Korporativna varnost

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

Letnik 2021, september • št. 26



Podelitev prestižnih nagrad

»Slovenian Grand Security Award«

Varnost velikih športnih dogodkov vedno predstavlja poseben izziv

Blaž Perko, generalni sekretar Olimpijskega komiteja Slovenije



S SISTEMSKIM VARNOSTNIM PREGLEDOM IN PENETRACIJSKIM (VDORNIM) TESTIRANJEM DO VEČJE KIBERNETSKE VARNOSTI

V okviru instituta deluje Center za informacijsko varnost, ki se v prvi vrsti ukvarja s področjem testiranja v IT okoljih oziroma varnostnimi pregledi.

- ⇒ Prepoznavanje in odkrivanje šibkih točk v organizacijah
- ⇒ Ocena skladnosti varnostnih politik
- ⇒ Ocena skladnosti vse programske in strojne opreme
- ⇒ Preizkusi ozaveščenosti zaposlenih o varnostnih vprašanjih
- ⇒ Odziv v primeru varnostnega incidenta na podlagi realno izvedljivih metod
- ⇒ Ravnamo se po več mednarodno priznanih metodologijah
- ⇒ Uporabljamo vrsto različnih programov in pripomočkov
- ⇒ Rezultat varnostnega testiranja so pisna poročila in so ključnega pomena pri zagotavljanju najvišjih standardov organizacije
- ⇒ Organizacijam priporočamo opravljanje varnostnega pregleda in testiranje v letnem intervalu ali po vsaki večji implementaciji oz. spremembi v IT okolju

Ekipa strokovnjakov Instituta za korporativne varnostne študije, ki je specializirana za kibernetsko varnost, bo s poglobljenim tehničnim znanjem ter pridobljenimi certifikati poskrbela za strokovno in neodvisno testiranje, ki vam bo razkrilo ranljivosti vašega informacijskega sistema.

Želite izvedeti več:
ICS Ljubljana / e-naslov: info@ics-institut.si / telefon: 05 90 54 300 / spletna stran: www.ics-institut.si

ICS

C|EH™ Certified Ethical Hacker

OFFENSIVE security OSCP

ISO 27001

CERTIFIKAT O USPEŠNO OPRAVLJENEM IZPITU ZA VODILNEGA PRESOJEVALCA ZA PODROČJE PR320: ISMS ISO 27001:2013

BUREAU VERITAS 1828

DPO

CERTIFIKAT O USPEŠNO OPRAVLJENEM ZAKLJUČNEM IZPITU NA SEMINARJU ZA POOBLAŠČENO OSEBO ZA VARSTVO OSEBNIH PODATKOV



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:
september 2021

Izvod revije je brezplačen

Naslovnica in slike:
ID 136191118 © Alexandersikov | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

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

Pred kratkim smo beležili 20. obletnico terorističnih napadov na ZDA, ki so korenito spremenili svet. Še posebej so bile v tem obdobju močno izražene spremembe varnostnega okolja in groženj, ki so pomembno vplivale na procese strateških razmerij med posameznimi deležniki v mednarodnih odnosih. Nekateri analitiki ocenjujejo, da je umik mednarodnih sil iz Afganistana in ponoven prihod Talibanov na oblast, strateški polom, ki bo imel za mednarodno okolje dolgoročne posledice. Razlogi in dejstva, ki so pripeljali do tega, so kompleksni in je situacijo nemogoče obravnavati v dimenziji črno-bele situacije. Pomembneje pa je razumeti, da se je tudi pandemija COVID-19 močneje zarezala v vse pore nacionalnih in mednarodnih odnosov, kot si sploh lahko predstavljamo in so dejanja, ki se dogajajo v času trajajoče epidemije, samo rezultat teh tihih tektonskih sprememb. Vse to pa ima pomemben vpliv tudi na poslovna in druga organizacijska okolja. Spremembe se dogajajo v ožjem družbenem okolju tudi v Sloveniji, kjer so vedno bolj izpostavljene napetosti v javnih in zasebnih okoljih. Vse te napetosti pa pomembno vplivajo tudi na zagotavljanje korporativne varnosti v organizacijskih okoljih. Vedno pogostejše pojavljanje nestrpnosti in napetosti, ki jih predstavlja radikalizacija stališč posameznikov ter ožjih interesnih skupin, lahko hitro prestopijo črto, kjer bo zagotavljanje varnosti postalo resen izziv. Od nestrpne komunikacije do izvajanja nasilja za uveljavljanje določenih stališč ni dolga pot. Nihče si ne želi, da bi AMOK situacije v naših organizacijah postale naslovna zgodba medijskega prostora. Če vse to postavimo v luč zahtevnih mednarodnih varnostnih izzivov, kot so kibernetska tveganja, nelegalne migracije, organiziran kriminal, terorizem, vedno močnejši vpliv naravnih nesreč na delovanje naših organizacij in seveda ponovno slabšanje epidemioloških kazalcev, lahko hitro ocenimo, da bo dinamika na področju zagotavljanja korporativne varnosti v naslednjem obdobju še intenzivnejša in bo od nas zahtevala ustrezno prilagodljivost ter popolnoma nove pristope. Zaradi navedenega je tako pomembno še močneje nadaljevati po poti izmenjave novih spoznanj in dobrih praks.

V tokratni številki revije smo ravno zaradi tega, del prostora namenili nagrajencem, da z našimi bralci podelijo dobre prakse, katere so jim omogočile prejem teh prestižnih nagrad. Poleg navedenega smo želeli vsebinsko osvetliti dovolj širok spekter strokovnih prispevkov, da v tem okviru prenesemo določene nove vidike in izkušnje tudi na področja, ki jih prinaša uvajanje novih tehnologij. Tudi področju kibernetske varnosti in uvajanju novih raziskav namenjamo pomemben spekter prispevkov v sami reviji, prostor pa dajemo tudi ostalim varnostnim vsebinam. Posebej bi želel izpostaviti strateško geopolitično oceno, ki jo tudi tokrat prinaša kolumna. Izkoristili smo priložnost in se pogovorili s pomembnimi strateškimi voditelji in strokovnjaki z različnih področij, ki z nami delijo svoje izkušnje in strateške poglede. Posebej velja izpostaviti nedavno končane Olimpijske igre v Tokiju, smo z varnostnega vidika namenili pomemben del pozornosti.

V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi v bodoče.

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
Peter Dermol, župan Mestne občine Velenje

MESTNA OBČINA VELENJE SMELO UVAJA NOVE PRISTOPE NA PODROČJU VARNOSTI

5



KOLUMNA
Vojko Volk, veleposlanik

ZAČETEK KONCA GLOBALIZACIJE

13



INTERVJU
Srečko Ocvirk, župan Občine Sevnica

VARNOST KOT POMEMBNA VREDNOTA OBČINE SEVNICA

18



INTERVJU
mag. Andrej C. Rant, skrbnik informacijske varnosti v ELES d.o.o.

INFORMACIJSKA VARNOST V ELEKTRO-ENERGETIKI DOBIVA NOVE RAZSEŽNOSTI

28



KVANTNA IZMENJAVA KLJUČA OBETA VISOKO STOPNJO VARNOSTI KOMUNIKACIJ

Kvantni ključi so zaporedja naključnih števil, ki se na daljavo vzpostavijo z izmenjavo posameznih fotonov, kvantov svetlobe in protokol izmenjave poteka po zakonih kvantne mehanike. Če bi kdo ta ključ poskušal prestreči, bi takoj pustil sled, ki bi sogovornikom omogočila, da vdor zaznajo in nemudoma ukrepajo.

37

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Peter Dermol, župan Mestne občine Velenje

MESTNA OBČINA VELENJE SMELO UVAJA NOVE PRISTOPE NA PODROČJU VARNOSTI

Varnost postaja izredno pomemben dejavnik zagotavljanja ustreznega okolja za nemoteno delovanje lokalnih skupnosti. Prebivalci temu namenjajo vedno večjo pozornost. Ob tej priložnosti smo se o pomenu lokalne varnosti in pomenu prejete nagrade Slovenian Grand Security Award pogovarjali z g. Petrom Dermolom.

Septembra vaša mestna občina praznuje občinski praznik. Kako pomembna je za vas kot župana varnost mestne občine, ki jo vodite, in kakšno stališče imajo do varnega okolja vaši občani?

V lokalni skupnosti veliko pozornosti namenjamo skrbi za različne skupine ljudi – otroke, mlade, starejše, invalide – vse z namenom, da se naši občani počutijo dobro in varno. Skrb za varno okolje je zagotovo na najvišjem mestu naših vrednot in ciljev. Verjamem, da se vsi zaposleni v občinski upravi zavedajo, da je naše delo, da ščitimo javni interes, in da je naš temeljni cilj, da se občani v Velenju počutijo dobro. Nenazadnje je dobro, da se tudi turisti počutijo varno. Ponosen sem, da nam tudi to v Velenju, še posebej z dobrim obiskom na Velenjski plaži, odlično uspeva. Nas je pa zadnje leto, ko smo se soočali z epidemijo, naučilo in poučilo, kako zelo pomembno je sodelovanje in povezovanje različnih služb, katerih osnovna naloga je nudenje in zagotavljanje varnosti. V Velenju smo dokazali, da imamo to res odlično urejeno in se lahko upravičeno pohvalimo, da smo primer dobre prakse na tem področju.

Mesta občina Velenje je prejemnica nagrade **»Slovenian Grand Security Award«** v kategoriji **»Najbolj varno mesto leta 2020«.**

Naši občani cenijo varno okolje, ki ga nudimo in zagotavljamo v Velenju. Vsi skupaj smo na prejeti naziv naj varno mesto v letu 2020 zelo ponosni. Posebna pohvala in zahvala je namenjena tudi celotni ekipi sodelavcev in institucijam, ki skrbijo za to, da je Velenje resnično varno mesto, nenazadnje pa tudi našim občankam in občanom, saj brez njih ne bi bili to, kar smo.

Mestne občine imajo za razliko od ostalih občin specifične izzive na področju zagotavljanja varnosti. Verjetno pa je skupno vsem, da se srečujete z relativno omejenimi viri. Kako vam uspe poleg vseh pristojnosti in nalog, postaviti zagotavljanje varnosti kot pomemben izziv za vas in vaše sodelavce. Kako se ga lotevate?

V Mestni občini Velenje se lahko pohvalimo predvsem z dobrim sodelovanjem in rednimi srečanji med različnimi subjekti – službami, ki se redno sestajajo v okviru Sosveta za varnost občank in občanov Mestne občine Velenje. Ta opravlja naloge, ki so usmerjene k zagotavljanju večje varnosti občanov, spodbujanju in vplivanju občanov na varnostno organiziranje, aktivnemu spremljanju, preprečevanju in odpravljanju različnih asocialnih pojavnosti. Sosvet skrbi tudi za razvijanje, uveljavljanje in zagotavljanje navodil in predpisov, ter posledično izvajanje ukrepov, ki prispevajo k večji varnosti, osveščenosti, medsebojni povezanosti ter pomoči na naslednjih področjih:

*avtor je član Slovenskega združenja korporativne varnosti



1. varnost, preventiva in reševanje problematike na področju kriminalitete in drugih odklonskih pojavov,
2. javni red in mir,
3. varnost, vzgoja in preventiva v cestnem prometu,
4. druga področja, ki neposredno ali posredno vplivajo na varnost občanov.

V sosvetu za varnost občank in občanov, ki deluje pod okriljem predsednika mag. Iztoka Morija, direktorja občinske uprave, sodelujejo predstavniki občinske uprave, Medobčinske inšpekcije, redarstva in varstva okolja, Upravne enote Velenje, Policijske postaje Prometne policije Celje, Centra za socialno delo Velenje, Zdravstvenega doma Velenje, Šolskega centra Velenje, Visoke šole za varstvo okolja, poveljnik občinskega gasilskega poveljstva Velenje, Aktiv ravnateljev osnovnih šol Velenje, Svet za preventivo in vzgojo v cestnem prometu in Mladinski center Velenje.

Sosvet obsega res širok nabor institucij in s tem zajamemo tudi vse starostne skupine občanov. S pravočasnimi in strokovnimi ukrepi lahko hitro preventivno ukrepamo in zajezimo pojav morebitnega tveganja.

V zadnjih desetih letih ste letos že drugič prejeli prestižno nagrado Slovenian Grand Security Award v kategoriji najbolj varno mesto. Nam zaupate recept za tako uspešno pot?

Naziv najbolj varno mesto v letu 2020 je potrditev večletnega kakovostnega in strokovnega dela številnih institucij in izjemnih posameznikov. Kriterij je torej visok in naš cilj je, da ta standard ohranjamo in se še izboljšujemo. Tudi zato smo nemudoma nadgradili naše aktivnosti, in sicer bomo še bolj pozorni na sprotno preverjanje občutka varnosti pri občanih (npr. ankete). V zadnjem času smo precej bolj pozorni tudi na osveščanje mladih o varnem spletnem komuniciranju. Vemo, da so prikrajšani za druženja in, da po socialnih omrežjih »klepetajo« precej več, kot bi si želeli.

Ob tej priložnosti bi se zahvalil tudi ekipi Inštituta za korporativno varnost, ki je zaznala prizadevanja in kakovost našega dela ter prepoznala Velenje kot primer dobre prakse.

Kakšno težišče namenjate varnostnemu sosvetu v občini in vključevanju različnih interesnih skupin na lokalnem nivoju pri zagotavljanju varnega okolja?

Sosvet za varnost občank in občanov MOV je pomembno posvetovalno telo za učinkovito zaznavanje problemov ter seznanjanje vseh članov oz. interesnih skupin s stanjem varnosti in morebitnih težav v lokalni skupnosti in na primeren in učinkovit način reševanje problematike.

Sosvet se sestaja občasno, ob pojavu posebnih nevarnosti pa so na pobudo župana sklicani tudi izredno.

Kako bi ocenili sodelovanje na lokalni ravni s pomembnimi institucijami, kot je na primer policija?

V naši lokalni skupnosti je sodelovanje zelo dobro in učinkovito – tako na vodstveni ravni (sestanki, sosveti), kot pri delu na terenu (skupne patrulje občinskih redarjev in policije). Sodelovanje med lokalno skupnostjo in policijo ima v Velenju tudi zelo dolgo tradicijo. Bilo je prepoznano kot primer dobre prakse (policija-redarstvo) in tudi večkrat izpostavljeno na različnih dogodkih. Dober rezultat sodelovanja se pozna tudi pri izvajanju vsakodnevnih nalog.

Vedno bolj smo izpostavljeni tveganjem, ki izhajajo iz informacijskega okolja. Ali v občini področju kibernetske varnosti namenjate dodatno pozornost?

Služba za informatiko Mestne občine Velenje skrbi za kibernetsko varnost. Zagotavljajo in izvajajo sistemske varnostne preglede, skrbijo za osnovno



Verjamem, da se vsi zaposleni v občinski upravi zavedajo, da je naše delo, da ščitimo javni interes, in da je naš temeljni cilj, da se občani v Velenju počutijo dobro. Nenazadnje je dobro, da se tudi turisti počutijo varno. Ponosen sem, da nam tudi to v Velenju, še posebej z dobrim obiskom na Velenjski plaži, odlično uspeva.

izobraževanje glede kibernetske varnosti, izvajajo obdobna izobraževanja o varni uporabi socialnih omrežij, skrbijo za pravilno in varno uporabo elektronske pošte, osebnih podatkov v spletu ipd. Zaposleni na področju informatike se tudi redno udeležujejo posvetov na temo kibernetske varnosti oziroma informacijske varnosti.

Uvajanju novih projektov, ki so posredno in neposredno povezani z dvigovanjem varnosti občanov, namenjate veliko pozornost. Nam lahko zaupate kakšen primer dobre prakse?

Policijska postaja Velenje in Skupna občinska uprava Savinjsko-šaleške regije (Služba medobčinske inšpekcije, redarstva in varstva okolja) sta na področju varnosti v lokalni skupnosti izoblikovali model, ki zelo dobro vpliva in pripomore k varnosti občanov na različnih področjih. Prav tako so se izvajale naloge iz pristojnosti policije in redarstva, s katerimi želimo odkrivati kazniva ravnanja in preprečevati različna prepovedana dejanja, kot so vandalizem, razne kršitve javnega reda in miru, kazniva dejanja ter varnost prometa. S prisotnostjo uradnih oseb v okolici šol, avtobusnih in železniških postaj se tako odkriva ter preprečuje nasilje med vrstniki. Ta oblika dela poteka tako v dnevnem, kot tudi v nočnem času. Občani so skupno delo občinskih redarjev in policistov zelo dobro sprejeli. Nenazadnje je navedena oblika dela zelo pomembna pri pomoči in sodelovanju z občani, kjer se krepi zaupanje in pozitiven odnos v skupnosti ter občutek varnosti pri ljudeh.

V okviru Mladinskega centra Velenje deluje »eMCe plac ozaveščа«, ki širi osveščanje o negativnih učinkih drog med mladimi.

V okviru projekta, Otrokom prijazno Unicefovo mesto, imamo v Velenju 20 varnih točk, kamor se lahko otroci in mladostniki zatečejo po pomoč, kadar so ogroženi ali pa so v stiski. V zadnjem letu smo preko občinske spletne strani obveščali tudi o Unicefovih varnih točkah v času, ko smo doma, kakšne oblike nasilja pretijo na spletu ter kako se obvarovati pred njimi.

Člani Medobčinske lokalne akcijske skupine za preprečevanje zasvojenosti z drogami Velenje so se pridružili 14. nacionalni konferenci ob mesecu preprečevanja zasvojenosti v virtualni obliki s sloganom Skupaj zmoremo več: opolnomočeni strokovnjaki – opolnomočeni mladostniki.

Skupaj z NEODVISEN.SI smo v okviru Medobčinske lokalne akcijske skupine za preprečevanje zasvojenosti z drogami Velenje organizirali dogodek IZZIVALEC ULICE ZA MLADE za dijake 3. in 4. letnikov Šolskega centra Velenje.

Kljub posebnemu letu, ki je bilo zaznamovano z epidemijo, smo ob občinskem prazniku v mesecu septembru organizirali prireditve, na katerih smo dosledno upoštevali priporočila za preprečevanje okužbe s koronavirusom. Tudi zato, ker so se občani počutili varno, je bil obisk prireditev nad pričakovanji.

Finančno smo podprli delo v terapevtski skupini zdravljenih alkoholikov Breza v Velenju. Še naprej spodbujamo delovanje Dnevnega centra za zmanjševanje škode zaradi drog Velenje, ki deluje preko Šenta (Slovensko združenje za duševno zdravje), Društvo Projekt Človek na CSD Velenje ter eMCe plac ozaveščа.

Mestna občina Velenje podpira tudi delovanje Medobčinske zveze prijateljev mladine Velenje (MZPM Velenje), ki s svojimi projekti preventivno deluje med otroki in mladino na področju varnosti v šolah in problematike nasilja. Na zasedanju otroškega parlamenta osnovnošolci razpravljajo o problematiki, povedo svoja mnenja in zahteve. MZPM Velenje že več let izvaja projekt Šola za starše, v sklopu katerega se enkrat mesečno odrasli srečujejo in s pomočjo predavateljev obravnavajo teme s področja vzgojne problematike. Posebno pozornost se posveča pojavu vrstniškega nasilja, varnosti otrok, zasvojenosti in komunikaciji, npr. varni uporabi interneta ipd.

Kaj bi za konec želeli sporočiti vašim občankam in občanom in seveda širši slovenski javnosti? Bo Mestna občina Velenje tudi v bodoče sledila svojim smelim načrtom zagotavljanja varnosti na svojem lokalnem nivoju?

Skrb za dobro in varno počutje naših občank in občanov je naša prioriteta in zagotovo bomo ta cilj zasledovali pri izvajanju vseh naših nalog tudi v prihodnje. Še naprej bomo posebno pozornost namenjali preventivnim ukrepom. K dobremu občutku varnosti naših občank in občanov lahko zagotovo največ storimo tudi sami, in sicer z rednim obveščanjem o naših aktivnostih. Dobro sodelovanje je ključ do uspeha, zato bomo še naprej sodelovali pri policijskih dejavnostih v lokalnem okolju. Potrebno je znati prisluhniti, slišati in nemudoma reagirati. Takojšnji odzivi v lokalni skupnosti so bistveni, da prepoznamo morebitna varnostna tveganja in problematiko. Sledijo posvetovanja in prave reakcije.

Lahko te dobre prakse skozi Združenje mestnih občin Slovenije prenesete tudi na ostala lokalna okolja?

Zagotovo bi se tovrstni model lahko uveljavil tudi v drugih mestih – in kjer je volja, je tudi pot. ■

Foto: Nik Jevšnik.

Varnostni prehodi za kontrolo dostopa v nadzorovana območja



- Visoka in nizka vrtljiva vrata, hitri prehodi, plačljivi prehodi.
- Integracija z obstoječimi sistemi.
- Nižji stroški fizičnega varovanja.
- Zvočni in svetlobni alarmi.
- Primerno za velik pretok uporabnikov.

ID Shop – zanesljiv partner za zagotavljanje kontrole pristopa v vaših objektih!

Varnostni prehodi na kritičnih območjih pomenijo več kot zgolj povečano varnost!

- Znižanje stroškov.
- Bolj nadzorovan pretok ljudi.
- Učinkovita integracija z obstoječo kontrolo pristopa v stavbi.
- Boljša učinkovitost pri doseganju višjih varnostnih standardov.



ID Shop nudi različne nivoje in mehanizme za zagotavljanje kontrole pristopa:

- **Mehanski sistemi zaklepanja** (cilindri, ključavnice, ključi, sistemski, generalni ključi, ...).
- **Mehatronski sistemi zaklepanja** (pametne kljuke, digitalni cilindri, elektronski ščiti, kartični pristop, ...).
- **Varnostni prehodi** (visoke, nizke vrtljive zapore, ...).

IDealni partner za identifikacijo in varnost

ID Shop, d. o. o. Litostrojska 44d, 1000 Ljubljana
T: +386 (0)1 500 40 50
E: info@idshop.si **W:** www.idshop.si

cominfo security first

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Blaž Perko, generalni sekretar Olimpijskega komiteja Slovenije

VARNOST VELIKIH ŠPORTNIH DOGODKOV VEDNO PREDSTAVLJA POSEBEN IZZIV

Pred kratkim končane olimpijske igre v Tokiu, so prava priložnost, da smo se pogovorili z g. Blažem Perkom, generalnim sekretarjem Olimpijskega komiteja Slovenije o varnostnih izzivih in izkušnjah, ki jih prinaša tako velik športni dogodek.

Olimpijske igre vedno predstavljajo zelo zahteven organizacijski izziv, ne samo za organizatorje, temveč tudi za nacionalne organizacijske komiteje. Kateri so bili izzivi, ki ste jim morali v fazi priprav posvetiti največ pozornosti?

Priprave na igre v Tokiu so bile zaradi posledic pandemije in z njimi povezanimi ukrepi zelo drugačne od ostalih iger, na katere smo se pripravljali. Največji izzivi so bili v fazi pred prestavitvijo iger za 1 leto povezavi z zagotovitvijo pogojev za trening kandidatov za nastop na igrah. Ob začetku epidemije so bili pri nas namreč ukrepi za izvajanje športnih dejavnosti zelo zaostreni, saj tudi za vrhunske športnike ni bil dovoljen trening, objekti so bili zaprti, prepovedano je bilo gibanje med občinami. V tem obdobju smo na različne načine iskali možnosti, da bi Vlada RS odobrila izjeme za izvajanje treningov pod kontroliranimi pogoji vsaj za to manjšo skupino kandidatov za nastop na igrah. Igre so bile nato s skupno odločitvijo vseh deležnikov, predsednik Gabrovec je bil eden prvih, ki je javno pozval k prestavitvi iger, prestavljene za 1 leto, kar je prineslo nove izzive. Potrebno je bilo reprogramirati celoten projekt - od finančne konstrukcije, organizacije aktivnosti, logistike,... kar ni tako enostavno**,** saj prestavitev za eno leto ne pomeni zgolj zamrznitev stanja za eno leto, ampak prinese cel kup sprememb in dodatnih stroškov. Pripravljalno in kvalifikacijsko obdobje za športnike se je podaljšalo za praktično eno leto. V vmesnem času se je pojavilo cepivo in v sodelovanju z državo smo se trudili umestiti olimpijce v eno izmed prednostnih skupin, takoj za najbolj rizičnimi in zdravstvenimi delavci, kar je bilo v tistem času izredno zahtevno, tudi politično vprašanje, danes pa je to recimo ravno nasprotno, ko se cepljenje spodbuja na vsakem koraku. Zadnji izziv nam je prinesla odločitev organizatorjev o prepovedi udeležbe tujih gostov na igrah, kar je pomenilo odpoved vrsto načrtovanih aktivnosti, od organizacije projekta »Slovenska hiša«, do aktivnosti za pokrovitelje, navijače in medije. Ob tem pa tudi strogi protokoli, ki so bili zahtevani za vse udeležence iger. Zahtevana je bila namreč predhodna najava gibanja vseh prisotnih preko posebnih aplikacij in vstop na Japonsko je bil možen izključno za akreditirane osebe s predhodno odobrenim načrtom gibanja znotraj odobrenih uradnih poti. Skratka dodatno delo in v nekaterih primerih dokaj kompleksno, saj so določene ekipe na japonskem pred igrami opravile tudi aklimatizacijske priprave. Ob vsem tem je bilo zahtevano tudi stalno poročanje o zdravstvenem stanju oziroma potencialnih simptomih COVID-19 olimpijske ekipe**,** ter obvezna testiranja pred odhodom in ob prihodu, kljub cepljenosti. Omeniti je potrebno tudi dodatno administrativno izjemno zahtevno delo, ki so ga ves čas morali opravljati naši sodelavci, saj so ja-

Varnost športnikov je kot rečeno prepuščena organizatorjem in državi, v kateri se igre odvijajo. Namenjajo ji ogromno pozornosti in tudi sredstev, saj si nobena država ne želi incidentov v času iger.

*avtor je član Slovenskega združenja korporativne varnosti

ponski protokoli birokratsko precej zahtevni. Ocenil bi, da so bile te igre, kar se, kompleksnosti dela nacionalnih olimpijskih komitejev tiče, najtežje do sedaj.

Varnost športnikov je tisti izziv, ki pri zaznavanju splošne javnosti, ki spremlja tako pomemben dogodek, kot so olimpijske igre, ni toliko v ospredju. Katere pripravljane korake izvajate na tem področju pred odhodom športnikov na tekmovanje?

Na olimpijskih igrah je za varnost udeležencev dolžan poskrbeti organizator v sodelovanju z državo in MOK. Ločeno se obravnavajo varnostni protokoli za različne skupine – za športnike, akreditirane spremljevalce, medije, goste in gledalce. Kar se športnikov tiče, je za njih, z varnostnega vidika, na samih igrah zelo poskrbljeno, saj se uporablja sistem premikanja znotraj varnostnih mehurčkov, kar jim omogoča akreditacija. Potencialno varnostno tveganje predstavlja gibanje izven teh poti, ki jih v času brez pandemije, kot je bil primer v Tokiju, tudi uporabljajo športniki. V zvezi s tem jih, odvisno od države v kateri so igre, predhodno opozorimo na največje nevarnosti in tveganja, povezani pa smo tudi s pripadniki Slovenske policije, ki načeloma potujejo z nami na igre in pomagajo v primeru težav v okviru pristojnosti in mednarodnega sodelovanja. V veliko pomoč pa so tudi slovenska veleposlaništva, s katerimi se tudi v fazi priprav dogovorimo za protokole sodelovanja.

Olimpijske igre v Münchnu 1972 so bile precedenčni primer, da je varnost športnikov lahko močno ogrožena tudi v olimpijskih vaseh. Kako pri izbiri nastanitve sodelujete z organizatorji? Ali se z njimi dogovarjate o kakšnih posebnih varnostnih ukrepih, ali to prepuščate organizatorjem?

Varnost športnikov je kot rečeno prepuščena organizatorjem in državi, v kateri se igre odvijajo. Namenjajo ji ogromno pozornosti in tudi sredstev, saj si nobena država ne želi incidentov v času iger. Večino dejavnosti na tem področju nam ostaja tudi skrito, vsekakor pa se po moji oceni in izkušnjah športniki na igrah počutijo varni. Izbira nastanitve znotraj olimpijskih vasi poteka v sodelovanju z organizatorji, vendar pri izbiri varnostni vidik niti ni tako pomemben dejavnik, saj so vse nastanitve vedno znotraj zaščitenega območja z enako stopnjo varnosti. Poseben primer, ki ga lahko omenim, se je zgodil recimo na igrah v Riu, kjer se je znotraj olimpijske vasi v času iger pojavil kar velik problem tatvin. Organizatorji so nato ugotovili, da je bil razlog za to organizirana akcija med čistilnim servisom in varnostno službo, ki je skrbela za varnost znotraj olimpijske vasi. Igre v Riu so bile tudi sicer z varnostnega vidika posebne igre

.

Letošnje olimpijske igre so bile zaradi epidemioloških razmer v mnogočem posebne. Kaj so bile tiste največje težave, s katerimi ste se srečevali pri organizaciji za udeležbo naših športnikov na tekmovanju?

Največ težav je bilo s prilagajanjem in čakanjem na končne odločitve zahtevanih protokolov. Igre so se zaradi pandemije odvile v do sedaj neznanem okolju in organizatorji so v sodelovanju z zdravstveno stroko poskušali zagotoviti vsem udeležencem in domačemu prebivalstvu varne igre. Če za slab mesec pripelješ v državo predstavnike praktično iz celotnega sveta, kjer so razmere in zdravstveni sistemi zelo različni, je normalno, da želiš izločiti čim več tveganja. Vse to pa je zahtevalo kar veliko potrpežljivosti pred sprejetjem končnih odlo-



čitev in to je za vse nas predstavljalo kar velik problem zaradi priprave in izvedbe. Potem, ko so bile odločitve sprejete, smo se prilagodili, problem pa je bil predvsem zaradi birokratsko administrativne zahtevnosti postopkov.

So imeli kateri naši športniki kakšne posebne zahteve glede varnosti? Kako se v primeru »super-zvezdnikov« rešujejo ta vprašanja? Kako lahko v tem pogledu primerjamo naše športnike s športniki drugih, mogoče bolj zvenečih držav? (Primer ZDA »Dream Team«)

Kljub temu, da je bil tokrat v reprezentanci super-zvezdnik Luka Dončić, nismo imeli posebnih varnostnih zahtev. Celotna logistika potovanj in bivanja je bila enaka kot sicer. Mogoče, bi bilo drugače v primeru, da bi bili prisotni tudi navijači oziroma drugi obiskovalci iger. Tudi sicer so športniki (super-zvezdniki) znotraj olimpijske vasi varni. Določeni se umaknejo predvsem zaradi miru, saj tudi znotraj olimpijske vasi določeni športniki pritegnejo ogromno pozornosti in jih kolegi v njihovem prostem času želijo ogovoriti, se slikati itd. V olimpijski vasi lahko srečate Novaka Djokovića, ali na prejšnjih igrah recimo Michaela Phelpsa, Usaina Bolta ali NBA zvezdnike kot recimo Tony-ja Parkerja, Emanuela Ginobilija. Drži pa, da so ameriški NBA zvezdniki nastanjeni izven olimpijske vasi z lastno varnostno logistiko in tradicionalno samo obiščejo olimpijsko vas v enem izmed prostih dni. Razlog za to so dodatne posebne nadstandardne zahteve, ki so jih imeli in so bile tudi z vidika stroškov bistveno višje, zato so sklenili dogovor in so bivali drugje ter tudi sami krili stroške.

Kakšno je bilo sodelovanje s slovensko ambasado v Tokiu?



Sodelovanje je bilo na izjemno visoki ravni. Že pred igrami smo z rednimi sestanki, obiski in obveščanjem zgradili zelo dobre odnose in zaupanje. Veleposlanica dr. Ana Polak Petrič, ki je tudi sama bila športnica in mednarodna sodnica v ritmični gimnastiki, zelo dobro razume »športno« dušo, zato je bila skupaj z ekipo pripravljena na izjemno pomoč. Žal se je z zaprtjem države spremenilo veliko načrtov in odpadle so praktične vse aktivnosti**,** zato smo v okviru možnega izvedli samo simbolične aktivnosti. V primeru obiska navijačev in močne gospodarske ter politične delegacije, pa bi bilo delo veleposlaništva verjetno eno bistvenih za uspešno izvedbo.

Kako ste reševali varnostna vprašanja na sami prireditvi ob obisku ministrice za šolstvo, znanost in šport?

Protokol organizatorja za obiske ministrov ne določa velikih posebnosti, kar je drugače v primeru obiska predsednika države oziroma predsednika vlade. Obisk ministrice smo zato soorganizirali z veleposlaništvom in njenim kabinetom. Za ministre se znotraj varnostnih protokolov akreditiranih oseb ne predvideva dodatne varnosti, kot je sicer zagotovljena za udeležence iger z oznako gost. To pomeni transport in gibanje znotraj za njih predvidenih poti in mehurčke z varnostnim preverjanjem na vhodih in bivanju v akreditiranem in varovanem hotelu.

Kakšno je v splošnem sodelovanje z MOK na področju varnosti? Ali obstaja kakšna organizacijska enota znotraj mednarodne institucije, ki skrbi za varnost oz. osveščanje na tem področju?

Sodelovanje poteka pred in med igrami, kjer se glede na varnostno tveganje v posamezni državi pripravijo in pojasnijo posebnosti. Znotraj projekta iger je posebno področje namenjeno varnosti in znotraj nacionalnih olimpijskih komitejev se praviloma imenuje tudi osebo zadolženo za to področje t.i. »Security Officer«. Večinoma se pred in med igrami posebej povežejo tudi enote policije države organizatorke in držav udeleženk, s katerimi potem sodelujemo pri izmenjavi informacij ter dodatno po potrebi.

Kako sama organizacija OKS rešuje tveganja na področju kibernetske in informacijske varnosti? Ste se mogoče že soočili s kakšnim vdorom v informacijski sistem, ali vdorom v socialna omrežja pod okriljem OKS? Je imel kdo od olimpijcev težave na tem področju?

Za kibernetsko varnost našega informacijskega sistema skrbi partnersko podjetje, zaposleni pa so se dolžni ravnati po internih pravilih informacijske varnosti. Večjih vdorov na srečo zaenkrat nismo imeli, nekaj manjših poskusov v informacijski sistem ter tudi v socialno omrežje, pa smo doživeli, vendar do sedaj tudi uspešno rešili. Zavedamo pa se ranljivosti in pomembnosti tega področja v bodoče in menim, da bo potrebno na tem področju nadgraditi obstoječe stanje. OKS je namreč lahko kar zanimiva tarča, zato je treba ravnati zelo odgovorno. Težav olimpijcev ne poznam oziroma nas o morebitnih težavah niso posebej obvestili, bo pa verjetno smiselno v naše do-izobraževalne programe, ki jih izvajamo z olimpijci, v bodoče dodati tudi del teh vsebin. ■

Foto: arhiv OKS.

Avtor: Vojko Volk / veleposlanik



KOLUMNA

ZAČETEK KONCA GLOBALIZACIJE

„Trgovinska vojna in napetosti v odnosih s tujimi vladami so povečali zaskrbljenost zaradi odvisnosti od uvoza. Kitajska se opazno usmerja v samozadostnost.“

/Julian Evans-Pritchard in Seana Yue, analitika Capital Economics, julij 2021/

Izraz ‚globalizacija‘ je bil v tem tisočletju v resnici predvsem drugo ime za vstop Kitajske na svetovni trg in v mednarodne trgovinske odnose. Prelomno je bilo leto 2001, ko Kitajska s soglasjem vodilnih gospodarstev sveta in z blagoslovom ZDA postane članica Svetovne trgovinske organizacije (WTO). Posledice globalizacije so se odtlej merile predvsem v ceni delovne sile in ceni transporta kontejnerja iz Kitajske do Evrope in do ZDA. Slednje se skoraj 20 let niso bistveno spreminjale. Dostopnost poceni kitajskega blaga je čez noč postala tolikšna, da se je splačalo uvažati dobesedno vse, od plastičnih kozarcev do toaletnega papirja. Cenenost delovne sile na Kitajskem pa je bila tolikšna, da se je splačalo skoraj vsako manufakturo preseliti na Kitajsko in od tam izdelke uvažati nazaj s poceni in hitro uslugo velike četverice svetovnih ladjarjev in z njimi povezanih logistov. Kitajska se je tudi sama lotila proizvodnje vsega, kar se je na zahodu zdelo kot premalo donosno. Nazadnje so bile na zahodu nekatere proizvodnje, še posebej pa v Evropi, praktično opuščene. To se je najbolje lepo videlo ob izbruhu krize Covid-19, ko je Evropa zgroženo ugotovila, da nima proizvodnje niti minimalnih količin čisto navadnih kirurških mask in vse ostale kirurške zaščitne opreme, vključno z razkužili in čistili, do kirurških plaščev in rokavic in drugih proizvodov, ki se nam ljudem na zahodu zdijo samoumevni a skoraj v celoti prihajajo iz Kitajske. Kitajska se je v provinci Yunan v začetku 90-ih lotila še gojenja in proizvodnje kave, najprej na veliko zgražanje zahodnih kavnih gigantov, ki pa so nazadnje začeli uvažati ceneno kitajsko kavno zrnje menda “solidne” kvalitete. Smo vedeli, da pijemo kitajsko kavo?

Tako je bilo z globalizacijo vse do lanskega poletja, ko je po prvi Covid krizi sledila skokovita rast svetovnega povpraševanja in so cene transporta kontejnerjev iz Kitajske prvič po 20 letih začele rasti. Potem je marca sledil pravi šok. Zgodba globalizacije, ki se je še do včeraj zdela enako neizbežna kot gravitacija, se je hudo zamajala v hipu, ko se je v Sueškem zalivu počez postavila velikanka za prevoz kontejnerjev. V šestih dneh, ki so bili porabljeni za rešitev nasedle ladje, je nastalo za okroglih 9 mrd evrov škode, blokiranih pa je bilo skupaj kar 450 ladij. Še lani poleti je bila cena prevoza kontejnerja iz Kitajske v sredozemsko Evropo okrog 1500 evrov, do danes pa je dosegla že skoraj neverjetnih 14 tisoč evrov. Kar je pri tem posebej pomembno so ocene poznavalcev trga ladjarjev in logistov, ki so prepričani, da tako nizkih cen prevoza kontejnerjev, kot so bile do lanskega poletja, ne bo nikoli več. Še več, pričakujejo celo, da cene ne bodo bistveno padle že zato, ker na ladjarje, ki uživajo domala monopolen položaj, ni mogoče izvajati učinkovitih pritiskov. Vodilni kontejnerski prevoznik Maersk je v letošnjem prvem tromesečju ustvaril za kar tretjino več prihodkov kot lani. Po dolgem času se dogaja, da so cene nafte na svetovnih trgih manj pomembne od cen transporta kontejnerjev. In to je znak, ki ga bodo morale vodilne

Po dolgem času se dogaja, da so cene nafte na svetovnih trgih manj pomembne od cen transporta kontejnerjev. In to je znak, ki ga bodo morale vodilne svetovne korporacije pravilno analizirati in razbrati možne posledice. A skoraj ni dvoma, da bo ves preostali svet poslej stremel za tem, da zmanjša odvisnost od uvoza iz Kitajske.

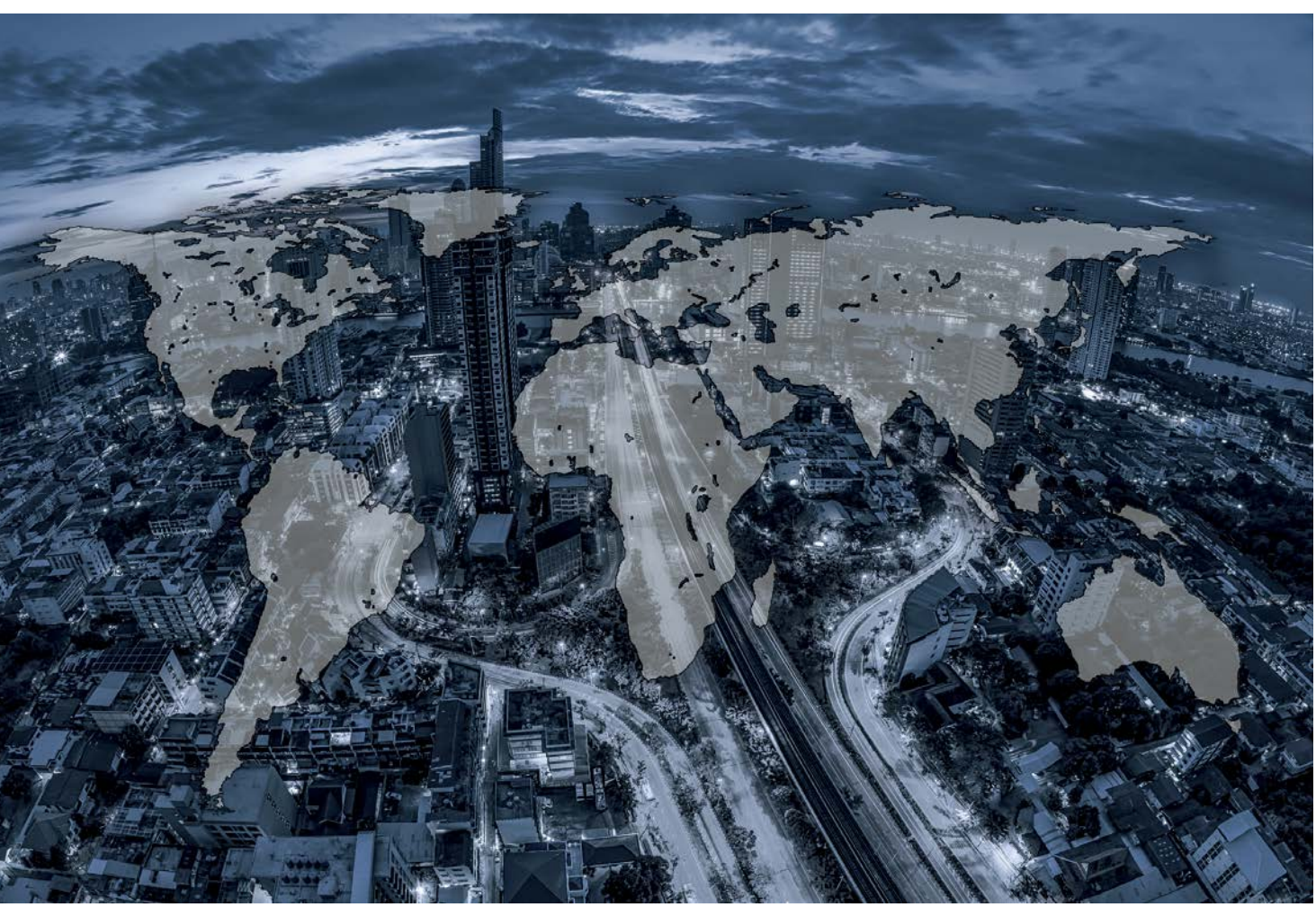
Če je prej kontejner cenejšega voluminoznega blaga uvožen iz Kitajske stal 25 tisoč evrov, stane zdaj skoraj 40 tisoč evrov. To pa je razlika, ki jo je težko prenesti naravnost na potrošnika in težko tudi kakorkoli drugače »optimizirati«. Alternativa so domači proizvajalci in to se že dogaja. Kitajski izvoz v zadnjem trimesečju sicer še vedno narašča zaradi zaostalih dobav.

svetovne korporacije pravilno analizirati in razbrati možne posledice. A skoraj ni dvoma, da bo ves preostali svet poslej stremel za tem, da zmanjša odvisnost od uvoza iz Kitajske.

Gospodarske posledice za EU

Prve kratkoročne posledice sprememb najbolj občutimo prav v EU. Dejstvo, da se je cena kitajskih izdelkov zaradi občutno dražjega transporta praktično čez noč znatno podražila, ugodno vpliva na evropske proizvajalce. Če je prej kontejner cenejšega voluminoznega blaga uvožen iz Kitajske stal 25 tisoč evrov, stane zdaj skoraj 40 tisoč evrov. To pa je razlika, ki jo je težko prenesti naravnost na potrošnika in težko tudi kakorkoli drugače »optimizirati«. Alternativa so domači proizvajalci in to se že dogaja. Kitajski izvoz v zadnjem trimesečju sicer še vedno narašča zaradi zaostalih dobav. Številke o rasti evropskega gospodarstva in kratkoročne napovedi pa že vse od širitve EU leta 2004 niso bile tako ugodne kot zadnje trimesečje. To je odraz ključnega nauka iz Covid krize, ki je v tem, da EU ne more imeti na stežaj odprtih vrat za kitajsko blago, ki je v vseh segmentih cenejše zato, ker gre za odraz ogromnih družbenih razlik in s tem sistemskega dumpinga. Gre za vsaj za zdaj večjo dostopnost Kitajske do strateških surovin, ki so osnova za proizvodnjo polprevodnikov oziroma čipov in vseh drugih bazičnih tehnoloških proizvodov. Drugič pa gre za enako pomemben, socialni dumping, začenši z bistveno nižjimi plačami in socialnimi standardi. Kitajska zahteva popolno odprtost zahodnih trgov, medtem ko svojega ne odpira, zato je postala tekmec, ki ogroža gospodarske in socialne temelje zahoda. Politične kompatibilnosti med zahodom in Kitajsko pa nikoli ni bilo in nič ne kaže, da bi se Kitajska v kratkem demokratizirala ter svojim ljudem priznala politične in socialne pravice, kot ljudem pritičejo. Kitajska je po tehnološkem razvoju že v prihodnosti, po socialni enakosti, pravičnosti in odnosu do manjšin, pa v je v srednjem veku.

Od nekoč obetajočih kitajskih projektov iz cikla ti. *svilne poti*, kakršen je bil predvsem One Belt One Road (OBOR) pobuda, v Evropi ni ostalo veliko, razen hude zadolženosti in odvisnosti povzročene na Balkanu. Najhuje je v Črni Gori in Srbiji, kjer kraljujejo kitajska gradbena podjetja in banke. Tudi hrvaški primer gradnje Pelješkega mostu s Kitajskim podjetjem China Road and Bridge Corporation je eden tistih, ko država





od svojega največjega gradbenega podviga, razen objekta samega, ne pridobi nobene dodane vrednosti. Domača podjetja pri gradnji mostu niso prišla do zaslužka niti do izkušenj in s tem kvalifikacij za prihodnje gradnje.

Po ZDA se poslej tudi evropske tehnološke družbe odpovedujejo sodelovanju s kitajskim podjetjem Huawei, pri gradnji jedrnih mobilnih omrežij za 5G pa na trg prihaja Nokia, tudi v Slovenijo. Nezaupanje med zahodom in Kitajsko se je nenazadnje utrdilo tudi zaradi vztrajanja Kitajske, da ne bo dopustila izvedbe nadzora neodvisnih strokovnjakov, ki bi v Wuhanu opravili pregled laboratorijev in skušali priti do dna dejstvom glede izbruha virusa že zato, da se kaj takega ne ponovi. K strateškemu gospodarskemu zasuku EU zagotovo prispeva tudi dejstvo, da se je zaradi Covid krize končno tudi Nemčija odrekla nevzdržni varčevalni monetarni politiki (*austerity*) in pristala na dolgoročno zadolževanje in masivno financiranje projektov za okrevanje evropskih gospodarstev. Spomin na čase, ko je Nemčija vztrajala pri drastičnih varčevalnih ukrepih pri reševanju bankrotirane Grčije, še ni zbledel. Kanclerka Angela Merkel, ki Grčiji ni popustila niti za cent, je čudežno pristala na odprtje evrskih trezorjev, kar že ta hip EU, ne samo rešuje, ampak ji obeta tudi rekordno gospodarsko rast, srednjeročno pa vsaj stabilnost. A tudi ta obet je seveda povsem ekonomski, v njem ni nepredvidljivosti sveta in političnih problemov, ki na ekonomijo vselej usodno vplivajo in jih je treba reševati. Če bi bila politika res tako nepomembna in odveč, kot si mnogi mislijo, bi svet vodili ekonomisti in raj bi se z neba spustil na zemljo. A bi bil zagotovo kitajski.

Strateške posledice ameriškega bega iz Afganistana

Že ta hip je jasno, da bodo posledice ameriškega umika, ali natančneje bega iz Afganistana pomembne za ves svet, ne samo za Evropo. Jasno je tudi, da prav Evropa dokončno postaja ključna kolateralna žrtev ameriških politik v Severni Afriki in na Bližnjem vzhodu. Krivda za to pa ni samo ameriška ampak je v veliki meri kriva tudi Evropa sama, posebej EU, ki je vse odločitve znotraj NATO in vsa varnostna vprašanja in vse vojaške posege v Severni Afriki in Bližnjem vzhodu prepuščala ZDA in s tem tudi njenim interesom. In kaj so bili ameriški interesi v tem delu sveta? Tako kot vselej zaščita naftnih virov in podpora Izraelu. Interesov Evrope v teh posegih ni bilo. V razlage, da se z orožjem narodom prinaša demokracijo, ni verjela niti Amerika sama. A ker so ZDA medtem postale energetsko praktično samozadostne, nafta pa se poslavlja, se poslavljajo tudi ameriški interesi iz trpeče regije. Ameriški umik zato ni taktične ampak strateške narave in strateške bodo tudi posledice. Izrael se bo moral sprijazniti s fizično vojaško odsotnostjo ZDA in zadovoljiti s politično in tehnološko podporo, kolikor je bo še ostalo. Evropa pa se bo morala zelo hitro strezniti in si priznati, da je prišel nov čas, v katerem bo na kocki njena prihodnost ali celo njen obstoj. Nauk številka ena pa bo; za varnost Evrope in njene soseščine mora v prvi vrsti poskrbeti Evropa sama!

> Kitajska zahteva popolno odprtost zahodnih trgov, medtem ko svojega ne odpira, zato je postala tekmec, ki ogroža gospodarske in socialne temelje zahoda. Politične kompatibilnosti med zahodom in Kitajsko pa nikoli ni bilo in nič ne kaže, da bi se Kitajska v kratkem demokratizirala ter svojim ljudem priznala politične in socialne pravice, kot ljudem pritičejo.

Kitajska je vsekakor močno odvisna od evropskega trga saj svojih tehnoloških dosežkov ne more prodajati praktično nikomur drugemu, ker drugi trgi nimajo ustrezne kupne moči ali pa Kitajsko močno ovirajo, tako kot ZDA. Tudi zato je odločitev Kitajske, da zmanjša svojo odvisnost od izvoza in se usmeri v samozadostnost logična in v resnici edina možna.

Posledice vseh ameriških intervencijskih polomov, od Libije, Libanona, Iraka, Sirije in Afganistana, ki so soseščina Evrope, seveda niso samo evropski ampak so svetovni problem. Predsednik Joe Biden se je za umik iz Afganistana, ki je bil katastrofalno slabo pripravljen, odločil zaradi podpore domače javnosti in dejstva, da ne more zmagati na prihodnjih volitvah z bremenom Afganistana na ramenih. Pri tem si je po pilatovsko umil roke, češ, da se je afganistanska vojska predala, namesto, da bi se "borila, kot je obljubila". Zamudil je priložnost, ko bo lahko ostal tiho. A to je skladno z ameriškim pregovorom, ki je tudi prikladen izgovor in pravi; „mi lahko pripeljemo konja do vode, ne moremo pa ga prisiliti, da jo pije". Za ZDA je ta konj seveda demokracija. Najbolj prizadete so in bodo države, ki so bile pred vojaškimi posegi v vseh svojih kakorkoli težavnih razmerah in revščini vsaj stabilne, danes pa so politično in socialno razsute, ljudje pa iz njih bežijo kamorkoli, samo da si rešijo življenje. Nobenega dvoma ni, da bo velik del beguncev prišel v Evropo po sredozemski in balkanski migrantski poti. Vse dosedanje evropske polemike o tem pa so strahotno jalove; dejstvo je, da begunci prihajajo in zanje bo treba nekako poskrbeti. Če ne bomo, se nam bo ponovil begunski kaos iz leta 2015.



Dejstvo je, da to zmoremo, navsezadnje je z industrijsko in prometno revolucijo v 19. stoletju prav Evropa globalizirala planet. Na koncu pa je svet globaliziral Evropo. Za dramatične spremembe je zato čas zdaj. Ali pa nikoli.

Odgovor je nova, zelena globalizacija

Seveda obstaja tudi druga plat medalje, ko gre za podražitev kitajskih izdelkov zaradi dražjega transporta. Prizadeti bodo vsi tisti, ki so v celoti odvisni od kitajskih tehnoloških izdelkov, v prvi vrsti polprevodnikov, brez katerih ne delujejo več ne telefoni, ne avtomobili in tudi ne gospodinjski aparati. Kitajska bo pri tem imela nekaj vzvodov za podražitve, za kopičenje zalog in upočasnjevanje dobav, prav veliko pa ne. Če bo zadrževala dobave in pretirano dražila bo škodila tudi sebi in lastni proizvodnji, na drugi strani pa se tako kot vedno slej ali prej odpre alternativa. Teh pa je več, od krožnega gospodarstva pa do alternativnih rešitev, kjer se lahko marsikje odprejo možnosti analognih rešitev, ki so hkrati tudi bolj vzdržne in predvsem bolj zelene, vse tja do razvoja alternativnih rešitev. Te pa obstajajo vedno, namesto litija pri baterijah že vstopa grafen, glede redkih zemeljskih kovin pa ob reciklaži in inovacijah obstaja še možnost novih nahajališč. Kitajska je vsekakor močno odvisna od evropskega trga saj svojih tehnoloških dosežkov ne more prodajati praktično nikomur drugemu, ker drugi trgi nimajo ustrezne kupne moči ali pa Kitajsko močno ovirajo, tako kot ZDA. Tudi zato je odločitev Kitajske, da zmanjša svojo odvisnost od izvoza in se usmeri v samozadostnost logična in v resnici edina možna. Zgled pa so seveda ZDA. Samozadostni ZDA in Kitajska bosta znamenje časa, novo obzorje, v katerem bosta obe skrbeli predvsem sami zase in še bolj dominirali nad svojo neposredno soseščino. In to z vsemi sredstvi in brez posebnih zadreg v odnosu do ostalega sveta, približno tako, tako kot je to pokazala Rusija z aneksijo Krima.

Kaj pa Evropa? Pesem Evrope je ta hip Elvisova "It's Now or Never". Edina resna alternativa evropski energetski odvisnosti, še prav posebej pa odvisnosti Nemčije od ruskega plina, so inovacije in skokovit tehnološki napredek, v katerega je treba izdatno investirati, tukaj in zdaj. Zdaj imamo za to usodne razloge:

- spremembe v svetu, ki so začetek konca globalizacije, kakršno smo poznali doslej;
- miselni in tehnološki preskok, ki naj bo začetek zelene globalizacije;
- nastajajoče politično soglasje o zeleni prihodnosti, ki je zgolj drugo ime za preživetje Evrope in z njo tudi planeta.

Dejstvo je, da to zmoremo, navsezadnje je z industrijsko in prometno revolucijo v 19. stoletju prav Evropa globalizirala planet. Na koncu pa je svet globaliziral Evropo. Za dramatične spremembe je zato čas zdaj. Ali pa nikoli. ■

Okrepite varnost

11. - 14. oktober 2021

4-dnevni tečaj

KIBERNETSKA VARNOST ICS/OT/IoT OKOLIJ

Kibernetski napadi na kritično infrastrukturo predstavljajo 5. največje globalno tveganje.

V obdobju enega leta od 2019 do 2020 so hekerski napadi porasli za kar 485 %.

Spoznajte, kako učinkovito vzpostaviti zaščito pred zlorabami in hekerskimi napadi in s tem zagotoviti neprekinjeno delovanje v industrijskih oz. procesnih okoljih in okoljih kritične infrastrukture.

Prenesite program

https://bit.ly/program-OT

info@smart-com.si

01 561 16 06

SMART COM

Zanesljiv, tehnološko napreden partner za kibernetsko varnost, informacijsko-komunikacijska omrežja in podatkovne centre.

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
Srečko Ocvirk, župan Občine Sevnica

VARNOST KOT POMEMBNA VREDNOTA OBČINE SEVNICA

Sodelovanje in ustrezna komunikacija med vsemi deležniki sta dva predpogoja, ki učinkovito zagotavljata uveljavljanje novih praks na področju varnosti lokalnega okolja. Ob tej priložnosti smo se o pomenu lokalne varnosti in pomenu prejete nagrade Slovenian Grand Security Award pogovarjali z g. Srečkom Ocvirkom.

Občina Sevnica je prejemnica nagrade **»Slovenian Grand Security Award«** v kategoriji **»Najbolj varna občina leta 2020«.**

Zaradi spremenjenih varnostnih dejavnikov, ki močno vplivajo na naša življenja, je varnost postala pomembna dobrina, ki je vedno bolj prisotna tudi v zavedanju ljudi. Kakšno stališče imajo do varnega okolja vaši občani?

Vidiki varnosti oziroma vidiki tveganja se v svetu z vse hitrejšim razvojem in z njim tempom življenja spreminjajo izredno hitro. Čutimo, da varnost kot vrednota močno raste na lestvici vrednot med občani in prebivalci. Gre za izjemno pomemben element bivanja ljudi.

Za manjše občine z omejenimi viri je, poleg vseh pristojnosti in nalog, zagotavljanje varnosti pomemben izziv. Kako se ga lotevate?

Občina Sevnica je s površino 272 kvadratnih kilometrov in 17.600 prebivalci ena večjih slovenskih občin, 12. največja po površini. Občina je razdeljena v enajst krajevnih skupnosti, ki imajo skupno 118 naselij. V tem prostoru deluje okrog 230 gospodarskih družb in skoraj 700 samostojnih podjetnikov. Zaznamujeta nas izredno razgibana pokrajina in podpovprečna gostota poseljenosti. V občini deluje raznolika industrija, skozi občino teče reka Sava. Različne vrste in pogostost naravnih nesreč prinašajo vedno nove in nove težke preizkušnje. Vse to predstavlja izredno širok spekter delovanja na področju zagotavljanja varnosti. Te odgovornosti pa se lotevajo izredno skrbne službe, od policije in gasilcev do zdravstvenih delavcev in pripadnikov Civilne zaščite.

V občini Sevnica se zelo trudimo povezovati vse te službe, ki na različnih področjih dela vplivajo na varnost življenja ljudi, tako z vidika splošne in prometne varnosti, zdravstvenega varstva, varstva starejših itd. Nobena od teh služb se z varnostjo ne ukvarja popolnoma ločeno, vse službe varovanje varnosti vključujejo kot del svojih rednih dnevnih aktivnosti. Povezovanje in dobro operativno sodelovanje nam daje rezultate, ki jih prepoznajo tudi strokovne službe. Predvsem pa je za nas kot občino in zame kot župana pomembno, da se občani počutimo varno v svojem okolju in da bivamo varno.

V praksi tako izvajamo raznolike aktivnosti na področju zagotavljanja večje varnosti z vključevanjem različnih družbenih struktur, od šol in vrtcev do aktivnega in starejšega prebivalstva. Z investicijami zagotavljamo večjo cestno-prometno varnost, preko šol in vrtcev veliko pozornosti posvečamo področju prometne varnosti, varnosti na spletu, skrbi za zdravje. Promoviramo varnost in osvetljujemo varnostno problematiko z dogodki, prireditvami in predstavami, kot so lutkovne predstave o varnosti v prometu za otroke. Izvajamo dobre medijske prakse obveščanja o pomenu varnosti preko struktur Civilne zaščite. Razširjamo javno mrežo defibrilatorjev. V zadnjem letu in pol je naše delo močno zaznamovalo dodatno spodbujanje prebivalcev pri spoštovanju ukrepov proti širjenju bolezni covida-19.

V zadnjih desetih letih ste letos že drugič prejeli prestižno nagrado Slovenian Grand Security Award v kategoriji

*avtorica je članica Slovenskega združenja korporativne varnosti



»najbolj varna občina«. Nam zaupate recept za tako uspešno pot?

V občini deluje socialno-varnostni sosvet kot primer dobrega sodelovanja med vsemi ustanovami, kar pomembno prispeva k skupni varnosti v širšem sistemu varnosti in zaščite. Med ključnimi vidiki varnosti je socialna varnost in povezanost občanov, hkrati pa tudi povezanost različnih služb in organizacij, ki v lokalnem okolju skrbijo vsaka za svoje področje varnosti – od policije, gasilcev, zdravstvenih delavcev in drugih služb v sistemu zaščite in reševanja. Prejeto priznanje je pohvala vsem in hkrati zelo odgovorna zaveza vseh, da se vsak dan znova povezano trudimo omogočati varno bivanje, življenje in delo.

Kakšno težišče namenjate varnostnemu sosvetu v občini in vključevanju različnih interesnih skupin na lokalnem nivoju pri zagotavljanju varnega okolja?

Socialno-varnostni sosvet je bil kot posvetovalni organ župana ustanovljen leta 2012. Sestavljajo ga predstavniki inštitucij, ki na območju občine Sevnica vsaka na svojem področju izvajajo javne naloge in zadolžitve s področij lokalne samouprave, socialе, zdravstva, javnega reda in varnosti, izobraževanja, zaposlovanja, družbenih dejavnosti in drugih.

Redna srečanja so namenjena izmenjavi informacij in poudarkov dela pristojnih javnih služb, kar pomembno pripomore k vzdrževanju socialno-varnostnega stanja v občini in s tem tudi nadgradnji kakovosti bivanja. Pomembna dodana vrednost sosveta je vzporedno proaktivno delovanje.

Sosvet pomeni dodatno obliko sodelovanja in povezovanja med javnimi službami, ki jim je skupna skrb za prijetno in varno bivanje v skupnosti. Pod sloganom »Mislimo varno, ravnajmo varno, bodimo varni« že vrsto let sodeluje pri aktivnostih in promociji varnostne tematike.

Vedno bolj smo izpostavljeni tveganjem, ki izhajajo iz informacijskega okolja. Ali v občini področju kibernetske varnosti namenjate dodatno pozornost?

Tveganja iz informacijskega okolja so vse bolj aktualna in zahtevajo vse več pozornosti in znanja. Pomembna strokovna podpora zaposlenim v občinski upravi na tem področju so aktualne informacije o kibernetskih tveganjih preko občasnih informativnih okrožnic, stalna nadgradnja in posodabljanje informacijskega sistema uprave ter strokovna podpora občinske informacijske službe, ne le zaposlenim na upravi, temveč posredno tudi javnim zavodom, katerih ustanoviteljica je občina. Predvsem so dobrodošle predstavitve konkretnih primerov nevarnosti iz vsakdanje prakse glede na specifiko dela, s katero se soočajo zaposleni in na katere morajo biti posebej pozorni.

Zaposleni redno javljajo potencialne nevarnosti in grožnje strokovni osebi, ki opravi pregled, poda analizo, navodila za ukrepanje in po potrebi izvede dodatne zaščitne ukrepe. Ta praksa sodelovanja vseh zaposlenih pri zagotavljanju varnosti se je že večkrat pokazala kot zelo učinkovita, ker samo s tehničnimi sredstvi ni mogoče zagotavljati zadostne stopnje varnosti,

Kot veliko pohvalo in priznanje k delovanju Socialno-varnostnega sosveta Občine Sevnica si štejemo tudi to, da je sosvet v letu 2016 prejel priznanje – bronasti znak Policije za sodelovanje in prispevek h krepitvi varnosti v lokalnem okolju.



saj se vse več groženj pojavlja z uporabo metod socialnega inženiringa.

V letu 2020 se je zaradi epidemije pojavila novost, vsaj občasno delo od doma, za skoraj vse zaposlene. Zato so bila, poleg zagotovitve tehničnih in varnostnih pogojev za dostop do službenega omrežja, opravljena tudi individualna izobraževanja z zaposlenimi o varnem načinu dela na daljavo in specifikah pri tem.

Kako bi ocenili sodelovanje na lokalni ravni s pomembnimi institucijami, kot je na primer policija?

Sodelovanje s policijo poteka odlično, praktično vsakodnevno na različnih ravneh, od operativnega usklajevanja, medsebojnega obveščanja, izmenjave informacij, aktivnega vključevanja policije v delo Sveta za preventivo in vzgojo v cestnem prometu, z Aktivom ravnateljev osnovnih šol občine Sevnica, promocijskih aktivnostih s področja varnosti, sodelovanja policije pri zaščitno-reševalnih akcijah znotraj razširjenega štaba civilne zaščite in seveda v veliki meri preko socialno-varnostnega sosveta, katerega članica je prav tako policija oziroma Policijska postaja Sevnica. Kot veliko pohvalo in priznanje k delovanju Socialno-varnostnega sosveta Občine Sevnica si štejemo tudi to, da je sosvet v letu 2016 prejel priznanje – bronasti znak Policije za sodelovanje in prispevek h krepitvi varnosti v lokalnem okolju.

Ocenjujem, da je prav medsebojna povezanost in hitra izmenjava ključnih informacij med odgovornimi službami za varnost enako pomembna, kot sta pomembna dobra infrastruktura in nadzor.

Kakšno stališče v občini zastopate pri uvajanju novih projektov, ki so posredno in neposredno povezani z dvigovanjem varnosti občanov? Nam lahko zaupate kakšen primer dobre prakse?

Občina Sevnica je v letu 2017 v sodelovanju s Policijsko postajo Sevnica in Socialno-varnostnim sosvetom Občine Sevnica zasnovala nov program in slogan, ki najbolj celovito predstavlja prizadevanja občine in ostalih inštitucij za zagotavljanje varnosti v lokalni skupnosti: »Mislimo varno, ravnajmo varno, bodimo varni«.

V sklopu programa je glede na ciljno skupino možno izvajati najrazličnejše aktivnosti, od dela z najmlajšimi občani, preko spoznavanja pasti prometa in drugih varnostnih vprašanj z lutkovno predstavo za otroke, predavanja, izvedba delavnic za starejše Ostanimo mobilni, prikaz dela policijskih enot za splošno javnost, prikaz dela drugih služb in druge aktivnosti. Slogan se smiselno umesti na vabila, letake in plakate za posamezne aktivnosti.

V preteklih letih je bilo tako v sklopu programa izvedenih že kar nekaj aktivnosti: poseben varnostno-preventivni dan za otroke, v sklopu katerega so si učenci predmetne stopnje vseh osnovnih šol sevniške občine ogledali lutkovno predstavo ter spoznali delo policistov – policijska vozila in opremo, delo posebnih specialnih enot policije, delo policijskega orkestra, prikaz borilnih veščin za samoobrambo, dan za večjo varnost ob tednu otroka, v sodelovanju z Agencijo za varnost prometa z najrazličnejšimi demo napravami, predstavitvijo delovanja drugih intervencijskih služb ter praktičnim prikazom reševanja s tehničnim posegom, predavanja o samozaščitnem ravnanju na delovnem mestu ob nepredvidenih situacijah, ki ogrožajo življenje, srečanja s predsedniki krajevnih skupnosti, izdelava letakov na temo osveščanja občanov o vlomih v avtomobile in stanovanja v sklopu akcije »Ne olajšajte dela tatovom«. Program se dopolnjuje in nadgrajuje z vedno novimi vsebinami.

Med drugimi primeri dobrih praks so tudi postavitve interaktivnih prikazovalnikov hitrosti v prometu in drugi.

Kakšen nasvet, o pomenu varnosti, bi za konec posredovali ostalim kolegom županom, da bi sledili vašemu primeru dobre prakse?

Ocenjujem, da je prav medsebojna povezanost in hitra izmenjava ključnih informacij med odgovornimi službami za varnost enako pomembna, kot sta pomembna dobra infrastruktura in nadzor. ■

Foto: arhiv Občine Sevnica.

Avtor: Denis Čaleta / Institut za korporativne varnostne študije*

INTERVJU
doc. dr. Milan Vršec,
častni član Slovenskega združenja korporativne varnosti

SMELO MORAMO KORAKATI NAPREJ PRI RAZVOJU POSLANSTVA KORPORATIVNE VARNOSTI

V današnjem zahtevnem varnostnem okolju smo v korporativni varnosti primorani iskati vedno nove poti pridobivanja ustreznih strokovnih kompetenc, ki nam bodo pomagale v organizacijskih okoljih ustrezno opravljati svoje poslanstvo.

Doc. dr. Milan Vršec je prejemnik nagrade **»Slovenian Grand Security Award«** v kategoriji **»Nagrada za življenjski prispevek na področju korporativne varnosti«.**

Ste eden od pionirjev raziskovanja na področju integralnih varnostnih procesov med katerimi ima korporativna varnost zelo velik pomen. Kako ocenjujete razvoj tega področja?

Najprej iskrena hvala za podelitev prestižne nagrade za življenjsko delo. S tem ste mi polepšali in obogatili mojo sedanjost in prihodnost, v kateri imam še nekaj želja in ciljev tudi na področju promoviranja in razvoja korporativne varnosti.

Glede na to, da sem imenovan kot eden od pionirjev raziskovanja integralnih varnostnih procesov moram seči 33 let nazaj, torej v leto 1988, ko je izšla moja prva knjiga z naslovom Splošna ljudska obramba in družbena samozaščita v SFRJ. Napisal sem jo kot raziskovalec v vsejugoslovanskem projektu na to temo, ki ga je v Sloveniji vodila Fakulteta za družbene vede. Leto pozneje sem začel samostojno raziskavo o vprašanjih varnosti v 30 večjih slovenskih podjetjih za potrebe doktorske disertacije. Tako sem leta 1992 doktoriral na temo varnosti v gospodarstvu, v podjetjih. Ker sem v raziskavi ugotovil, da je bilo pri menedžmentu in varnostnih strokovnjakih kar precej zanimanja za dognanja in spoznanja v raziskavi, sem leto pozneje – na podlagi doktorske disertacije - napisal (drugo) knjigo z naslovom Varnost podjetja- tokrat drugače. Vesel sem bil, da je knjiga naletela na ugodna tla in da je še danes berljiva za tiste, ki se ukvarjajo z upravljanjem korporativne varnosti in nasploh z varnostnimi vprašanji. V podjetjih, v katerih sem izvajal raziskave in tudi v nekaterih drugih podjetjih, se je pokazal tudi interes za usposabljanje varnostnih menedžerjev. Odzval sem se tako, da sem v letu 1997 v okviru svojega samostojnega podjetja Panorama Security najprej izdelal in razposlal štiri modulni program specializacije za pridobitev strokovnega naziva varnostni menedžer, na katerega se je v kratkem času prijavilo 16 kandidatov. Hitro sem zbral predavateljsko ekipo, najel prostore za izvedbo programa v koncernu Lek in zaprosil Center RS za poklicno izobraževanje, da mi podeli certifikat. No, tu se je pa zalomilo. Certifikata nisem dobil, zato je moj resni namen usposabljanja varnostnih menedžerjev padel v vodo. Nekaj mojega namena pa se je le uresničilo, ko sem, kot habilitirani visokošolski učitelj docent, na Fakulteti

*avtor je član Slovenskega združenja korporativne varnosti



za varnostne vede, na visokošolskem, fakultetnem, magistrskem in doktorskem programu, razvil in izvajal kar nekaj predmetov s področja korporativne varnosti. Šele čez dobrih 20 let je moj prvotni namen dobil smisel na Fakulteti za podjetništvo, kjer smo (dr. Denis Čaleta, dr. Milan Vršec, mag. Miran Vršec) pred leti razvili magistrski program na omenjeno izobraževalno temo. Moje veselje je bilo nepopisno, četudi z nekoliko osivelimi lasmi.

Od mojih začetnih časov raziskovanj, pisanj in predavanj se je ogromno spremenilo. Nastala je nova zakonodaja, novi varnostni in drugi standardi, nove varnostne politike, nova varnostna, poslovna in druga tveganja, spremenila pa se je tudi struktura in moč varnostnih groženj, ki se v zadnjih letih osredotočajo na kibernetske grožnje. Pandemija, epidemija, kup lažnih novic, afer in teorij zarote je vse skupaj še bolj zakompliciralo. Torej se pred tiste, ki se ukvarjajo z upravljanjem korporativne varnosti, postavlja paleta izzivov, ki jim bo kos le profesionalni pristop. Tak pristop je sposobna razvijati le taka institucija, ki ima pravo poslanstvo, pravo vizijo, prave cilje in pravo ekipo, ki tak pristop obvlada. Pred leti, ko sta dr. Denis Čaleta in mag. Miran Vršec ustanovila Inštitut za korporativne varnostne študije in malo pozneje še Slovensko združenje korporativne varnosti, se je začelo povsem novo obdobje promocije, dojemanja in razvoja korporativne varnosti. Nastale so vsakoletne nacionalne in mednarodne konference, mesečna srečanja članov, sodelovanje z vidnimi strokovnjaki, intenzivno pridobivanje somišljenikov skozi korporativne člane in skozi naročanje projektnih storitev. Nastala je tudi revija Korporativna varnost, ki gospodarske in druge družbe, poslovni svet in posameznike seznanja z aktualnimi temami s področja korporativne varnosti in širše. Dodana vrednost v delovanju inštituta pa je ukvarjanje z mednarodnimi in nacionalnimi varnostnimi projekti, ki trasirajo pot vraščanja korporativne varnosti v kritično infrastrukturo. Ugotavljam torej, da sta inštitut in združenje naredila velike korake v razvoju korporativne varnosti. Ti koraki so vedno daljši in lahko pričakujemo, da bodo ustvarjene vezi inštituta in združenja, ki bogatijo, še naprej gradile poti do uspeha.

Kritična infrastruktura ima zaradi pomena njenega neprekinjenega delovanja med organizacijami še posebej pomembno mesto. Menite, da se je strateški management v teh organizacijah začel zavedati pomena korporativne varnosti, kot pomembnega orodja za zagotavljanje neprekinjenosti delovanja njihovih organizacij?

S sinom Miranom sva imela v kritični infrastrukturi v zadnjih petnajstih letih 16 projektov uvajanja integralnih varnostnih sistemov v posamezne gospodarske družbe, ki upravljajo s kritično infrastrukturo. Zato med drugim tudi dobro poznava kakšno varnostno filozofijo ima strateški menedžment v posameznih sektorjih kritične infrastrukture. Še največje razumevanje vloge korporativne varnosti in uvajanja integralne varnosti v poslovne procese in politiko upravljanja imajo strateški menedžerji v energetiki in informacijsko-komunikacijskih družbah. V teh dveh sektorjih se tudi zavedajo pomembnosti neprekinjenega poslovanja in kriznega vodenja, ker imajo izdelane načrte neprekinjenega poslovanja in krizne načrte, nekateri pa

tudi načrte kriznega komuniciranja. Pri vseh pa je še nedodelano testiranje načrtov z vsakoletnimi scenariji vaj za posamezne izredne dogodke, šepa pa tudi določanje rezervnih lokacij.

Kot ustanovitveni član Slovenskega združenja za korporativno varnost in njegov prvi predsednik imate poseben odnos do te asociacije. Kako ocenjujete njen razvoj v tem obdobju?

Kot prvi predsednik sem, s pomočjo sodelavcev, Denisa in Mirana, poskušal vzpostaviti prve korake za prepoznavnost in poslanstvo združenja. Bil sem zadovoljen, da sem imel priložnost vsaj nekaj prispevati k začetnemu zagonu združenja, saj se je že na prvih srečanjih prvotnih članov pokazalo, da je ustanovitev združenja pravi zadetek. V okolju, torej pri posameznikih in v gospodarskih družbah, se je pokazal interes za članstvo, ki se je iz leta v leto povečevalo. V veselje mi je, da so koristnost članstva v združenju prepoznali tudi vidni strokovnjaki in pomembne gospodarske družbe v kritični infrastrukturi in v drugih sektorjih gospodarstva.

Kje vidite tiste priložnosti za razvoj Slovenskega združenja korporativne varnosti, da bo še bolj prodoren pri uveljavljanju strokovnih standardov na področju korporativne varnosti?

Če sem realen, pošten in korekten lahko rečem, da je združenje že doslej uresničevalo svoje poslanstvo v razvoju korporativne varnosti in razširjanju miselnosti o koristnosti varnostnih mehanizmov. Mesečna srečanja, konference, posveti, projektne storitve, svetovanje in drugo so aktivnosti, ki prepričajo, da je združenje ubralo pravo pot. Če pa želi združenje še bolj v živo zarezati v vsebino korporativne varnosti, bi bilo morda smiselno premisliti o plačljivih profesionalnih delavnicah ali seminarjih, na katerih bi obravnavali naslednje teme: ocenjevanje ranljivosti in ogroženosti družb, upravljanje varnostnih tveganj, načrtovanje neprekinjenega poslovanja in kriznega vodenja, načrtovanje in izvajanje vaj po scenarijih izrednih dogodkov, pridobivanje kompetenc za menedžerje korporativne varnosti. To so ključne teme, ki bi - vsaj v kritični infrastrukturi - našle zadostno število interesentov.

Je stopnja znanj, ki jih imajo korporativno varnostni managerji v Sloveniji primerljiva z mednarodnim okoljem?

Mislim, da so se skozi leta delovanja Inštituta za korporativne varnostne študije in Slovenskega združenja za korporativno varnost znanje, izkušnje in dobra praksa korporativnih varnostnih menedžerjev občutno izboljšali. Dokaz za to so številne udeležbe članov združenja na mesečnih srečanjih, na nacionalnih in mednarodnih konferencah tar drugih dogodkih, kjer se na temelju raziskovalnih spoznanj in na visoki strokovni ravni obravnavajo številne aktualne in razvojne teme korporativne varnosti.(tekst za okvir) To se vidi tudi iz številnih intervjujev priznanih strokovnjakov in iz številnih člankov, ki jih v reviji Korporativna varnost prispevajo člani združenja in drugi zainteresirani menedžerji in strokovnjaki. S tega zornega kota ocenjujem, da so slovenski korporativni varnostni menedžerji v znanju in izkušnjah konkurenčni tujim tovrstnim menedžerjem. Nekaj potrditev te ocene smo dobili pri tujih strokovnjakih, s katerimi sodelujemo v pripravah in izvedbah medna-





rodnih konferenc Dnevi korporativne varnosti. Nekaj znanja pa so nekateri korporativno varnostni menedžerji dobili tudi na Fakulteti za varnostne vede in na Fakulteti za podjetništvo. Mislim, da se bo v prihodnosti znanje tovrstnih menedžerjev še okrepilo, kajti Inštitut za korporativne varnostne študije, s svojim združenjem, diha s polnimi pljuči tudi na področju usposabljanja korporativnega varnostnega menedžmenta.

Kateri so tisti izzivi, ki bi jih s stališča svojih dolgoletnih izkušenj izpostavili, da stojijo pred menedžerji korporativne varnosti pri nadaljnjem razvoju te profesije?

O izzivih menedžerjev korporativne varnosti sem pisal že leta 2010, s prispevkom na nacionalnem posvetu. Že takrat sem poudaril, da so v prvi vrsti pomembni menedžerji korporativne varnosti v kritični infrastrukturi, v kateri je treba občutno izboljšati varnostne mehanizme. Kajti v tistih letih se je na podlagi evropske Direktive o kritični infrastrukturi (2008) začelo intenzivneje govoriti in pisati o pomembnosti posameznih sektorjev kritične infrastrukture, ki omogočajo normalno delovanje države, gospodarstva, civilne družbe in prebivalstva. Izpostavil sem, da se pred menedžerje korporativne varnosti postavljajo naslednji izzivi: usposabljanje za pridobitev kompetenc, prepričevanje strateškega vodstva v lastni organizaciji o koristnosti varnostnih mehanizmov, uvajanje standardov v sisteme varovanja in obvladovanje metodologij za ocenjevanje ranljivosti, ogroženosti in varnostnih tveganj. To so še danes, ko so razmere bolj kaotične kot takrat, glavni izzivi za menedžment korporativne varnosti. Ključni izziv pa je vendarle ta, da si menedžerji korporativne varnosti pridobijo višjo stopnjo kompetenc in si s tem ustvarijo manevrski prostor za bolj prodorno prepričevanje človeških virov v lastni organizaciji o pomembnosti varovanja, premoženja, procesov, znanja, vrednot in ljudi. (tekst za okvir) Lepa možnost pridobivanja profesionalnih kompetenc je v magistrskem programu Upravljanje s tveganji in korporativna varnost na Gea College - Fakulteta za podjetništvo. Sem pa nekoliko razočaran, ker se menedžerji korporativne varnosti v kritični infrastrukturi in v drugih sektorjih industrije in gospodarstva prepočasi zavedajo svoje vloge pri predlaganju varnostnih izboljšav in potrebe po ustreznem izobraževanju in usposabljanju,

Letos ste prejeli prestižno nagrado »Slovenian Grand Security Award« za življenjsko delo. Kakšni občutki so vas prevevali ob prejemu nagrade?

Bil sem prijetno presenečen, ko mi je bilo sporočeno, da mi bo podeljena prestižna nagrada za življenjsko delo. Nikoli nisem niti pomislil, da se mi bo zgodilo kaj takega. Vsakdo je lahko ponosen, če se mu pripeti tako odmeven dogodek. Ko sem malo bolj prevetril mojo raziskovalno, izobraževalno in projektno pot sem sprevidel, da sem pa le ustvaril nekaj koristnega za širšo uporabo na področju korporativne varnosti in varnostne vede in da je to nekdo ovrednotil kot življenjsko pomembno. Ob taki nagradi se resnično prebudiš, dobiš novo dimenzijo motivacije, da ustvariš še kaj, poseben občutek pa je, da si bil koristen človek na katerega se lahko še računa. Skratka, iskreno se zahvaljujem vsem v Inštitutu za korporativno varnostne študije in v Slovenskem združenju za korporativno varnost, ki so mi izkazali čast in mi vlili dodatno gorivo za vzdrževanje volje in moči pri ustvarjanju koristnih stvari.

Poleg tega me ob tej priložnosti prevevajo prijetni občutki, da si del te prestižne nagrade zasluži tudi moja družina: delovna skrbna in ustvarjalna soproga Heda ter vrhunska strokovnjaka sinova Miran in Erik, ki sta vedno pripravljena na podporo. Zato globok poklon moji dragi družini za vse kar je dobrega storila zame in za moje dosežke.

V obrazložitvi nagrade je bilo zapisano, da ste bili na področju razvo-

ja strokovnih vsebin korporativne varnosti kot »petelin, ki je prezgodaj zapel«. Ste imeli kdaj težave v svoji poklicni karieri zaradi trenutnega nerazumevanja okolja, kjer ste ustvarjali?

Moji prvi koraki na področje varnosti in zaščite so se pričeli leta 1984, v sklopu Fakultete za družbene vede in sicer v vlogi raziskovalca na področju varnosti in zaščite. Ampak takrat še nisem prezgodaj pel. Prezgodnje petje se je začelo, ko sem za potrebe doktorata izpeljal dokaj obsežno in zahtevno raziskavo o varnostnih mehanizmih v industriji in gospodarstvu. Ob spoznanjih in ugotovitvah v raziskavi se je začelo globoko in preveč resno razmišljanje o rešitvah in izboljšavah. No, tu se je pa začelo moje prehitevanje po »levi in desni«, ki pa ni imelo možnosti za takojšnjo uporabo v praksi. Prezgodnje je bilo zlasti to, da sem navajal oceno ranljivosti, ogroženosti in tveganj, obvladovanje izrednih dogodkov, vzpostavljanje varnostnega menedžmenta, uvajanje varnostnih in drugih standardov, sprejemanje varnostnih politik, izdelavo načrtov varovanja, projektiranje integralnih varnostnih sistemov idr. Da sem »petelin s prezgodnjim petjem« sem se v polni meri zavedal, ampak, kot se temu reče, »nisem mogel iz svoje kože«, in sem napisal knjigo o varnosti podjetij, ki naj bi dolgoročno vnesla v varnostno filozofijo podjetij nekaj svežine. Govoril sem s številnimi odgovornimi v podjetjih, ki so mojo knjigo prebrali, in so spoznali, da je vsebina knjige temelj za uvajanje sodobnega in učinkovitega sistema varovanja. V vsej svoji poklicni karieri nisem imel konkurenčnih nasprotnikov, le ljudi, ki niso razumeli, ali niso hoteli razumeti, sicer pa sem užival v svojem prezgodnjem petelinjem petju.

Kaj bi ocenili, kot največji strokovni dosežek v svoji bogati karieri?

V moji pestri karieri je bilo kar nekaj prelomnic, ki jih vidim tudi kot doseganje uspešnih etapnih rezultatov. Izpostavljam nekaj najbolj vidnih in argumentiranih dosežkov.

Prvič: Neizmerno sem vesel, da se z varnostno stroko in s področjem korporativne varnosti profesionalno, podjetniško, poslovno, izobraževalno in projektno ukvarja tudi moj sin Miran, ki je z »veliko žlico« zajel ta področja in ga vsestransko nadgradil. Poleg tega je visoko konkurenčen tudi na področju zasebnega varovanja – na trgu varnostnih storitev. Dosežek pa je, da sta moje strokovno znanje in moj motivacijski sistem padla na plodna tla.

Drugič: Z mojo knjigo Varnost podjetja – tokrat drugače sem dosegel, da je moje prezgodnje petelinje petje po mnogih letih dočakalo postopno uresničevanje v praksi. Mislim, da je ta knjiga – strokovno gledano - moj najboljši izdelek.

Tretjič: S številnimi varnostnimi projekti v kritični infrastrukturi sva s sinom Miranom, v zadnjih letih pa tudi z Denisom, vnesli v posamezne gospodarske družbe, ki upravljajo s kritično infrastrukturo, nekaj novosti in posodobitev v procese korporativne varnosti. To se s projekti nadaljuje in vesel sem tega.

Moj največji samostojni projekt pri projektiranju integralnih varnostnih sistemov pa se je zgodil v letih 1996/97, ko sem, ob podpori letališkega varnostnega menedžerja dve leti uvajal integralno varnost v sistem varovanj na Letališču Ljubljana - Brnik, sedaj letališče Jožeta Pučnika. Pri tem je nastalo nekaj več kot 1500 strani projektnega gradiva. Izdelal sem vse potrebne varnostne dokumente: varnostni elaborat, varnostno politiko, oceno ogroženosti in tveganj, 32 načrtov za obvladovanje vseh izrednih dogodkov, ki se lahko zgodijo na letališču in v zraku, program usposabljanja in druge dokumente. To je bil projekt, ki je bil metodološka, delno pa tudi strokovna podlaga kasnejšim projektom.

Kaj so tisti napotki, ki jih kot starosta tega področja, lahko položite na dušo mlade generacije, ki smelo koraka po vaših stopinjah?

Ekipi, ki upravlja in vodi Inštitut za korporativno varnostne študije in Združenje korporativne varnosti želim, da še naprej razvija svoje organizacijske, komunikacijske, strokovne, raziskovalne in poslovne sposobnosti za uresničevanje poslanstva in ciljev obeh inštitucij. To je relativno mlada in prodorna, vztrajna, pogumna in neustrašna ekipa, ki je sposobna razvijati visoko stopnjo sinergije v promociji in razvoju sodobnih pogledov na upravljanje korporativne varnosti. Kajti v negotovi prihodnosti, z mnogimi izzivi, bodo omenjene vrline še naprej trasirale prave poti do uspehov. ■



Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

Članstvo v združenju je prostovoljno.

Združenje ima redne, korporacijske in častne člane.

www.ics-institut.si

Članstvo v združenju vam lahko olajša obvladovanje tveganj v vaših organizacijskih sredinah. SKUPAJ SMO MOČNEJŠI!

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

www.ics-institut.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Andrej C. Rant, skrbnik informacijske varnosti v ELES d.o.o.*

INFORMACIJSKA VARNOST V ELEKTRO-ENERGETIKI DOBIVA NOVE RAZSEŽNOSTI

Vedno močnejša kompleksnost delovanja sektorja zagotavljanja električne energije in uvajanje novih tehnoloških rešitev predstavlja pomembne izzive, ki so še posebej izraženi v povezavi z zagotavljanjem informacijske varnosti.

Pred kratkim ste prevzeli izredno pomembno dolžnost skrbnika informacijske varnosti (CISO) v ELES-u. Kateri so tisti cilji, ki so vas vodili, da ste sprejeli to izredno zahtevno in odgovorno funkcijo?

Na področje informacijske varnosti gledam kot na izjemen izziv, saj je obsežno, hitro razvijajoče se področje, podvrženo nenehnim spremembam. Od akterjev na tem področju zahteva stalno pripravljenost, budnost, proaktivnost pri pripravljanju odzivov na obstoječe in prihajajoče grožnje ter neprestano rast in izboljševanje. Poleg strokovnega znanja moje delo zahteva širše poznavanje delovanja družbe ELES, njenega poslanstva, strategije in vloge v širšem okolju. Lahko rečemo, da je področje informacijske varnosti stičišče različnih svetov, kjer ti nikoli ni dolgčas.

Sicer pa me na to področje »vleče« že kar precej let, med drugim sem ga izbral tudi za temo svoje magistrske naloge. Že dlje časa spremljam trende in skušam prispevati k boljši informacijsko varnostni ozaveščenosti oziroma kulturi, začenši s sorodniki in prijatelji, nato pa postopoma tudi širše. Že od nekdaj sem eden tistih, ki vsakič znova opozarja, kako pomembno je varno ravnanje v kibernetskem prostoru. Če si za primer sposodim besede nekoga drugega: geslo je kot spodnje perilo – ne razkazuj ga, redno ga menjaj in ne deli ga z neznanci.

Z vidika groženj v današnjem kibernetskem prostoru lahko označim možnost popolne osamitve sistema kot luksuz, kot najlažjo pot, ki pa je dandanes vedno bolj nerealna. A hkrati to nikakor ne pomeni, da je odgovor brezglavo in nepremišljeno odpiranje v svet, uvajanje modernih, a nepreverjenih tehnoloških rešitev oziroma izvajanje storitev brez upoštevanja dobrih praks.

Kateri so tisti varnostni izzivi, ki bodo po vašem mnenju v prihodnosti posebej pomembni za energetski sektor?

Pri oskrbi z električno energijo se v prihodnosti obetajo marsikatere spremembe. Z vidika zagotavljanja informacijske varnosti je njihov skupni imenovalec zagotovo nadaljnje povečevanje potrebe po medsebojni komunikaciji (na primer daljinsko vodenje in odčitavanje, razpršenost virov električne energije, internet stvari) in povečevanje odvisnosti od informacijskih sistemov in storitev – predvsem vpeljevanje novih tehnologij, kot so: umetna inteligenca (AI), poslovna inteligenca (BI), navidezna resničnost (AR), podatkovno rudarjenje, strojno učenje, veriženje blokov (blockchain).

Širitev kibernetskega prostora pri oskrbi z električno energijo in povečevanje njegove kompleksnosti pa seveda prinaša nova tveganja in grožnje informacijski varnosti, nove vektorje napada in s tem predstavlja velik izziv v iskanju ravnotežja med funkcionalnostjo, varnostjo, in ekonomsko upravičenostjo.

ELES je izredno močno vpet v mednarodne energetske tokove. Kako ob tej potrebi po izmenjavi ključnih

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

podatkov na eni strani in zahtevami kibernetske varnosti na drugi, zagotavljati skladnost z mednarodnimi in nacionalnimi zahtevami različnih regulatorjev?

Z enim stavkom: z uvedbo informacijsko varnega načina izmenjave podatkov. To je seveda lahko zapisati, a bistveno težje izvesti. K sreči delujemo v okolju, ki se zaveda pomena oskrbe z električno energijo, in predvsem v tem nismo sami.

ELES je član evropskega združenja sistemskih operaterjev elektroenergetskega omrežja ENTSO-E, ki je že pred leti identificiralo in s pomočjo vseh deležnikov ustrezno obravnavalo potrebo po varni in zanesljivi izmenjavi podatkov v evropskem prostoru. Poiskali smo varne rešitve, izmenjali poglede na dobre prakse v lokalnih okoljih, razvili namensko platformo za izmenjavo podatkov ter sprejeli minimalne varnostne zahteve za izvajanje mednarodne izmenjave podatkov. Na ELES smo bili v letošnjem letu deležni dveh neodvisnih zunanjih presoj implementacije na ENTSO-E sprejetih varnostnih kontrol v naš prostor. Presoji sta pokazali, da smo pri prenosu in upoštevanju varnostnih kontrol v naše informacijsko okolje uspešni.

Poleg ENTSO-E je pozornost preskrbi z električno energijo pokazala tudi Evropska komisija, ki je poleg prenove direktive NIS (predlog Direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji) in predloga nove direktive EU, o odpornosti kritičnih subjektov, (RCE) zaprosila agencijo ACER za pripravo dodatnih, specifičnih varnostnih pravil, ki bodo usmerjena v varnost čezmejnih pretokov električne energije (Framework Guideline on sector-specific rules for cybersecurity aspects of crossborder electricity flows).

Vsa nova pravila, regulative, standardi, presoje, revizije in podobno prinašajo tudi nove obremenitve, vendar sam na njih gledam kot na zelo dobrodošle, saj prinašajo usmeritve, prenos novih dobrih praks in zunanji pogled na učinkovitost deležnikov pri zagotavljanju informacijske varnosti.

Kako po vaši oceni poiskati pravo ravnotežje med uvajanjem novih tehnoloških rešitev v delovanje elektro energetskih sistemov in tradicionalno težnjo po relativni avtonomnosti ter ločenosti ključnih delov tega sistema?

Širitev kibernetskega prostora pri oskrbi z električno energijo in povečevanje njegove kompleksnosti pa seveda prinaša nova tveganja in grožnje informacijski varnosti, nove vektorje napada in s tem predstavlja velik izziv v iskanju ravnotežja med funkcionalnostjo, varnostjo, in ekonomsko upravičenostjo.

Z vidika groženj v današnjem kibernetskem prostoru lahko označim možnost popolne osamitve sistema kot luksuz, kot najlažjo pot, ki pa je dandanes vedno bolj nerealna. A hkrati to nikakor ne pomeni, da je odgovor brezglavo in nepremišljeno odpiranje v svet, uvajanje modernih, a nepreverjenih tehnoloških rešitev oziroma izvajanje storitev brez upoštevanja dobrih praks.

Pri vpeljevanju novih rešitev in uvajanju novih povezav je potrebna skrbnost, načrtovanje in testiranje, saj prav zaradi pomena preskrbe z električno energijo ni veliko prostora za napake.

Z odpiranjem in povezovanjem do sedaj ločenih omrežij, se je možnost zlorabe oziroma napada bistveno povečala, zato je na nas še večja odgovornost, da energetsko okolje ustrezno varujemo in zaščitimo. Vsaka sprememba, vsaka novost mora temeljiti na celoviti oceni informacijskih groženj. Ob vpeljevanju novih rešitev se večkrat spomnim na star oglas lokalnega proizvajalca gum: »kaj ti bo moč brez kontrole«, saj ima analogijo z informacijsko varnostjo – kaj ti bodo nove storitve, če pa niso varne in/ali varno upravljane.

Človek še vedno predstavlja najpomembnejši dejavnik, tudi na področju informacijske varnosti. Kaj bodo tisti vaši prioritetni pristopi pri dvigovanju varnostnega zavedanja med zaposlenimi v ELES-u?

Da, se povsem strinjam – človek je najpomembnejši dejavnik na področju informacijske varnosti, čemur pritrjujejo tudi raziskave vzrokov posameznih informacijskih incidentov in razkritij. ELES je dokaj hitro identificiral pomembnost posameznika in že pred leti pričel z izvajanjem programov usposabljanja in ozaveščanja, uvedbo navodil, pravil, nadzora. S tem smo pozitivno vplivali na informacijsko varnostno vedenje posameznikov.

Moj cilj je to nadgraditi z izgradnjo in vzdrževanjem visoke ravni informacijsko varnostne kulture v družbi ELES. To pomeni, da vsi deležniki v organizaciji poenotijo informacijsko varnostno ravnanje





in, da tako ravnanje postane uveljavljen, celo podzavesten način izvajanja opravil v vseh fazah načrtovanja, upravljanja in rabe informacijskih sredstev in storitev.

Neprekinjenost delovanja je ključni imperativ za vsako resno organizacijo, še posebej pa tisto, ki upravlja s kritično infrastrukturo. Kakšno vlogo ima po vašem pri tem informacijska varnost?

Zelo pomembno. Da so kibernetske grožnje v porastu, kažejo raziskave, poročila in statistike o uspešnih kibernetskih napadih – tudi na kritično infrastrukturo. Te napade lahko delimo na dve vrsti. Prvi vplivajo »samo« na prekinitev zagotavljanja storitev in z uspešnim ukrepanjem njihov neposreden vpliv takoj ugasne. Drugi pa povzročijo dejanske mehanske poškodbe na specializirani namenski opremi, ki jo je težko nadomestiti, zato je težja in dolgotrajnejša tudi odprava posledic takega uspešnega kibernetskega napada.

Družba ELES se pomena neprekinjenosti poslovanja in vpliva informacijskih tveganj nanj dobro zaveda, zato je že pred leti naslovila to problematiko s sistemskim pristopom, ki ga je potrdila s pridobitvijo certifikata ISO 27001. Lani smo, na podlagi zahtev Zakona o informacijski varnosti, prenovili tudi sistem upravljanja neprekinjenega poslovanja. Ocenjujem, da se upravljanje neprekinjenosti poslovanja na splošno izboljšuje, a vseeno za nekatere žal še vedno velja izjava Richarda Clarka: »Če porabite več za kavo kot za informacijsko varnost, bodo vdrli v vaš informacijski sistem. Pravzaprav si v tem primeru to tudi zaslužite.«

Danes si težko predstavljamo, da bi bila organizacija popolnoma izolirana od dinamičnega varnostnega okolja in dejavnikov, ki na različnih nivojih upravljajo elektro-energetski sistem. Kako po vašem mnenju združiti celoten elektro-energetski sektor v logičen, dobro delujoč sistem, na področju zagotavljanja informacijske varnosti, ki bo zagotavljal komplementarnost namesto podvajanja?

Osebno menim, da je razmislek o iskanju sinergij na področju upravljanja kibernetske varnosti v verigi preskrbe z električno energijo – predvsem zaradi kroničnega pomanjkanja izkušenega strokovnega kadra in visokih stroškov – ne le smiseln, temveč celo nujen. Še posebej v majhni državi, kot je Slovenija, kjer so si gospodarske družbe hitro konkurenca pri iskanju ustreznih kadrov in obenem same težko nosijo veliko finančno breme zagotavljanja kakovostne informacijske varnosti. Ne smemo pozabiti tudi na pričakovanja EU, ki jih bo zaradi pomanjkanja strokovnih kadrov (na primer za vzpostavitev regionalnih in nacionalnih panožnih CSIRT), težko izpolniti.

Različnih pogledov na to, kako združiti celoten elektro-energetski sektor na področju zagotavljanja informacijske varnosti, je veliko. Osebno bi v zvezi s tem želel izpostaviti predvsem dvoje: da je zagotavljanje neprekinjene oskrbe z električno energijo bistveno, to pričakuje od nas tudi Evropa, ter da se stvari na področju kibernetske varnosti pri nas zaenkrat odvijajo prepočasi. Zato pričakujem, da bo na tem mestu morala odločilno vlogo odigrati tudi država s svojimi organi, ki je, enako kot tudi EU, že prepoznala pomembnost informacijske varnosti pri oskrbi z energijo in ji v zadnjem času posveča večjo pozornost. ■

Foto: Vladimir Habjan, Eles d.o.o.

Cyber Security Is What We Do



SmartIS

PAMETNI INFORMACIJSKI SISTEMI

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
Ingo Falk Pash Wallersberg,
član Slovenskega združenja korporativne varnosti

ZASEBNO VAROVANJE BO S PRAVIM RAZUMEVANJEM POTREB NJEGOVEGA RAZVOJA V PRIHODNOSTI ŠE PRIDOBIVAL NA POMENU

Pred strateškim vodstvom države stojijo pomembni izzivi za umestitev nove vloge zasebnega varovanja, ki je nujna zaradi hitro se spreminjajočega varnostnega okolja. Največji pomen bo potrebno usmeriti v zagotavljanje partnerskega odnosa in aktivne dvosmerne komunikacije med državo in izvajalci dejavnosti zasebnega varovanja.

Ingo Falk Pash Wallersberg je prejemnik nagrade **»Slovenian Grand Security Award«** v kategoriji **»Nagrada za življenjski prispevek na področju korporativne varnosti«.**

Vaša strokovna biografija je impresivna in vas na zemljevidu strokovnjakov s področja varnosti, postavlja med najbolj izpostavljene strokovnjake. Pomemben del svoje kariere ste še posebej namenili zasebnemu varovanju, ki je pomembno orodje v procesu strateške korporativne varnosti v organizacijah pri obvladovanju varnostnih tveganj. Kako ocenjujete razvoj tega področja?

Razvoj na tem področju, in sicer tako glede statusne opredelitve zasebnega varovanja in organizacijske opredelitve te dejavnosti znotraj izvršne veje oblasti, t.j. razmerij do ustreznih ministrstev, Policije in inšpekcijskih služb ter ureditve usposabljanja in izobraževanja, predvsem pa njegove vloge in pomena na področju zagotavljanja varnosti v sodobni družbi – kljub nekaterim premikom v zadnjih dveh desetletjih - ostaja v celoti daleč izpod potreb, ki jih narekujejo izzivi sodobnega časa in zahteve kakovostnega delovanja nosilcev te dejavnosti. To ni samo problem v Sloveniji, ampak – z različnimi odstopanji – enako na evropski ravni. To lahko z vso odgovornostjo rečem, saj sem v preteklosti vrsto let neposredno strokovno in projektno sodeloval tudi na tej ravni.[1]

Kot minister v osamosvojitveni vladi zelo dobro poznate tudi ustroj in delovanje državnega mehanizma. Imate občutek, da država premalo razume pomen zasebne varnosti, ki ga ima le ta za zagotavljanje varnosti v širši družbeni skupnosti?

Absolutno. O tem sem tudi v svojih strokovnih prispevkih - tako na državni kot na panožni ravni – mnogokrat opozoril. Razmerje med Policijo in zasebnim

*avtorica je članica Slovenskega združenja korporativne varnosti

varovanjem, ki je praviloma pravno in dejansko opredeljeno v odnosu enosmerne subordinacije, niti ne dopušča resnega premika. Zasebno varovanje razvojno dobiva svoj pravi status v tehnološko in računalniško - medijsko visoko razvitih družbah. Na pragu vhoda v takšno družbo stojimo. Bistvo zasebnega varovanja je po-moč – pomagati tam ali tisti (pravni ali fizični) osebi, ki ji grozi osebna ali premoženjska nevarnost, in sicer preventivno. To pomeni tudi izvedbo strokovno izjemno zahtevnih projektov za varovanje (ne le osebne, materialne, ampak še posebej intelektualne) lastnine, v katere poseg (tatvino, rop, še posebej ponarejanje) lahko učinkovito prepreči – glede na okoliščine primera – le specialno, visoko strokovno načrtovano in izvedeno varovanje. Za Slovenijo, ki je glede na velikost svojih proizvodnih kapacitet na evropskem gospodarskem prizorišču zelo šibek člen, imata področji intelektualne lastnine in avtorskih pravic še prav poseben pomen (ki se ga v javnosti še veliko premalo zavedamo).

Kako gledate na stopnjo varnostnega zavedanja strateškega managementa v organizacijah? Se vaš trud, ki ste ga vlagal na to področje obrestuje?

Strateški management, t.j. strokovno vodstvo za razvoj poslovanja, je na področju zasebnega varovanja v Sloveniji šibko razvit. To je – ob majhnem tržišču in nesorazmerno velikem številu ponudnikov teh storitev - tudi razumljivo. Glavna obremenitev vodstev ostaja ohranitev obstoječih in pridobivanje novih naročil varovanja na praviloma osnovni, najnižji kakovostni ravni in predvsem (razen v izjemnih primerih) po najnižji možni ceni. Položaj je še toliko bolj brezupen, ker se – ob izpolnjenih minimalnih zakonskih pogojih – lahko z varovanjem ukvarja praktično vsak izvajalec (družba ali zasebnik) – in sicer poleg drugih dejavnosti, ki jih opravlja (v pomenu svoje glavne ali stranske dejavnosti). Številne analize in pobude, ki sem jih v 17 letnem obdobju svojega aktivnega vodstvenega dela v tej panogi – tako v Sloveniji kot na evropski ravni – dal, so trčile predvsem ob steno boja varnostnih družb za preživetje – kar samo po sebi priča o pretežni kakovosti takšnega varovanja.

> Razvoj Združenja je izjemen – ne le glede na porast članstva in njihove resnično pomembne strokovne in vodstvene reference, pač pa predvsem glede na organizacijo izjemno kakovostnih strokovnih srečanj in konferenc, še posebej vsakoletnega mednarodnega strokovnega simpozija Slovenskega združenja korporativne varnosti, kakor tudi zaradi tvornega sodelovanja pri več evropskih projektih zasebnega varovanja.

Določen razvoj je v dosedanjem 27 letnem obdobju (po sprejetju prvega zakona o zasebnem varovanju v Republiki Sloveniji) mogoče ugotoviti na ravni t.i. tehničnega varovanja, predvsem pa pri lastnem (fizičnem in/ali tehničnem) varovanju velikih družb oziroma finančnih, gospodarskih ali komunalnih asociacij. V tem obsegu bi lahko na zastavljeni vprašanji pozitivno odgovoril, t.j, da se je zavedanje vodilnega kadra v teh družbah oziroma asociacijah o pomembnosti varovanja v tem obdobju ustrezno okrepilo.

Že daljše obdobje ste eden izmed najbolj aktivnih članov Slovenskega združenja korporativne varnosti. Kako ocenjujete njegov razvoj v tem obdobju?





Razvoj Združenja je izjemen – ne le glede na porast članstva in njihove resnično pomembne strokovne in vodstvene reference, pač pa predvsem glede na organizacijo izjemno kakovostnih strokovnih srečanj in konferenc, še posebej vsakoletnega mednarodnega strokovnega simpozija Slovenskega združenja korporativne varnosti, kakor tudi zaradi tvornega sodelovanja pri več evropskih projektih zasebnega varovanja. Prav posebej je treba opozoriti tudi na vrhunske strokovne prispevke in študije, ki jih Združenje objavlja v svoji izjemno kakovostni strokovni reviji »Korporativna varnost«. Nedvomno je Združenje danes strokovno najpomembnejša inštitucija na področju zasebnega varovanja pri nas.

Kje vidite tiste priložnosti za razvoj Slovenskega združenja korporativne varnosti, da bo še bolj prodoren pri uveljavljanju profesije na področju korporativne varnosti?

Ne gre le za priložnosti, pač pa – z mojega vidika - za aktualne potrebe, da dejavnosti zasebnega varovanja damo njen resnični pomen in s tem omogočimo njen strokovni razvoj. Varovanje je dejavnost, ki ima visoke etične imperative. Obstoječa zakonodaja – deloma tudi na mednarodni ravni (držav članic EU) - to bistveno zanemarja. Glede na to, da je sedaj v teku raziskovalni projekt »Primerjava ureditve dejavnosti zasebno varnostnih subjektov v Sloveniji in državah članicah EU«, ki poteka v okviru »Ciljnega raziskovalnega programa - CRP 2019«, je nujno, da se Združenje – kolikor tega še ni storilo – takoj poveže s slovenskimi sodelavci na tem projektu (ki naj bi bil dokončan do 31.10.2021)[2] Ne glede na ta raziskovalni projekt pa je za kakovosten razvoj dejavnosti zasebnega varovanja v Sloveniji nujno, da se v zakonu o zasebnem varovanju temeljni pogoji, ki jih morajo izpolnjevati družbe ali posamezniki za opravljanje te dejavnosti, ponovno temeljito preverijo. Predvsem je nujno potrebno, da se krog dejavnosti, ki jih izvajalci zasebnega varovanja, lahko opravljajo poleg varovanja, bistveno skrči,[3] na vsak način pa uveljavi zahteva, da mora biti njihova glavna[4] dejavnost varovanje. Varovanje, s katerim se zagotavlja neovirano izvrševanje temeljnih ustavnih pravic, nikakor ne more biti le neka stranska dejavnost. Prav tako pa je varovanje (ki predpostavlja zaupen odnos naročnika do njegovega izvajalca in pomeni mandatno razmerje med njima) nujno dejavnost, pri kateri morajo veljati najstrožji etični kriteriji.

Kateri so tisti izzivi, ki bi jih s stališča svojih dolgoletnih izkušenj izpostavil, da stojijo pred managerji korporativne varnosti pri nadaljnjem razvoju te profesije?

Na več posvetih našega Združenja so bili nekateri od teh izzivov predstavljeni. Sam bi na tem mestu posebej izpostavil naslednja, mednarodno aktualna primera:

- kraja intelektualne lastnine (izumov, tehničnih izboljšav) ali avtorskih pravic ter trženje ponaredkov originalnih, na tržiščih uveljavljenih izdelkov,

- ogrožanje ljudi ali pravnih oseb ter njihovega premoženja v pogojih nezakonitih migracij ter nevarnost podobnih dogajanj in posegov v prihodnosti.

Navedena primera izhajata iz aktualnih obtožb oziroma dogajanja na področjih svetovne trgovine (USA –Kitajska)[5] in pandemične (svetovne) širitve t.i. corona virusa (domnevno prav tako iz Kitajske).

Na podlagi navedenega je uspešno varovanje nujno vezano na pritegnitev ustreznih visoko strokovnih izvedencev, katerih izvid in mnenje sta nujni sestavini varnostnega elaborata.

Letos ste prejeli prestižno nagrado »Slovenian Grand Security Award« za življenjsko delo. Kakšni občutki so vas prevevali ob prejemu nagrade?

Ob prejemu te nagrade s strani strokovno najpomembnejšega združenja na področju slovenskega zasebnega varovanja me je prevevalo globoko čustvo hvaležnosti. Čustvo, ki mi v tistem trenutku ni pustilo, da bi kot vabljen gost na tem uglednem simpoziju na kratko spregovoril – čeprav sem si vnaprej pripravil nekaj misli v odgovor na obe večno odprti vprašanji: »KAJ JE VARNOST?« in »KAJ JE VAROVANJE?«

V obrazložitvi nagrade je bilo zapisano, da je vaš »neutrudni duh izražen tudi skozi družbene aktivnosti, ki nakazujejo vašo strokovno širino in pripravljenost razdajanja na različnih družbeno pomembnih področjih povezanih z varnostjo«. Kateri so tisti življenjski mejniki, ki so vas kot človeka in strokovnjaka najbolj oblikovali v vaši bogati karieri?

Reči moram, da sta me usodno izklesala strahoten čas druge svetovne vojne, ki je z najtežjimi udarci zbrisala mojo družino in me v najbolj zgodnji mladosti neposredno soočila s smrtjo, ter izjemna sreča, da sem se kot otrok iz te groze nenadoma znašel v varnem zavetju svoje babice, znane slovenske pesnice Lili Novy. Najbrž so bili v teh usodnih časih na začetku mojega življenja položeni temeljni kamni moje poklicne poti. Na njej me spremlja ne-varnost neprekinjeno od samega začetka, to je od moje pravne in odvetniške kariere v takratnih enoznačnih časih, iz katerih sem neposredno stopil na voz prve demokratično izvoljene slovenske Vlade, do razburkanega, nevarnega časa vojne, v katerem se je slovenska država končno rešila spon zvezne komunistične armade in države. Takrat sem s kolegi takoj, celo eno leto pred sprejetjem prvega zakona o zasebnem varovanju, ustanovil poklicno Zbornico na tem področju. Poklicno varovanje, njegove dileme in razvoj so postali in ostali vse do danes v Sloveniji in Evropi stalna preokupacija v mojem življenju. In ta krog moje poslovne in strokovne poti se sklepa zdaj na tej moji zadnji strokovni postaji – Slovenskemu združenju korporativne varnosti.

> Varovanje, s katerim se zagotavlja neovirano izvrševanje temeljnih ustavnih pravic, nikakor ne more biti le neka stranska dejavnost. Prav tako pa je varovanje (ki predpostavlja zaupen odnos naročnika do njegovega izvajalca in pomeni mandatno razmerje med njima) nujno dejavnost, pri kateri morajo veljati najstrožji etični kriteriji.

Kaj bi ocenili, kot največji strokovni dosežek v svoji bogati karieri?

O tem sam ne morem soditi. Pomembnih dosežkov je bilo več (od depolitizacije zasebnega varovanja in ustreznega gospodarskega organiziranja te dejavnosti ter aktivnega strokovnega sodelovanja v slovenskem in evropskem prostoru).[6]

Kaj so tisti napotki, ki jih kot starosta tega področja, lahko položite na dušo mlade generacije, ki smelo koraka po vaših stopinjah?

Varnost je v nenehnem spopadu z nevarnostjo. To je običajno stanje. Varovanje mora najprej preprečiti, da do poskusa vdora nevarnosti sploh pride. Čim dlje je pri tem uspešno, tem višjo oceno zasluži. Če do vdora pride, ga pravo varovanje učinkovito kaznuje. Škoda mora biti čim manjša, storilec pa v zanki varovanja učinkovitih ovir in pobranih sledov čim prej prijet. Sliši se enostavno. A v današnjem svetu računalniških in laserskih razsežnosti ni. ■

1 Tako v neformalni asociaciji zbornic ali združenj na področju zasebnega varovanja vseh nekdanjih republik bivše SFRJ (ki sem jo več let koordiniral) kot nato v evropskem združenju zasebnega varovanja CoESS (v katerega sem slovensko Zbornico zasebnega varovanja takrat tudi včlanil) in sodeloval ali vodil več evropskih projektov s tega področja, celo dva dvo-letna za vsa reprezentativna združenja zasebnega varovanja iz vseh takrat obenem z R Slovenijo v EU sprejetih držav, dodatno pa še iz (takrat v EU še ne sprejete) R Hrvaške ter (vse do danes v EU še nesprejete) R Severne Makedonije (takrat še »Makedonije«).

2 Ki so: doc. dr. Miha Dvojmoč kot vodja projekta in prof.dr.Branko Lobnikar, izr. prof. dr. Andrej Sotlar in doc. dr. Katja Prislan kot člani.

3 Obstoječa ureditev drugih omejitev od tistih po določbi 1.odst. 18.čl. ZZasV ne pozna, kar je že doslej popolnoma nevzdržno.

4 ali celo edina

5 Gre za obtožbe USA zoper Kitajsko (za poskus kraje njene tehnologije za letalske motorje, za poskus kraje postopkov izdelave čipov ipd.).

6 Vsekakor sta bili tudi strokovno in politično v času slovenske samoobrambne vojne v obdobju 1990 -1992 posebnega varnostnega pomena formalna vključitev Slovenije v mednarodno združenje Alpe-Jadran ter organizacija in izvedba varnostno uspešne zaščite in transporta tujih gostov iz slovenskih turističnih središč v Avstrijo.

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

VSAK VAREN DAN SE ZAČNE KOT VSAK SKRBNO NAČRTOVAN VARNOSTNI SISTEM



ZARJA ELEKTRONIKA

se ponaša s projektiranjem in izvedbo tehnično najzahtevnejših varnostnih sistemov, ki so plod lastnega znanja, razvoja in sledenja svetovnim trendom.

INTEGRACIJSKI SISTEMI:

- Sistem samodejnega odkrivanja in javljanja požara;
- Sistem javljanja vloma;
- Videonadzorni sistem;
- Grafično nadzorni sistem z vizualizacijo dogodkov;
- Sistem javljanja plina;
- Stabilni gasilni sistem;
- Načrtovanje varnostnih sistemov (tehnično projektiranje;
- Registracija delovnega časa;
- Nadzor dostopa in elektronki nadzor nad ključi.

"IZDELAVA SISTEMOV PO MERI KUPCA"

NAPREDNE TEHNOLOGIJE VAROVANJA

Smo ekskluzivni zastopnik za profesionalno opremo najvišjega kakovostnega razreda Tecnoalarm

ZARJA ELEKTRONIKA

Avtor: prof. dr. Anton Ramšak / Univerza v Ljubljani Fakulteta za matematiko in fiziko



KVANTNA IZMENJAVA KLJUČA OBETA VISOKO STOPNJO VARNOSTI KOMUNIKACIJ

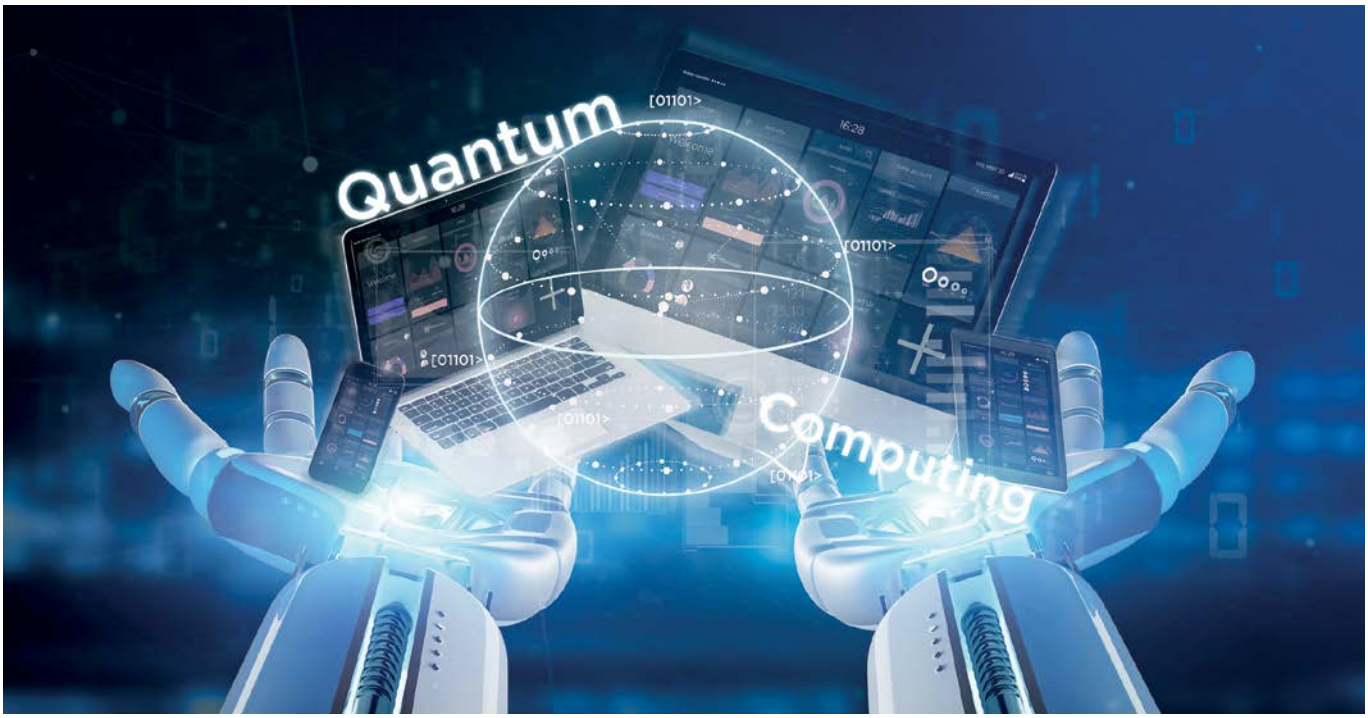
»Ne vem, zakaj je to uporabno, vendar sem prepričan, da boste kmalu to lahko obdavčili« je Michael Faraday odgovoril britanskemu finančnemu ministru Williamu Gladstoneu, ko ga je ta vprašal, čemu sploh služijo njegovi eksperimenti. Faraday je bil pomemben britanski fizik, ki je sredi devetnajstega stoletja raziskoval pojave v zvezi z elektriko; po njem je tudi imenovan eden od osnovnih zakonov elektromagnetizma. Bil je tudi izumitelj, znana je Faradayeva kletka, ki ščiti pred elektromagnetnim sevanjem. In res se je čez petdeset let z Nikolo Teslo začelo obdobje vsesplošne elektrifikacije.

Izum, razvoj in uporaba parnega stroja je bila posledica potrebe bo črpanju vode v britanskih premogovnikih in je vodila do industrijske revolucije.

Parni stroji so začeli delovati še pred popolnim fizikalnim razumevanjem teorije termodinamike, ki se je dokončno razvila prav na podlagi izkušenj s parnimi stroji. Tako je bil za vedno pokopan »perpetum mobile«, tj. stroj, ki bi deloval brez dovajanja goriva. To je vodilo do rojstva novih temeljnih fizikalnih zakonov – do energijskega in entropijskega zakona. Z razumevanjem elekromagnetizma in termodinamike ob koncu devetnajstega stoletja se je zdelo, da se je razvoj fizike dopolnil in da morajo znanstveniki samo še natančneje določiti osnovne konstante ter se usmeriti v razvoj uporabnih naprav na osnovi fizikalnih zakonov.

Prav zato je bilo na začetku dvajsetega stoletja veliko presenečenje, ko so z eksperimenti ugotovili, da vendarle še ne razumemo vsega. Izmerili so, da je hitrost svetlobe konstantna, kar je vodilo do Einsteinovega odkritja enačb relativnostne teorije. Morda se ne zavedamo, vendar tehnologija naprav za satelitsko navigacijo deluje izključno na podlagi Eisteinovih enačb. Enako nepričakovano in nepojasnjeno v okviru klasičnega razumevanja sveta in fizike je bilo odkritje fotoelektričnega pojava. Tudi tega je pojasnil Einstein; to odkritje je v naslednjih desetletjih vodilo v razvoj povsem nove fizike, tj. kvantne mehanike. Na primer fotovoltaične sončne celice delujejo prav na podlagi tega odkritja. Pojem kvant, ki se je na začetku nanašal na nekakšne osnovne pakete energije, je vpeljal Max Planck po latinski besedi »quantum«, ki v slovenskem prevodu pomeni »toliko« ali »koliko«. Kasneje se je izkazalo, da ni kvantizirana le energi-

Zaradi posebnega delovanja kvantno mehanskih šifrirnih »ključev« bo prihajajoča tehnologija omogočala doseganje do sedaj nedosegljivo visoke stopnje varnosti sogovornikov. Kvantni ključi so zaporedja naključnih števil, ki se na daljavo vzpostavijo z izmenjavo posameznih fotonov, kvantov svetlobe in protokol izmenjave poteka po zakonih kvantne mehanike. Če bi kdo ta ključ poskušal prestreči, bi takoj pustil sled, ki bi sogovornikom omogočila, da vdor zaznajo in nemudoma ukrepajo.



ja, ampak je to temeljna lastnost večine merljivih fizikalnih količin, opazljivk, in je zato izraz kvantna mehanika zelo primeren.

Razvoj kvantne mehanike

V naslednjih letih je sledil nesluten razvoj, ko so fiziki lahko v okviru formalizma kvantne mehanike pojasnili najprej strukturo atomov in atomskih jeder, nato lastnosti osnovnih delcev ter končno nenavadne lastnosti snovi, kot sta superprevodnost in magnetizem. Zaradi izrednega uspeha novega orodja je bil leta 1935 članek Einsteina in sodelavcev ponovno nepričakovan; z njim so opozorili, da formalizem kvantne mehanike v sebi skriva nepričakovano »strašljivo delovanje na daljavo« (ang. »spooky action at the distance«), kot je pojav poimenoval Einstein. Iz enačb, in ne z eksperimentom, je odkril eno od najznačilnejših lastnosti kvantne mehanike, »kvantno prepletenost« (ang. »quantum entanglement«) delcev, kot jo je še istega leta poimenoval eden od očetov kvantne mehanike, Erwin Schrödinger, ki je pojav omenjal kot paradoks. Takrat namreč ni bilo povsem jasno, ali gre za pomanjkljivost teorije ali je res možno, da v naravi obstaja tako nenavadno delovanje, kot so ga napovedovale enačbe.

Od takrat je minilo pol stoletja, dokler niso glede kvantne prepletenosti francoski fiziki v osemdesetih letih prejšnjega stoletja končno potrdili pravilnosti enačb kvantne mehanike. Eksperimentalni rezultati so se povsem ujemali s teorijo; znan je takraten komentar: »Le kako bi Einstein komentiral rezultate?«. Izkazalo se je, da je fizikom uspelo samo na podlagi teoretičnih raziskav odkriti pojav, ki bo sedaj, šele po sto letih kvantnega razvoja, bistveno spremenil tehnologijo elektronskih naprav, ki jih uporabljamo tako za računanje kot za prenos in obdelavo informacij.

Kvantni računalniki realnost, kitajski znanstveniki so vodilni na svetu

V prvo kvantno revolucijo lahko uvrstimo naprave, na katere smo se že povsem navadili in se niti ne zavedamo, da so plod načrtovanja z uporabo zakonov kvantne mehanike – to so na primer računalniki, mobilni telefoni in satelitska navigacija. V drugi kvantni revoluciji, ki je sedaj na pohodu in temelji na izrabi kvantne prepletenosti, prehajamo v razvoj naprav, katerih zmogljivosti si trenutno sploh še ne znamo predstavljati. Gre za razvoj kvantnih računalnikov in s kvantno-mehanskimi zakoni narave zaščiteno komunikacijo. Kaj to pomeni? Pred dobrim mesecem so kitajski znanstveniki z Univerze v Hefeiu objavili novico, da jim je uspelo izdelati kvantni računalnik, ki je že med testnim delovanjem v dobri uri razrešil matematični problem, ki bi ga največja obstoječa gruča klasičnih računalnikov nepretrgoma računala več kot osem let. Polna zmogljivost bo še bistveno večja. Pred takimi računalniki ni varen noben obstoječi kriptografsko zaščiten sistem podatkov ali komunikacij; ustrezno zaščito omogoča samo tehnologija, ki sloni na zakonih kvantne mehanike.

Zaradi posebnega delovanja kvantno mehanskih šifrirnih »ključev« bo prihajajoča tehnologija omogočala doseganje do sedaj nedosegljivo visoke stopnje varnosti sogovornikov. Kvantni ključi so zaporedja naključnih števil, ki se na daljavo vzpostavijo z izmenjavo posameznih fotonov, kvantov svetlobe in protokol izmenjave poteka po zakonih kvantne mehanike. Če bi kdo ta ključ poskušal prestreči, bi takoj pustil sled, ki bi sogovornikom omogočila, da vdor zaznajo in nemudoma ukrepajo.

Da si lažje predstavljamo, zakaj in v čem je kvantna komunikacija drugačna od klasične, naj najprej predstavimo osnove klasičnega prenosa podatkov, ki ga v takšni ali drugačni obliki uporabljamo že zelo dolgo. Zgodovinsko so največkrat sporočila prenašali različni sli, celo golobi pismonoše. Tehnično se pri takih prenosih pojavi več izzivov, in sicer si predvsem želimo zanesljivost in hitrost prenosa informacije. Dodatno je pogosto potrebno uporabiti zaščito vsebine sporočila, kar se je v vsej zgodovini izvajalo na zelo različne načine šifriranja. V okviru današnje tehnologije je že zelo dobro rešen problem zanesljivega in hitrega komuniciranja. Tajnost sporočil pa kljub nespornemu napredku kriptograf-

skih metod še vedno ni zadovoljiva. Sporočila so običajno zaščitena z geslom, šifrirnim ključem. Če bi za vsako sporočilo uporabili nov ključ, na primer zaporedje naključnih števil in enake dolžine, kot je samo sporočilo, bi bila varnost popolna. Vendar to v praksi v večini primerov ni izvedljivo, saj je prenos ključa enako zahteven kot prenos samega sporočila. V praksi imamo krajša gesla, ki jih večkrat uporabimo.

V četrtek, 5. avgusta, je bila med srečanjem ministrov za digitalno politiko skupine G20 v Trstu prva javna demonstracija kvantne komunikacije med tremi državami - Italijo, Slovenijo in Hrvaško. Prvič v zgodovini je bil omogočen popolnoma kvantno šifriran prenos med vozlišči treh držav, in sicer med Trstom, Ljubljano in Reko.

Zagotavljanje tajnosti podatkov

Za zagotavljanje tajnosti prenešenih podatkov torej potrebujemo čim daljše geslo, ki naj bo poznano le pošiljatelju in prejemniku. Problem nastane, ko želimo to geslo prenesti z ene lokacije na drugo, ker pri tem prenosu v okviru klasičnih metod prenosa podatkov ne moremo izključiti možnosti prisluškovanja. Kot primer naj služi prenos sporočila s svetlobnimi bliski, kot so dejansko nekoč med seboj komunicirali z ene na drugo ladjo. Z ladje »A« sporočamo tajno sporočilo na ladjo »B« tako, da z močnim reflektorjem z »A« pošiljamo snop svetlobe v smer »B«, kjer opazovalci beležijo zaporedje svetlobnih bliskov in pri tem lahko uporabljajo Morsejevo abecedo.

Sporočilo je lahko še dodatno zaščiteno s šifro, kar zaenkrat ni bistveno. Težava pri takem načinu komuniciranja je v tem, da isto sporočilo lahko vidi vsak opazovalec »C«, ki se nahaja v smeri svetlobnega snopa, na primer, na podmornici nekje daleč za ladjo »B«. Opazovalec »B« z opazovanjem sporočil ne more vedeti, ali je tudi opazovalec »C« prejel sporočilo. Povsem enako je pri pošiljanju sporočil po telegrafskem električnem kablu, s klasičnim telefonom ali pri sodobnem digitalnem penosu informacij. Danes na primer komuniciramo preko optičnih vlaken, kjer se na binarni način prenašajo zaporedja ničel in enic, kar v svojem bistvu ni bistveno drugače, kot je bilo nekoč sporočanje s svetlobnimi bliski.

Posamezni svetlobni blisk v optičnem kablu vsebuje na milijone osnovnih »paketkov« svetlobe – kvantov svetlobe. Če torej informacijo pošiljamo s klasičnimi bliski, je mogoče nekaj fotonov, izmed milijonov poslanih, neopaženo prestreči (kot je lahko opazovalec »C« iz podmornice prisluškoval komunikaciji med omenjenima ladjama). Enako je v primeru pošiljanja signalov z električnim tokom, kjer je v toku na milijone elektronov.

Kvantni način komuniciranja

Pri kvantnem načinu komuniciranja ne pošiljamo svetlobnih bliskov, ampak *posamezne fotone*. Fotoni so najmanjši gradniki elektromagnetnega polja in jih v okviru klasičnih enačb ne moremo obravnavati. Opisujejo jih enačbe kvantne mehanike; v zvezi s kvantno komunikacijo je pomembno, da so fotoni nedeljivi in jih ni mogoče podvojiti (kopirati). Fotone, tako kot običajno svetlobo, okarakteriziramo s polarizacijo valovanja, ki je lahko npr. v vodoravni





ali v navpični smeri, kjer ena predstavlja število 0 in druga število 1. Če pošiljamo posamezne fotone, lahko informacijo sporočamo ravno s pomočjo polarizacije. Težava nastopi pri večjih razdaljah, ker se svetloba v optičnih vlaknih absorbira, kar konkretno pomeni, da se določen delež poslanih fotonov izgubi, tako bi se izgubila tudi informacija. Na razdalji Postojna – Ljubljana, na primer, je prepuščenih zgolj 4% fotonov. Zato se »A« in »B« dogovorita, da »A« pošilja fotone ob točno določenih časih, zato lahko vse poslane fotone oštevilčijo: prvi poslani, drugi, tretji, ... trideset milijonti itd., približno 70 milijonov se jih pošlje na sekundo. Naslovnik »B« detektira posamično poslane fotone in v določenem času jih zbere npr. nekaj tisoč. Ker ve, kdaj naj bi fotoni prispeli, lahko vsakega prejetega oštevilči in nato podatek o času prejema posameznih fotonov sporoči pošiljatelju »A«. Tako oba točno vesta, katere od poslanih fotonov je prejemnik dejansko prejel. Dogovorita se, da bo ravno to zaporedje ničel in enic ključ za nadaljnjo komunikacijo.

Zakaj naj bi bila ta komunikacija varnejša od klasične?

Predvsem je pomembno dejstvo, da je vsak foton enkraten, in če ga prisluškovalec »C« prestreže, ga naslovnik ne more več in zato ve, da se je foton ali absorbiral ali je bil prestrežen. Po drugi strani pa naslovnik »B« za vsak prejeti foton ve, da ga ni prestregel nihče drug; prejeti foton se lahko vključi v kvantni ključ. V resnici postopek le ni tako preprost. Načeloma bi neka oseba »C« fotone lahko prestrezala (ne prisluškovala) in bi takoj nato naslovniku pošiljala druge fotone (kopiranje ni mogoče). Zato sta že leta 1984 Charles Bennett and Gilles Brassard predlagala kvantni protokol, imenovan BB84, ki omogoča izvedbo prenosa fotonov, kjer se povsem izključi možnost uporabnega prestrezanja fotonov. Postopek vključuje dve različni vrsti polarizacije fotonov in ustrezen protokol, ki izbira posamezne polarizacije, vendar je v osnovi prenos podatkov podoben kot v poenostavljenem opisu. Na ta način se lahko med »A« in »B« vzpostavi t.i. kvantni ključ in nato se lahko z njim zašifrirana sporočila pošilja na običajen način.

Opisan postopek je le ena od možnosti vzpostavitve skupnega ključa, od katerih ima vsaka svoje prednosti in tudi pomankljivosti, kar pa zaenkrat še sodi v področje raziskav. Obstaja tudi protokol, ki povsem temelji na osnovah kvantne prepletenosti, je pa nekoliko bolj zahteven za izvedbo. Vsekakor v okviru kvantne tehnologije prisluškovanje (skoraj...) ni mogoče, je pa sama izvedba tehnološko izredno zahtevna, kar je tudi razlog, da se šele sto let po odkritju zakonov kvantne mehanike počasi vzpostavlja njihova uporaba. Naprave, ki omogočajo izvedbo takšnih povezav, so namreč zaenkrat še v poskusni fazi; možen je le nakup posameznih laboratorijskih komponent, iz katerih znanstveniki sami sestavijo ustrezno kvantno napravo, na primer laserske izvore in detektorje posameznih fotonov.

V četrtek, 5. avgusta, je bila med srečanjem ministrov za digitalno politiko skupine G20 v Trstu prva javna demonstracija kvantne komunikacije med tremi državami - Italijo, Slovenijo in Hrvaško. Prvič v zgodovini je bil omogočen popolnoma kvantno šifriran prenos med vozlišči treh držav, in sicer med Trstom, Ljubljano in Reko.

Pred nagovorom slavnostnih gostov so fiziki vzpostavili kvantni ključ, glasbeniki Akademije za glasbo Univerze v Ljubljani, Akademije za glasbo Univerze v Zagrebu in tržaškega konservatorija „Giuseppe Tartini“ pa so nato po vzpostavljeni zvezi izvedli krajšni glasbeni program, pri čemer so s t. i. kvantno kriptografijo v celoti izkoriščali revolucionarno tehnologijo popolnoma varnega prenosa zvoka in slike. Vzpostavljeni ključ je bil dolg 4096 bitov, bi pa brez težav lahko vspostavili skoraj poljubno dolgo zaporedje.

Kvantno komunikacijo so izvedli skupaj fiziki v treh državah: v Ljubljani na Fakulteti za matematiko in fiziko Univerze v Ljubljani v okviru raziskovalne skupine prof. dr. Rainerja Kaltenbaeka in raziskovalnega projekta ARRS »Razvoj komponent za vzpostavitev nove evropske mreže za kvantno komunikacijo«, ki ga vodi prof. dr. Anton Ramšak; v Zagrebu je eksperiment potekal v izvedbi fizikov z Inštituta Ruđer Bošković in v Trstu z Oddelka za fiziko Univerze v Trstu ter CNR. Optično povezavo Trst –Postojna –Ljubljana je zagotovil Telekom Slovenije, ki je tudi omogočil uporabo svojega prostora Telekoma v Postojni, kjer so znanstveniki pred dogodkom izvedli preklop kvantnega kriptografskega ključa.

Nov mejnik v kvantni komunikaciji je tudi uspeh slovenskih raziskovalcev

Predstavitev je tako zgodovinsko prva uporaba kvantnih zakonov narave izven znanstvenih laboratorijev med tremi državami in z namenom popolnoma varne komunikacije, pri čemer je bilo uporabljeno standardno telekomunikacijsko omrežje. Zaradi svoje strateške lege se s tem Ljubljani in Sloveniji na stičišču glavnih evropskih komunikacijskih poti zahod-vzhod in sever-jug odpirajo povsem nove možnosti polne vzpostavitve in izkoriščanja te nove tehnologije.

Za zaključek lahko parafraziramo Faradayevo napoved, da bo sledilo tudi obdavčenje uporabe kvantne prepletenosti, kar bo znak, da smo opravili zaključni korak pri prehodu kvantne mehanike v vsakdanje življenje. Vedno znova se je namreč potrdilo, da vlaganje v osnovno znanost privede do vsakodnevno uporabnih rezultatov, vendar pogosto ne nujno v zelo kratkem času. ■

Ustvarjamo popolnoma povezan, pametni svet

HUAWEI IdeaHub

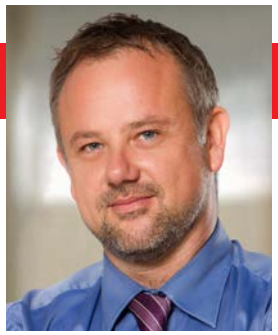
Nov stil Pametna pisarna

3 v 1 Tabla | Projektor | Spletni sestanek



HUAWEI

Avtor: Boris Grivić / Green Twin



DIGITALNI DVOJČKI SKOZI PRIZMO KORPORATIVNE VARNOSTI

Dinamično varnostno in poslovno okolje od nas zahteva vedno nove, izboljšane pristope na področju obvladovanja ključnih procesov v naših organizacijah. Nove tehnologije nam danes omogočajo, da z ustrezno vizualizacijo in z ustrezno analitiko podatkov, ki jih dobivamo v realnem času, sprejemamo bolj učinkovite odločitve in pri tem bolj varčno upravljamo z viri, ki jih imamo na voljo. Tem procesom se ne bomo mogli ogniti niti na področju upravljanja s korporativno varnostjo.

Obvladovanje vse večjega števila, vse bolj kompleksnih sistemov, postaja vse bolj zahtevno. Tabelarični prikazi zato izgubljajo svoj pomen in vse bolj se uveljavljajo tri, štiri in pet dimenzionalni prikazovalniki in nadzorni centri. Naj najprej pojasnimo pomen dimenzionalnosti. Kadar imamo pred sabo 3-dimenzionalni pogled na nek sistem ali zgradbo, vidimo širino, dolžino in globino. Če temu prikazu dodamo podatke ali dogodke, ki nastajajo in se prikazujejo v realnem času, govorimo o 4-dimenzionalnem pogledu. Če temu dodamo še stroške, ki tudi nastajajo v realnem času, govorimo o 5-dimenzionalnem pogledu. Seveda lahko dodajamo še druge dimenzije, kot na primer stroške, ki bodo šele nastali, energija, ki se bo porabila, itd.

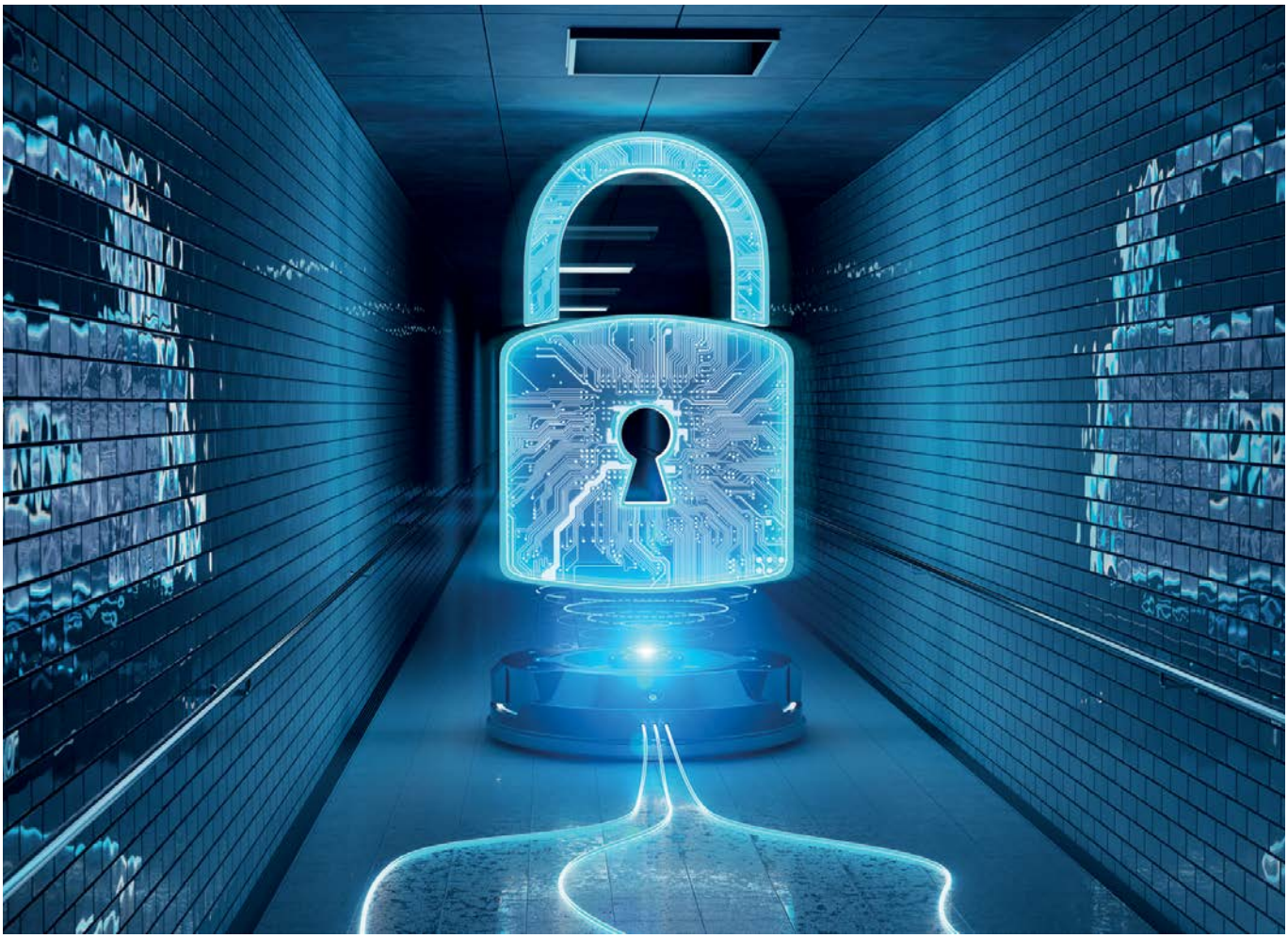
Pri zadostni količini kvalitetnih podatkov in podatkov iz zunanjih virov (npr. gibanje cen elektrike v prihodnjih letih), se že lahko vpelje strojno učenje. Potem sledi le še korak do umetne inteligence.



Slika 1

Digitalni dvojčki (slika 1) poleg tega, da prikazujejo stavbo, sredstva, stroje, zaposlene in sisteme v realnem času, običajno nudijo tudi precej bolj sofisticirano poslovno analitiko. Vzemimo za primer, da ste direktor ali vodja korporativne varnosti v družbi, ki ima še 6 hčerinskih podjetij in ta podjetja imajo še vsaka po eno hčerinsko podjetje, ter 4 oddelke. Vodje iz teh podjetjih lahko poročajo svojim nadrejenim, vendar to terja čas teh vodij, kvaliteta informacij je lahko vprašljiva, podatke je potrebno zbrati in obdelati.

V primeru digitalnih dvojčkov, in temu primerne poslovne analitike, poročila izdeluje aplikacija, ki podatke zbira največkrat preko senzorjev, IoT naprav in obstoječih aplikacij. Tako se v realnem času tvorijo izkazi poslovnega izida, stanja na računih podjetij, poročila o incidentih, poročila o prisotnih zaposlenih, temperaturah, porabah energije, itd. Četudi se ti podatki generirajo avtomatično in ni človeškega faktorja, ki bi vplival na kvaliteto podatkov, torej, da se lahko nanje zanesemo, pa bi bil pregled vseh teh že v poročila pretvorjenih podatkov ponovno nepregleden.



Modernejša poslovna analitika je tako tudi postala multidimenzionalna. Posamezna poročila je tako mogoče odslej gledati precej plastično, in sicer v 3D obliki strukture same družbe, hčerinskih družb, vseh oddelkov, vse do zadnjega stroja ali alarmnega senzorja.

Tako se tudi sama struktura in organigrami naredijo v obliki 5D digitalnega dvojčka, kjer je mogoče dodajati neomejeno število entitet in sredstev.

Večina ponudnikov poslovne analitike običajno pošilja poročila vodstvu 1-3 x dnevno, določeni pošiljajo podatke in rezultate prejšnjega dne, ker morajo njihovi strežniki preko noči preračunati ogromne količine podatkov. V modernejši poslovni analitiki pa se podatki »čistijo« že na licu mesta ter se dalje pošiljajo samo uporabni podatki ali pa celo rezultati. Ti podatki se potem ne obdelujejo na enem mestu, pač pa se razdelijo na več sklopov in preračunavajo vzporedno. Rezultat tega je ta, da dobivajo uporabniki poročila v dejanskem realnem času, in sicer z zamikom cca 0.7 sekunde.

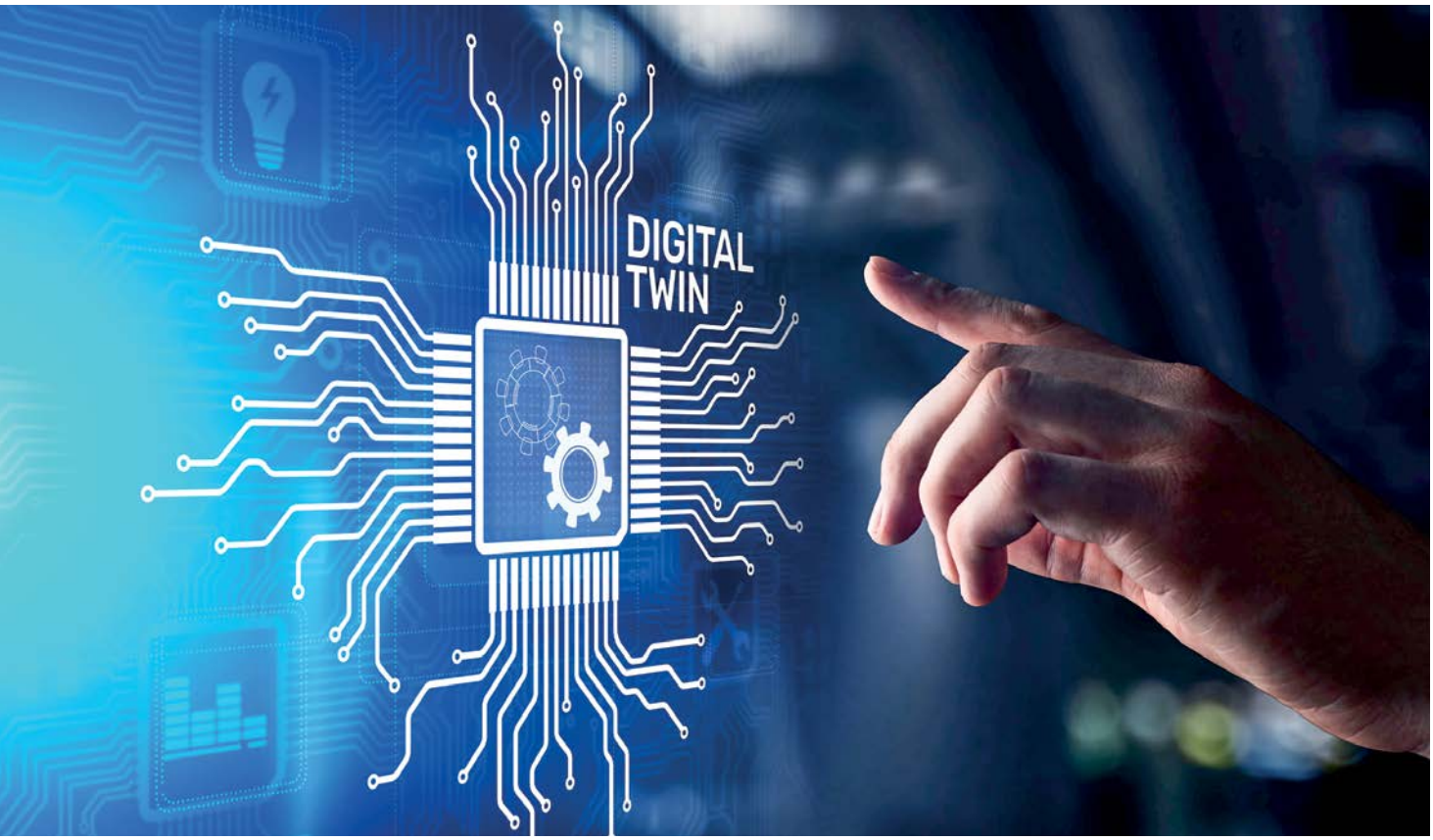
Tako hitra poslovna analitika pa omogoča tudi povratno krmiljenje procesov, kar pri nekaj ur, ali en dan starem poročilu, nikakor ni možno.

Ta ista hitrost, ki izvira iz distribuiranosti rezultatov in podatkov, pa omogoča še eno pomembno lastnost modernih digitalnih dvojčkov, in sicer to, da je mogoče iti v preteklost in »zagnati« vse dogodke na določen dan. Na primer za tri mesece nazaj, eno uro pred varnostnim incidentom. Na ta način je mogoče narediti hitro rekonstrukcijo vseh dogodkov, torej od prisotnosti zaposlenih in obiskovalcev, stanja senzorjev, temperatur, vremenskih razmer, prižganih/ugasnjenih naprav in strojev, itd., ter ugotoviti vzroke za nastanek incidenta.

Takšna baza podatkov, kombinirana s strojnim učenjem in umetno inteligenco, pa bo znala kaj kmalu v prihodnosti tudi napovedati incidente oziroma odstotek možnosti incidenta.

Prikazovalniki nam omogočajo spremljanje različnih velikosti organizacij. Sprehajanje po takšni strukturi je hitro in učinkovito, podatki pa se zbirajo od vseh organizacij in njihovih sredstev hkrati, četudi te organizacije uporabljajo različne aplikacije (npr. ERP). S klikom na katerikoli del strukture se opazova-

Ta ista hitrost, ki izvira iz distribuiranosti rezultatov in podatkov, pa omogoča še eno pomembno lastnost modernih digitalnih dvojčkov, in sicer to, da je mogoče iti v preteklost in »zagnati« vse dogodke na določen dan. Na ta način je mogoče narediti hitro rekonstrukcijo vseh dogodkov, ter ugotoviti vzroke za nastanek incidenta.

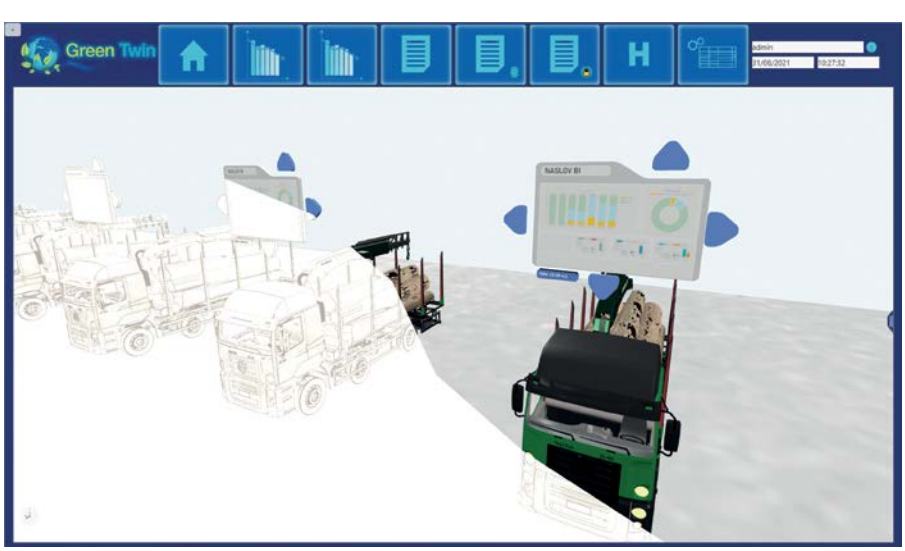


lec premakne v posamezno podjetje ali oddelek. Lahko pa si poglede tudi prednastavi. Različne zaslonske slike in kombinacije prikazovalnikov nam lahko omogočajo pregled incidentov na področju varnosti, porabo energije, konsolidiran izkaz poslovnega izida za celo skupino, učinkovitost strojev, število prisotnih delavcev, stanje na računu. Opazovalec se lahko pomika levo in desno s kurzorji in gleda poročila v realnem času, za nivo v katerem se nahaja. S pritiskom na kurzor dol ali gor se opazovalec pomakne nivo nižje ali višje. Zadaj je tako viden spodnji nivo oziroma bolj podrobni podatki.

Posebnost naprednejših digitalnih dvojčkov pa je tudi ta, da je mogoče posamezno napravo, stroj, zgradbo ali vozilo narediti iz več posameznih sklopov (npr., sklopka, stekla, elektromotor, kolesa, alarmni sistem, itd.), ter potem vsak sklop voditi in opisati posebej ter ga posebej spremljati z ločeno senzoriko. Na ta način je mogoče vedeti za vsak požarni javljalnik točno kdaj je bil vgrajen, kakšno ima stopnjo detekcije, kdo ga je vgradil in koliko je stal. Pri novogradnjah so ponavadi ti podatki enaki za vse javljalnike. A ko se le ti s časom menjajo, bodisi zaradi poškodb ali dotrajanosti, se sledljivost hitro izgubi in se niti ne ve več, kateri javljalnik je v garanciji in kdaj je bil vgrajen. Seveda, javljalnik požara je le eden od primerov, zgradba je sicer lahko sestavljena iz več 10.000 sklopov in stvari, katere pa je nujno potrebno spremljati, če želimo maksimalen ekonomski in varnostni učinek.

Slika 2 prikazuje primer transparentnosti kamionov, pri katerem ima vsak del kamiona svoj ID, na katerega je mogoče vezati delovne naloge in podatke iz sledenja vozil (npr.: prevoženi kilometri). Primer avtomatiziranega procesa vzdrževanja pa je sledeč: Pnevmatika Goodyear tip X dim. 230/80 traja 40.000 km. Naprava za sledenje vozil stalno sporoča prevožene kilometre, aplikacija pa izračunava povprečje. Kamion prevozi tedensko 1.000 km. Dobavni rok za pnevmatike je 14 dni.

Ko bodo pnevmatike imele prevoženih 38.000km, bo aplikacija generirala delovni nalog, ki bo opremljen s tipom in številom pnevmatik, podatki o kamionu, šoferju ter strošku in ga bo poslala pogodbenemu vulkanizerju. Ta ima dovolj časa, da dobavi in zamenja pnevmatike. Ko se delovni nalog zaključi, aplikacija znova spremlja pnevmatike.



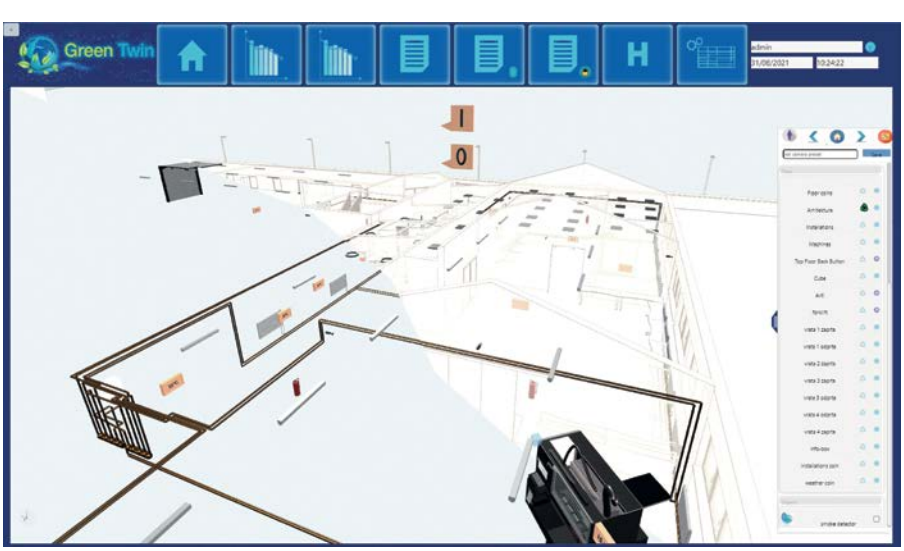
Slika 2



Enaka funkcija aplikacije je zelo uporabna tudi pri pregledu dejansko izvedenih instalacij, kjer postane arhitektura prosojna ali pa nevidna. Leva polovica slike 3 prikazuje nevidno arhitekturo, desna pa prosojno. Izstopajo instalacije.

Moderni digitalni dvojčki torej niso orodje le za določeno področje, npr. varnosti, vzdrževanja, energetike, financ, itd, temveč so primerno orodje za vse oddelke. To precej olajša tudi implementacijo digitalnega dvojčka, saj si ga običajno želi uvesti več vodij z upravo hkrati.

Prav tako novi poslovni modeli in cene aplikacije niso več vezani na število uporabnikov, temveč imajo možnost neomejenega števila uporabnikov, s čimer se spodbuja čim širša uporaba med zaposlenimi in poslovnimi partnerji. Ta način, poleg dviga digitalnih kompetenc, zagotavlja tudi širšo paleto zbranih podatkov, kar dodatno veča učinkovitost in uporabnost dvojčka, ter veča bazo podatkov za strojno učenje in umetno inteligenco, pa tudi za iskanje relacij med posameznimi podatki: npr. vpliv vlage in temperature na količino izmeta v proizvodnji ali pa število nesreč v odvisnosti od vremena v določenem delu dneva.



Slika 3

Iz vidika kibernetske varnosti se vgrajuje oprema, ki si medsebojno pošilja kriptirane podatke skupaj s časovnim odtisom. Slednji je zelo pomemben zato, ker je vedno unikaten in sinhroniziran s centralo. Tako torej ni mogoče podatkov posneti in jih predvajati nadzornemu sistemu, ter tako zmesti sistem in povzročiti kreacijo napačnih poročil. Veliko večjih podjetij se zaradi varnosti še vedno odloča za to, da taka aplikacija teče na njihovem strežniku. Vendar pa je potrebno povedati, da so sodobni oblaki velikokrat bolj varni kot lokalni strežnik. Seveda mora aplikacija biti sposobna pojaviti se v obeh oblikah, velikokrat pa se uvede tudi t.i. hibridna oblika, ko glavna aplikacija teče na lokalnem strežniku, določeni podatki pa se pošiljajo v oblak in tam obdelujejo. V teh primerih gre za nekritične podatke (npr. končna poslovna analitika ali statistika delovnih nalogov) katerih zloraba ne bi imela učinka na samo podjetje, vendar pa kljub temu uporabljajo kriptografijo. ■

Secured 5G Networks



Ericsson's evolved network security is the pioneer of a simpler yet more robust era of telecom security. Our market-leading solutions equip service providers with autonomous, end-to-end telecom security – built in to each layer of the network and securing all connected things everywhere, all the time.

www.ericsson.com/en/security

ERICSSON

Avtorja: Božo Recko in Jure Habbe / Silver Bullet Risk (SBR)





KAKO IZBOLJŠAMO KORPORATIVNO VARNOST S SISTEMATIČNIM UPRAVLJANJEM ŠKODNIH DOGODKOV

Upravljanje korporativne varnosti je neločljivo povezano z obvladovanjem škodnih dogodkov, saj v podjetjih in organizacijah vedno prihaja do neželenih situacij z negativnimi posledicami. Zato je pomembno, da jih učinkovito obvladujemo in poskrbimo, da se ne ponavljajo.

Za razumevanje obravnavane tematike je zelo pomembno razumevanje dveh pomembnih pojmov in sicer, kaj je škodni dogodek in katere procese zajema dejavnost korporativna varnost. **Škodni dogodek** ali incident se zgodi nepredvideno oz. nepričakovano in ima neposreden ali posreden vpliv na poslovanje. Večinoma povzroči motnje delovanja organizacije in povzroči škodo. **Korporativna varnost** pa je namenjena preprečevanju uresničitve različnih tveganj ter jo zagotavljamo s fizičnim in tehničnim varovanjem, informacijsko varnostjo, varnostjo in zdravjem pri delu in drugimi varnostnimi ukrepi.

Vendar prav na tem področju v praksi opažamo številne možnosti za izboljšave. Podatki o škodnih dogodkih se namreč marsikje zgolj beležijo v zapisnike in shranjujejo v preglednicah, nepovezani in razpršeni po različnih organizacijskih enotah, kar ima več slabosti.

Od nepotrebne administracije in izgube časa z evidencami in poročili ter zamudnega urejanja odškodninskih postopkov z zavarovalnicami, do predvsem nepreglednosti podatkov, zaradi česar lahko spregledamo opozorilne znake za uresničitev večjih tveganj z občutno materialno, poslovno, socialno in drugo škodo.

Pri zagotavljanju korporativne varnosti škodne dogodke celovito in učinkovito obvladujemo s sistematičnim pristopom, ki ga imenujemo upravljanje incidentov (ang. Incident Management) ter pomeni pristope in postopke za zaznavanje, prijave, obvladovanje, analize in preprečevanje škodnih dogodkov z ustreznimi ukrepi.

Ključni cilji upravljanja škodnih dogodkov

S sistematičnim upravljanjem škodnih dogodkov dosegamo naslednje cilje:

Nadzor nad učinkovitostjo upravljanja je ena od ključnih faz v celotnem sistemu upravljanja škodnih dogodkov in je v naših organizacijah nemalokrat zanemarjena. Nikakor ne moremo izboljševati stanja, če nad procesom nimamo ustreznega nadzora in predvsem jasne slike o potrebnih izboljšavah.



- Informacije o škodnih dogodkih na vseh poslovnih področjih se zbirajo na enem mestu in na dokumentiran način, se trajno shranjujejo, so ustrezno ovrednotene, zaščitene in v vsakem trenutku prispevajo k oceni dejanskega stanja korporativne varnosti organizacije.
- Škodne dogodke lahko analiziramo, klasificiramo in ugotovimo njihov vpliv na posamezna področja poslovanja.
- Ugotavljamo in odpravljamo lahko njihove temeljne vzroke (ang. Root Causes), ki pogosto niso očitni na prvi pogled.
- Vsem notranjim in zunanjim deležnikom, ki so pomembni pri obravnavi škodnih dogodkov, zagotavljamo dostop do ustreznih podatkov.
- Za zagotavljanje korporativne varnosti imamo na voljo podatke o škodah in pogostosti, kar omogoča merljivo ovrednotenje obstoječih varnostnih tveganj, identifikacijo novih tveganj, preverjanje učinkovitosti varnostnih ukrepov, določanje kazalnikov tveganj in natančnejše merjenje učinkovitosti varnostnih procesov.
- Preprečujemo ponovitve enakih ali podobnih škodnih dogodkov in eskalacije, ki bi povzročile veliko škodo, prekinitve poslovanja ali celo ogrozile obstoj organizacije.
- Po potrebi zavarujemo dokaze za nadaljnje postopke.

Vzpostavitev sistema upravljanja škodnih dogodkov

Za vzpostavitev sistematičnega upravljanja škodnih dogodkov so posebej pomembna štiri področja.

Sprejem politike upravljanja škodnih dogodkov. Politika formalizira zavezanost organizacije k sistematičnemu upravljanju škodnih dogodkov, zagotavlja podporo vodstva, določa kadrovske in druge vire, opredeljuje vloge, odgovornosti in pristojnosti, določa kriterije in podobno. Politika je lahko samostojen dokument ali del druge ustrezne dokumentacije, kot je na primer politika upravljanja korporativne varnosti.

Priprava postopkov in orodij. Postopki vsebujejo kriterije za identifikacijo, način prijave in možnost anonimne prijave, nabor obveznih podatkov pri prijavi, kriterije za razvrščanje, kriterije za ocenitev škode, način predlaganja in sprejetja ukrepov, kriterije za merjenje učinkovitosti ukrepov, obveščanje in komuniciranje z javnostmi, izobraževanje in usposabljanje. Prav tako določa programska orodja za obvladovanje podatkov in procesov pri upravljanju škodnih dogodkov.

Določitev pristojnosti in odgovornosti. Z uvedbo sistematičnega upravljanja škodnih dogodkov zaposleni prevzemajo določene pristojnosti in odgovornosti, ki se jih po potrebi formalno vključi v njihove delovne naloge.

Programi izobraževanja. Sestavni del upravljanja škodnih dogodkov je izobraževanje in ozaveščanje vseh zaposlenih. Izobraževanje mora zajeti splošne teme o prepoznavi in vplivu škodnih dogodkov na poslovanje ter specializirane vsebine glede izvajanja postopkov za zaposlene s posebnimi nalogami in odgovornostmi.

Obvladovanje škodnih dogodkov

Učinkovito obvladovanje škodnih dogodkov poteka v petih ključnih korakih.

Takojšen odziv. Vzpostavi se pravila za takojšnji odziv in ublažitev za tipične scenarije ter splošne smernice za nepredvidene scenarije. Pravila vsebujejo priporočen način in varnost ravnanja, postopke in hierarhijo obveščanja ter druge ukrepe. Opredeljeni morajo biti tudi postopki in vrstni red obveščanja organov pregona, gasilcev, nujne pomoči, civilne zaščite in drugih, kadar je potrebno.

Prijava škodnega dogodka. Ob pojavu škodnega dogodka se omogoči čim hitrejša in čim bolj enostavna prijava. Postopek prijave mora omogočati vnos minimalnega nabora podatkov in njihovo sprotno dopolnjevanje, ko so na voljo.

Obravnava škodnega dogodka. Odgovorni preverijo popolnost in pravilnost podatkov, vključijo morebitne druge deležnike za obravnavo, poskrbijo za natančno klasifikacijo škodnega dogodka, ga razvrstijo glede na sprejete kriterije in poskrbijo za predloge korektivnih in preventivnih ukrepov. Pomembno je, da se ugotovijo in odpravijo temeljni vzroki za nastanek škodnih dogodkov. Po potrebi se poskrbi za zaščito in ohranitev verodostojnosti dokazov ter vključitev pristojnih organov.

Ukrepi. Za ublažitev posledic in preprečitev ponovitve škodnih dogodkov se predlaga in ovrednoti ustrezne korektivne in preventivne ukrepe. Po odobritvi se določi odgovorne za izvedbo, pripravi terminske in finančne načrte ter zagotovi sredstva. Prav tako se poskrbi za vse potrebne aktivnosti, s katerimi odpravimo posledice škodnih dogodkov.

Zaključitev škodnega dogodka. Ko so zbrani vsi podatki, vzpostavljeni in delujoči ukrepi, zaključene vse finančne postavke in je popolnoma odstranjen vpliv na poslovanje, se škodni dogodek zaključi, čeprav se po potrebi lahko vrne v obravnavo. Ko so podatki arhivirani, se smiselno uporabljajo za analize in poročanje.

Nadzor učinkovitosti upravljanja škodnih dogodkov

Nadzor nad učinkovitostjo upravljanja je ena od ključnih faz v celotnem sistemu upravljanja škodnih dogodkov in je v naših organizacijah nemalokrat zanemarjena. Nikakor ne moremo izboljševati stanja, če nad procesom nimamo ustreznega nadzora in predvsem jasne slike o potrebnih izboljšavah. Zaradi navedenega v tem delu procesa izvajamo naslednje ukrepe:

Poročanje. Vzpostavljeno mora biti poročanje o škodnih dogodkih. Obseg in pogostost poročanja sta odvisna od potreb organizacije in mora potekati na vseh nivojih, kjer so podatki pomembni za odločanje.

Analiza škodnih dogodkov. Metode analiziranja morajo zagotavljati rezultate, ki prikazujejo trende in vplive po pomembnih kriterijih ter so uporabni pri načrtovanju preprečevalnih ukrepov na vseh področjih in ravneh vodenja. Hkrati odgovornim za korporativno varnost pomagajo pri pripravi in utemeljitvi predlogov potrebnih izboljšav in investicij.

Spremljanje učinkovitosti. Pomembno je, da so vzpostavljeni postopki, kriteriji in odgovornosti za preverjanje učinkovitosti upravljanja škodnih dogodkov, vključno z ekonomsko učinkovitostjo izvedenih ukrepov.

Orodje za upravljanje škodnih dogodkov

Za izvajanje opisanih postopkov potrebujemo ustrezno orodje za obvladovanje podatkov in procesov. Ena od možnih rešitev je Silver Bullet Incident (SBI), ki omogoča, da celoten proces upravljanja škodnih dogodkov – od prve prijave in obvladovanja, do analiz, poročanja in izračunov finančnih posledic – poteka brezpapirno, vsi podatki so ves čas zbrani na enem mestu, pregledni in na voljo vsem, ki jih potrebujejo za analize, ukrepanje ali poročanje. ■



WWW.SILVERBULLETRISK.COM

Vabilo na 6. strokovno konferenco o upravljanju tveganj

»Učinkovito upravljanje tveganj kot temelj za poslovno odločanje in uspešnost«

Upravljanje tveganj večini podjetij in organizacij še vedno predstavlja izziv. Številni se namreč ustavijo že pri prvem vprašanju: "Ali in zakaj je upravljanje tveganj sploh potrebno?" Še težje pa je, ko je proces že v veljavi, a ne prinaša uporabne vrednosti pri poslovnem odločanju in uspešnosti nasploh.

Zato se bomo prav tej temi v celoti posvetili na 6. strokovni konferenci o upravljanju tveganj in vam v družbi priznanih strokovnjakov odgovorili na številna vprašanja, s katerimi se pri upravljanju tveganj srečujemo pri svojem vsakdanjem delu.

Na primerih dobre prakse v slovenskih podjetjih pa vam bomo tudi pokazali, kako učinkovito in praktično uporabno upravljanje tveganj dosežemo v svojem podjetju ali organizaciji.

Pridružite se nam 21. oktobra 2021 ob 9. uri v Kongresnem centru Lifeclass v Portorožu.

SLOVENIAN GRAND SECURITY AWARD
ICS
2020
INOVATIVNA VARNOSTNA REŠITEV LETA

Informacijska platforma Silver Bullet Risk pa je tudi letošnji prejemnik prestižne ***Slovenske nagrade varnosti v kategoriji inovativna varnostna rešitev***, ki jo podeljuje Institut za korporativne varnostne študije ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti in SE Europe Security Award (SEECSA).

PODJETJE SILVER BULLET RISK JE SPECIALIZIRANO IN VODILNO NA PODROČJU CELOVITEGA UPRAVLJANJA IN OBVLADOVANJA TVEGANJ V SLOVENIJI.

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*



PRED VRATI SO NOVI RAZISKOVALNO-TEHNOLOŠKI PROJEKTI V OKVIRU PERSPEKTIVE HORIZON 2020

Nova tehnološka, organizacijska in procesna spoznanja so ključna za nadaljnji razvoj ustreznih pristopov na področju obvladovanja kompleksnih varnostnih tveganj za neprekinjeno delovanje kritične infrastrukture. V okviru že zaključene raziskovalne perspektive EU HORIZON 2020 so bili izbrani trije izredno pomembni razvojni projekti, v katerih imajo ključno vlogo tudi slovenski partnerji, ki so člani Slovenskega združenja za korporativno varnost.

Kompleksnost groženj in negativnih vplivov s strani okolja, ki obdaja naše organizacije, se iz leta v leto stopnjuje. Grožnje se med seboj korelirajo in s tem dobivajo dodatne dimenzije negativnih vplivov, ki niso več omejeni samo na eno organizacijo, lokalno skupnost ali določeno regijsko območje, temveč so vedno bolj meddržavno pogojene in prinašajo medsektorske in čezmejne posledice. Zaradi navedenega je potrebno neprestano iskati nove poti, kako v operativno delovanje naših zahtevnih sistemov, še posebno tistih, ki upravljajo s kritično infrastrukturo, vnašati najnovejše prakse in nove tehnološke rešitve, ki nam omogočajo boljše situacijsko zaznavanje in pristope za obvladovanje tveganj ter groženj. Poleg negativnih vplivov naravnih in tehnoloških nesreč, vedno večjo težo dobivata dva pomembna področja groženj, in sicer grožnje, ki izhajajo iz informacijskega in ožje kibernetskega prostora ter grožnje, ki jih povzroča človek, kot eden najpomembnejših agregatov in dejavnikov v sistemih zagotavljanja integralne korporativne varnosti naših organizacij. Zaradi navedenega, nas posebej veseli, da imajo organizacije iz Republike Slovenije, pomembno vlogo pri izvajanju razvojno-raziskovalnih projektov na področju EU in so kot take prepoznane, kot pomembni partnerji teh projektov. Še posebej pa smo ponosni na to, da je večina teh organizacij tudi v članstvu Slovenskega združenja za korporativno varnost. V mesecu septembru in oktobru začenjajo s svojim delovanjem trije izredno pomembni EU projekti s področja zaščite kritične infrastrukture, zagotavljanja varnosti na javnih površinah, predvsem pred terorističnimi grožnjami in seveda s področja kibernetske varnosti. Ti trije mednarodni projekti so: (1) APPRAISE – Facilitating Public & Private security operators to mitigate terrorism scenarios against soft targets (2) PRECINCT - Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with focus on district or regional protection in (3) CyberSEAS - Cyber securing energy data services. V nadaljevanju bomo kratko predstavili osnovna težišča teh treh pomembnih projektov.

APPRAISE

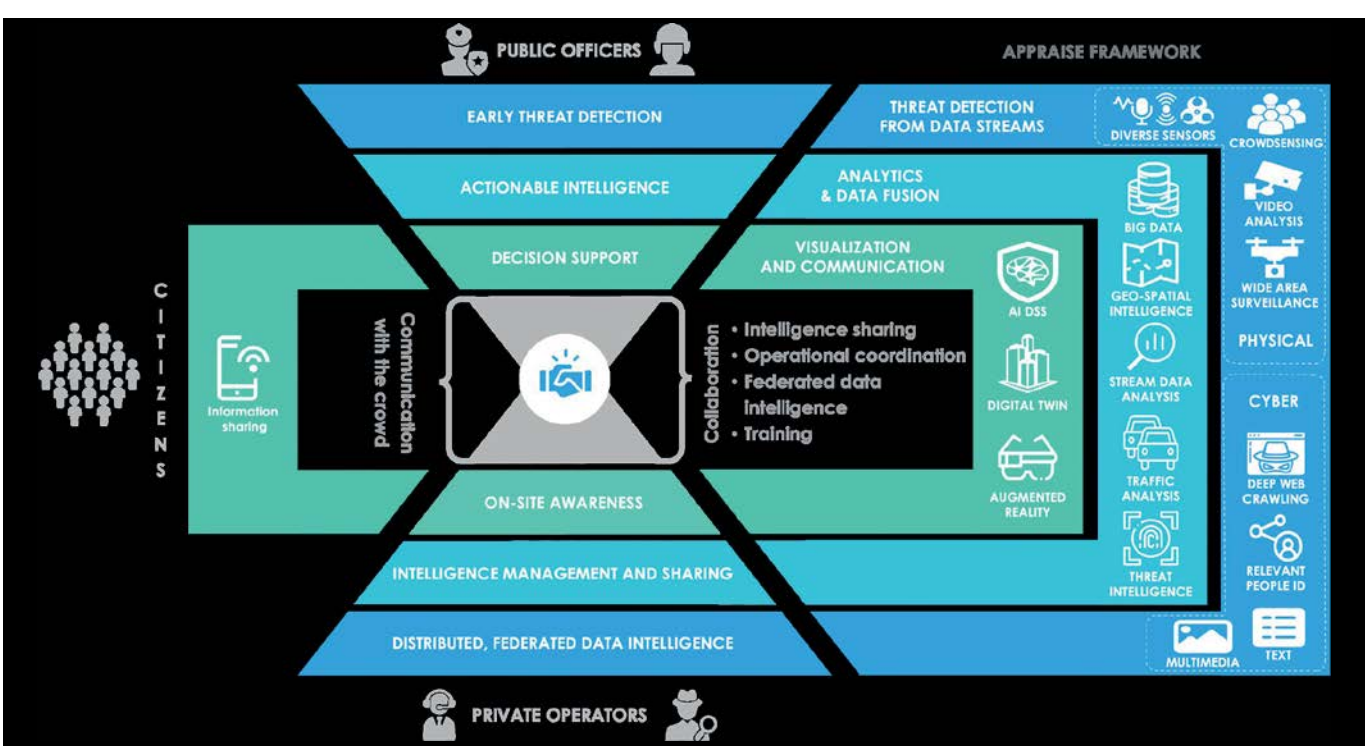
APPRAISE želi doseči učinkovitejše in proaktivno zagotavljanje varnosti v EU na javnih površinah s posebnim poudarkom na t.i. »mehkih tarčah«. To želi doseči z: (1) izboljšanjem sedanjih zmogljivosti izvajalcev javne in zasebne varnosti, s poudarkom na učinkovitejšemu izkoristku večje količine javnih baz podatkov in (2) vzpostavitvijo uspešnega okvirja sodelovanja s povečanjem racionalizacije in izrabe zmogljivosti, ki so na voljo. APPRAISE predlaga nov globalno

*avtorica je članica Slovenskega združenja korporativne varnosti

integriran, vključujoč in sodelovalni pristop za zagotavljanje varnosti mehkih tarč, ki temelji na združevanju, analizi, korelaciji in izmenjavi vseh ustvarjenih pomembnih podatkov. Celoten koncept APPRAISE je ponazorjen na shemi 1, kjer je zaznavanje fizične in kibernetske grožnje označeno z modro barvo, analitika velikih podatkov za inteligentno delovanje in napovedovalno analitiko, je prikazana s svetlo modro ter vizualizacijska in komunikacijska orodja, ki so ponazorjena z zeleno barvo. Shema prikazuje kateri od podatkov so v uporabi javnih in zasebnih varnostnih organizacijah ter javnosti, ki je tudi pomemben uporabnik dela teh informacij. V središču je prikazan vidik sodelovanja, ki se rezultira z uporabo ustreznih orodij, kot tehnična pomoč, pri zagotavljanju tega cilja. Za odkrivanje zgoraj omenjenih fizičnih in kibernetskih groženj APPRAISE uvaja nove rešitve in zmogljivosti, ki jih lahko uporabljajo varnostni strokovnjaki zasebnega in javnega okolja, odvisno od njihove razpoložljive infrastrukture. Ti vključujejo (i) rešitve videoanalize za omrežja CCTV za odkrivanje orožja in sumljivih predmetov, analize množice v realnem času in zaznavanje nenormalnega vedenja posameznikov in množice, (ii) (pol) avtomatski sistemi za nadzor širšega območja z uporabo brezpilotnih letal, (iii) odkrivanje terorističnih dejanj, kot so eksplozije in streli z uporabo zvočnih senzorjev, (iv) neposredne grožnje, kot so nelegalna uporaba materialov CBRN in uporaba dronov, kot sredstva napada, in (v) kibernetski napadi na nadzorno infrastrukturo. Poleg tega bodo za zbiranje informacij uvedene funkcije množičnega zbiranja informacij s strani udeležencev teh dogodkov. Vsa orodja za obdelavo podatkov bodo razmeščena bodisi na robu omrežja ali na lokalni strežniški ravni, kar bo zagotavljalo interoperabilnost z obstoječimi sistemi C2 in ohranjanje skladnosti GDPR v postopkih izmenjave podatkov. APPRAISE bo razvil tudi zmogljivosti, ki bodo varnostnim strokovnjakom omogočale izboljšanje njihovih operativnih zmogljivosti izvajanja (1) spletne analize vsebine, (2) oceno tveganja mehkih tarč, (3) pridobivanje obveščevalnih podatkov o grožnjah, in (4) pametno in učinkovito vizualizacijo podatkov v večdimenzionalnem sistemu, ki temelji na digitalnem dvojčku ter (5) sistemom za sprejemanje odločitev, ki temelji na podpori umetne inteligence. Spletni modul za analizo vsebine bo pridobival podatke (besedilne, vizualne in zvočne) iz javnih spletnih virov in virov iz temnega interneta ter na podlagi tega izvedel multimodalno analizo, da bi v njej pridobil kazalnike bližnjih napadov na mehke tarče. Za identifikacijo omrežij in določenih posameznikov bo opravljena analiza družbenih omrežij, kjer se bodo zaznavali indikatorji za organizacijo napadov ali s tem povezane propagandne kampanje. Rezultat modulov za odkrivanje groženj in spletnih modulov za analizo vsebine, bo skupaj s podatki o pametnih mestih, vizualiziran na digitalni osnovi in bo omogočal intuitivno zavedanje situacije v realnem času. Izboljšanje sodelovanja izvajalcev zasebne varnosti z organi za zagotavljanje javne varnosti je v središču projekta APPRAISE. Namen projekta je spodbujati izmenjavo informacij in krepiti operativno sodelovanje. Informacijski sistem, ki bo varen pred kibernetskimi vdori bo namenjen izmenjavi podatkov v standardizirani obliki. Vzpostavljeni multifunkcijski informacijski sistem bo v omejenem obsegu na voljo tudi izvajalcem zasebne varnosti z namenom zagotavljanja boljšega operativnega situacijskega zavedanja in možnosti večnivojskega izmenjevanja ključnih operativnih podatkov.

V projektu bodo organizirani pomembni pilotni primeri, ki bodo predstavljali različne oblike možnih tipov javnih prireditvenih prostorov. Le ti bodo naslednji (1) meddržavni primer organizacije velikega kolesarskega tekmovanja v Baskiji med Francijo in Španijo; (2) ATP teniški turnir v Torinu v Italiji; (3) trgovsko zabaviščni kompleks BTC-City v Ljubljani in (4) mednarodna sejemska infrastruktura v Gdansku na Poljskem.

Slovenski partnerji tega projekta so Ministrstvo za notranje zadeve-Policija, BTC City in Institut za korporativne varnostne študije.

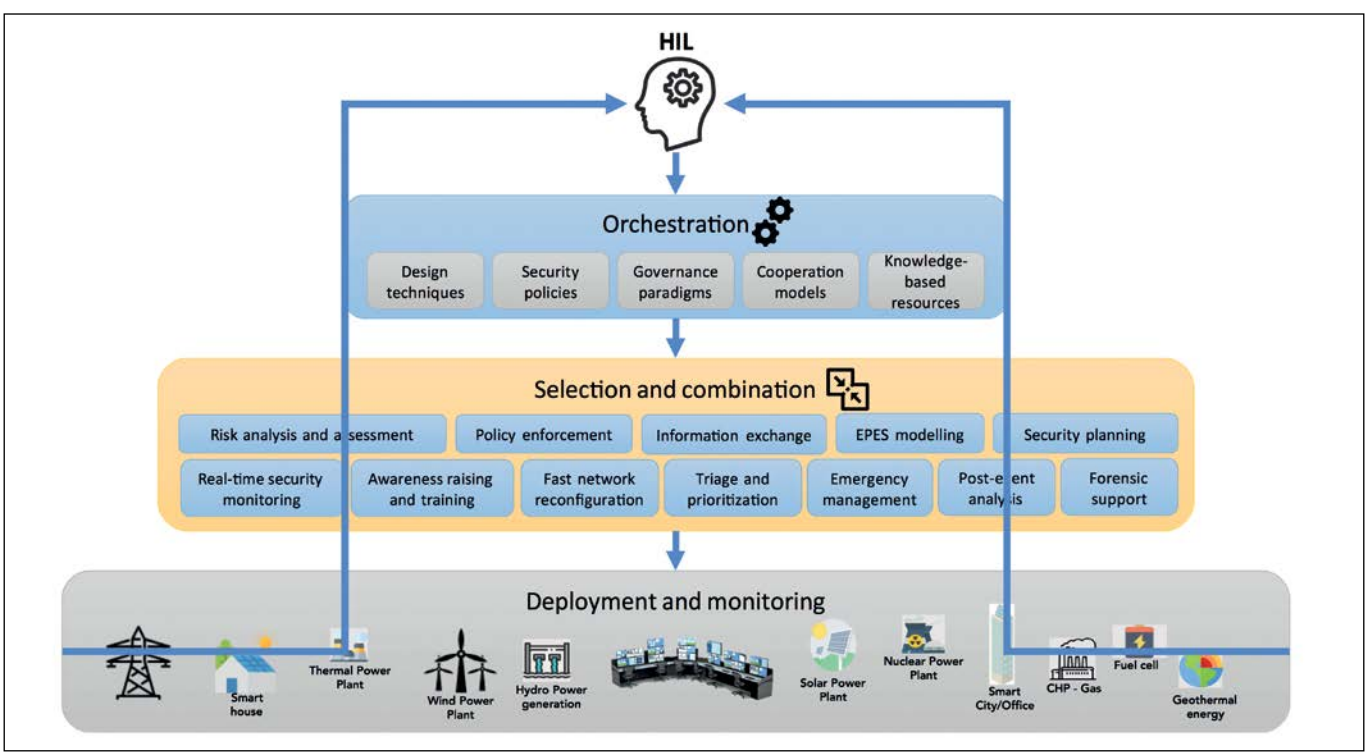


Shema 1 – koncept APPRAISE

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021981".

CyberSEAS

Cilj projekta CyberSEAS (Cyber Securing Energy Data Services) je izboljšati splošno odpornost verig oskrbe z energijo in jih zaščititi pred motnjami, ki izkoriščajo okrepljene interakcije, modele razširjene vključenosti zainteresiranih strani in potrošnikov, kot poti za zapletene kibernetske napade. Tveganja še dodatno izpostavljajo prisotnost slabih osnov pri razvoju sistemov in vse večjo povezljivost energetske infrastrukture, v katerem imajo pomembno mesto shrambe podatkov in vedno večje število deležnikov, ki so vključeni v elektro-energetski sistem. Projekt ima tri strateške cilje: 1) boj proti kibernetskim tveganjem, povezanim z napadi, ki imajo najpomembnejši vpliv na elektro-energetski sistem; 2) zaščita potrošnikov pred kršitvami osebnih podatkov in kibernetskimi napadi; in 3) povečanje varnosti skupnega podatkovnega prostora vezanega na delovanje elektro-energetskega sistema. Vsi trije cilji so enako pomembni, saj kibernetski kriminalci spreminjajo taktiko v prid večstopenjskim napadom, pri katerih je kraja občutljivih podatkov predpogoj za pravi napad. Le to jim omogoča, da povečajo škodo in dobiček, medtem ko so tradicionalni kibernetski napadi na infrastrukturo odražajo skozi neposredne napade na infrastrukturo in so običajno ciljno usmerjeni v onemogočanje nadzornih sistemov in manj v podatke. Akterji groženj, zlasti veliki, kot so nacionalne države, izvajajo tudi zapletene napade, ki spodbujajo odvisnosti od dobavne verige, in ta trend se še naprej povečuje, kot je bilo poudarjeno v analizi, ki jo je julija 2020 opravil NATO. V zadnjem obdobju, pa je potrebno vedno močneje upoštevati scenarije, kjer so uporabniki sistemov vedno bolj vključeni v delovanje teh sistemov. V teh primerih podatki o porabnikih postajajo vse bolj občutljivi. Za dosego teh ciljev CyberSEAS ponuja odprt in razširljiv ekosistem s 30 prilagodljivimi varnostnimi rešitvami, ki zagotavljajo učinkovito podporo ključnim dejavnostim, zlasti: (1) ocene tveganja; (2) interakcijo s končnimi napravami; (3) varen razvoj in uvajanje novih storitev in naprav; (4) varnostno spremljanje dogodkov v realnem času; (5) izboljšanje spretnosti in ozaveščenost; (6) certificiranje, upravljanje in sodelovanje. Rešitve CyberSEAS so potrjene za doseganje stopnje tehnološkega razvoja na nivoju TRL-7 s poskusnimi kampanjami, sestavljenimi iz več kot 100 scenarijev napadov, preizkušenih v treh laboratorijih, preden se bodo preselili v eno od šestih pilotnih infrastruktur.



Shema 2 - The CyberSEAS ekosistem

"The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020560".

Slovenski pilot tega mednarodnega projekta je izredno močan in je sestavljen iz organizacij ELES, PETROL, INFORMATIKA s podporo vseh elektro distribucijskih podjetij, SI-CERT in Instituta za korporativne varnostne študije.

PRECINCT

Kritične infrastrukture EU so vse bolj ogrožene zaradi kibernetsko-fizičnih napadov in naravnih nevarnosti. Raziskave in nastajajoče rešitve se osredotočajo na zaščito posameznih KI, vendar so medsebojni odnosi med posameznimi kritično-infrastrukturnimi sektorji postali vse bolj zapleteni. Ukrepi na primer v pametnih mestih, obvladovanje kaskadnih učinkov in omogočanje hitrega okrevanja, pa postajajo vse pomembnejši in zelo zahtevni. Cilj projekta PRECINCT je povezati zasebne in javne deležnike informacijske tehnologije na geografskem območju s skupnim pristopom upravljanja kibernetske in fizične varnosti, ki bo državljanom in infrastrukturi prinesel ustrezne mehanizme zadostne zaščite.

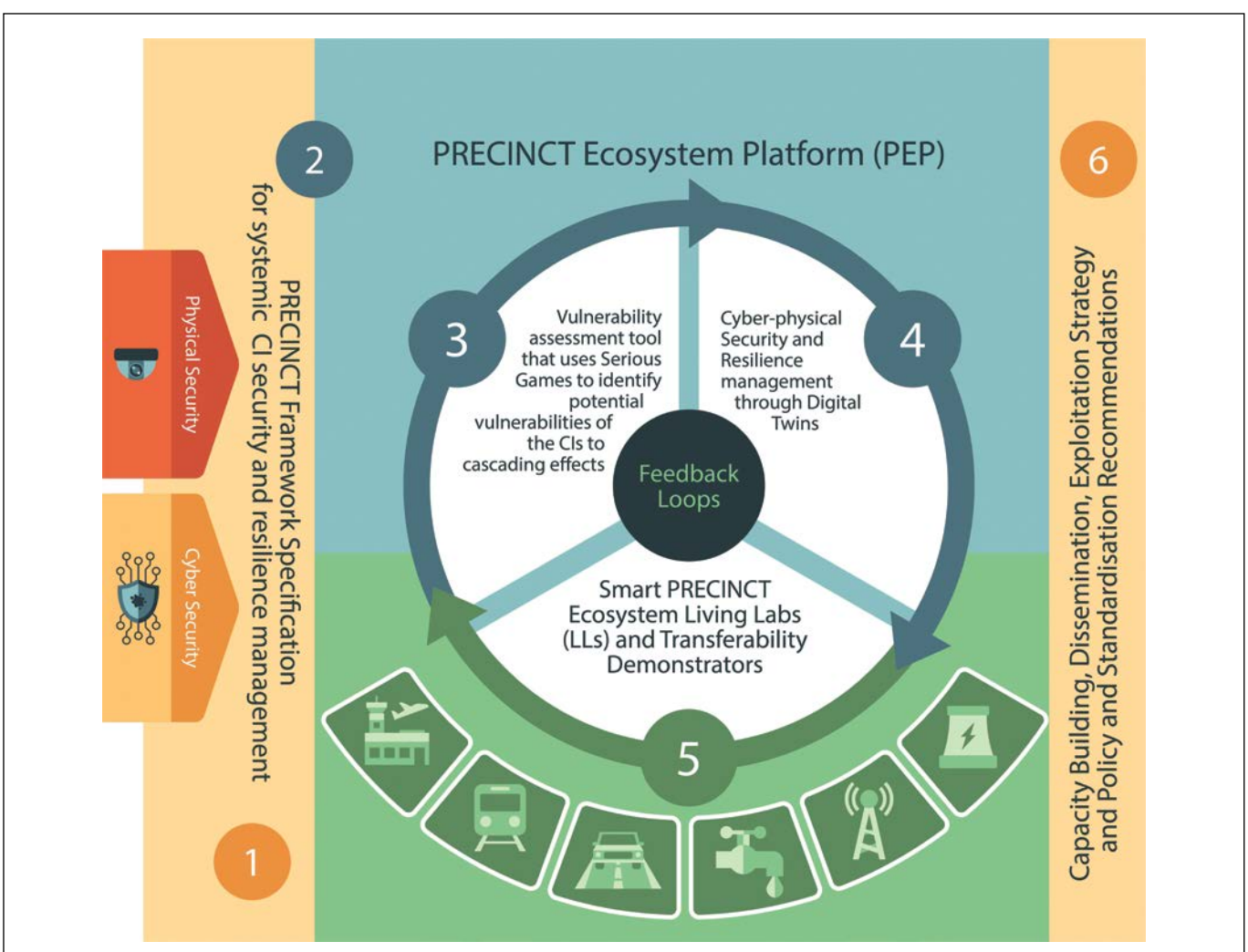
Projekt bo predstavil koncept pametnih odpornih okoli, ki bodo razviti v štirih živih laboratorijih. Kaskadni učinki bodo obravnavani skozi različne scenarije, ki bodo simulirali grož-

nje v multimodalnem prometu, energiji, oskrbi z vodo in IKT/telekomunikacijah. Te kritične infrastrukture temeljijo na medsebojni odvisnosti med temi vidnimi in zelo medsebojno povezanimi okolji, ki zajemajo kibernetske fizične in hibridne scenarije groženj. Zahteve za pristop k celovitemu upravljanju kibernetsko-fizične varnosti, vključno z javno-zasebnimi partnerstvi, bo iskal poti za doseganje harmonije med organizacijo družbe in gospodarskim razvojem. Pomembno bo doseči optimalno ravnovesje med tveganjem, stroški in zahtevami glede varnosti ter odpornosti. To bo v nadaljevanju nudilo ustrezno podlago za obveščanje o taktičnih in strateških možnostih naložb na posameznem območju. V ta namen bo PRECINCT gradil na nedavnih in naprednih pristopih KI v štirih predlaganih živih laboratorijih. Projekt bo zagotovil modelno podprto in vključujočo platformo za kibernetsko-fizično varnost in upravljanje odpornosti za pametne in odporne regije. Glavni rezultati projekta, prikazani na shemi 3, so:

(1) Okvirna specifikacija PRECINCT za sistematično upravljanje varnosti in odpornosti kritičnih infrastruktur, ki izpolnjuje industrijske zahteve, pridobljene s strani zainteresiranih deležnikov v živih laboratorijih in vključuje nove vpoglede iz referenčnih projektov EU. (2) Sodelujoča platforma za kibernetsko-fizično varnost in upravljanje odpornosti, ki sodeluje med različnimi ustanovami in omogoča zainteresiranim stranem, da razvijejo ekosisteme PRECINCT, ki podpirajo umetno inteligenco, in storitve podpore za večjo odpornost. (3) Orodje za ocenjevanje ranljivosti, ki uporablja simulacijska orodja za preigravanje scenarijev, ki omogoča ugotavljanje potencialnih ranljivosti kritične infrastrukture do kaskadnih učinkov in za ugotavljanje izboljšav odpornosti na ravni vsake posamezne kritične infrastrukture ter usklajenih ukrepov. (4) PRECINCT digitalni dvojčki za predstavitev topologije in metapodatkov kritičnih infrastruktur, ki ustrezajo ustreznim profilom odvisnosti, z uporabo strojnega učenja z zaprto zanko (ML) za odkrivanje nepravilnosti in opozorilnih pogojev ter za optimizirano aktiviranje odzivnih in omilitvenih ukrepov ter avtomatizirano forenziko. (5) Ekosistemi Smart PRECINCT, razporejeni v štirih velikih živih laboratorijih in v demonstratorjih potrditve prenosljivosti, bodo na podlagi meritev zagotovili dokaze o ciljnih prednostih. (6) PRECINCT-ovi trajnostni učinki, vključno z izgradnjo zmogljivosti, razširjanjem, izkoriščanjem, strategijo odpornosti ter priporočili politike in standardizacije.

Slovenski partnerji tega projekta so Mestna občina Ljubljana z Mestnim redarstvom, Telekom Slovenija, Elektro Ljubljana, Slovenske železnice, Ljubljanski potniški promet (LPP), Prometni inštitut in Institut za korporativne varnostne študije.

O vseh projektih, ki začnejo s svojim delovanjem v mesecu septembru in oktobru vas bomo redno obveščali. ■



Shema 3 - The PRECINCT ecosystem

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021668".

13. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

LJUBLJANA, 24.—25. MAJ 2022



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**
- **NAJBOLJŠI PRISPEVEK 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 INSTITUTA WWW.ICS-INSTITUT.SI!

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*



REPORTAŽA

DNEVI KORPORATIVNE VARNOSTI IN PODELITEV SLOVENIAN GRAND SECURITY AWARD

Odmeven mednarodni dogodek »Dnevi korporativne varnosti 2021« je organiziral Institut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti. Osrednja tema je bila posvečena povečanju odpornosti organizacij v dobi digitalizacije, s poudarkom na izzivih kibernetske varnosti in zaščite kritične infrastrukture. V okviru dogodka so bile podeljene prestižne letne nagrade Slovenian Grand Security Award.

Uspešno se je zaključilo še eno poglavje tradicionalne mednarodne konference »Dnevi korporativne varnosti«. Organizacija konference je bila zaradi razmer tudi letos zahteven organizacijski izziv, ki pa smo ga skupaj z vsemi udeleženci in podporniki konference, izpeljali na odličen način. Konferenca je tokrat potekala 25. in 26. maja 2021. Zaradi razmer je potekala v nekoliko spremenjenem formatu in sicer v hibridni obliki. Prvi dan se je odvila v spletnem okolju, drugi dan pa je potekala kombinirano. Del prireditve se je dogajal v živo v veliki dvorani Centra urbane kulture, Kino Šiška v Ljubljani z neposrednim prenosom v splet, nadaljevanje pa zopet v spletni obliki.

Kljub temu smo imeli priložnost videti ogromno odmevnih predavanj in štiri vsebinsko zelo bogate okrogle mize, z udeleženci, ki so predstavljali strateški management in vrh strokovne javnosti. Vsebinski del dogodka je potekal on-line. Le ta je omogočil, da je bila konferenca spremljana v širšem mednarodnem prostoru, saj je bilo letos na dogodku zastopano občinstvo in predavatelji kar iz 19 držav. Del prireditve, ki se je sicer odvil v živo ob strogih ukrepih NIJZ, pa je po dolgem času ponudil zadovoljstvo in možnost osebnega stika in druženja strokovne javnosti.

Sponzorji konference so nam skozi različne kanale in oblike predstavili najno-







*avtor je član Slovenskega združenja korporativne varnosti







vejše produkte na tehnološkem in procesnem delu, ki bodo v prihodnosti lahko v pomoč pri učinkovitem obvladovanju tveganj na področju korporativne varnosti s posebnim poudarkom na kibernetski varnosti in zagotavljanju odpornosti naših organizacij.

Cel niz strokovnih dogodkov skozi konferenčni program je tudi tokrat omogočil tkanje novih strokovnih poznanstev, izmenjavo novih izkušenj in seveda strokovne afirmacije posameznih strokovnjakov ter ponudnikov varnostnih rešitev. Letošnja rdeča nit je bila posvečena povečanju odpornosti organizacij v dobi digitalizacije, s poudarkom na izzivih kibernetske varnosti in zaščite kritične infrastrukture.

Prvi dan v znamenju informacijske varnosti

Otvoritveno predavanje je tokrat pripadlo strokovnjaku za kibernetsko varnost iz podjetja Telekom Slovenije. Nadaljevala sta mednarodna strokovnjaka s področja telekomunikacij, ki sta odprla zanimivo razpravo o morebitnih tveganjih s pojavom nove tehnologije 5G.

V nadaljevanju je bila pozornost namenjena kritični infrastrukturi in pregledu nekaterih projektov, ki jih financira Evropska komisija. Izpostaviti gre dobre prakse in spoznanja projekta Infrastress, v katerem sodeluje tudi Institut za korporativne varnostne študije.

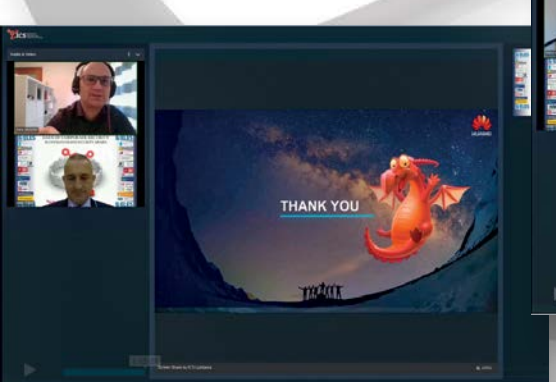
V zaključnem delu so strokovnjaki razpravljali o kibernetski varnosti v kritični infrastrukturi in upravljanju s tveganji v takih sistemih. Odvila se je tudi odmevna okrogla miza s strokovnjaki s področja korporativne in informacijske varnosti. Odgovarjali so na vprašanja, kako zagotoviti odpornost kritičnih organizacij za neprekinjeno delovanje v času informacijske družbe in tudi, kakšne spremembe je prinesla epidemija.

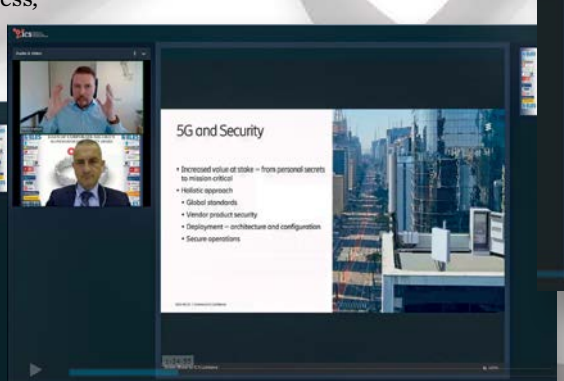
Prvi dan je zaključil dr. Vadnjal s predavanjem o pasteh in nevarnostih odprtega bančništva in direktive PSD2 ter o nujnosti nadzora nad tretjimi ponudniki storitev.

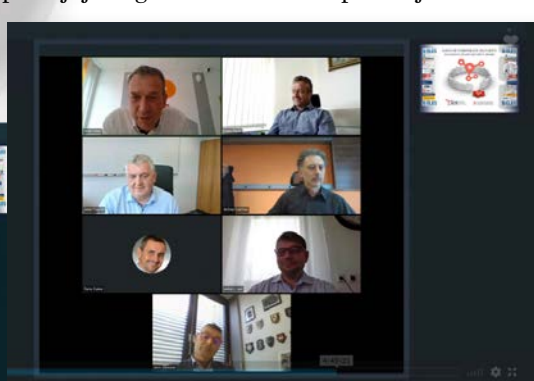
Vsebino prvega dne bi vsekakor lahko združili v nekaj pomembnih ugotovitev, ki bodo v prihodnje imele ključni vpliv na dvigovanje odpornosti družbe in organizacij pred tveganji in grožnjami. Pospešitev sodelovanja in sooblikovanja normativnega, regulatornega, strokovnega in operativnega okolja bo možno doseči samo s skupnimi koraki, kjer bodo vsi deli pomembnih strokovnih entitet iz javnega in zasebnega okolja izvajali aktivnosti v isti smeri za dosego splošnega cilja. To pa je obvladljivo in varno okolje, kjer bo imela informacijska varnost še posebej pomembno mesto. Prihajamo namreč v obdobje digitalizacije, kjer bo za ustrezen razvoj družbe potrebno postaviti dovolj trdne temelje, ki bodo omogočali obvladljivo okolje delovanja. Organizacije, še posebej tiste, ki upravljajo s ključnimi procesi, kot so kritična infrastruktura ali bistvene storitve, bodo morale še poglabljati zavedanje o pomembnosti varnosti in s tem kreirati ustrezne podporne mehanizme pri zagotavljanju odpornosti njihovih sistemov. Vendar za korak naprej potrebujemo širše okolje razumevanja, kjer bo potreba po odporni družbi postala ponovno pomembna vrednota. Procesi digitalizacije, razpršenosti in seveda nove tehnologije nas postavljajo v situacijo, kjer lahko vsak posameznik postane del tveganja za nemoteno delovanje širših sistemov.

V drugem dnevu počastili »svetilnike odličnosti«

Institut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti vsako leto podeljuje nagrade za dosežke s področja













korporativne varnosti. **„Slovenska velika nagrada varnosti“** oziroma **„Slovenian Grand Security Award“** je prestižna nagrada s področja varnosti v Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Uradna podelitev nagrad se je zgodila 26. maja 2021 v Ljubljani v okviru drugega dne dogodka Dnevi korporativne varnosti 2021.

Podelitvi so s svojimi nagovori dali posebno težo g. Alojz Kovšca, predsednik Državnega sveta RS, g. Aleš Mihelič, državni sekretar Ministrstva za infrastrukturo, g. Uroš Lampret, državni sekretar Ministrstva za obrambo, mag. Stanislav Vrečar, namestnik Generalnega direktorja Policije in mag. Aleksander Mervar, direktor ELES. Predsednik organizacijskega odbora konference dr. Denis Čaleta se je v otvoritvenem nagovoru v imenu organizacijskega odbora zahvalil vsem, ki so se v teh težkih trenutkih zavzemali, da so naše organizacije in družba neprekinjeno delovale. Hkrati je poudaril, »da gre v primeru nagrajencev za svetilnike odličnosti, ki se jim bomo trudili slediti tudi vsi ostali«.

Letošnji prejemniki prestižnih nagrad »Slovenian Grand Security Award« za dosežke v preteklem letu so:

- Nagrado za »najboljšega korporativno varnostnega managerja« je letos prejel **g. Božidar Dajčman** iz podjetja Nova KBM d.d.
- Nagrado za najbolj varno podjetje je tokrat prejelo podjetje **Luka Koper d.d.**
- Nagrado za »najbolj inovativno varnostno rešitev« je prejelo podjetje **Silver Bullet Risk d.o.o.**
- Za »najbolj varno mesto« je nagrado prejela **Mestna občina Velenje**, v kategoriji »najbolj varna občina« pa **Občina Sevnica.**
- **Osrednja informativna oddaja Dnevnik Televizije Slovenija** pa je prejela nagrado v kategoriji »najbolj inovativna medijska podpora«.
- Podeljeni pa sta bili tudi dve nagradi za »življenjsko delo« in sicer sta jo prejela **doc. dr. Milan Vršec** in **g. Ingo Falk Pasch Wallersberg.**

V okviru svečane podelitve se je odvila okrogla miza z vodilnimi managerji pomembnih slovenskih organizacij, ki so izpostavili ključne vidike na temo »Uvajanja novih digitalnih rešitev in strateški izzivi zagotavljanja varnosti ter neprekinjenega delovanja organizacij«. Z nami so svoje poglede delili mag. Aleksander Mervar, direktor ELES d.o.o., dr. Mitja Štular, član uprave Telekoma Slovenije d.d., mag. Valentin Hajdinjak, predsednik uprave DARS d.d. in mag. Roman Žnidarič, izvršni direktor CETIS d.d.

Konferenca se je po svečani podelitvi nadaljevala v spletnem okolju. Predstavljeni so bili sodobni pristopi z zanimivimi tehničnimi rešitvami na področju korporativne varnosti. Zadnji del dvodnevne konference je pripadel okrogli mizi, na kateri so sogovorniki razkrili, kaj v prihodnosti prinašajo spremembe zakonodajnih okvirov v EU na področju zagotavljanja kritične infrastrukture.

V zaključku se lahko vsem, ki ste bili del tega odličnega dogodka, še enkrat iskreno zahvalimo, in vas, kot tudi vso ostalo zainteresirano strokovno javnost, povabimo na naslednjo mednarodno konferenco Dnevi korporativne varnosti, ki bo v maju 2022. Tokrat v upanju, da bomo celoten dogodek izpeljali v živo in se vrnili v normalne tirnice medsebojnih srečanj in komunikacije. Do takrat pa ostanite na varni strani sveta tudi s pomočjo izkušenj, ki smo jih skupaj pridobili na zaključenem dogodku. ■







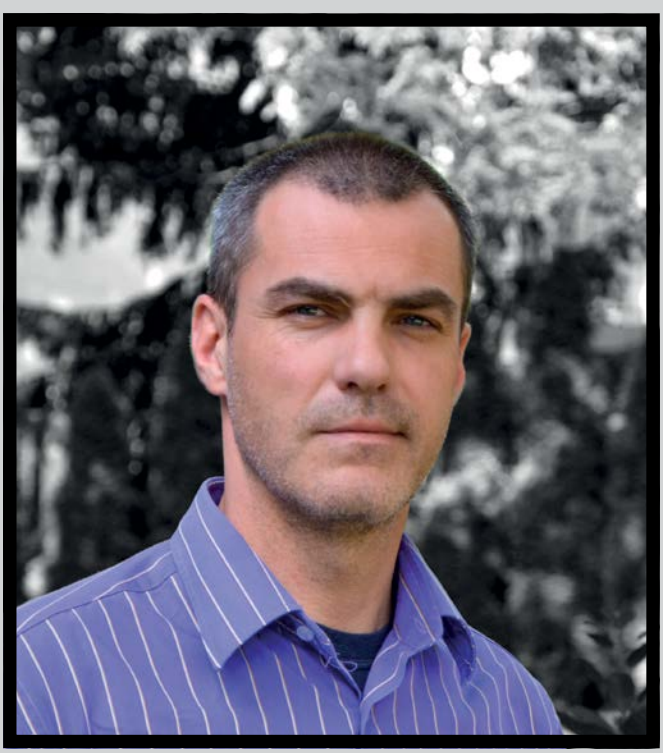
DOMNU PIRKMAJERJU V SPOMIN IN SLOVO

Pred časom nas je pretresla novica, da nas je mnogo prezgodaj zapustil naš prijatelj in strokovni kolega Domen Pirkmajer. Domen je bil eden izmed ustanovnih članov Slovenskega združenja korporativne varnosti in promotor tega za družbo pomembnega področja. S svojo strokovno kompetentnostjo in pozitivnim pristopom je vrsto let sooblikoval delovanje združenja in pomembno pripomogel, da se je dejavnost korporativne varnosti, kot pomemben proces, uveljavila v organizacijah. Še posebej je svoj trud posvečal uveljavljanju korporativne varnosti v organizacijah, ki upravljajo kritično infrastrukturo. Tudi sam je namreč vrsto let neutrudno postavljal ta sistem v Termoelektrarni Toplarni Ljubljana (TE-TOL), kjer je bil dolga leta korporativni varnostni manager.

Za svoj trud in požrtvovalni prispevek za razvoj tega področja sta ga neodvisna komisija Slovenskega združenja za korporativno varnost in Institut za korporativno varnost leta 2011 predlagala za podelitev nagrade za »korporativno varnostnega managerja leta«, ki jo je takrat tudi prejel in postal eden izmed prvih prejemnikov te prestižne nagrade. Svoje poglede in dobre prakse je vrsto let objavljal v reviji Korporativna varnost in tako pomagal, da so se tudi njegovi kolegi učili iz njegovih izkušenj.

S svojim pozitivnim pristopom do življenja je bil zaželen sogovornik in sopotnik na različnih mednarodnih strokovnih ekskurzijah iz katerih se je vračal še bogatejši z novimi spoznanji, ki jih je neutrudno uveljavljal v praksi svojega organizacijskega okolja. To mu je omogočalo, da je bil vedno slišan pri svojih predlogih za uveljavljanje višje stopnje varnosti, kot nujnega predpogoja za uspešno delovanje organizacij, kjer je služboval.

Velikost njegove osebnosti pa se je vedno zrcalila v dejstvu, da kljub pohvalam, ki jih je prejemal iz različnih družbenih okolij, je sam skromno stal na stališču, da je bolj kot to pomembno, »da je tvoje delo cenjeno in opaženo kot dobro, saj vsakdo na svoji delovni poti potrebuje signale, da se njegovo delo razvija v pravo smer«.



Kolegu Domnu se iskreno zahvaljujemo za vse trenutke, ki jih je preživel v okviru svojih prijateljev in strokovnih kolegov znotraj Slovenskega združenja za korporativno varnost. S svojim dojemanjem sveta in stroke nas je vsa ta leta delal boljše in za to smo mu večno hvaležni.

Spomin nanj bo vedno z nami, ko bomo nadaljevali po poti, ki jo je tudi sam načrtoval in to je zavzemanje za pomen varnosti, kot pomembne dobrine celotne družbene skupnosti.

Domen, hvala za vse!

člani Slovenskega združenja korporativne varnosti



VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

360° varnost vam zagotavlja **najsodobnejšo kibernetsko zaščito**. Na mobilni, stacionarni, oblačni in lastni infrastrukturi, ki je lahko tarča kibernetskega napada ali zlorabe. Zaradi vedno večje kompleksnosti kibernetskega okolja in varnostnih groženj brez kibernetske varnosti digitalni razvoj ni mogoč. Človekova zmožnost uvida v dogodke in povezovanje informacij pa je kljub vsej tehnologiji nepogrešljiva. Zato naj za vas vse dni in noči skrbijo naši **strokovnjaki Operativnega centra kibernetske varnosti (OCKV)**, ki ves čas spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske napade.

Ob morebitnem kibernetskem napadu vam zagotovijo omejitev napada in zmanjševanje škode, zbiranje in zavarovanje dokazov, zagotavljajo revizijsko sled in vas sproti seznanijo s pomembnimi dogajanji, ki jih zaznajo. OCKV Telekoma Slovenije je certificiran **po mednarodnem standardu za informacijsko varnost ISO 27001**, ob tem pa ima Telekom Slovenije tudi **certifikat za neprekinjeno poslovanje ISO 22301**. Naše storitve s področja 360° varnosti so tako primerne za podjetja vseh velikosti, saj OCKV za vsakogar poišče ustrezne rešitve.

telekom.si/poslovni

TelekomSlovenije

Za več informacij o prodajni ponudbi obiščite www.telekom.si ali pokličite 080 70 70. Telekom Slovenije, d.d., Ljubljana.