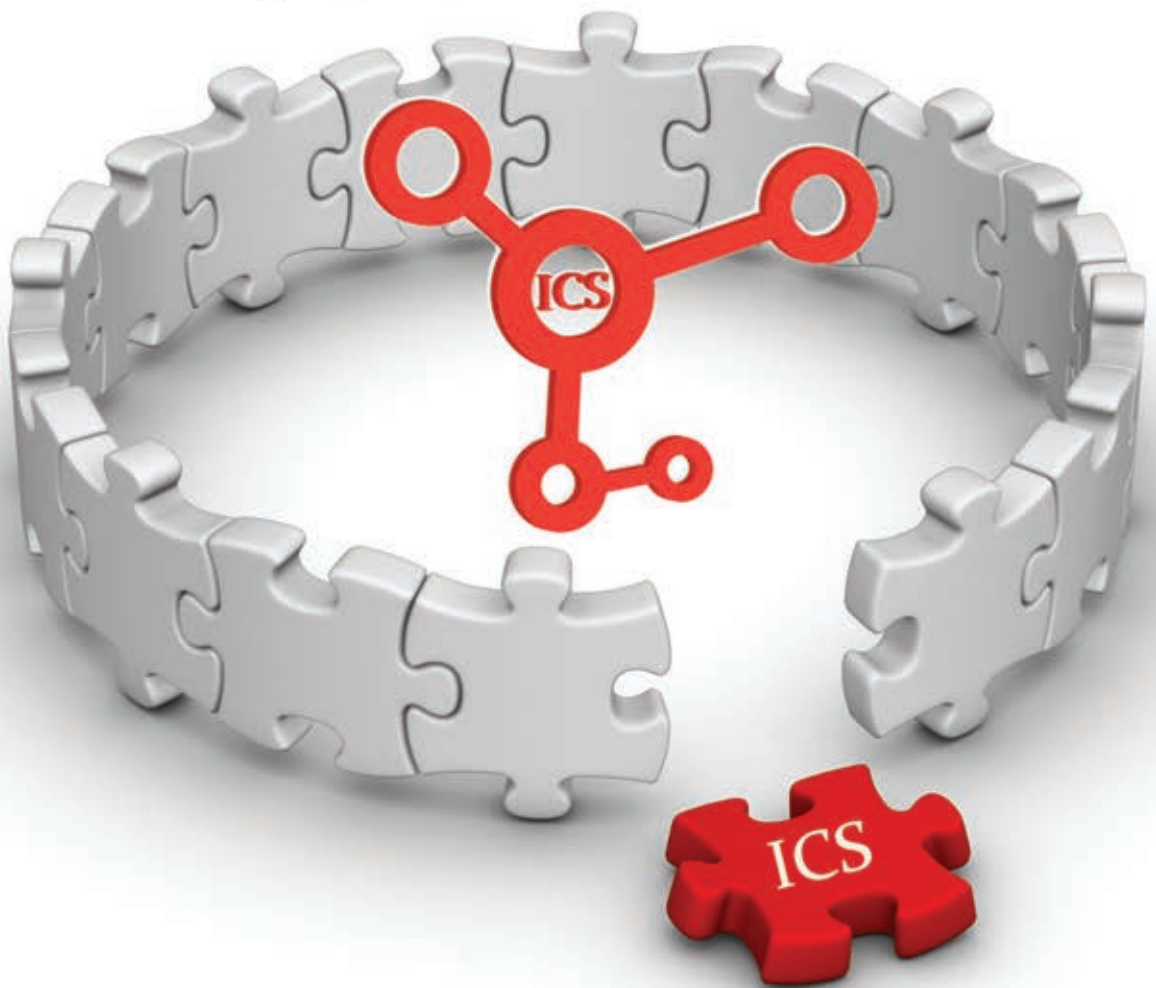
9. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

INFORMACIJSKA VARNOST DANES IN JUTRI

Ljubljana, 14. — 15. marec 2018



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI