Korporativna varnost

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

Letnik 2023, oktober • št. 33

Tradicionalna 15. mednarodna konferenca Dnevi korporativne varnosti Brdo pri Kranju, 13.-14. maj 2024

Slovenska policija soočena z vedno večjo kompleksnostjo varnostnega okolja

Mag. Senad Jušić, Generalni direktor Policije

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

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:
tiskano v Sloveniji

Datum izida:
oktober 2023

Izvod revije je brezplačen

Naslovnica in slike:
Illustration 125486217 © Nmedia | Dreamstime.com.
Arhiv ICS

ISSN 2232-6170

Kompleksnost globalnega varnostnega okolja nam tudi za trenutek ne pusti sprostiti misli, da končno v celoti obvladujemo delovanje naših organizacij. Nenehni izzivi, ki niso povezani samo z varnostnimi vplivi, temveč so razpršeni skozi celoten spekter tveganj, nas nenehno držijo v stanju napetosti in iskanja ustreznih rešitev, kako učinkovito upravljati naše organizacije. Če v ta okvir dodamo še nerealna pričakovanja lastnikov, ki jim je v večini mar samo za trenutni dobiček, kakor za celovit in dolgoročni razvoj organizacij, po tem res lahko rečemo, da je krizno stanje postala vsakodnevna rutina. V takih razmerah je nujno potrebno energijo in omejene vire usmerjati v čim bolj učinkovito izrabo. V tem okviru pa je nujno iskanje sinergij in izogibanje silosnega delovanja. Pri tem ima tudi korporativna varnost, kot ena izmed ključnih poslovnih dejavnosti, zelo velik pomen. Velikokrat smo že izpostavili, da so ravno taka krizna stanja tisti »zvezdniški trenutek«, ko mora korporativna varnost kot celota, izpolniti pričakovanja, ki jih imajo od nje strateški managerji. Ob dejstvu pomanjkanja visoko strokovnega kadra, ki bi bil sposoben v celoti razumeti strokovni obseg potreb za učinkovito delovanje ob teh dinamičnih spremembah, se tudi v tem okviru pojavlja cel kup izzivov. Eden od pomembnih je tudi neprestano menjavanje strokovnega vodstvenega kadra na področju korporativne varnosti. Zaradi pomembnosti tega procesa so začele predvsem vsakokratne gospodarsko-politične vladajoče elite to funkcijo enačiti s svojim prevzemnim plenom. To ima za posledico nekritično menjavanje kadra, ki je v tako omejenem kadrovskem bazenu, kot ga premore Republika Slovenija, resen strokovni izziv. S tem se prekinja tudi potrebna integriteta in neprekinjenost izgrajevanja ključnih sistemskih odgovorov na vedno nova krizna stanja v našem družbenem okolju.

Ravno tem vsebinam je v tokratni številki revije Korporativna varnost namenjena ustrezna strateška pozornost. Skozi izbrane intervjuje imamo možnost slišati tako strateški nivo odločevalcev, ki upravljajo pomembne nacionalne organizacije, kakor tudi strokovnjake, ki neposredno izvajajo svoje aktivnosti v okviru procesa korporativne varnosti. Poseben del namenjamo tudi glavnemu nacionalnemu koordinatorju za popoplavno obnovo po tragičnih poplavah, ki so prizadejale ogromno škodo prebivalcem, gospodarstvu in infrastrukturi na velikem delu Slovenije. Poleg navedenega smo želeli v tokratni številki revije vsebinsko osvetliti dovolj širok spekter ostalih strokovnih prispevkov in vsebin, ki bodo v pomoč strokovni javnosti pri iskanju potrebnih rešitev in strateške modrosti za ustrezno upravljanje varnostnih tveganj s katerimi smo dnevno soočeni. 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

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

INTERVJU
mag. Senad Jušić, Generalni direktor Policije

SLOVENSKA POLICIJA SOOČENA Z VEDNO VEČJO KOMPLEKSNOSTJO VARNOSTNEGA OKOLJA

Varnostno okolje postaja vedno bolj kompleksno, kar tudi od organov nacionalne varnosti zahteva ustrezno dinamiko prilagajanja na nove izzive. Slovenska policija smelo koraka po poti učinkovitega prilagajanja vsem varnostnim izzivom, ki stojijo pred našo družbeno skupnostjo. O glavnih izzivih in pričakovanjih smo se pogovarjali z mag. Senadom Jušićem, ki je pred kratkim nastopil polni mandat na čelu slovenske policije.

Najprej nam dovolite, da vam čestitamo ob imenovanju na to pomembno funkcijo. Kaj so tista vodila, ki so vas pripeljala do odločitve, da prevzamete to pomembno dolžnost?

V slovenski policiji je veliko dobrega. Biti zaposlen v policiji je odgovornost in čast. Odgovornost do ljudi, s katerimi delamo, do ljudi, katerim pomagamo in do države, kateri služimo. Nositi policijsko uniformo in značko kriminalistične policije je čast, saj je to simbol državnosti. V svoji, več kot 32 let dolgi policijski karieri, sem predan temu zavedanju. To so tista vodila, ki me prevevajo z navdihom in ambicioznostjo, da smo lahko še bolj uspešni in učinkoviti pri uresničevanju poslanstva slovenske policije.

Kako vidite nadaljnji razvoj Policije v teh zahtevnih gospodarskih in družbenih okoliščinah?

Naj uvodoma izpostavim, da slovenska policija dobro opravlja svoje naloge. Zagotavlja visoko stopnjo varnosti vsem prebivalkam in prebivalcem Slovenije. Zato se moram v prvi vrsti zahvaliti vsem policistkam in policistom ter ostalim zaposlenim, ki vsakodnevno predano delajo, da vsi mi lahko varno živimo. To je nenazadnje tudi poslanstvo policije - da dela za ljudi in tako mora biti tudi v prihodnje. Moja naloga pa je, da poskrbim, da bodo policisti imeli vse potrebno, da bodo lahko to uspešno izvajali še naprej.

Osnova je vsekakor vzpostaviti ustrezen karierni sistem, ki je ena izmed mojih prioritet.

Policija je namreč z vidika upravljanja s človeškimi viri, karier-nega in plačnega sistema, vpeta v enotni javno uslužbenski sistem ter plačni sistem javnega sektorja. Javno uslužbenski normativni okvir premeščanja kadra, ocenjevanja, napredo-

Zaradi drugačnih vrednot in prioritet mlajših generacij prepoznavamo tudi izziv zadrževanja kadra. Predvsem se to odraža v obdobjih gospodarske rasti, ko trg delovne sile nudi večje možnosti zaposlovanja v drugih, predvsem gospodarskih panogah.

*avtor je član Slovenskega združenja korporativne varnosti

vanja, nagrajevanja ter plačne ureditve ne zasledujejo v zadostni meri potreb hierarhičnega sistema v Policiji.

Zaradi različnih parcialnih posegov v določene skupine delovnih mest, ki so nastali kot posledica sklepanja stavkovnih sporazumov, so se hkrati pojavila vse večja plačna nesorazmerja in anomalije pri prehajanju na zahtevnejša delovna mesta (npr. izgube plačnih razredov pri premeščanju na zahtevnejša delovna mesta, enako ali nižje plačilo na delovnih mestih z zahtevnejšimi nalogami, itd.). Slednje povzroča izjemno nestimulativno delovno okolje za izbor izkušenega kadra za zasedbo zahtevnejših delovnih mest. To je bil povod, da je bila v letu 2016 ustanovljena Delovna skupina za pripravo izhodišč kariernega sistema v Policiji, ter v letu 2019 Delovna skupina za pripravo predloga kariernega sistema Policije. Ugotovitve navedenih delovnih skupin so bile izhodišče za delo Delovne skupine za vzpostavitev kariernega sistema v Policiji v 2023, ki je vodstvu Policije in Ministrstva za notranje zadeve, podala predlog umestitve kariernih delovnih mest policistov ter določenih sprememb in dopolnitev javno uslužbenske zakonodaje in zakonodaje plačnega sistema. Predlagane spremembe zakonodaje bi lahko bile ustrezna podlaga za nadaljnje urejanje kariernega sistema v policiji.

Kako med mladimi zagotoviti ustrezno zanimanje za poklic policista?

V policiji se zadnjih pet let močno angažiramo z različnimi aktivnostmi promocije poklica policist in zaposlitvenih možnosti. Leta 2018 smo ustanovili posebno delovno skupino za promocijo zaposlovanja. Na podlagi treh izvedenih raziskav smo pripravili Strategijo promocije policijskega poklica 2023–2025, v kateri smo opredelili ciljno populacijo, ključne motivacijske dejavnike in način izvajanja promocije. Na podlagi strategije smo izvedli usposabljanje 22 policistov - promotorjev iz različnih policijskih uprav, kateri bodo izvajali promocijo poklica policista na regionalnem nivoju v srednjih šolah, kariernih sejmih, med prazniki in na drugih sejemskih dogodkih.

Poleg promocije v živo pa smo močno okrepili tudi promocijo zaposlovanja in predstavitve Policije na socialnih omrežjih (Facebook (Meta), Instagram, Tik Tok, platforma X).

Poleg izziva pomlajevanja kadra, se soočamo tudi z izzivom motivacije zaposlenih za prevzemanje zahtevnejših in vodstvenih nalog. Veljavna javno uslužbenska ureditev ter zakonodaja in plačni sistem, s prepoznanimi anomalijami, demotivacijsko vpliva na vodenje karierne poti v hierarhičnih organizacijah, kot je Policija.

Zaradi drugačnih vrednot in prioritet mlajših generacij prepoznavamo tudi izziv zadrževanja kadra. Predvsem se to odraža v obdobjih gospodarske rasti, ko trg delovne sile nudi večje možnosti zaposlovanja v drugih, predvsem gospodarskih panogah.

Opremljenost policije ne sledi potrebam realnega okolja in tempu, ki bi si ga verjetno vsi želeli. Kaj lahko naredite na področju opremljanja in s tem dvigovanja učinkovitosti dela Policije?

Oprema policistov za varno opravljanje nalog je ena mojih ključnih prioritet. Slovenski policisti so danes dobro opremljeni, imajo ustrezno zaščitno opremo, ustrezna vozila in tako mora biti tudi v prihodnje.

Druga plat pa je, da živimo v času visokega tehnološkega napredka. Zagotovo drži star pregovor, da so kriminalci vedno korak pred nami. Menim, da so naši kriminalisti sicer dobro usposobljeni za pregon vseh vrst kriminalitete, prav tako je po mojem mnenju ustrezna tudi zakonodaja, ki mogoče potrebuje zgolj nekaj »kozmetičnih popravkov« v smislu sledenja času in napredku tehnologij.

Izobraževanje in usposabljanje verjetno tudi naprej ostaja ključna komponenta vložkov v kadrovski potencial Policije. Kakšni so vaši načrti na tem področju?

Kot že rečeno, moramo v prvi vrsti zagotovi stabilen sistem zaposlovanja novih policistov, kjer bomo naš napor usmerjali v kvalitetno promocijo poklica in nagovarjanje mladih za vpis na Višjo policijsko šolo. V letošnjem letu smo prvič izvedli tudi drugi vpisni rok za kandidate VPŠ, ki je pokazal, da je bila odločitev pravilna, saj smo sprejeli več kot 30 novih študentov na VPŠ. S to prakso bomo nadaljevali tudi v prihodnje. Poklic policista želimo približati mlajšim generacijam in s tem okrepiti policijske postaje, ki so žal prepogosto kadrovsko podhranjene.

Po vstopu Republike Hrvaške v schengensko območje smo vsem policistom nadzornikom državne meje ponudili možnost vpisa v izredni študij na Višji policijski šoli, s čimer bodo lahko tudi v bodoče opravljali dela in naloge na območnih policijskih postajah v notranjosti.

Skladno s filozofijo vseživljenjskega učenja namenjamo velik poudarek tudi nenehnemu usposabljanju in izpopolnjevanju policistov, saj so nova znanja ključ za strokovno in profesionalno opravljanje nalog policije. Pri usposabljanjih bomo še naprej posebno pozornost namenili področju medvrstniškega nasilja, nasilja v družini, uporabi policijskih pooblastil in delu v večetničnih skupnostih. Prav tako bomo razvijali sodelovanje z evropskimi institucijami za izpopolnjevanje in usposabljanje ter se aktivno vključevali v njihove projekte.

Novost na področju usposabljanja je usposabljanje kandidatov za varovanje objektov, katere varuje policija, kjer smo v letošnjem letu pričeli z usposabljanjem že 2. generacije kandidatov.

Policistom bomo tudi v prihodnje omogočali izobraževanja v zunanjih institucijah, kjer pridobivajo specifična znanja za opravljanje policijskih nalog.

Menite, da združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti, lahko predstavlja odgovor na obvladovanje zahtevne varnostne situacije in ali so lahko taka združenja ustrezen partner Policiji pri zagotavljanju njenega osnovnega poslanstva?

Združevanje različnih družbenih skupin, kot na primer Združenje korporativne varnosti, lahko pripomore k obvladovanju varnostne situacije. Učinkoviti bomo le ob sodelovanju Policije, organizacij za zagotavljanje varnosti in gospodarskih družb. Cilj vseh deležnikov mora biti zagotavljanje varnosti v družbi, kot celoti. Izmenjava izkušenj in informacij, predvsem specifičnih znanj o varnostnih tveganjih v poslovnih okoljih, zagotovo prispeva k boljšemu razumevanju in obvladovanju teh tveganj. Kot primer lahko izpostavimo, da je za hiter odziv ob naravnih nesrečah najbolj pomembno usklajeno delovanje vseh deležnikov, tudi gospodarskih družb.

Izmenjava izkušenj in informacij, predvsem specifičnih znanj o varnostnih tveganjih v poslovnih okoljih, zagotovo prispeva k boljšemu razumevanju in obvladovanju teh tveganj.

Prehod kadra iz Policije v strukture korporativne varnosti je postala ena izmed pomembnih relacij med obema strukturama. Menite, da taki procesi vezi med obema sistemoma še dodatno krepijo?

Zaposleni v policiji se dobro zavedajo, da je sodelovanje mogoče le v skladu z zakonskimi okviri in spoštovanjem človekovih pravic. Ocenjujemo, da prehod kadra iz Policije v strukture korporativne varnosti, prinaša številne prednosti in krepi vezi med obema sistemoma. Najpomembnejši je zagotovo prenos pridobljenih strokovnih znanj iz policije v gospodarstvo, in sicer preiskovanje, analiza tveganj, izkušnje z upravljanjem kriznih situacij, komunikacijske veščine, ipd. Ne glede na navedeno, se je potrebno zavedati, da obstajajo tudi določeni etični in pravni vidiki na katere v policiji opozarjamo, zlasti glede varstva podatkov in občutljivih informacij.

Kako gledate na potrebo po prenosu različnih znanj med obema strukturama?

V kolikor je prenos znanj izveden pravilno, lahko prinese številne prednosti. Tako za policijo kot tudi za gospodarstvo je namreč poznavanje tveganj in pripravljenost na varnostne izzive izrednega pomena. Skupaj lahko sodelujemo tudi v zakonodajnih postopkih in pripravi drugih predpisov. Gospodarstvo zagotavlja tudi tehnologijo, ki jo policija uporablja. Samo gospodarske družbe, ki razumejo specifična področja policijskega dela, lahko to prenesejo v razvojne in prodajne procese. V policiji in gospodarstvu poteka stalno izobraževanje in usposabljanje, Slovenija kot majhna država pa mora čim bolj izkoristiti svoje potenciale.

Zaščita kritične infrastrukture je proces, kjer je potrebno sodelovanje vseh pooblaščenih deležnikov. Kako na tem področju ocenjujete sodelovanje med policisti in strokovnjaki na področju korporativne varnosti v organizacijah?

Sodelovanje ocenjujemo kot dobro. Čeprav gre za kompleksne sisteme, izmenjava informacij poteka v smeri preprečevanja incidentov in zagotavljanja varnosti. Ob tej priložnosti bi rad izpostavil pomembnost strokovnjakov na področju korporativne varnosti za izdelavo načrtov zaščite in varnostnih postopkov ter za izvajanje skupnih vaj. Pomembno je, da se vsi deležniki zavedamo svojih pristojnosti in odgovornosti. Poslovna kultura lahko pomembno vpliva tudi na število prijav korupcije in drugih kaznivih dejanj, povezanih z gospodarstvom.

Družbeno stanje na področju dojemanja varnosti v Sloveniji ni na ustreznem nivoju. Kako to varnostno kulturo in zavedanje, tako pri posameznikih, kakor tudi pri vodilnih strukturah organizacij javnega in zasebnega okolja, dvigniti na ustreznejši nivo?

Slovenija je varna država, ena varnejših v Evropi in svetu. Kolegice in kolegi iz dneva v dan s predanostjo opravljajo svojo službo. To zagotovo vpliva tudi na zavedanje, kako pomembna je varnost, ki se večini zdi samoumevna. Na policiji se tega zavedamo, zato ob vsakem zaznanem odklonskem pojavu, ki bi lahko vplival na varnostno situacijo, obveščamo širšo in strokovno javnost o samem pojavu, morebitnih posledicah ter ukrepih za preprečevanje nastajanja posledic, ki bi zmanjševali varnost.

Vprašanje pa je, kako smo kot družba pripravljeni na določene varnostne izzive, kot so npr. kibernetski napadi, kjer bomo le z ustreznim vlaganjem v tehnološki razvoj in potrebno znanje lahko odvrnili te grožnje. Pri tem seveda pričakujemo tudi podporo zasebnega sektorja in ostalih deležnikov.

Nelegalne migracije so med drugim postale resen varnostni izziv, s katerim se sooča slovenska policija. Kako se boste organizirali za obvladovanje tega varnostnega problema, ko vidimo, da Republika Hrvaška zelo težko zagotavlja varovanje svoje zunanje schengenske meje?

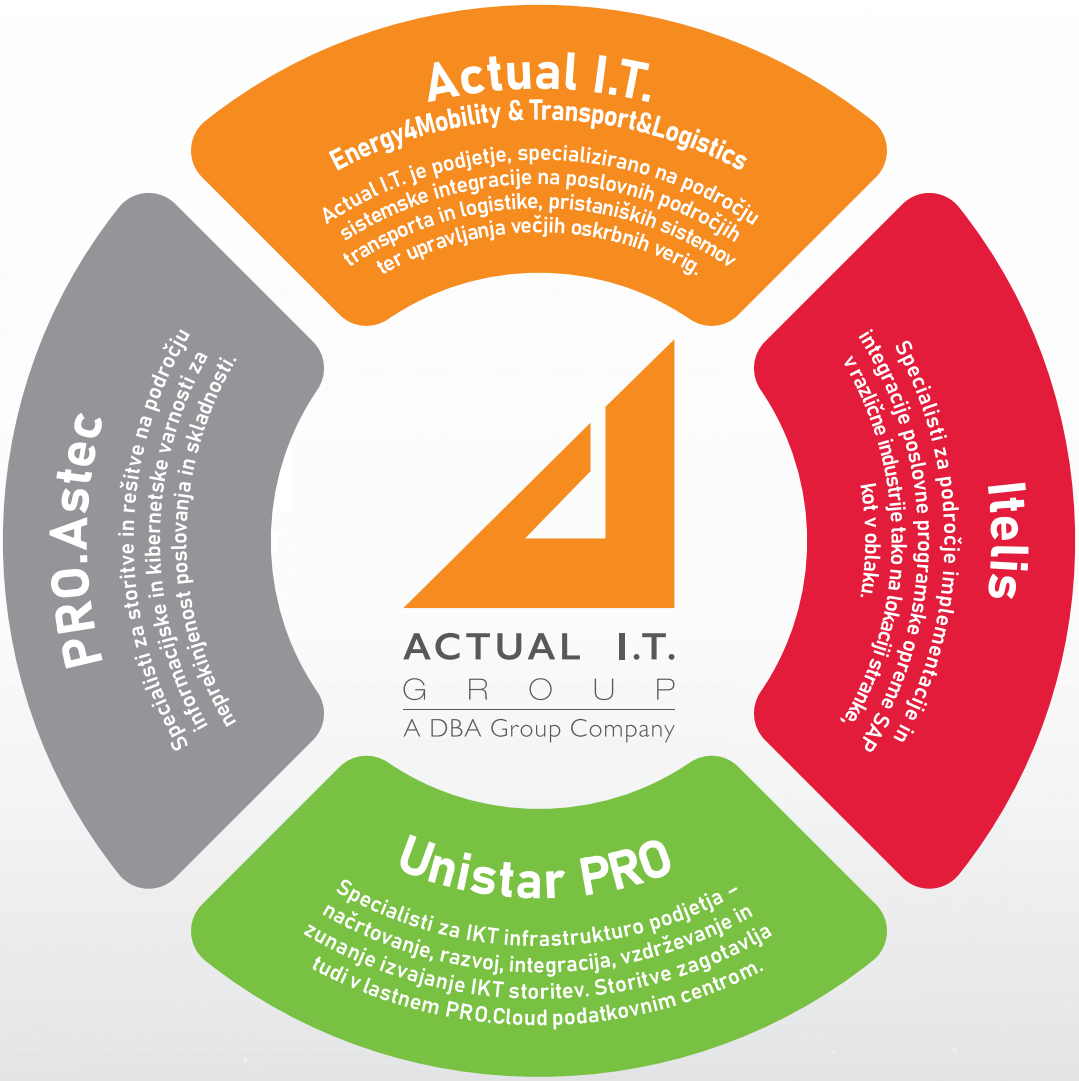
Uvodoma naj pojasnim, da je sodelovanje med slovensko in hrvaško policijo že tradicionalno dobro. Ravno v preteklih dneh sva imela v Brežicah z ravnateljem hrvaške policije, gospodom Nikolo Milino, srečanje na to temo. Dogovorila sva se, da bosta policiji nadaljevali z okrepljenim sodelovanjem v okviru mešanih patrulj in drugih skupnih aktivnosti, pri čemer si na regionalni in lokalni ravni dnevno izmenjujemo operativne podatke in se tudi dnevno usklajujemo glede na časovne in krajevne zgostitve problematike, ter na podlagi tega nato načrtujemo poostrene nadzore. S tem bomo zagotavljali še bolj optimalno razporeditev mešanih patrulj. Prav tako smo se dogovorili, da se bodo v aktivnosti vključili tudi kriminalisti z namenom odkrivanja in preiskovanja kaznivih dejanj tihotapljenja oseb. Za uspešno upravljanje migracij pa bomo uporabili vsa tehnična sredstva, ki jih imata policiji obeh držav na voljo.

Dejstvo je, da je schengensko območje velik dosežek, ki ga je treba ohraniti. Vendar pa za njegovo normalno delovanje in celostno upravljanje z migracijami potrebujemo dobro varovane zunanje meje EU, zato sem hrvaškega kolega pozval k dodatni okrepitvi nadzora na zunanji schengenski meji oziroma zunanji meji Evropske unije, saj bi to nedvomno prispevalo k zmanjšanju sekundarnih migracij in nedovoljenih vstopov v Slovenijo. Na tem mestu bi posebej rad izpostavil, da je odgovornost za učinkovito upravljanje migracij dolžnost vseh držav na zahodno balkanski poti. Naša dolžnost je, da jim pri tem pomagamo in nudimo ustrezno pomoč ter podporo.

Nenazadnje pa slovenska policija uspešno izvaja vse potrebne ukrepe za preprečevanje, odkrivanje in preiskovanje nezakonitih migracij, med katerimi je tudi odkrivanje organiziranih hudodelskih združb, ki se ukvarjajo s tihotapljenjem ljudi. Letos je policija do 4. oktobra 2023 obravnavala 260 primerov (v enakem obdobju lani 148), v katerih je bilo prijetih 291 tihotapcev ljudi (od tega 283 tujcev in 8 slovenskih državljanov) s 1730 migranti. Za 261 tihotapcev je bil odrejen pripor. ■

Foto: arhiv Policije

Ob tej priložnosti bi rad izpostavil pomembnost strokovnjakov na področju korporativne varnosti za izdelavo načrtov zaščite in varnostnih postopkov ter za izvajanje skupnih vaj. Pomembno je, da se vsi deležniki zavedamo svojih pristojnosti in odgovornosti.



ACTUAL I.T. astec ITELIS UNISTAR PRO

IT360°

www.actual-it.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Boštjan Šefic, vodja Službe Vlade Republike Slovenije za obnovo po poplavah in plazovih*

NARAVNE NESREČE SO POSTALA REALNA STALNICA SODOBNEGA SVETA

Tudi Republika Slovenija ni imuna na pojav naravnih nesreč z vsemi posledicami, ki jih le te prinašajo. V zadnjem obdobju si negativni vplivi narave sledijo v zelo kratkih časovnih intervalih. Zaradi navedenega je proces odpravljanja posledic postal velik izziv s katerim se sooča celotna družba. O ključnih korakih pri zahtevni obnovi po nedavnih tragičnih poplavah smo se pogovarjali z g. Boštjanom Šeficem.

Pred nedavnim je Slovenijo prizadela verjetno največja naravna nesreča v vsej njeni zgodovini. Najprej nam dovolite, da vam še enkrat čestitamo ob imenovanju na to pomembno koordinacijsko dolžnost in vam zaželimo čim več modrosti in uspeha. Nam lahko na kratko opišete vaše zadolžitve in pristojnosti na dolžnosti Vladnega koordinatorja za obnovo po poplavah.

Hvala za čestitke. Sam in celotna ekipa bomo res potrebovali veliko energije in predvsem potrpežljivosti pri iskanju optimalnih rešitev, da pridemo do zastavljenih ciljev. To je na eni strani čim prej in čim bolj učinkovito pomagati ljudem, na drugi strani zagotoviti celovito obnovo vsega, kar je bilo uničeno, ter vzpostaviti pogoje za nov/nadaljnji razvoj vseh prizadetih regij. Predvsem pa, samo skupno delo vseh ministrstev, različnih državnih organov, županov in njihovih ekip ter vseh ostalih, ki lahko kakorkoli pripomorejo k doseganju zastavljenih ciljev, lahko pripelje do njihove realizacije. Pri tej nalogi res pričakujem enotnost in pozitivno energijo. Sem optimist in hkrati realno gledam na razmere, zato vem, da to ne bo lahko. Sam bom naredil vse, da k temu kar najbolj pripomorem. Moja naloga državn ega sekretarja oziroma vodje Službe Vlade RS za obnovo po poplavah in plazovih je v prvi vrsti usmerjanje, spremljanje izvajanja obnove ter zagotovitev usklajenega delovanja vseh, ki so vključeni v ta proces. V okviru službe deluje tudi Državna tehnična pisarna, ki bo pregledala vse objekte in svetovala, pripravljala projekte, pomagala pri pridobivanju dovoljenj in zagotavljanju finančne konstrukcije, izvajala projekte, če bodo investitorji tako želeli, izvajala nadzor in druge naloge. V okvir službe sodi neposredna pomoč ljudem, zlasti na področju brezplačne pravne pomoči, psihosocialne pomoči, skrb za starejše in ranljive skupine ter vrsta drugih nalog.

Vsa ministrstva in občine ohranjajo svoje pristojnosti in predvsem odgovornosti. Izpostavljam predvsem slednje. Tisto, kar je pomembno, je skupno delovanje v korist ljudi in skupnosti.

Že v preteklosti ste imeli pred seboj pomembne izzive in zadolžitve, naj spomnimo samo situacijo z velikim migrantskim valom pred nekaj leti. Vendar se da čutiti, da je ta koordinacijska funkcija še za odtenek bolj zahtevna. Kako jo vi osebno dojemate?

Vse dosedanje naloge, od reševanja razmer v KIK Kamnik, ki je bil v stečaju in smo morali odstraniti ogromno količino eksplozivnih in nevarnih snovi do mi-

*intervjuvanec je član Slovenskega združenja korporativne varnosti

gracij, so bile zahtevne naloge, vendar je sedanja daleč najbolj kompleksna, zahtevna in težavna. Na eni strani so ljudje, ki so bili hudo prizadeti v tej naravni nesreči in se srečujejo z različnimi stiskami, na drugi strani pa ogromno uničene infrastrukture in domov. Vse bo potrebno sanirati in obnoviti.

Zagotoviti moramo pogoje za maksimalno učinkovito delovanje vseh državnih podsistemov. Pri tem se srečujemo z nekaterimi, ki so bili v preteklih letih in desetletjih zapostavljeni, tako finančno kot kadrovsko. Pri drugih je razumevanje razmer podcenjeno, na tretji strani pa se srečujemo s parcialnimi interesi. Vse skupaj terja enormno količino razumevanja, pozitivne naravnanosti, energije in vztrajnosti. Sem pa prepričan, da bo v tem času potrebno kakšno področje reformirati zato, da bo lahko učinkoviteje delovalo.

Čeprav so vse oči uprte v vas, kot osrednjo koordinacijsko figuro za poplavne sanacije, je potrebno verjetno poudariti, da resorna ministrstva in tudi lokalne oblasti ne bodo mogle pobegniti od svoje domače naloge, ki jo bo potrebno pri tej sanaciji opraviti na različnih nivojih? Kaj so vaša glavna sporočila glede tega?

Vsa ministrstva in občine ohranjajo svoje pristojnosti in predvsem odgovornosti. Izpostavljam predvsem slednje. Tisto, kar je pomembno, je skupno delovanje v korist ljudi in skupnosti. Torej, usmerjenost k že omenjenim skupnim ciljem. To hkrati pomeni, da na področjih, kjer se nam pristojnosti in naloge stikajo, delo opravimo usklajeno. Pomembno bo tudi skupno določanje prioritet na posameznih področjih. To zahteva premišljen pristop, konstruktiven pogovor o odprtih problemih in izzivih. Nujno bo v ozadje postaviti posamične interese ter razumeti, da tako obsežna sanacija na tako velikem območju ne more potekati brez skupnega dela, medsebojnega poslušanja in slišanja.

Menite, da bo največji izziv uskladiti ravno državne in lokalne interese ne samo pri sanaciji temveč tudi pri dojemanju potrebe po resnejšem načrtovanju bodočih prostorskih načrtov za širjenje strnjenih naselij?

To ni nikoli enostavno. Pri nobenem vprašanju. Sedaj se bo izkazalo, koliko smo sposobni pogledati čez lastne plotove tako na državni kot lokalni ravni. Pokazala se bo sposobnost delovati za interes ljudi in skupnosti, bodisi lokalnih, bodisi širših državnih. Že samo urejanje vodotokov, ki zahteva celovit pristop k sanaciji in bistvenem zmanjševanju tveganj za ljudi in njihovo premoženje, bo terjalo ukrepe, kjer bo potrebno postaviti v ospredje interes skupnosti pred osebnimi interesi ter interese posamezne lokalne skupnosti pred interese širšega območja ali več drugih lokalnih skupnosti.

Na državni ravni bo potrebno stremeti k boljšemu sodelovanju resorjev in iskanju soglasja o optimalnih rešitvah. Celo v sedanjih razmerah se srečujemo s tem, da se posamezen problem prenaša iz resorja na resor. To ni sprejemljivo. Res pa je, da smo uspeli manjši premik že narediti, absolutno pa ni zadosten.

Menite, da je danes znanje in tehnologija že na tem nivoju, da bi se take dogodke lahko v naprej predvidelo?

Znanost in tehnologija sta naredili izjemen napredek. Pri napovedovanju sta na marsikaterem področju zelo uspešni. Ne nazadnje, izjemen vremenski pojav, s katerim smo se srečali, je bil pravočasno napovedan. Tokrat so se vremenoslovci izkazali. Opozorila so bila pravočasna. Dejstvo je tudi, da so naši strokovnjaki s svojimi poplavnimi kartami zelo dobro, vsaj na nekaterih območjih, napovedali možnost velikih poplav. Vprašanje je, zakaj se je ponekod dovolilo graditi, navkljub velikim tveganjem.

Tehnologija se intenzivno razvija, vendar so tudi dogajanja vedno bolj ekstre-

mna. Zato je nujno, da uvajamo čim več novega znanja in tehnologije v spremljanje vseh potencialnih groženj. Oboje moramo intenzivneje vpeljati v naše vsakdanje delo. Ni skrivnost, da na nekaterih področjih ne sledimo zadnjim standardom. Seveda pa imamo tudi izjemne posameznike, time in organizacije, ki se zavedajo pomena znanja in tehnološkega napredka, zato v to ogromno vlagajo.

Prepričan sem, da nam bodo podnebne spremembe prinašale nove ekstreme. Zato bo potrebno poslušati znanost, resno pristopiti k predlaganim rešitvam v smeri pravočasnih priprav in večanja odpornosti na vseh področjih, od umeščanja v prostor kot načina gradnje in boljšega usklajevanja našega življenja z naravo. Investiranje v ljudi, znanje in tehnologijo je ključnega pomena, pomembnost pa se bo še stopnjevala.

Med poplavami se je ponovno pokazala potreba po neprekinjenem delovanju ključne kritične infrastrukture in tudi ključnih državnih organov. Po izjavah udeleženih v poplavah in medijskih informacijah je bilo kar nekaj izzivov pri zagotavljanju osnovnih procesov in dobrin, kot so elektrika, pitna voda in telekomunikacijske storitve. Kakšna je vaša ocena varnostnega strokovnjaka in ali menite, da so bili ključni deležniki na tem področju dobro pripravljeni?

Zagotavljanje neprekinjenega delovanja kritične infrastrukture je vedno ključnega pomena za delovanje celotne družbe. Zato je nujno ves čas analizirati in preigravati različne scenarije, v katerih bi se lahko znašli. Ti scenariji morajo biti vedno bolj zahtevni, saj se tudi okoliščine spreminjajo in zaostrujejo. Torej, stalno usposabljanje in nadgrajevanje v smeri neprekinjenega delovanja.

Zagotavljanje neprekinjenega delovanja kritične infrastrukture je vedno ključnega pomena za delovanje celotne družbe. Zato je nujno ves čas analizirati in preigravati različne scenarije, v katerih bi se lahko znašli.

Zadnja naravna nesreča je bila huda in narava je pokazala svojo moč. Uničene je bilo veliko infrastrukture. V obnovi bo potrebno povečati odpornost na vseh navedenih področjih. V takšnih in morda še hujših naravnih pojavih seveda ni mogoče zagotoviti, da škoda ne bi nastala oziroma, da posledic ne bi bilo. Marsikje pa bi lahko bile manjše.

Odziv na nesrečo pa je bil, po moji oceni, dober in hiter. Upoštevajoč vse okoliščine je bila razmeroma hitro vzpostavljena oskrba z vodo, elektriko in telekomunikacijskimi storitvami. Ostajajo posamezna območja, kjer se morajo zgraditi novi odseki vodovodov, imamo območja, ki imajo še vedno slabo pokritost na področju telekomunikacij ali oskrbe s plinom. Vse navedene težave se morajo v mesecu oktobru odpraviti.

Civilna zaščita je ena od stalnic odzivnega sistema, ko govorimo o obvladovanju naravnih nesreč, ki so se začele pogosteje pojavljati, kot smo bili navajeni v preteklosti. Menite, da so pri njeni organizaciji in delovanju še možne izboljšave predvsem pri usklajevanju lokalnega in državnega nivoja delovanja?

Imamo dober sistem. Po njegovi zaslugi in zaslugi predanih pripadnikov, od

gasilcev, jamarjev, gorskih reševalcev, Slovenske vojske, policije, nujne medicinske pomoči in vseh ostalih, ne bi takšne nesreče obvladali praktično brez neposrednih žrtev. To moramo poudariti in ceniti. V tujini so zaradi tega dejstva impresionirani.

Ne le zaradi pogostosti, temveč predvsem zaradi obsežnosti in zahtevnosti bo potrebno resno analizirati zadnje večje naravne nesreče in identificirati slabosti odzivnega sistema, ter jih z ustreznimi ukrepi odpraviti. Pri tem imam v mislih organizacijo in vodenje. Občinski štabi, zlasti v nekaterih občinah, so preprosto kadrovsko prešibki za vse naloge, ki jih morajo opraviti ob takšnih nesrečah, nimajo zadostne strokovne podpore in vzdržljivosti za obvladovanje razmer v daljšem obdobju. Zato bi veljalo razmisliti o krepitvi regijskih štabov, morda narediti nekatere spremembe glede regij in jih uskladiti z regijami nekaterih drugih podsistemov. Seveda je to stvar resnega premisleka.

Večkrat sem izpostavil svoje prepričanje, ki temelji ne le na teoretičnih razmišljanjih pač pa praktičnih izkušnjah, da bi moral sistem zaščite in reševanja imeti samostojno vlogo in položaj znotraj nacionalno-varnostnega sistema s položajem samostojne agencije, ki bi bila neposredno vezana na Vlado, oziroma predsednika vlade, kot je to v primeru Slovenske obveščevalno-varnostne agencije. Tudi umeščenost poveljnika Civilne zaščite sodi bližje Vladi.

Moje prepričanje je, da je potrebno o vsem dobro premisliti in narediti načrt preoblikovanja, ki bi bil izveden po fazah, saj tako pomemben sistem ne smemo destabilizirati s hitrimi reformami. Zmanjšanje njegove učinkovitosti bi bil lahko v marsičem nevarno za zagotavljanje naše varnosti.

Poplavljeno je bilo tudi veliko število gospodarskih objektov. Menite, da je gospodarstvo namenjalo področju zagotavljanja neprekinjenosti poslovanja dovolj veliko pozornosti? V zadnjem obdobju smo imeli občutek, da se je več pozornosti polagalo na informacijsko področje manj pa na zagotavljanje delovanja v okviru bazičnih naravnih nesreč. Kakšna je vaša ocena?

Vsa področja so pomembna. Informacijsko področje, digitalizacija in varnost informacijskih sistemov so ključni za delovanje podjetij.

Imamo dober sistem. Po njegovi zaslugi in zaslugi predanih pripadnikov, od gasilcev, jamarjev, gorskih reševalcev, Slovenske vojske, policije, nujne medicinske pomoči in vseh ostalih, ne bi takšne nesreče obvladali praktično brez neposrednih žrtev. To moramo poudariti in ceniti. V tujini so zaradi tega dejstva impresionirani.

Izkazalo se je, da so tudi v gospodarstvu podcenili nekatera tveganja, med njimi tudi poplavno ogroženost. Posamezna podjetja se nahajajo ob vodotokih, ki že nepoučenemu opazovalcu dvignejo obrvi. Razlogov za to je verjetno več. Gre za razpoložljivost zemljišč, interese glede zaposlovanja in razvoja posameznih krajev in regij ter druge dejavnike, ki so pomembni za posamezne investicije ter doseganje profitabilnosti. Verjamem, da smo se ob tej hudi preizkušnji naučili, da moramo v prihodnje upoštevati tudi ostale dejavnike in tveganja. V sedanjih razmerah bomo morali predvsem ukrepati v smeri večje zaščite teh objektov pri čemer bodo morali sodelovati tako gospodarstvo in posamezni gospodarski subjekti kot lokalne in državne oblasti. Pogled nazaj je pomemben predvsem s stališča, da iz te in drugih nesreč naredimo ustrezne zaključke in se česa naučimo. Pri nadaljnjem delu pa moramo te izkušnje upoštevati in ustrezno ukrepati.

Potrebno se je dotakniti graditve sistema za zgodnje alarmiranje in obveščanje s katerim v Sloveniji zamujamo. Ravno pravočasno alarmiranje in obveščanje v takih razmerah ključno prispeva k zmanjšanju števila človeških žrtev in posledično tudi materialne škode. Menite, da bo nedavna nesreča dala še dodatni potisk odgovornim, da ta sistem čimprej implementirajo v operativno uporabo?

Tu ni dileme. Mora biti. Z vašo ugotovitvijo se namreč strinjam. To velja za vse potencialne naravne in druge nesreče. Poseben pomen ima to pri plazovih. Kakovosten nadzor nekaterih plazov je ključen za pravočasno ukrepanje. Trenutno nam grozi veliko res velikih plazov, ki lahko neposredno ali posredno ogrozijo ljudi in njihovo premoženje ter povzročijo enormne posledice. Zato je vzpostavitev njihovega nadzora in pravočasno alarmiranje izjemnega pomena.

Vsaka investicija v tej smeri se povrne z neskončno vrednostjo. Vsako življenje, ki se reši na ta način, je vredno več kot sredstva, ki jih vlagamo v ta sistem. Vsaka preprečitev ali zmanjšanje nastanka škode je zelo hitro povrnjena. Razumeti moramo, da vlaganje v to ni strošek, je najboljša zavarovalna polica ob naravnih nesrečah. Skupaj s predanimi ljudmi v sistemu zaščite in reševanja predstavlja zagotovilo, da bomo ob prihodnjih ekstremnih dogodkih imeli še boljše rezultate.

Za konec, ali lahko strokovna združenja kot je Slovensko združenje za korporativno varnost tvorno pomaga pri dvigovanju zavedanja o potrebnih sistemskih korakih zagotavljanja neprekinjenosti delovanja ključnih infrastrukturnih in procesnih aktivnosti za boljše obvladovanje varnostnih tveganj, ki jih med drugim prinaša narava skozi naravne ujme?

Pred časom ste mi v drugem kontekstu postavili podobno vprašanje. Tudi tokrat poudarjam, vsak lahko v skladu s svojim poslanstvom in znanjem pripomore k ozaveščanju pomembnosti preventivnih ukrepov za zmanjšanje tveganj v primeru naravnih nesreč. V prihodnosti bo to še pomembneje. Slovensko združenje za korporativno varnost ima v prvi vrsti to vlogo v gospodarstvu. Lahko je pomemben spodbujevalec tudi pri iskanju boljših strokovnih in tehničnih rešitev, ter na področju povečevanja odpornosti gospodarstva s tega zornega kota. Ekonomske rezultate lahko podjetja dosegajo le, če se jim zagotovi stabilno okolje v vseh pogledih, tudi varnostnem v najširšem pomenu. Kot novi član združenja bom predlagal, da premislimo in na tem področju oblikujemo program naših aktivnosti. Dejstvo je, da ima združenje preko svojih uglednih članov ugled in vpliv, ki ga mora izkoristiti za to, da naše gospodarstvo postane odpornejše tudi na tem področju. ■

Foto: arhiv Službe Vlade RS za obnovo po poplavah in plazovih

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

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.

GEN SKUPINA

Občina Slovenska Bistrica

Onkološki inštitut Institute of Oncology Ljubljana

Melamin

Mercator

CAA

SMART COM

URSIV

telemach

SIEMENS

NIJZ Nacionalni inštitut za javno zdravje

ELEKTRONČEK

Ministrstvo za infrastrukturo

Javni medobčinski stanovanjski sklad Maribor

GENERALI

Telekom Slovenije

Pošta Slovenije

Mestna občina Ljubljana

PETROL Energija za življenje

AKRAPOVIČ

4AIPES

interblock Luxury Gaming Products

triglav

Informacijske storitve in inženiring, d.o.o. INFORMATIKA

smartis Pametni informacijski sistemi

Elita i.b. d.o.o.

SPICA

DARS

ZARJA ELEKTRONIKA

UNISTAR PRO

NovaKBM

LON

CINKARNA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

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

KOLUMNA

SISTEM NEPREKINJENEGA DELOVANJA POSTAJA SINE-QUA NON DELOVANJA NAŠIH ORGANIZACIJ

Vpliv sodobnega varnostnega okolja je vedno močnejši in pogostejši, kar naše organizacije postavlja pred resne izzive kako organizirati varno poslovanje v svojih poslovnih okoljih. Zagotavljanje dobro delujočega sistema neprekinjenega delovanja je postala nujna komponenta, s katero se v zadnjem obdobju ukvarja, ne samo strokovni del organizacij, temveč tudi strateški management. Vodstvo organizacij si pri vodenju le teh ne more več dovoliti igranja na srečo, saj so posledice vseh negativnih vplivov okolja postale prehude in lahko pomenijo trajno prenehanje poslovanja.

Če smo bili do nedavnega navajani, da so si krize sledile v več letnih intervalih, nas okolje, v katerem delujejo naše organizacije, vsak dan opominja, da je čas tega »luksuza« na žalost minil. V zadnjih nekaj letih smo soočeni s konstantnim pojavljanjem kriznih stanj, ki so si praktično začela slediti v verižnem vrstnem redu. Da bo situacija še bolj zahtevna so se začela pojavljati tudi krizna stanja, ki smo jim še pred desetimi leti namenjali obrobno vlogo v naših ocenah ogroženosti in identifikaciji tveganj ter smo jih v večini primerov uvrščali v kategorijo dogodkov, ki sicer predstavljajo visoko tveganje, vendar so po verjetnosti praktično nemogoči. Grožnje, ki lahko do temeljev zamajajo naše organizacije, prihajajo iz celega spektra možnih vzrokov in nikakor niso omejena samo na vojne spopade, migracije, teroristična dejanja in druga dejanja kriminalne podlage. Vedno bolj smo soočeni z visokimi izzivi, ki jih prinaša okolje v obliki naravnih nesreč, katere so po svoji jakosti presegle vsa možna pričakovanja. Tukaj je potrebno omeniti tudi del, ki je vezan na tehnološke nesreče. Poleg navedenega, pa nikakor ne moremo spregledati tveganja, ki ga prinaša moderna digitalizirana družba, ki je vedno bolj odvisna od delovanja informacijsko komunikacijske teh-

V tem smo kot družba postali popolnoma odvisni od delovanja nekaterih ključnih infrastrukturnih sektorjev, kjer pa že manjši krizni vplivi resno zamajejo delovanje celotnih sistemov. Če v ta okvir vzamemo še soodvisnost in kaskadne učinke, ki jih povzročajo vplivi ene infrastrukture oz. sektorja na drugega, dobimo zares kompleksno situacijo, kjer je razumevanje procesov v naših organizacijah ključnega pomena.

*avtor je član Slovenskega združenja korporativne varnosti

nologije. Pametna mesta in druge tehnološke rešitve ne delujejo brez električne energije in podpore informacijske tehnologije. V tem smo kot družba postali popolnoma odvisni od delovanja nekaterih ključnih infrastrukturnih sektorjev, kjer pa že manjši krizni vplivi resno zamajejo delovanje celotnih sistemov. Če v ta okvir vzamemo še soodvisnost in kaskadne učinke, ki jih povzročajo vplivi ene infrastrukture oz. sektorja na drugega, dobimo zares kompleksno situacijo, kjer je razumevanje procesov v naših organizacijah ključnega pomena. Seveda se na tem mestu verjetno mnogim postavlja vprašanje zakaj je poznavanje lastnih procesov organizacije tako nujno, da zagotavljamo neprekinjenost delovanja v različnih kriznih situacijah, s katerimi smo dnevno soočeni pri našem poslovanju. Pomembno je razumeti, da ker smo vedno soočeni z omejenimi kadrovskimi, finančnimi in drugimi viri, je torej nemogoče vse procese v organizaciji smatrati kot ključne za delovanje in preživetje organizacije. Skozi ustrezno analizo moramo biti v organizaciji sposobni realno oceniti kateri so tisti procesi brez katerih podjetje ne more preživeti oz. lahko utrpi velike finančne in druge posledice. Na drugi strani pa se je potrebno zavedati, da so določeni procesi taki, da se lahko v kriznih situacijah, za določeno časovno obdobje, v svoji intenziteti nekoliko zmanjšajo ali pa v celoti začasno zaustavijo. To nam omogoča, da lahko organizacije nujno potrebne vire in energijo usmerijo v obvladovanje negativnih učinkov, ki jih v tistem trenutku prinaša kritična situacija ali krizno stanje, ki ima močne negativne vplive na zagotavljanje neprekinjenega poslovanja naših organizacij. Po enakem principu morajo delovati tudi nekateri državni sistemi na tistih segmentih, kjer je zaradi velikosti kriznega stanja le država tista, ki s svojimi viri zagotavlja dovolj robustnosti in sposobnosti zagotavljanja njenega poslanstva v območjih velikih kriznih stanj. Tak tipičen primer se je pojavil ob zadnjih katastrofalnih poplavah, ki smo jim bili priča v Republiki Sloveniji.

Osredotočenost pri izboljšanju obstoječega stanja začne megliti potreba po zagotavljanju fokusa v reševanje vedno novih izzivov, s katerimi so dnevno soočene posamezne organizacije. Seveda pa ima to za posledico, da sistemi neprekinjenega delovanja v organizacijah v večini primerov nikoli niso ustrezno posodobljeni, zato smo priča ponavljanju vedno novih napak.

Ali smo pri tem uspešni je težko oceniti, saj stanje v realnosti vsekakor ni črno belo. Imamo primere organizacij, ki se iz preteklih izkušenj nekaj naučijo in želijo te izkušnje preliti v izboljšanje stanja zagotavljanja sistema neprekinjenega delovanja v njihovem organizacijskem okolju. V večini primerov pa je spominski moment po negativnih vplivih kriz relativno kratek. Osredotočenost pri izboljšanju obstoječega stanja začne megliti potreba po zagotavljanju fokusa v reševanje vedno novih izzivov, s katerimi so dnevno soočene posamezne organizacije. Seveda pa ima to za posledico, da sistemi neprekinjenega delovanja v organizacijah v večini primerov nikoli niso ustrezno posodobljeni, zato smo priča ponavljanju vedno novih napak.

V vsakem primeru, pa je potrebno razumeti, da je uveljavljanje sistema neprekinjenega poslovanja izredno zahteven proces, ki ga večina organizacij ni sposobna narediti popolnoma samostojno. V tem primeru se morajo nasloniti na zunanjo ekspertno podporo.

K resnosti problema je, odločneje kot v preteklosti, pristopila tudi EU, saj skozi dve pomembni direktivi CER[1] in NIS-2[2] države članice, posredno pa tudi sektorske koordinatorje in operaterje kritične infrastrukture, potiska v smeri večjega sodelovanja, realnega načrtovanja in grajenja zmogljivosti, ki so predvsem usmerjeni v višjo stopnjo robustnosti ključnih sistemov in procesov ter s tem tudi v boljšo prožnost delovanja v času kriznih razmer. Celoten fokus se iz infrastrukturne perspektive premika na področje zagotavljanja celostnih storitev. Ključnega pomena v tem okviru bo tudi zagotavljanje ustrezne metodologije stresnih testov, ki bodo lahko z boljšo gotovostjo prikazovali realno stanje pripravljenosti vseh ključnih deležnikov za delovanje v kriznih stanjih. Ravno uveljavljanje sistema neprekinjenega poslovanja v naših organizacijskih okoljih ima pomemben del pri zagotavljanju celovitosti, prožnosti in zadostne robustnosti ključnih procesov, pa naj si gre tukaj za posamezne gospodarske organizacije, organizacije, ki so upravljalci bistvenih storitev in infrastrukture ali pa državo kot celoto, ki mora skozi svoje ključne podsisteme zagotavljati neprekinjenost delovanja širše družbene skupnosti.

Če se povrnemo na zagotavljanje neprekinjenosti delovanja naših organizacij, moramo biti sposobni na podlagi dejanske ocene, kaj je zares glavni proces v naši organizaciji, le tega pogledati skozi prizmo vplivov različnih groženj in tveganj in jih ustrezno rangirati. Tistim grožnjam in tveganjem glavnih procesov v organizaciji, pa se je potrebno v procesu zagotavljanja neprekinjenega poslovanja, skozi podrobne načrte, v katerih so zajeti vsi glavni ukrepi in viri za ustrezno upravljanje teh tveganj na tisto raven, ki še zagotavlja neprekinjenost delovanja teh procesov, ustrezno posvetiti. V okviru načrtovalnega dela je potrebno še posebej izpostaviti nekaj ključnih delov sistema neprekinjenega poslovanja in sicer jasno postavljena strategija, ki vključuje vse pomembne metodološke in operativne korake, na podlagi katerih se upravljajo vsi kritični procesi v organizaciji ter jasno določena krizna ekipa z vsemi pristojnostmi in odgovornostmi. Poseben segment v tem okviru predstavlja krizno komuniciranje, ki je v času krize eden od ključnih delov celovitega sistema zagotavljanja neprekinjenosti delovanja v naših organizacijah. V tem obsegu je potrebno zajeti krizno komuniciranje skozi celoten spekter ciljnih skupin, med katerimi nikakor ne smemo pozabiti interne javnosti, torej zaposlenih v naših organizacijah.

Za pomembno učinkovitost delovanja sistema zagotavljanja neprekinjenega poslovanja pa ima verjetno odločilen pomen ustrezna usposobljenost zaposlenih, ki se zagotavlja skozi različne oblike usposabljanj, vaj, stresnih testov in strokovnih razprav (analiz) skozi katere je potrebno zbirati dobre prakse in izkušnje. Vsak sistem je neprestano delujoči mehanizem, ki mora imeti v svojem delu jasno opredeljen korak posodabljanja pripravljenih načrtov in pristopov za upravljanje kriznih stanj in zagotavljanje neprekinjenega delovanja ključnih procesov v naših organizacijah.

Realna analiza stanja v Slovenskem gospodarstvu še vedno kaže na dejstvo, da preveč organizacij temu področju ne namenja dovolj velike pozornosti, kar za seboj prinaša vedno nove težave ob krizah, ki si sledijo. To posledično pomeni tudi slabšo prožnost in pripravljenost ter slabšo konkurenčno kondicijo na zahtevnem globalnem trgu. Del odgovornosti bodo morali na svoja ramena v prihodnje prevzeti tudi lastniki, saj je neustrezno zagotavljanje robustnosti preživetja na koncu predvsem njihov problem. Najeti strateški managerji se v zadnjem obdobju prehitro selijo iz ene organizacije v drugo, pod krinko potrebne dinamičnosti prevzemanja novih poslovnih priložnosti, kar je za sistemski pristop na tem pomembnem področju zelo problematično. Zaradi tega, v večini primerov, tudi niso popolnoma predani uveljavljanju zahtevnih procesov neprekinjenega poslovanja v svoje organizacije, saj gre za dolgotrajen in zahteven proces, ki nima kratkoročnih finančnih učinkov pri finančni uspešnosti poslovanja njihovih organizacij.

V vsakem primeru, pa je potrebno razumeti, da je uveljavljanje sistema neprekinjenega poslovanja izredno zahteven proces, ki ga večina organizacij ni sposobna narediti popolnoma samostojno. V tem primeru se morajo nasloniti na zunanjo ekspertno podporo. Na žalost pa tukaj ponovno trčimo na problem kvalitete storitev pri vpeljevanju neprekinjenega poslovanja, ki jih je možno dobiti na slovenskem tržišču. V tem delu so naročniki spet prepuščeni določeni iznajdljivosti, predvsem pa tudi sreči, da uspejo za izvedbo tega zahtevnega področja izbrati ustrezne strokovne in referenčne zunanje partnerje. Na tem področju se je kot pozitivno pokazala izmenjava izkušenj in informacij skozi določene strokovne asociacije, kjer so združene pomembne organizacije. Slovensko združenje za korporativno varnost v tem okviru vsekakor predstavlja pomemben pozitiven primer, ki ga je potrebno ustrezno izpostaviti.

Za zaključek lahko z gotovostjo ocenimo, da nas na področju uvajanja sistemov neprekinjenega delovanja naših organizacij čaka še ogromno trdega dela in potrebne motivacije. Samo razumevanje delovanja lastnih sistemov ter razumevanje soodvisnosti z ostalim okoljem, ki obdaja naše organizacije, lahko da tisto potrebno podlago, na kateri bodo v nadaljevanju izvedeni ustrezni ukrepi, viri in načrti za ustrezno obvladovanje kriznih vplivov na naše organizacije. Silosni pristopi, ki smo jih še vedno vse prevečkrat deležni, tako na državnem kakor tudi med organizacijskem nivoju, samo hromi potrebno razumevanje dejanskega stanja in prinaša nepotrebno razpršenost potrebnih virov, ki bodo v prihodnosti vedno bolj omejeni. Iskanje potrebnih sinergij, tako znotraj kakor tudi zunaj naših organizacij, mora biti ključ do rešitve. Upamo, da bo uveljavljanje zadnjih evropskih direktiv v nacionalni pravni red sledilo tej ideji iskanja sinergij in komplementarnosti pristopov v smeri skupnega naslavljanja rešitev realnih izzivov kako zagotoviti neprekinjenost delovanja ključnih segmentov. ■

1 The Critical Entities Resilience Directive (Direktiva o odpornosti kritičnih subjektov)

2 Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (direktiva o varnosti omrežij in informacij 2)

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
mag. Marko Mišmaš, direktor Agencije za komunikacijska omrežja in storitve Republike Slovenije*

NEPREKINJENOST DELOVANJA KLJUČNIH KOMUNIKACIJSKIH OMREŽIJ TUDI V PRIHODNJE POMEMBEN FOKUS DELOVANJA AKOS

Nenehen tehnološki razvoj na eni strani, na drugi strani pa vedno večja intenziteta cele vrste varnostnih izzivov, pred sektor informatike in telekomunikacij postavljata resne strokovne dileme, kako ustrojiti sistem, da bo dovolj robusten in sposoben neprekinjenega delovanja. O perečih razvojnih vidikih smo se pogovarjali z mag. Markom Mišmašem, novim direktorjem AKOS.

Najprej nam dovolite, da vam čestitamo ob imenovanju na to pomembno funkcijo. Nam lahko prosim zaupate nekaj o vaših predhodnih referencah, ki bodo vsekakor pomembne za upravljanje te odgovorne funkcije?

Najlepša hvala za čestitke! Po izobrazbi sem magister telekomunikacij, na agencijo pa prihajam iz industrije, kjer sem delal 22 let. V svoji karieri sem delal v različnih sektorjih; telekomunikacijah, energetiki in avtomobilski industriji na različnih vodstvenih funkcijah v razvoju in prodaji. Skupno vsem trem je ime Iskra; Iskratel, Iskraemeco in Iskra Mehanizmi. Agencijo pa poznam zelo dobro, saj sem bil zadnja dva mandata tudi član Sveta agencije, ki predstavlja njen nadzorni organ.

Strateški varnostni izzivi, pred katerimi stoji Slovenija kot del mednarodnega okolja, bodo imeli pomemben vpliv na delovanje AKOS-a. Kje pričakujete največje izzive, ki sledijo področjem, ki jih upravljate v vaši agenciji?

Z uveljavitvijo oz. implementacijo NIS 2 se na področju zagotavljanja varnosti za nekatere sektorje, ki so tudi v pristojnosti agencije, obetajo kar precejšnje spremembe. Kot konvergentni regulator in še zlasti regulator in nadzorni

> Kot konvergentni regulator in še zlasti regulator in nadzorni organ za varnost sektorja elektronskih komunikacij, ki so ključne za zagotavljanje številnih ostalih storitev kritične infrastrukture, čutimo na tem področju veliko odgovornost. Hkrati pa vidim odlično priložnost, da prav z izkušnjami iz sektorja elektronskih komunikacij, pri spopadanju z varnostnimi izzivi pomagamo ostalim sektorjem, ki jih agencija nadzira.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

organ za varnost sektorja elektronskih komunikacij, ki so ključne za zagotavljanje številnih ostalih storitev kritične infrastrukture, čutimo na tem področju veliko odgovornost. Hkrati pa vidim odlično priložnost, da prav z izkušnjami iz sektorja elektronskih komunikacij, pri spopadanju z varnostnimi izzivi pomagamo ostalim sektorjem, ki jih agencija nadzira. Ker postajajo strateški vidiki pri varnostnih izzivih vedno bolj pomembni, sem vesel, da imamo na tem področju vzpostavljeno (tudi zakonsko) sodelovanje z URSIV. URSIV je pristojni nacionalni organ za informacijsko varnost, enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja, preko SNAV pa je umeščen tudi v sistem nacionalne varnosti. URSIV kot del Skupine za sodelovanje NIS ter agencija smo, v okviru mednarodnih organizacij ENISE in BEREC, pomembno vpeti v mednarodno okolje, kjer se zagotavlja potreben pretok informacij. Med pristojnimi nacionalnimi organi se na mednarodnem nivoju vzpostavlja tudi nujno potrebno čezmejno sodelovanje, saj vemo, da varnostni izzivi nikakor niso prostorsko omejeni zgolj na posamezne države.

Dejanska implementacija v poslovanje in delovanje zavezancev pa bo naslednja pomembna in zahtevna faza. Tukaj sem vesel, da je agencija tudi članica Slovenskega združenja za korporativno varnost, kjer se na srečanjih članov in konferencah veliko razpravlja o dobrih praksah in resničnih primerih. V pomoč članom pa je tudi vedno močnejši Inštitut za korporativno varnost.

Krize si v zadnjem obdobju kar sledijo, s tem pa je še bolj izpostavljen pomen kritične infrastrukture, zlasti varnost in odpornost komunikacijskih sistemov. Menite, da so se operaterji informacijsko komunikacijskih storitev ustrezno odzvali na izzive teh kriz?

Operaterji se na te krize odzivajo konstantno in se pripravljajo tudi za prihodnje izzive. Je pa glede na pomembnost sektorja in odvisnost celotne družbe od teh storitev potrebno razmisliti, kako bi lahko to infrastrukturo naredili še bolj odporno in kako lahko različni deležniki, tudi država, pri tem pomagajo.

Približuje se zimsko obdobje in ob tem spet opozorila o možnem pomanjkanju določenih energentov. Ste uspeli telekomunikacijsko področje ustrezno pripraviti na te izzive in realno oceniti, katera je tista infrastruktura in procesi, ki v primeru redukcij električnega toka ne smejo ostati brez le te?

Medsebojna soodvisnost je ključno in predhodno vprašanje. Omrežja nikoli ne bodo mogla delovati brez električne energije in prekinitev napajanja bo zagotovo vedno vplivala na delovanje omrežja. Manj problematični so krajši in lokalni izpadi, za daljše in obsežnejše pa je nujno potrebno sodelovanje vsaj navedenih sektorjev. Elektronska komunikacijska omrežja so zelo razvejana. Za ilustracijo, v Sloveniji imajo trije mobilni operaterji na dostopovnem delu prek 4000 lokacij in vse bi bilo potrebno opremiti z rezervnim napajanjem. Cena tega je seveda

močno odvisna od zmogljivosti, to pa na koncu vedno plača končni uporabnik. Ker je agencija, ki poleg regulacije trga skrbi tudi za zaščito uporabnikov, skupaj z operaterji tovrstne težave že prepoznala, je aktivno pristopila k iskanju različnih načinov za čim bolj učinkovit spopad tudi z izzivom pomanjkanja električne energije zaradi izvajanja redukcij.

Pred nekaj časa je bil sprejet nov Zakon o elektronskih komunikacijah (ZEKom-2). Sedaj počasi prihaja dovolj dolg časovni okvir od sprejema, da lahko naredite prve analize o uspešnosti uveljavitve teh zakonskih dopolnil. Ste zadovoljni s hitrostjo in resnostjo implementacije določil pri vseh zavezanih subjektih?

Ker gre za precejšnje število sprememb, med njimi tudi takšnih, za katere je potrebno prilagajanje poslovanja, je ta hip to kljub vsemu še nekoliko preuranjeno. Če se recimo navežem na poglavje o varnosti, smo s pripravo podzakonskih aktov, ki so bili za agencijo najtrši oreh, trenutno v zaključni fazi. Od uveljavitve ZEKom-2 je agencija pripravila in v Uradnem listu objavila že 33 splošnih aktov. Od treh splošnih aktov, ki urejajo varnost in jih je agencija pripravila v sodelovanju z URSIV, je javno posvetovanje zaključil še zadnji, agencija pa je tudi že objavila odgovore na pripombe, prejete v tem posvetovanju. Ta zavezuje operaterje, ki storitve ponujajo kritičnim subjektom. Prihodnji zavezanci so bili kar intenzivno vpleteni v sam postopek sprejemanja navedenih predpisov. Agencija je prav zaradi vseh sprememb, ki jih ti podzakonski predpisi vpeljujejo, z operaterji organizirala tudi več delavnic, na katerih se je odvijala zelo odprta razprava. Hkrati pa je bilo potrebno za prilagoditev prihodnjim zavezancem dopustiti tudi dovolj dolgo prehodno obdobje za prilagoditev oziroma implementacijo pravil.

Kaj pomembnega se je zgodilo na ravni EU, kar bo vplivalo tudi na vaše delovanje in na splošno na delovanje sektorja telekomunikacij?

Med najpomembnejšimi akti, čeprav priporočilne narave, je bil zagotovo Nabor orodij za kibernetsko varnost 5G (t.i. 5G Toolbox). Evropska komisija bdi nad državami članicami in implementacijo vseh priporočilnih, tako tehničnih kot tudi strateških ukrepov. V juniju je Skupina za sodelovanje NIS izdala že drugo poročilo o nacionalnih implementacijah ukrepov. Vesel sem, da bo Slovenija s sprejetjem prej omenjenih splošnih aktov in po sprejemu ZEKom-2 veliko večino ukrepov uspešno implementirala v svoj pravni red. Dejanska implementacija v poslovanje in delovanje zavezancev pa bo naslednja pomembna in zahtevna faza. Tukaj sem vesel, da je agencija tudi članica Slovenskega združenja za korporativno varnost, kjer se na srečanjih članov in konferencah veliko razpravlja o dobrih praksah in resničnih primerih. V pomoč članom pa je tudi vedno močnejši Inštitut za korporativno varnost. Pred nami pa je še veliko izzivov, npr. konec leta bo v javnem posvetovanju Evropska certifikacijska shema za 5G varnost, pripravlja pa se še kar nekaj novih predpisov s področja (kibernetske) varnosti.

Pred nami so tudi pomembni koraki uveljavitve dveh pomembnih evropskih direktiv CER in NIS 2. Ste ustrezno vpeti v medsektorske načrtovalne korake za uvajanje teh dveh direktiv v naš pravni sistem?

Agencija je aktivno spremljala že sprejemanje navedenih predpisov. S sprejemom NIS-2 se je področje varnosti elektronskih komunikacij premaknilo iz okvira elektronskih komunikacij v okvir NIS. Natančneje, določila NIS-2 so razveljavila 40 in 41. člen Evropskega zakonika o elektronskih komunikacija, ki urejata varnost in poročanje incidentov. Vsebinsko se za sektor elektronskih komunikacij kljub vsemu ne spreminja zelo veliko, saj NIS-2 precej sledi obstoječi ureditvi v Zakoniku. Nekatere prilagoditve v nacionalni zakonodaji bodo verjetno potrebne in tu pričakujemo dobro in tesno sodelovanje z enotno kontaktno točko po NIS, ki je v Sloveniji URSIV. V implementaciji CER pa vidimo še kako potrebno komplementarno ureditev k NIS, kjer pa bodo kompetence in izkušnje agencije kot konvergentnega regulatorja lahko prav tako koristne.

Kibernetska varnost postaja vedno bolj pereči izziv za organizacije, državo in tudi mednarodno skupnost. Na področju kritične infrastrukture so se uveljavile določene spremembe, kjer je naloge nosilca sektorja »informacijsko komunikacijskih omrežij in sistemov« prevzel Urad RS za informacijsko varnost. Je sodelovanje z omenjenim URSIV na ustrezni ravni in prinaša potrebne rezultate za krepitev tega kompleksnega sektorja, kjer imate ravno vi

skozi resorni zakon (Zekom-2) izredno velika pooblastila vezana na telekomunikacijske operaterje?

Z URSIV dobro sodelujemo. Naša najtežja skupna naloga je bila priprava podzakonskih aktov s področja varnosti na podlagi ZEKom-2. Sodelovanje med organoma je urejeno z ZEKom-2, na njegovi podlagi agencija poroča URSIV tudi o incidentih, ki jih je prejela s strani operaterjev elektronskih komunikacij. Ker je obstoječa podlaga, torej ZEKom-2, za sodelovanje med organoma še relativno nova, kar prav tako velja za prenašanje NIS 2 v nacionalni pravni red, si oboji prizadevamo za krepitev formalnega in neformalnega sodelovanja. S tem namenom smo se odzvali tudi prijaznemu vabilu ICS za vključitev v evropski projekt ENDURANCE, ki je namenjen prav iskanju sinergij in izboljšanju sodelovanja med ključnimi akterji za delovanje kritične infrastrukture.

Na področju kibernetske varnosti bo verjetno potrebno narediti še veliko smelih korakov, še posebej na področju pridobivanja ustreznih strokovnjakov. S tem izzivom se verjetno srečujete tudi na AKOS?

S pomanjkanjem ustreznih strokovnjakov se soočajo že podjetja, tudi večja, kaj šele državni organi. Pri tem delimo zelo podobno usodo z drugimi regulatorji v Evropi. Kar nas rešuje, če smem tako reči, je, da smo dobro vpeti tako v nacionalno mrežo kot tudi v mednarodno okolje. Združenja, kot je vaše, in vedno številčnejši dogodki ter konference na nacionalnem parketu, pripomorejo k pridobivanju novih znanj in izobraževanju obstoječega kadra. Trudimo se biti precej aktivni tudi na evropskem nivoju, kjer so naši strokovnjaki člani ekspertnih delovnih skupin s področja kibernetske in informacijske varnosti v ENISI in združenju BEREC.

Ob zadnji tragični naravni nesreči se je ponovno odprla žolčna razprava o tem zakaj Slovenija zamuja z uvajanjem učinkovitega sistema javnega obveščanja in alarmiranja v primeru večjih nesreč. Kako lahko AKOS pomaga, da čimprej dobimo ta delujoč sistem, kjer bo vsak državljan, ki se nahaja na določenem ogroženem območju pravočasno obveščen o možnih grožnjah?

Agencija s svojim članom sodeluje v delovni skupini za pripravo Uredbe, ki ureja vzpostavitev tega sistema, ni pa seveda njen nosilec. Zamude zato težko komentiram. So se pa že spomladi tudi na tem področju zgodili pomembni premiki, osnutek je že bil v javnem posvetovanju in po vedenju agencije tudi na izvedbeni ravni uvedba sistema ni več tako daleč.

Kako ste zadovoljni z vašim delovanjem v okviru Slovenskega združenja korporativne varnosti? Boste tudi vi nadaljevali zagovarjanje aktivne participacije AKOS znotraj tega pomembnega združenja?

Prepričan sem, da je ICS res super okolje za izmenjavo dobrih praks, tako na mesečnih srečanjih članov Slovenskega združenja za korporativno varnost kot tudi vseh ostalih dogodkih in konferencah, ki jih organizira Institut za korporativne varnostne študije. Agencija si bo prizadevala po svojih najboljših močeh, z vsem svojim znanjem in izkušnjami, tudi v prihodnje prispevati h konstantni rasti zavedanja o pomembnosti informacijske varnosti v državi. ■

Informacijske storitve in inženiring, d.o.o.

INFORMATIKA

Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

Med elementi ključne infrastrukture je energetika druga najbolj izpostavljena panoga, trendi intenzivne digitalizacije poslovanja in integracije operativnih in poslovnih sistemov pa izpostavljenost kibernetskim napadom še povečujejo.

Vplivi kibernetskih napadov na različna področja v energetiki:

PROIZVODNJA
Prekinitve storitev in napadi z izsiljevalsko programsko opremo (ransomware) na elektrarne in alternativne proizvajalce energije.

Možni vzroki:
zastareli sistemi za proizvodnjo in razvijajoča se infrastruktura čiste energije, zasnovana brez upoštevanja varnosti.

PRENOS
Hude motnje v dostavi energije odjemalcem s prekinitvami delovanja storitev na daljavo.

Možni vzroki:
pomanjkljivosti fizičnega varovanja omogočajo dostop do sistemov za nadzor omrežja.

DISTRIBUCIJA
Motnje v delovanju razdelilnih postaj, ki vodijo do regionalnih motenj v distribuciji in prekinitve delovanja storitev za odjemalce.

Možni vzroki:
porazdeljeni energetski sistemi in omejeni mehanizmi varnosti vgrajeni v SCADA sisteme.

PORABNIKI
Kraja podatkov o uporabnikih, prevare na področju podatkov o porabi in motnje v delovanju storitev.

Možni vzroki:
veliko tarč za napade z razširjeno mrežo različnih IoT naprav, vključno s pametnimi števci in električnimi vozili.

ČAS JE ZA ODLOČILEN KORAK

INFORMATIKINI strokovnjaki lahko pomagamo pri vzpostavitvi sodobnega sistema aktivne zaščite pred kibernetskimi in drugimi grožnjami, ki temelji na ključnih storitvah **VOC**:

- zaznavanje in obravnavanje incidentov kibernetske varnosti,
- odkrivanje ranljivost v informacijskih sistemih,
- izvajanje testov vdorov,
- vzpostavitev sistemov vab,
- modeliranje groženj,
- preverjanje izvorne kode,
- definiranje varnostnih izhodišč za informacijske sisteme,
- preverjanje prisotnosti in analiza škodljive kode,
- poročanje incidentov deležnikom ter
- ozaveščanje in usposabljanje.

VOC zagotavlja skladnost z zakonodajo, zmanjšanje škode v primeru incidenta in podporo neprekinjenem poslovanju podjetja. Združevanje okrog sektorskega varnostnega operativnega centra zagotavlja vzpostavitev domensko specifičnih načinov varovanja, ki so bolj prilagojeni panogi in so zato bolj učinkoviti.

VOC INFORMATIKE temelji na najnovejših tehnoloških rešitvah in vrhunskih produktih vodilnih svetovnih proizvajalcev.

www.informatika.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Jure Griljc, v.d. direktorja Javne agencije za civilno letalstvo Republike Slovenije*

V LETALSKEM SEKTORJU IMA VARNOST ŠE VEDNO POSEBNO MESTO

Tudi letalski sektor se ne more izogniti vedno večjim varnostnim izzivom, ki stojijo pred širšo družbeno skupnostjo. V zadnjem obdobju se na področju brezpilotnih zrakoplovov dogajajo pomembne spremembe, ki so vezane na učinkovite poizkuse zakonske ureditve omenjenega področja. Še dodatne izzive pa navkljub temu predstavljajo varnostna tveganja, ki jih prinaša ta hitro razvijajoči se del letalskega sektorja. Nekaj ključnih misli o izzivih, ki stojijo na tej poti, nam je zaupal g. Jure Griljc.

Najprej nam dovolite, da vam čestitamo ob imenovanju na to pomembno funkcijo. Nam lahko prosim zaupate nekaj o vaših predhodnih referencah, ki bodo vsekakor pomembne za upravljanje te odgovorne funkcije?

Pred prihodom na Agencijo sem bil več kot 14 let zaposlen v Policiji, kjer sem zasedal več vodstvenih funkcij, nazadnje sem vodil Sektor uniformirane policije na Policijski upravi Koper. Zadnja leta sem se poklicno vedno več ukvarjal z letalstvom. V času mojega dela na kriminalistični policiji sem sodeloval, vodil ali usmerjal večino preiskav letalskih nesreč in incidentov, ki so se zgodili na območju policijske uprave. Bil sem tudi namestnik vodje delovne skupine, ki se je ukvarjala z uvedbo brezpilotnikov v policijo. V sklopu tega sem napisal tudi učbenik za usposabljanje policistov za delo z droni in bil tako teoretični kot tudi praktični inštruktor letenja z brezpilotnimi zrakoplovi v Policiji. Glede na to, da je šlo za povsem novo področje dela, smo že takrat veliko sodelovali tudi s kolegi iz agencije; In nenazadnje sem tudi pilot z licenco športnega pilota.

Strateški varnostni izzivi pred katerimi stoji Slovenija, kot del mednarodnega okolja, bodo imeli tudi pomemben vpliv na delovanje Javne agencije za civilno letalstvo. Kje pričakujete največje izzive, ki sledijo področjem, ki jih upravljate v vaši agenciji?

Trenutno se s strokovnimi službami na Agenciji intenzivno ukvarjamo z usklajevanjem novega Zakona o letalstvu, ki nujno potrebuje spremembe. Sedanji je že zastarel, sprejet je bil namreč leta 2001, nazadnje pa spremenjen leta 2010, in kot tak ne omogoča več učinkovitega dela pristojnih inštitucij. Sprejem novega Zakona je potreben tudi zaradi novosti v letalstvu, ki v zadnjih letih vstopajo na to področje, vse s ciljem zagotavljanja kar največje varnosti v letalstvu, kar je

Glede na podatke o številnosti prodaje brezpilotnikov, ki iz leta v leto le narašča, gre pri tej vrsti deležnikov za pomemben del letalske populacije, zato nas veseli, da se vsako leto poveča tudi število oseb, ki se pri slovenski Agenciji registrirajo kot operatorji in opravijo tudi osnovno teoretično usposabljanje.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

tudi prvi in glavni cilj regulatornih in nadzornih letalskih oblasti.

Agencija je sicer v odlični kondiciji, kar priznava tudi Evropska agencija za civilno letalstvo – EASA, ki slovenske strokovnjake priporoča državam, ki potrebujejo pomoč pri reševanju neskladij v svojih državah, prav tako pa strokovnjaki naše Agencije redno sodelujejo pri izvedbi EASA inšpekcij pri drugih nacionalnih letalskih oblasteh.

V lanskem letu smo v pravni red Republike Slovenije prevzeli EU uredbo o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov. Kako ocenjujete uspešnost korakov za uveljavitev te uredbe pri zavezanih posameznikih in organizacijah?

Brezpilotni zrakoplovi so v letalstvu še vedno relativno novo in zelo specifično področje. T.i. »klasični uporabniki« naših storitev, torej piloti, kontrolorji in letalske organizacije, ki se ukvarjajo s šolanjem ali pa npr. z vzdrževanjem zrakoplovov, drugače gledajo na svet letalstva. Piloti na daljavo, kot jih opredeljuje nova evropska regulativa, pa v večini primerov (še) nimajo tistega pravega letalskega razmišljanja in zavedanja, da tudi oni, s svojimi zrakoplovi, posegajo v zračni prostor.

Glede na podatke o številnosti prodaje brezpilotnikov, ki iz leta v leto le narašča, gre pri tej vrsti deležnikov za pomemben del letalske populacije, zato nas veseli, da se vsako leto poveča tudi število oseb, ki se pri slovenski Agenciji registrirajo kot operatorji in opravijo tudi osnovno teoretično usposabljanje. Žal, kljub stalnemu osveščanju uporabnikov, še nismo na nivoju, ki ga želimo doseči, torej, da bi bilo registriranih in usposobljenih vsaj večina lastnikov brezpilotnih zrakoplovov.

Pomembno področje, ki ga ureja ta uredba je vsekakor povezano z licenciranjem brezpilotnih plovil in operatorjev. So pristopi prinesli dovolj preglednosti, da lahko rečemo, da obvladujete to zahtevno področje?

Morda za začetek pojasnilo: nova evropska pravila ne »licencirajo« brezpilotnih zrakoplovov ampak fizične osebe oz. organizacije, ki so glede na zahteve Izvedbene Uredbe Komisije (EU) 2019/947 dolžne opraviti registracijo operatorja.

Gre za osebe ali organizacije, ki so odgovorne za brezpilotne zrakoplove, ki jih imajo v uporabi. V veliko pomoč nam je že omenjena spletna aplikacija UAS Repozitorij, ki deluje na uporabnikom prijazen način, vključuje sodobne programske rešitve, hkrati zagotavlja vse relevantne zakonodaje s področja upravnega postopka, upravnega poslovanja in varstva osebnih podatkov. Z gotovostjo in ponosom lahko potrdimo, da z najvišjo ravnjo preglednosti, zanesljivosti in varnosti obvladujemo zahtevano področje.

Veliko vprašanj se še vedno poraja glede območij prepovedi preletov za brezpilotna plovila. Lahko kratko opišete postopek kako ključni subjekti, ki upravljajo kritično infrastrukturo lahko zagotovijo, da bo nad njihovo infrastrukturo ustrezno identificirano in tudi izvedeno območje prepovedi preletov brezpilotnih plovil?

Na podlagi 5. člena Uredbe o izvajanju izvedbene uredbe Komisije (EU) o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov, lahko zavezanci svoja območja kritične infrastrukture že sedaj razglasijo kot geografska območja, kjer je letenje z brezpilotnimi zrakoplovi prepovedano.

Takšni primeri v Sloveniji že obstajajo, in sicer na območju Luke Koper in na območju TEŠ 6. Kot geografsko območje, nad katerim je v odprti kategoriji prepovedano leteti, pa je določeno tudi celotno električno omrežje, ki ga upravlja ELES. Kršitev prepovedi je malo, se pa dogajajo. Agencija je za prikaz teh prepovedanih območij uporabila spletno rešitev, ki uporabniku v vsakem trenutku omogoča, da s pomočjo pametnega telefona, tablice ali pa računalnika pogleda ali se nahaja na območju, na katerem so omejitve.

Kaj pomembnega se bo dogajalo v bližnji prihodnosti na ravni EU, kar bo imelo pomemben vpliv tudi na vaše delovanje in na splošno za upravljanje področja brezpilotnih plovil? Kaj se dogaja z regulacijo avtonomnih platform z brezpilotnimi plovili, uporabo brezpilotnih plovil za raznos paketov, zdravil in ostale logistične storitve?

Na območju EU veljajo relativno stroge omejitve za letenje z brezpilotnimi zrakoplovi, še posebej, ko govorimo o kompleksnih letalskih operacijah, kamor nesporno spadajo tudi operacije, ki jih omenjate.

Dejavnost prenosa in dostave različnih paketov se sicer že vrši v nekaterih kitajskih provincah, v EU pa tega verjetno še ni pričakovati prav kmalu. Tovrstna dejavnost se bo v prihodnje razvijala v U-space okolju in v t.i. certificirani kategoriji, ki jo evropska uredba že opredeljuje, pri čemer bo tovrstne zrakoplove certificirala EASA in to po podobnih postopkih certifikacije in preverjanja začetne ter stalne plovnosti, kot to velja za ostale, pilotirane zrakoplove.

Lahko povem tudi, da v Sloveniji že deluje delovna skupina strokovnjakov, ki preučuje različne vidike in dejavnike letalskih operacij z brezpilotnimi zrakoplovi. Pričakujem, da bo ta delovna skupina preučila vse vidike teh operacij in podala mnenje, ki bo posledično pripeljalo do odločitve, kako in na kakšen način v prihodnje urediti to področje, je pa to seveda povezano z zanimanjem operatorjev, s tehničnimi rešitvami na trgu in seveda tudi s finančno vzdržnostjo.

Kakšne ukrepe na agenciji izvajate na področju zagotavljanja kibernetske varnosti? Letalski nadzorni sistemi so vedno bolj odvisni od delovanja informacijsko komunikacijskih sistemov.

Na agenciji se zavedamo varnostnih tveganj povezanih z zagotavljanjem informacijske oz. kibernetske varnosti, zato smo z Uradom Vlade Republike Slovenije za informacijsko varnost julija letos podpisali sporazum o sodelovanju na področju informacijske in kibernetske varnosti. Agencija ima na tem področju ustanovljeno tudi delovno skupino za »Part-IS«, ki skrbi za vsebine informacijske varnosti.

Pomembno vprašanje se vedno znova odpira okoli učinkovitosti sistemov za obrambo pred brezpilotnimi plovili. Imajo organi v Sloveniji zadostna pooblastila in tudi sredstva

Na podlagi 5. člena Uredbe o izvajanju izvedbene uredbe Komisije (EU) o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov, lahko zavezanci svoja območja kritične infrastrukture že sedaj razglasijo kot geografska območja, kjer je letenje z brezpilotnimi zrakoplovi prepovedano.

za učinkovito obrambo pred nedovoljenimi preleti brezpilotnih plovil nad prepovedanimi območji?

V svetu je poznanih nekaj različnih metod za identifikacijo in onemogočanje letenja brezpilotnih zrakoplovov, so pa ti sistemi po večini dragi in kompleksni. Poznamo sisteme, ki v brezpilotnike izstreljujejo različne naboje ali mreže, pa lovljene dronov s pticami in podobno.

Glede na različne analize, pa tudi fizična preizkušanja na terenu, se je zaenkrat kot najučinkovitejša izkazala opcija z motenjem radijskega signala, pri čemer pa gre omeniti, da ima v Sloveniji trenutno zgolj Policija zakonsko pooblastilo za takšno motenje radijskega signala.

Strokoven kader je v zadnjem obdobju resen izziv vseh visoko strokovnih institucij. Kako se s tem spopadate v agenciji?

Agencija je letalski strokovni organ, ki mora zagotavljati najvišjo raven strokovnosti na področju letalstva v Sloveniji. Zato so tudi vstopni pogoji za zasedbo delovnih mest, predvsem letalskih nadzornikov na agenciji visoki. Za ohranjanje kompetenc zaposlene kontinuirano usposabljamo tako v tujini kot doma, tistim z letalskimi licencami pa omogočamo tudi vzdrževanje izurjenosti z letenjem v Slovenski vojski in operaterjih. Zaenkrat se lahko pohvalimo z visoko usposobljenim in kompetentnim kadrom, ki ga za določene naloge v svoje kroge vabi celo EASA.

Kako ste zadovoljni z vašim delovanjem v okviru Slovenskega združenja korporativne varnosti? Boste tudi vi nadaljevali zagovarjanje aktivne participacije Agencije znotraj tega pomembnega združenja?

Slovenija nesporno potrebuje takšno strokovno združenje, kot je Slovensko združenje korporativne varnosti.

Agencija za civilno letalstvo bo tudi v prihodnje, kot delček v varnostnem mozaiku, z veseljem sodelovala v združenju in s tem, verjamem, da pripomogla k boljši skupni varnosti. ■

Foto: arhiv Javne agencije za civilno letalstvo RS

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Tomaž Jeretina, mag., pooblaščenec in vodja oddelka za varnost v Gorenjski banki d.d., Kranj*

UPRAVLJANJE VARNOSTNIH TVEGANJ JE V BANČNEM SISTEMU ŠE POSEBEJ IZPOSTAVLJENO

Učinkovito obvladovanje tveganj je postalo nujen predpogoj za učinkovito in varno delovanje bančnega sistema. Temu posebno mesto namenjajo tudi v Gorenjski banki, ki je s svojo mednarodno vpetostjo, izpostavljena celemu nizu različnih varnostnih tveganj. O pristopih in izkušnjah s tega področja smo se pogovarjali z g. Tomažem Jeretino.

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Katera področja so posebej zaznamovala vaš karierni razvoj?

Z upravljanjem varnostnih tveganj sem se prvič srečal v kemijski industriji, kjer sem izdeloval presoje vpliva kemikalij na okolje, ljudi in živali. To je bilo obdobje, ko sem začutil, da je področje neprekinjenega poslovanja in upravljanje varnosti nekaj, kar bo moja stalnica v prihodnosti, zato me je karierna pot odnesla na področje snovalca in nadzornika varnostnih ukrepov, izvajalca usposabljanj in preglednika linijskih postrojev. Mešanica izkušenj me je odnesla tudi v finančni sektor, kjer se že skoraj dve desetletji ukvarjam z različnimi varnostnimi izzivi, kot so neprekinjeno poslovanje, preprečevanje in reševanje prevar, zlorab, bankomatsko poslovanje, ter ostalimi izzivi tehniške, mehanske in informacijske varnosti.

Skupni imenovalec bi lahko zaključil s spoznanjem, da je kariera varnostnega managerja prepletena s pestrim naborom izzivov, stalnim prilagajanjem različnim okoliščinam, veliki odgovornosti in neprestanim izpopolnjevanjem znanja.

V zadnjem obdobju ste zelo močno vpeti v upravljanje varnostnih tveganj v bančnem sistemu Gorenjske banke. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost vaše banke?

V Gorenjski banki se zelo dobro zavedamo pomembnosti ustreznega razumevanja sprememb kompleksnega varnostnega okolja, saj smo del bančne skupine, ki deluje tudi v mednarodnem okolju in ima varnost morda še večjo težo pri konkurenčni prednosti. Slednjo gradimo s stalnim ocenjevanjem tve-

Skupni imenovalec bi lahko zaključil s spoznanjem, da je kariera varnostnega managerja prepletena s pestrim naborom izzivov, stalnim prilagajanjem različnim okoliščinam, veliki odgovornosti in neprestanim izpopolnjevanjem znanja.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Lahko imamo najboljša krmila informacijskih sistemov, visoko raven informacijske varnosti, a vendar je raven varnosti visoka le toliko, kot je varen najšibkejši člen celotne verige, zato je ključen celovit in strokoven pristop na vseh segmentih.

ganj, proaktivnim izobraževanjem zaposlenih, investiranjem v nove varnostne tehnologije in s hitrim adaptiranjem na nepričakovane situacije oz. spremembe v varnostnem okolju.

Banke so pogosto tarča kibernetskih napadov, saj razpolagajo z ogromnimi finančnimi podatki in sredstvi strank, zato je ključno, da imajo vzpostavljene trdne varnostne bariere in tako zagotavljajo visoko raven dolgoročnega zaupanja strank in zaposlenih. Pri tem ne gre pozabiti, da so naše stranke ranljiva tarča za prevare in zlorabe v svojem domačem okolju oziroma na spletu, zato je pomembna naloga bank, da jih ozaveščamo tudi o varnostni kulturi v okoljih, ki niso v domeni ponudnikov plačilnih sredstev.

Vsekakor ne gre pozabiti, da so banke podvržene striktni, stalno spreminjajoči se regulativi, kar pa zagotavlja obvladovanje pravnih tveganj in skupaj s tehnološko organizacijskimi rešitvami povečuje zaupanje v institucijo.

Bančni sektor je zaradi regulativnih zahtev in varnostnih tveganj, ki se vedno bolj selijo v informacijsko okolje, zelo specifičen pri svojem delovanju. Kako kompleksni so v tem okviru koraki za obvladovanje informacijskih tveganj, katerim je podvrženo delovanje vašega podjetja?

Že osnovni bančni procesi predstavljajo bazen kompleksnih rešitev, ki so v večini zajete v strogi regulativi. Če dodamo dejstvo hitrega razvoja plačilnih storitev, digitalizacije in globalizacije ter dovršenih kibernetskih napadov, pa je obvladovanje informacijskih tveganj ključna naloga za obstoj vsake organizacije. Stranke si želijo in zahtevajo digitalno, brezkontaktno in 24/7 storitev ter hkrati pričakujejo visoko raven zaupnosti in varnosti podatkov, pozabljajo pa, da so v tem procesu lahko najšibkejši člen, zato je poleg izpopolnjenih tehnoloških rešitev, ključno varnostno ozaveščanje vseh deležnikov. Lahko imamo najboljša krmila informacijskih sistemov, visoko raven informacijske varnosti, a vendar je raven varnosti visoka le toliko, kot je varen najšibkejši člen celotne verige, zato je ključen celovit in strokoven pristop na vseh segmentih.

Informacijska varnost nikakor ni enkraten projekt, temveč je kontinuitetno spremljanje in ocenjevanje tveganj, planiranje in testiranje ter nenehno prilagajanje že sprejetih ukrepov glede na nove grožnje. Celovita obravnava tveganj in nenehno prilagajanje ukrepov sta ključna za uspešno upravljanje informacijske varnosti.

Se v Republiki Sloveniji po vaše dovolj zavedamo pomembnosti področja informacijske varnosti? So ukrepi, ki jih izvaja država na tem področju ustrezni ali pogrešate konkretnejše ukrepe?

Digitalna preobrazba družbe in storitev je terjala sprejetje številnih uredb in direktiv, ki so tudi našo državo spodbudile k sprejetju raznih strategij, politik, aktov in ustanovitev organov, ki bodo v prihodnosti obrambna linija pri zagotavljanju ustreznega nivoja informacijske varnosti, ukrepanja v primeru inci-

dentov ter učinkovite sanacije eventualnih posledic in hitrega okrevanja. K temu bosta gotovo svoj delež tudi v prihodnje prispevala Urad RS za informacijsko varnost in SI-CERT.

Osebno ocenjujem, da obrambni nacionalno varnostni sistem predstavlja temelj za zaščito kritične infrastrukture in za izvajanje bistvenih storitev ter varnost ostalih deležnikov. Vsekakor pa bo potrebno nadaljevati s sistematičnim in proaktivnim pristopom za zagotavljanje zadostnih varnostnih pogojev za varno delovanje gospodarstva, življenje posameznika in družbe kot celote. Pri tem pa ne smemo pozabiti, da 100% varnosti ni in da se vseh globalnih groženj ne more eliminirati in odgovoriti v celoti na vprašanja, kot so: Kaj pa, če je onemogočeno delovanje primarne in hkrati vseh sekundarnih sistemov/lokacij, ali če ni zagotovljena dobava elektrike za kritično infrastrukturo, ter če ne bi bilo več ponudnikov različnih nadzornih plošč, kot sta Google in Apple? Imamo scenarije za take primere?

K višjemu nivoju informacijske varnosti vseh deležnikov oz. pravnih oseb, ki so bistvene za gospodarstvo in družbo ter so močno odvisne od IKT, bo gotovo velik delež prispevala tudi nova direktiva NIS2. Določen napor pa bo treba narediti tudi na ozaveščanju oz. če hočete promociji vrednote odgovornosti do lastne varnosti in zavedanja, da mora vsak v prvi vrsti poskrbeti za svojo varnost in se ne zgolj in samo naslanjati na skrb države.

Včasih imamo občutek, da se vse preveč naporov usmerja samo v področje informacijske varnosti in, da pozabljamo na pomen fizičnih in tehničnih ukrepov zagotavljanja varnosti. Sistemi so namreč kompleksni in eden brez drugega težko delujejo. Človek pa še vedno predstavlja pomemben varnostni izziv. Kako vi gledate na to potrebo po celovitih pristopih za zagotavljanje korporativne varnosti?

S tehnološkim razvojem in rapidno rastjo spletnih prevar in kibernetskih napadov je logična posledica povečanje pozornosti na področju informacijske varnosti. Vsekakor pa se je potrebno zavedati dejstva, da brez celovitega pristopa na vseh segmentih varnosti, ne bo dosežene optimalne ravni prevencije, kar napadalci hitro zaznajo in izkoristijo sebi v prid. Ne gre pozabiti primerov kibernetskih napadov, ki so bili aktivirani z nepooblaščenim vstopom v objekte organizacij in aktivacijo škodljive kode oz. instalacijo ransomware-a na nezaščitenih delovnih postajah, ali preko vnosa in priklopa zasebnega računalnika v omrežje organizacije.

Poleg segmentacije omrežja, aplikativnih omejitev, nadzora digitalne infrastrukture in storitev ter doslednega izvajanja tehničnih in fizičnih ukrepov na samih mikrolokacijah, je ključna tudi varnostna ozaveščenost in kultura vseh deležnikov, tako zaposlenih, strank kot obiskovalcev.

Gorenjska banka stalno vlaga v digitalno infrastrukturo in varnost, velik napor pa posveča usposabljanju in ozaveščanju zaposlenih in strank. Pri tem je pomembno, da informacije in obvestila strank ne naletijo na gluha ušesa in so dostavljena personalizirano, saj tako dosežejo svoj preventivni učinek. Zelo pomembno je, da se deležniki zavedajo in so stalno informirani tudi o novih tveganjih, ki jih prinaša npr. umetna inteligenca, novih načinih spletnih prevar in ukrepih za zaščito ter ravnanje pred, med in po incidentih.

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

Nosilci ključnih funkcij v finančnih institucijah se zavedajo varnostnih tveganj, saj so deležni rednih analiz varnostnih tveganj, poročil o incidentih s predlogi za obvladovanje tveganj ter eventualno sanacijo posledic. Lahko rečem, da se ne zaznava težav pri prepričevanju strateškega managementa, če so predočene ustrezne ocene in analize, z utemeljenimi razlogi za zagotovitev dodatnih sredstev oz. investicij v procese korporativne varnosti banke. Pomemben korak pri boljšem upravljanju korporativne varnosti oz. zagotavljanju optimalnega procesa ocenjevanja učinka izvedenih ukrepov ter pravočasnega sprejemanja korektivnih ukrepov je tudi direkten dostop varnostnih managerjev do uprave in umestitev oddelka za varnost neposredno pod upravo.

Vsekakor pa je v odnosu vodstva do varnostnih vprašanj pomembno tudi zaupanje vodstva v celotno ekipo, ki skrbi za

Gorenjska banka stalno vlaga v digitalno infrastrukturo in varnost, velik napor pa posveča usposabljanju in ozaveščanju zaposlenih in strank. Pri tem je pomembno, da informacije in obvestila strank ne naletijo na gluha ušesa in so dostavljena personalizirano, saj tako dosežejo svoj preventivni učinek.

Skozi dolgoletno članstvo v Slovenskem združenju korporativne varnosti smo v Gorenjski banki prepoznali visoko dodano vrednost članstva k upravljanju naše varnosti in absolutno pozdravljamo tovrstna združenja strokovnjakov.

korporativno varnost, kar je sad dolgoročnega sodelovanja, kompetenc in preteklih izkušenj.

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

Banke so podvržene restriktivni regulativi in rednemu nadzoru s strani regulatorja, kar posledično pomeni, da je strateški management direktno seznanjen z zahtevami in morebitnimi odstopanji od regulative tudi na področju varnosti. Dober primer ozaveščanja strateškega managementa v bankah poteka tudi preko Združenja bank Slovenije, kjer smo strokovnjaki iz posameznih področij združeni v Odbore in delovne skupine, katerih člani smo zavezani k redni obravnavi tekoče problematike na posameznem področju, izmenjavi izkušenj, snovanju enotnih ukrepov in poročanju upravnemu odboru, ki ga praviloma sestavljajo predsedniki oz. člani uprav posameznih bank.

Ocenjujem, da se tudi v ostalih podjetjih strateški management čedalje bolj zaveda, da je korporativna varnost eden od ključnih področij za uspešno upravljanje podjetja. Pri tem imamo veliko vlogo tudi strokovnjaki korporativne varnosti, ki z uspešnim obvladovanjem operativnih tveganj dokazujemo višjemu vodstvu, da se vlaganje v varnost splača in je lahko konkurenčna prednost.

Potrebno pa si je naliti čistega vina, da se varnostna ozaveščenost strateškega managementa poveča ob incidentih in zmanjša, ko jih ni, zato je zelo pomembno, da odgovorne osebe za varnost proaktivno spremljamo varnostne incidente pri ostalih pravnih osebah, v lokalnem okolju, državi in izven meja ter relevantno poročamo strateškemu managementu o tem in tako vzdržujemo raven ozaveščenosti tudi v navidezno mirnem času.

V zadnjem obdobju smo bili tudi v Republiki Sloveniji podvrženi izrednim naravnim vplivom, ki so doživeli vrh v tragičnih avgustovskih poplavah. Ustrezna urejenost sistema neprekinjenega poslovanja zaradi tega dobiva nove razsežnosti. Kako se tega lotevate v vaši banki?

V zadnjih katastrofalnih poplavah smo bili priča neverjetni stopnji naravne nesreče oz. hkratni poplavi po večini države, kar bi si težko zamislili v najbolj dodelanem načrtu neprekinjenega poslovanja. Naučili smo se, da ne smemo zaspati na obstoječih analizah, ki bazirajo na dosedanjih izkušnjah, temveč moramo pri pripravi in revidiranju načrta neprekinjenega poslovanja, t.i. BCP-ja, obravnavati najbolj črne scenarije in predvsem realizirati smiselne ukrepe. BCP ne sme ostati samo teorija na papirju, temveč mora rezultirati v konkretnih ukrepih in stalnem testiranju na novo sprejetih potrebnih ukrepih. Pri upravljanju neprekinjenega poslovanja se je pokazala potreba po večji pozornosti pri izbiranju mikro in makro lokacij podjetja, zagotavljanju procesne varnosti, dostopa do objektov in evakuacije, ne samo iz primarnih, temveč tudi sekundarnih lokacij.

Avgustovske poplave so nas postavile tudi pred izziv hitrega adaptiranja na spreminjajoče se situacije, saj je bilo potrebno v zgodnjih jutranjih urah aktivirati krizni štab in takoj pričeti z zaščito in reševanjem ljudi in premoženja. V organizacijah je bilo potrebno upoštevati tudi aspekt, da so zaposleni najprej reševali imovino na svojih domovih in niso bili na voljo za ukrepanje v podjetju. Vse to in nove napovedane grožnje bo potrebno v prihodnosti implementirati v revizije načrta neprekinjenega poslovanja in še bolj dosledno izvajati testiranje realnih situacij. Zadnji izredni dogodki so nas naučili, da morajo biti navodila za ukrepanje posameznikov ob izrednih razmerah kratka, logična, jasna, brez teoretiziranja, tako, da jih akterji hitro ozavestijo in so ob škodnih dogodkih ukrepi čim hitreje realizirani.

Vlaganje v izobraževanje kadrovskih potencialov organizacije je tista potrebna kvaliteta, ki tudi na področju varnostnega zavedanja, loči uspešna podjetja od povprečnih. Menite, da v vaši organizaciji posvečate dovolj pozornosti vlaganju v izobraževanje ključnih kadrov na področju obvladovanja varnostnih tveganj?

Kontinuitetno in zadostno izobraževanje ključnih kadrov na področju obvladovanja varnostnih tveganj je temeljni gradnik za učinkovito upravljanje varnosti v posamezni organizaciji. Uspešne organizacije prepoznavajo nenehno izobraževanje in varnostno ozaveščanje svojih zaposlenih in strank, kot investicijo v človeški kapital in se zavedajo, da je to najmočnejše orožje posameznika in podjetja v boju zoper obstoječa in nova varnostna tveganja. Brez stalnega izobraževanja se kaj hitro zgodi strokovna stagnacija, ki lahko vodi v nova operativna tveganja ali celo propad podjetja.

Gorenjska banka ima vzpostavljen zelo dober sistem zagotavljanja in posredovanja strokovnih vsebin in usposabljanj ključnih kadrov na področju obvladovanja varnostnih tveganj. Zagotovljen je sistem elektronskega izobraževanja z raznolikim naborom vsebin, do katerih lahko vsi dostopamo kadarkoli in kjerkoli.

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

Absolutno. Izmenjava znanja in dobrih praks je na področju korporativne varnosti ključnega pomena, saj v varnosti ni enoznačnih odgovorov, ni črne in bele situacije, temveč je veliko nians, ki pa jih lahko obvladujemo le z znanjem, sodelovanjem in nesebično delitvijo dobrih praks.

Skozi dolgoletno članstvo v Slovenskem združenju korporativne varnosti smo v Gorenjski banki prepoznali visoko dodano vrednost članstva k upravljanju naše varnosti in absolutno pozdravljamo tovrstna združenja strokovnjakov.

Verjamemo in se bomo trudili, da tudi mi s svojimi izkušnjami pripomoremo h graditvi odličnosti združenja, njenih članov in varnosti družbe kot celote. ■

Ključavnice za pametne sisteme pisarniških in garderobnih omaric v sodobnih delovnih prostorih

Za varne možnosti shranjevanja osebnih stvari, dokumentov, garderobe, paketov, delovne opreme zaposlenih ali obiskovalcev.

Minimalistične ključavnice, ki se zlahka zlijejo z dizajnom vašega prostora, brez težav pa jih lahko namestite tudi na obstoječe omarice in odklepate z obstoječimi mediji.

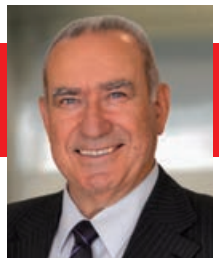
- Različni načini odklepanja (RFID medij, koda, mobitel) in napajanja (baterije ali On-line).
- Upravljanje preko centralnega terminala ali vsake omarice kot samostojne enote.
- Dodatne funkcije: USB polnjenje, osvetlitev, svetlobni in zvočni alarmi,...

IDealni partner za identifikacijo in varnost

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

Gantner
www.gantner.com

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



POMEMBNOST SLUŽBE ZA KORPORATIVNO VARNOST PRI UPRAVLJAVCIH KRITIČNE INFRASTRUKTURE IN IZVAJALCIH BISTVENIH STORITEV

Uvodoma je potrebno ugotoviti, katere dejavnosti so opredeljene kot kritična infrastruktura, kdo so upravljavci kritične infrastrukture in kdo izvajalci bistvenih storitev. Po 4. členu Zakona o kritični infrastrukturi so kot kritična infrastruktura opredeljene naslednje dejavnosti: energetika, informacijsko-komunikacijska omrežja in sistemi, promet, prehrana, preskrba s pitno vodo, zdravstvo, finance in varovanje okolja. Gospodarske družbe, zavodi in državne institucije v teh dejavnostih pa so lastniki in/ali upravljavci kritične infrastrukture. Po 5. členu Zakona o informacijski varnosti in 4. člena Uredbe o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev, pa so zavezanci (izvajalci bistvenih storitev) dolžni zagotavljati tudi informacijsko in komunikacijsko varnost, ki je opredeljena kot bistvena storitev.

Izvajalci bistvenih storitev so subjekti, ki delujejo na naslednjih področjih: energija, digitalna infrastruktura, oskrba s pitno vodo, zdravstvo, promet, bančništvo in infrastruktura finančnega trga, prehrana in varstvo okolja. Posebej je torej poudarjeno, da upravljavci kritične infrastrukture, ki so po 19. členu Zakona o kritični infrastrukturi dolžni zagotavljati neprekinjeno poslovanje, hkrati dolžni zagotavljati tudi informacijsko in komunikacijsko varnost. Ob navedenem pa se pojavlja tudi vprašanje, kaj je korporativna varnost in kaj v okviru tega je služba za korporativno varnost. V bistvu gre za upravljanje celovite varnosti in celovitega varovanja premoženja, ljudi, znanja in vrednot v vseh razmerah. Gre torej za varnost in varovanje od »A« do »Ž«, torej gre za obvladovanje varnosti in zdravja pri delu, varstva pred požari, varstva okolja, varovanja podatkov, informacij in komunikacij, varstva pred naravnimi in drugimi nesrečami, varovanja arhivov, varovanja dobrega imena ter obvladovanja ranljivosti, ogroženosti in varnostnih tveganj. Nekaj organizacij v kritični infrastrukturi že ima vzpostavljeno službo za korporativno varnost, ki se je pokazala kot ustrezna in učinkovita za dvigovanje kakovosti varnostnih mehanizmov ter celovitega in učinkovitega upravljanja z varnostnimi tveganji. Zato so v naslednjih točkah predstavljena ključna izhodišča za vzpostavitev korporativne varnosti in pripadajoče službe, ki naj motivirajo menedžment pri upravljavcih kritične infrastrukture in pri izvajalcih bistvenih storitev, da še bolj spoznajo pomembnost obstoja, delovanja in posodabljanja službe za korporativno varnost.

*avtorja sta člana Slovenskega združenja korporativne varnosti

Pravna in strokovna izhodišča za vzpostavitev službe za korporativno varnost

Za upravljanje korporativne varnosti zakonodaja ne zahteva ustanovitev službe za korporativno varnost, določa pa imenovanje kontaktne in odgovorne osebe ali več takih oseb za sodelovanje z drugimi upravljavci kritične infrastrukture, z nosilci sektorjev kritične infrastrukture in s področnim ministrstvom. Je pa to vendarle neka podlaga za vzpostavitev določene službe, ki skrbi za uravnoteženost delovanja in razvoja posameznih področij varnosti in za krovno/strateško upravljanje varnostnih tveganj in celovite varnosti.

Pravna izhodišča

Področje varnosti, varovanja in zaščite ureja ogromno predpisov. V nadaljevanju je navedenih nekaj ključnih zakonov in podzakonskih aktov, ki so ključni za upravljanje korporativne varnosti in sicer: Zakon o varnosti in zdravju pri delu, Zakon o varstvu pred naravnimi in drugimi nesrečami, Zakon o varstvu pred požarom, Zakon o varstvu okolja, Zakon o kemikalijah, Zakon o varstvu osebnih podatkov, Zakon o tajnih podatkih, Zakon o poslovni skrivnosti, Zakon o informacijski varnosti, Zakon o elektronskih komunikacijah, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih, Zakon o kritični infrastrukturi, Zakon o zasebnem varovanju, Zakon o obrambi z Uredbo o objektih in okoliših objektov posebnega pomena za obrambo in s predpisi, ki urejajo organiziranost in delovanje civilne zaščite, Uredba o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev, Uredba o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev. Odgovorne osebe za posamezna področja varnosti so dolžne poskrbeti za to, da so izdelani vsi dokumenti, ki jih določa posamezen zakon.

Strokovna izhodišča – standardi

Za zagotavljanje zahtevane ravni kakovosti in varnosti ljudi, premoženja, znanja, izkušenj in drugega ter za zagotavljanje neprekinjenega delovanja in poslovanja organizacij, ki upravljajo s kritično infrastrukturo, so pomembni naslednji standardi: standardi sistema vodenja kakovosti SIST EN ISO 9001:2015 (krovni standard, ki je v bistvu podlaga za vse druge standarde), standardi kakovosti, varnosti in obvladovanja tveganj v zdravstvenem sektorju – varnost zdravstvenega osebja in pacientov - DNV, ACI, AACIS, EN 15224, ISO 15189, standardi neprekinjenega poslovanja SIST EN ISO 22301, standardi varovanja informacij SIST EN ISO/IEC 27001:2017, standardi varnosti in zdravja pri delu SIST ISO 45001:2018, standardi varnosti in sledljivosti živil SIST EN ISO 22000:2018 – HACCP, standardi, ki so obvezni na področju zasebnega varovanja, okolijski standardi ISO 14001, standardi upravljanja tveganj ISO 31000, COSO ERM in drugi.

Varnostna področja in varnostna dokumentacija kot vsebinska izhodišča vzpostavitve službe za korporativno varnost

Vsebino vzpostavitve in delovanja službe za korporativno varnost določajo varnostna področja in varnostna dokumentacija.

Služba za korporativno varnost je krovna služba, ki upravlja korporativno varnost oziroma integralni varnostni sistem. Vzpostavitev službe za korporativno varnost je v bistvu projekt, ki dolgoročno zagotavlja uravnoteženo delovanje in razvoj posameznih področij varnosti.

Med varnostna področja spadajo naslednja področja: fizično varovanje premoženja in ljudi z varnostniki, gasilci in redarji, tehnično varovanje z elektronsko, mehansko in elektromehansko opremo, varstvo pred požari, varnost in zdravje pri delu, varstvo okolja, varstvo pred naravnimi in drugimi nesrečami – organiziranost zaščite in reševanja, varovanje informacij in elektronskih komunikacij – računalniška, informacijska, omrežna, kibernetska in komunikacijska varnost, obvladovanje terorističnih in kibernetskih groženj, varstvo osebnih podatkov, varovanje tajnih podatkov, varovanje poslovnih skrivnosti, varovanje dokumentarnega in arhivskega gradiva ter arhivov, varovanje konkurenčnih prednosti, intelektualne lastnine, ugleda in dobrega imena, strokovno (varnostno) izobraževanje in usposabljanje, varnostna kultura in poslovna etika, civilna zaščita in civilna obramba, upravljanje varnostnih tveganj, upravljanje standardov kakovosti, upravljanje varnostnih standardov.

Upravljanje navedenih varnostnih področij in s tem upravljanje korporativne varnosti, mora biti urejeno z ustrezno **varnostno dokumentacijo**, ki obsega: projektno dokumentacijo o vzpostavitvi korporativne varnosti in službe za korporativno varnost, projektno dokumentacijo izvedenih sistemov tehničnega varovanja in mehanske zaščite, načrt fizičnega

Vzpostavitev službe za korporativno varnost je, v teh varnostno turbulentnih in negotovih časih, zagotovo ena izmed pravih rešitev organizacijskega, kadrovskega in vsebinskega posodabljanja obstoječih varnostnih rešitev. Zato večjim gospodarskim družbam, zavodom in drugim organizacijam, ki upravljajo s kritično infrastrukturo predlagamo, da ustanovijo službo za korporativno varnost, kot krovno službo na področju zagotavljanja visoke stopnje varnosti.

varovanja, pogodbe z zunanjimi izvajalci na posameznih področjih zasebnega varovanja in detektivske dejavnosti, analizo in oceno ranljivosti in ogroženosti, analizo in oceno varnostnih tveganj s katalogom tveganj, krovno varnostno politiko in izvedene varnostne politike (politiko varovanja informacij in druge izvedene politike za posamezna varnostna področja), varnostno strategijo, kodeks varnostne in poslovne etike, program varnostnega usposabljanja, politiko in načrt neprekinjenega delovanja in poslovanja, načrt obvladovanja izrednih dogodkov z opredelitvijo odzivov na posamezne izredne dogodke, krizni načrt z rezervno lokacijo in avtonomnim napajanjem z električno energijo, notranji pravni red, ki ureja področje korporativne varnosti – poslovniki, pravilniki in varnostna navodila, dokument (navodilo) o poročanju nastalih izrednih dogodkov, dokument (navodilo) o nadzoru notranje varnosti, z navedbo načina sodelovanja z notranjo kontrolo in revizijo, dokument (navodilo) o varnostnih zahtevah za poslovne partnerje, dokument (navodilo) o varnostnih zahtevah in nadzoru nad zunanjimi pogodbenimi izvajalci.

Upravljanje varnostnih področij in posledično upravljanje varnostne dokumentacije je zahtevna naloga krovnega vodstva ter vseh vodstvenih struktur in služb. Vendar pa je profesionalno obvladovanje te zahtevne naloge možno le s službo za korporativno varnost, ki ima kompetentno vodstvo in kompetentne zaposlene. Torej je sestavni del kadrovske politike tudi premišljen pristop h kadrovanju tistih ljudi, ki profesionalno delajo na posameznih varnostnih področjih in na upravljanju korporativne varnosti kot celote.

Kadrovski vidik službe za korporativno varnost

Služba za korporativno varnost je krovna služba, ki upravlja korporativno varnost oziroma integralni varnostni sistem. Nekdo pač mora upravljati s celovitim sistemom varnosti tako, da se trajno, učinkovito in uspešno zagotovi visoka stopnja varovanja ljudi, premoženja in vrednot. Če upoštevamo kaj je korporativna varnost in iz nje izpeljan celovit sistem varnosti, je služba za korporativno varnost tista služba, ki ji je treba organizacijsko, kadrovsko, prostorsko in finančno zagotoviti neodvisno in učinkovito upravljanje korporativne varnosti. Vzpostavitev službe za korporativno varnost je v bistvu projekt, ki dolgoročno zagotavlja uravnoteženo delovanje in razvoj posameznih področij varnosti.

Vodenje službe za korporativno varnost je visoko zahtevna vodstvena funkcija, ki neposredno odgovarja krovnemu vodstvu, in ki sodi v kolegij generalnega direktorja. Vodja mora imeti široka pooblastila glede koordinacije delovanja in razvoja posameznih področij varnosti ter strokoven in argumentiran vpliv in moč v procesu razreševanja varnostnih vprašanj in mora biti tudi ustrezno nagrajen. Menedžment korporativne varnosti je potemtakem visoko profesionalni menedžment, ki po varnostni stroki, izobrazbi, navadah, vedenju, etiki, vrednotah in odnosih do ljudi in okolja daje zgled urejenega menedžmenta. Glavne kompetence - znanja, izkušnje, spretnosti, sposobnosti in veščine - tovrstnega menedžmenta, so naslednje:

- sposobnost reševanja problemov, zapletov, konfliktov in kompromisnih rešitev,
- kritično razmišljanje pred odločitvami,
- ustvarjalno razmišljanje za sprejemanje razumnih in uresničljivih odločitev,
- upravljanje s človeškimi viri, ki usmerja v motiviranost in nenehno usposabljanje za dvigovanje kakovosti dela in poslovanja ter v razvijanje varnostne kulture in poslovne etike,
- organizacijske in komunikacijske sposobnosti za kakovostno izvajanje nalog in ukrepov,
- zavedanje o koristnosti razvijanja čustvene inteligence,
- sposobnost osredotočiti se na ključne (življenjsko pomembne) zadeve,
- razvijanje sposobnosti za obvladovanje pogajalskih situacij ob sklepanju pogodb in sporazumov,
- razvijanje kognitivne fleksibilnosti – sposobnost razreševanja nepričakovanih dogodkov, poglobljeno analiziranje podatkov in informacij ter oblikovanje varnostnih, organizacijskih in drugih izboljšav.

Upoštevanje navedenih kompetenc je pogoj, da krovno vodstvo in kadrovska služba zagotavlja ustrezne ljudi (zlasti) na izpostavljena delovna mesta. Dobro je, da se pri pridobivanju novih varnostno izpostavljenih kadrov stremi v smer, da imajo posamezni kandidati čim več ustreznih kompetenc, kar olajša začetno obvladovanje delovnih nalog. Pridobivanje in izboljševanje kompetenc poteka tudi skozi sistem trajnostnega varnostnega in drugih oblik usposabljanja.

Vzpostavitev službe za korporativno varnost je, v teh varnostno turbulentnih in negotovih časih, zagotovo ena izmed pravih rešitev organizacijskega, kadrovskega in vsebinskega posodabljanja obstoječih varnostnih rešitev. Zato večjim gospodarskim družbam, zavodom in drugim organizacijam, ki upravljajo s kritično infrastrukturo predlagamo, da ustanovijo službo za korporativno varnost, kot krovno službo na področju zagotavljanja visoke stopnje varnosti. Naš predlog temelji na načelih varovanja in zaščite kritične infrastrukture (10. člen ZKI), ki so: načelo celovitega pristopa, načelo odgovornosti, načelo zaščite pred vsemi vrstami nevarnosti in tveganji, načelo neprekinjenega načrtovanja in poslovanja ter načelo izmenjave podatkov in informacij. Na tej osnovi krovno vodstvo poskrbi, da vzpostavitev službe za korporativno varnost temelji na strokovni presoji potreb po izboljšanju učinkovitosti varnostnih mehanizmov in na notranji pravni podlagi. ■

Avtor: mag. Marko Mihalič / Institut za korporativne varnostne študije*

KORPORATIVNO VARNOSTNO OKOLJE IN NEDOVOLJENA TRGOVINA - GLOBALNO VODENJE MEDNARODNIH PREISKAV

V današnjem globaliziranem poslovnem okolju je korporativna varnost postala pomembna skrb organizacij v različnih panogah. Zaščita sredstev, zmanjševanje tveganj in zagotavljanje celovitosti poslovanja so ključnega pomena za trajnostni uspeh. Resen izziv, s katerim se pri tem soočajo podjetja, je grožnja nezakonite trgovine. Nedovoljena trgovina zajema različne nezakonite dejavnosti, kot so tihotapljenje, ponarejanje, pranje denarja in kršitve intelektualne lastnine. Vse to pa ima lahko hude posledice za podjetja in gospodarstva po vsem svetu.

Uvod

Vodenje mednarodnih preiskav zaradi nedovoljene trgovine je zapletena in večplastna naloga. Ker nedovoljena trgovina presega geografske meje in deluje v tajnem omrežju, morajo strokovnjaki za varnost podjetij sprejeti globalni pristop, da bi razkrili in onemogočili te kriminalne operacije. To zahteva sodelovanje in usklajevanje med različnimi zainteresiranimi stranmi, vključno z organi odkrivanja in pregona, regulativnimi organi, industrijskimi združenji in mednarodnimi partnerji.

Nedovoljena trgovina predstavlja izjemno kompleksno in nenehno spreminjajoče se področje. Napačno bi bilo verjeti, da se tovrstne nezakonite dejavnosti odvijajo izključno zunaj naših meja, saj ima Slovenija svoje posebnosti, med katerimi majhnost države in neustrezna regulativa predstavljata ključne dejavnike, ki spodbujajo pojav nedovoljene trgovine. Ob upoštevanju še naše geografske lege postane očitno, zakaj smo v preteklih letih opažali povečanje takšnih aktivnosti pri nas.

Okolje korporativne varnosti in boj proti nezakoniti trgovini

Varnostno okolje podjetij in ukrepe za boj proti nedovoljeni trgovini je treba obravnavati kot dve plati iste medalje. Med-

Nedovoljena trgovina predstavlja izjemno kompleksno in nenehno spreminjajoče se področje. Napačno bi bilo verjeti, da se tovrstne nezakonite dejavnosti odvijajo izključno zunaj naših meja, saj ima Slovenija svoje posebnosti, med katerimi majhnost države in neustrezna regulativa predstavljata ključne dejavnike, ki spodbujajo pojav nedovoljene trgovine.

*avtor je član Slovenskega združenja korporativne varnosti

Za učinkovito zaščito blagovne znamke sta potrebna zaupanje med partnerji in dolgoročna prizadevanja. Tega ni mogoče in se ne sme opraviti v kratkem času.

tem, ko so v nekaterih podjetjih ekipe, ki se osredotočajo na ti dve področji del istega oddelka pa v številnih drugih podjetjih, ti dve ekipi delujeta neodvisno. Izvajanje ustreznih varnostnih ukrepov in ukrepov za preprečevanje nedovoljene trgovine je ključnega pomena za zmanjševanje tveganj ter med drugim tudi zaščite ugleda podjetja, dobička in pravnega položaja. Zato vedno priporočamo vzpostavitev tesnega sodelovanja med obema ekipama.

Obravnavali bomo ključne ukrepe, ki jih je nujno izvesti, da bi se uspešno in učinkovito spopadli z nedovoljeno trgovino ter zagotovili uspešno izvajanje protiukrepov. Pomembno je razumeti, da ta seznam ni izčrpen, saj je treba vsak ukrep prilagoditi specifičnim potrebam in okoliščinam vsakega posameznega podjetja.

Natančno opredelite problem

Prvi ključni korak pri tej nalogi je jasna opredelitev problema. Nedovoljena trgovina je zelo zapletena in se nenehno razvija. Spomnim se, da, ko sem se v preteklosti pridružil svojemu nekdanjemu delodajalcu, je bil boj proti nezakoniti trgovini le boj med dvema različnima vrstama nezakonite trgovine. Imeli smo ponaredke in kontrabant. Ponaredki so izdelki, izdelani brez soglasja lastnika blagovne znamke. Kontrabant pa so pristni izdelki, ki so med distribucijo nekako preusmerjeni v nezakonito trgovino, zato jih lahko imenujemo preusmerjeni izdelki. V tistem času so imeli vsi večji akterji v industriji poseben oddelek za boj proti nezakoniti trgovini. Poleg tega so organi odkrivanja in pregona (Law Enforcement Agencies - LEA) učinkovito in neprekinjeno izvajali pregon, uničevali objekte in posledično znatno oteževali delovanje ponarejevalcev.

Zato je nastala nova vrsta nezakonitega izdelka. Tobačna industrija jih je poimenovala nedovoljeni beli izdelki (Illicit Whites - IW). Proizvajalci so te izdelke večinoma zakonito izdelovali, vendar so jih le redko prodajali v državi, v kateri so jih izdelovali. Te iste blagovne znamke IW so bile v številnih državah po svetu zakonito prisotne le v omejenem obsegu ali pa sploh niso bile prisotne. Ta nova vrsta izdelkov je bila ustvarjena večinoma za tihotapljenje. Glede na to, da je tobačna industrija ena od najstrožje reguliranih industrij in da morajo biti izdelki opremljeni s posebnimi lokalno opredeljenimi zdravstvenimi opozorili in fiskalnimi znamkami ali oznakami, jih ti izdelki niso imeli. Na embalaži nekaterih od njih je bila le navedba „Samo za izvoz“. Če se vrnete v nekatera poročila Olafa ali Europola, lahko preberete, kako velika je bila tovrstna trgovina in je na nekaterih območjih še vedno prisotna in kako pomembno je bilo in je, da zakonita, regulirana tobačna industrija ponovno opredeli to vprašanje in razvije nove ukrepe za boj proti novemu konkurentu, ki ne igra po pravilih.

Preden zaključimo to poglavje, bi rad omenil nadaljnji razvoj in nove vrste nezakonitih izdelkov, povezanih z novimi tehnologijami. V mislih imam naprave, ki se uporabljajo za segrevanje tobaka. Te naprave, ki so bile neustrezno predelane, spadajo tudi med nezakonito trgovino. V šali bi lahko te naprave poimenovali „Frankensteinove“, saj so vanje vgrajeni vsi mogoči in nemogoči deli.

Te naprave so lahko imele nekaj originalnih delov, lahko pa so imele tudi originalne dele iz drugih naprav, ki jih ne bi smeli najti v tej posebni napravi. Nazadnje so baterije lahko brez kakršnekoli oznake, zato jih lahko imenujemo neoznačene ali generične baterije. Ponovno poudarjamo, da je razumevanje vrste težav v industriji ključnega pomena za vzpostavitev prave strategije za učinkovit boj.

Vključite ustrezne notranje oddelke

Drugi korak je, da v ocenjevanje vključite ustrezne notranje oddelke. Če boste vse notranje zainteresirane strani uskladili že na začetku, ne boste dosegli le njihove pripadnosti, temveč boste pospešili tudi postopke odobritve, ki so v velikih podjetjih običajno eno od „ozkih grl“. Dodatno pa bodo različni oddelki, ki sodelujejo v ocenjevanju, omogočili dovolj časa komercialnemu in prodajnemu oddelku, da bosta pripravljena za ukrepanje, ko bo nezakonito blago uspešno umaknjeno s trga. Če pride do te vrzeli, je nujno, da se pripravi primerna rešitev za zadovoljstvo potrošnikov. V nasprotnem primeru obstaja tveganje, da bodo vaši konkurenti izkoristili to težko pridobljeno tržno priložnost, ki bi se vam lahko ponovno izmaknila.

Preverite razpoložljivost notranjih podatkov

Naslednji korak v procesu je preverjanje razpoložljivosti internih podatkov. Začnite z obstoječimi notranjimi viri podatkov in jih nato kombinirajte z javno dostopnimi informacijami. V vaših različnih oddelkih se skoraj zagotovo že nahajajo obsežne količine podatkov, ki jih je treba ustrezno analizirati. Šele, ko pregledate vse interne podatke, se lahko posvetite pridobivanju novih, koristnih in informativnih podatkov. Obstaja več ponudnikov, ki vam lahko pomagajo pri skrbnem spremljanju, zagotavljanju informacij o nezakoniti dobavni verigi, analizi prodajnih mest, forenziki, o preprečevanju pranju denarja in splošnem upravljanju teh podatkov.

Če povzamemo, priporočljivo je, da poznate in razumete svoj problem v zvezi z nedovoljeno trgovino iz preprostega razloga, kajti zmanjšanje prodaje ni vedno posledica nedovoljene trgovine.

Kdo so vaši notranji in zunanji zavezniki?

Da bi se lahko borili proti nezakoniti trgovini, morate imeti jasna pravila igre. Najbolje bi bilo, če bi oblikovali preproste, a učinkovite operativne postopke in jih po možnosti digitalizirali. Standardni Operativni Postopek (SOP) se morda sliši preveč usmerjen v kazenski pregon, zato bi priporočali nekaj bolj vpadljivega, na primer Preiskovalni standard. Predlagamo, da vse obvezne dejavnosti vključite v dva sklopa. Vsak od njiju naj vsebuje posebne potrebne dejavnosti. Prepričani smo, da bi lahko na podlagi potreb stranke natančno prilago-

dili obvezne dejavnosti tako, da bi jih bilo čim manj. Imeti vse na spletu je bistveno za zagotavljanje ustreznih odobritev in za uporabo načela samo enkratnega vnosa v platformo.

Osredotočite se na notranje zaveznike

To je pomembno z vidika lažjega razumevanja dejanskega problema in zmanjšanje tveganja za ugled, povezanega z nezakonito trgovino. Zagotavljanje ustrezne forenzične podpore s strani notranje ekipe ali zunanjih partnerjev je ključnega pomena za pospešitev postopka preverjanja. Prosite svojo forenzično ekipo, da ustvari »prstne odtise« ponaredkov in na koncu ponaredke združi po vrstah strojev, lokacijah ali blagovnih znamkah. Pozneje toplo priporočamo redna industrijska srečanja, povezana z nezakonito trgovino s konkurenti, da bi primerjali in združevali različne »prstne odtise«. Ne bomo omenjali vseh oddelkov, ki jih je treba vključiti v razprave, ampak jih bomo navedli le nekaj: korporativna varnost, prodaja in komerciala, pravna služba, proizvodni oddelek, oddelek za korporativne zadeve itd.

Raziščite in gradite tudi zunanje zaveznike

Posebna industrijska združenja, distributerji, dobavitelji, pridelovalci, različne gospodarske zbornice itd. so le nekateri od zaveznikov, ki so potrebni v boju proti nezakoniti trgovini. Jasno je, da so organi odkrivanja in pregona tisti, ki izvajajo nadzor. Odkrito in pregledno sodelovanje je bistvenega pomena.

Pri obravnavi nezakonite trgovine morajo podjetja vzpostaviti zanesljive varnostne ukrepe za zaščito svojega premoženja, intelektualne lastnine in ugleda blagovne znamke. Mednarodne preiskave zahtevajo skrbno usklajevanje med različnimi zainteresiranimi stranmi, vključno z organi odkrivanja in pregona, pravnimi ekipami in ustreznimi vladnimi organi.

Običajno je potrebno veliko časa in vztrajnosti za začetek ustreznega operativnega sodelovanja, vendar vam lahko zagotovimo, da se bo ta čas dobro povrnil.

Izogibati se morate načinu „ustavi se in pojdi“. Ko namreč podjetje potrebuje organe odkrivanja in pregona, so ti organi vaši najboljši prijatelji le do takrat, dokler ne rešijo vaše težave. Če pa z njimi nehate sodelovati prehitro, tudi oni ne bodo več tako sodelovali, kot bi vi želeli, ko boste njihovo pomoč ponovno potrebovali.

Za učinkovito zaščito blagovne znamke sta potrebna zaupanje med partnerji in dolgoročna prizadevanja. Tega ni mogoče in se ne sme opraviti v kratkem času. Nenazadnje je vaš

prijatelj sovražnik vašega sovražnika! Konkurenca je na vaši strani. Pazite, kako boste sodelovali, pri tem pa upoštevali vse proti konkurenčne zakone. Svetujemo vam, da mora biti konkurenca eden od vaših zaveznikov, če se nameravate resno boriti proti nezakoniti trgovini.

Ko boste imeli izdelan standard preiskave, ki se bo v celoti izvajal in bo na voljo na spletu, boste lahko nadaljevali. Za učinkovit boj proti temu pojavu uporabite vse zaveznike, vključno s konkurenco.

Spremenite problem v priložnost

Pripravite dobro igro ali dober bojni načrt za uravnoteženje kratkoročnih zmag in dolgoročnih ciljev. Če ste pravilno opredelili vse notranje in zunanje bitke, ki jih morate dobiti, v primerjavi z dejavnostmi, ki jih je samo zaželeno imeti, vam bo uspelo.

Nikoli ne smete ogroziti dolgoročnih ciljev samo zato, da bi bilo vaše vodstvo zadovoljno. Bodite ustvarjalni in načrtujte svoje dejavnosti tako, da poberete »nizko viseče zrelo sadje«, da boste vedno imeli nekaj novega za poročanje.

Usklajevanju z organi odkrivanja in pregona morate nameniti čas. In to zelo veliko časa. To je maraton in ne sprint. Vedno morate imeti v mislih, da so organi odkrivanja in pregona tisti, ki izvajajo pregon, in to ni v pristojnosti lastnika blagovne znamke in tudi ne v vaši pristojnosti. Sodni postopki lahko trajajo nekaj let, da se zaključijo, zato bodite potrpežljivi.

Nazadnje je organiziranje rednih usposabljanj ena od najboljših poti za ohranjanje stikov z organi odkrivanja in pregona. Vedeti morate, da se organi odkrivanja in pregona ukvarjajo z veliko izdelki, zato ste vi zadolženi, da jim razložite in delite vaša spoznanja. Na teh dogodkih se morajo organi odkrivanja in pregona seznanjati z najnovejšimi trendi, pri čemer se ti dogodki ne smejo obravnavati kot marketinški sestanki.
Če povzamemo, čas je denar, zato ju pametno uporabite!

Spremljajte razmere in jih izboljšujte

Pri rednem spremljanju upoštevajte ista merila. Le tako si boste zagotovili primerljive podatke, ki vam bodo pomagali pri vzpostavljanju notranjega in zunanjega zaupanja.

Le z jasnimi meritvami boste namreč lahko razumeli trende v panogi in sezonskost v primerjavi z vplivom nezakonite trgovine. Več kot širite podatke znotraj in zunaj podjetja, bolje je. Jasno pa mora biti, da se pri deljenju operativnih obveščevalnih podatkov to ne upošteva.

Industrija ali organi odkrivanja in pregona za boj proti nedovoljeni trgovini so le nekateri zavezniki, kjer lahko izmenjujete svoje forenzične podatke. Vedno poiščite način, kako biti del pogovora, da boste imeli najboljši pogled na vse vidike problematike.

Ob upoštevanju vsega navedenega je bistveno, da spremljate, kaj se dogaja. Kot že rečeno, je nedovoljena trgovina izjemno močna in nenehno razvijajoča se zver. Lahko se zgodi, da se bo z bojem proti nedovoljeni trgovini na enem področju njena pojavnost zmanjšala. Sočasno pa bi se lahko povečala na sosednjih območjih. Ustrezno spremljanje je zato nujno, da bi se izognili tako imenovanemu učinku balona.

Zaključek

Pri obravnavi nezakonite trgovine morajo podjetja vzpostaviti zanesljive varnostne ukrepe za zaščito svojega premoženja, intelektualne lastnine in ugleda blagovne znamke. Mednarodne preiskave zahtevajo skrbno usklajevanje med različnimi zainteresiranimi stranmi, vključno z organi odkrivanja in pregona, pravnimi ekipami in ustreznimi vladnimi organi. Kot je bilo omenjeno, so v nadaljevanju navedene nekatere bistvene aktivnosti pri upravljanju mednarodnih preiskav, ki lahko vključujejo:

- Zbiranje obveščevalnih podatkov: Zbiranje natančnih in pravočasnih obveščevalnih podatkov je ključnega pomena za prepoznavanje nezakonitih trgovinskih dejavnosti in razumevanje obsega problema. To lahko vključuje spremljanje dobavnih verig, izvajanje tržnih raziskav in sodelovanje s kolegi iz panoge.
- Pravna in regulativna skladnost: Pri mednarodnih preiskavah je treba dobro poznati lokalne zakone, predpise in jurisdikcije. Skladnost s pravnimi zahtevami je bistvena za zagotavljanje veljavnosti dokazov in ohranjanje celovitosti preiskave. Ustrezno upravljanje je zato eden od najpomembnejših pogojev za uspešen boj proti nezakoniti trgovini.
- Partnerstva za sodelovanje: Vzpostavljanje trdnih odnosov z organi odkrivanja in pregona in drugimi ustreznimi organizacijami lahko poveča učinkovitost mednarodnih preiskav. Izmenjava informacij in sodelovanje pri skupnih operacijah lahko privedeta do boljših rezultatov.
- Tehnologija in analitika podatkov: Uporaba naprednih tehnologij in orodij za analizo podatkov lahko pomaga pri odkrivanju vzorcev, prepoznavanju ključnih akterjev, vpletenih v nezakonito trgovino, in razkrivanju skritih povezav. Kriminalistika, digitalna forenzika in analiza podatkov imajo ključno vlogo v sodobnih preiskavah.

To je le nekaj primerov, kaj bi podjetje lahko uvedlo ali bi moralo uvesti, da bi imelo učinkovito arhitekturo zaščite blagovnih znamk in pametno upravljanje mednarodnih preiskav na globalni ravni.

Ker bomo tej tematiki v okviru Instituta za korporativne varnostne študije (ICS) in Združenja za korporativno varnost v prihodnosti posvetili več pozornosti, bom ta članek zaključil z izpostavitvijo primerov dobre prakse v Sloveniji. Čeprav še vedno čakamo na uveljavitev sistemskih rešitev, želimo pohvaliti slovenske organe odkrivanja in pregona za njihove izjemne dosežke v številnih uspešnih akcijah. Vsi primeri jasno izpostavljajo, da je lahko borba proti nezakoniti trgovini tudi uspešna. ■

ZAVEZANI SMO H GRADNJI OMREŽIJ, KI SO VARNA, STABILNA IN ZANESLJIVA

VARNOST, BREZ KOMPROMISOV

HUAWEI

Avtor: Ddr. Aleš Jug / Slovensko združenje za požarno varstvo

POŽARNA VARNOST KOT POGOJ ZA ZAGOTAVLJANJE NEPREKINJENEGA POSLOVANJA PODJETJA

Osnovo za zagotavljanje požarne varnosti v podjetju najpogosteje predstavljajo predpisi. Preko teh država zagotavlja minimalno raven požarne varnosti in vseh ostalih elementov varnosti.

Po doktrini je ključni cilj požarnovarnostnih predpisov v Sloveniji in drugod po svetu varnost ljudi, ki se morajo v primeru požara hitro in varno evakuirati. Varnost premoženja je drugotnega pomena in je prepuščena lastniku oziroma investitorju. To pomeni, da mora za zagotavljanje ustreznih ravni požarne varnosti poskrbeti lastnik. Pri tem gre navadno za vprašanje in dilemo, kako visok nivo požarne varnosti zagotoviti. Temelj za to predstavlja analiza požarnih tveganj, ki pove do kakšnih požarnih scenarijev lahko v podjetju pride ter opredeli stopnjo požarne varnosti, ki se nanaša na organizacijske, tehnične in gradbene ukrepe. Požarnim tveganjem prilagojeni požarno varnostni ukrepi bodo preprečili, da požar napreduje iz prostora nastanka ter povzroči večjo materialno škodo na objektu in opremi. Kljub zgledno opravljeni oceni požarnih tveganj ter izvedenim požarno varnostnim ukrepom, pa lahko po požaru v podjetju še vedno prihaja do daljših zastojev v obratovanju. Eden od boljših požarnovarnostnih ukrepov je »šprinklerski« sistem za gašenje požarov. Ta vgrajena stabilna naprava za gašenje požarov bo v primeru požara opravila svojo funkcijo in ob pravilni izvedbi požar tudi pogasila. Zaradi vode, ki bo tekla iz »šprinklerskih« šob bo na opremi in objektu kljub visoki stopnji požarne varnosti še vedno nastala škoda, ki lahko povzroči daljše zastoje. Na popravilo ali zamenjavo z vodo poškodovanega stroja se lahko čaka tudi več mesecev, proizvodnja pa bo v tem času stala.

Ena od možnosti, da lahko v podjetju na temo varnosti naredijo več, je načrtovanje neprekinjenega poslovanja podjetja in uvedba politike neprekinjenega poslovanja podjetja. Le to se navadno poda v načrtu neprekinjenega poslovanja podjetja. Podlaga za izdelavo načrta neprekinjenega poslovanja podjetja je standard SIST EN ISO 22301:2019 - Varnost in vzdržljivost - Sistem vodenja neprekinjenosti poslovanja. Gre za kontinuiran proces preko katerega se podjetje pripravi na morebitne motnje, kot so naravne in druge nesreče, kibernetski vdori, požari in eksplozije, zapleti na domačih in tujih trgih in motnje v oskrbovalni verigi.

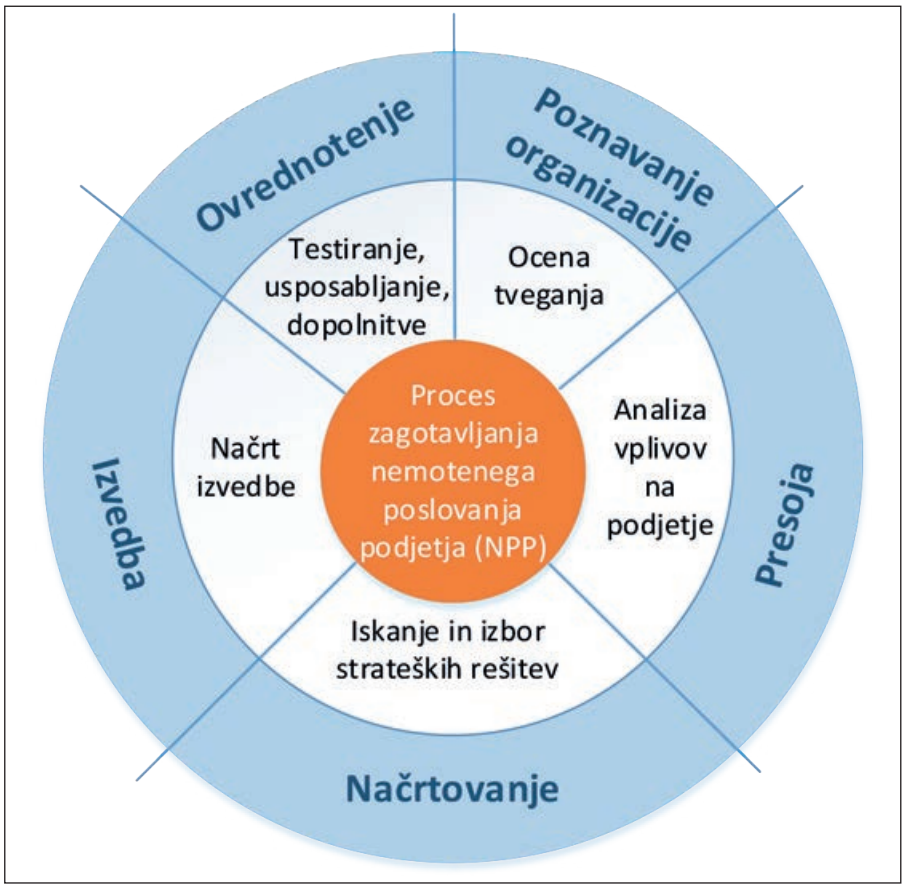
Po podatkih zbranih s strani zavarovalnice Allianz podjetjem v letu 2023 grozijo naslednja tveganja:

Požarnim tveganjem prilagojeni požarno varnostni ukrepi bodo preprečili, da požar napreduje iz prostora nastanka ter povzroči večjo materialno škodo na objektu in opremi. Kljub zgledno opravljeni oceni požarnih tveganj ter izvedenim požarno varnostnim ukrepom, pa lahko po požaru v podjetju še vedno prihaja do daljših zastojev v obratovanju.

- kibernetski napadi,
- motnje zaradi prekinitve poslovanja,
- makroekonomski trendi,
- energetske krize,
- spremembe predpisov,
- naravne katastrofe,
- klimatske spremembe,
- pomanjkanje kadrov,
- požari in eksplozije,
- politična tveganja in nasilje.

Našteta tveganja kažejo, da so podjetja skozi življenjski cikel izpostavljena celemu nizu nevarnosti. Varnost je zgolj ena izmed njih. Tako tuje kot domače analize kažejo, da je na motnje pripravljeno približno 30% večjih in okoli 20% manjših podjetij. Na letni bazi se z motnjo poslovanja, ki jo povzroči eno izmed prej naštetih tveganj, sooča skoraj vsako peto podjetje.

Izdelava načrta neprekinjenega poslovanja podjetja poteka preko več faz (slika 1), ki podjetju omogočajo celovit pregled nad tveganji, posledicami, pričakovanimi ukrepi, odzivom v primeru motnje in samem procesu okrevanja. Prva stopnja izdelave načrta neprekinjenega poslovanja podjetja je opredelitev tveganj in ogroženosti. Tu podjetje presodi, čemu in v kakšni meri je lahko izpostavljeno. Kot osnova velja najmanj seznam prej podanih tveganj.



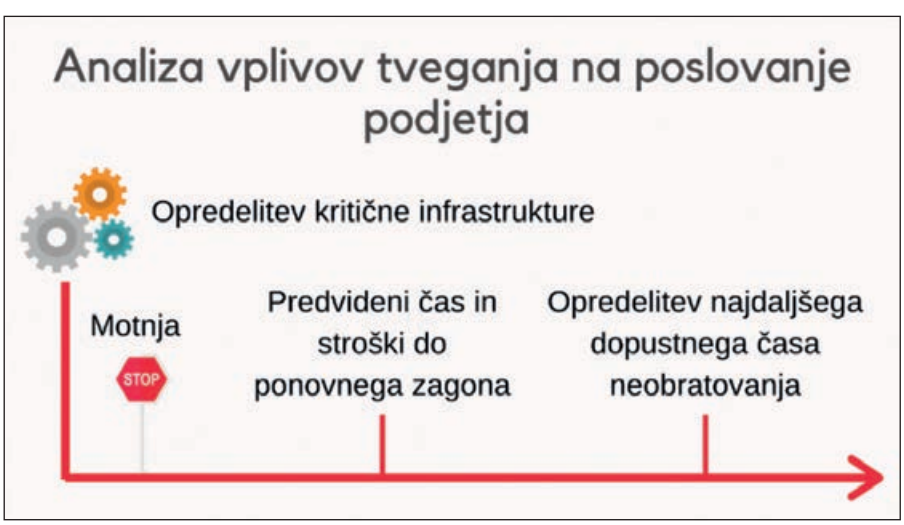
Slika 1: Faze v izdelavi načrta neprekinjenega poslovanja podjetja

Oceni tveganj sledi detajlna analiza vplivov prepoznanih tveganj na podjetje. Le to se izdela s pomočjo analize vplivov (business impact analysis). Analiza vplivov na poslovanje podjetja je sistematičen postopek za določitev in oceno možnih učinkov prekinitve na poslovanje, ki je posledica motnje, povzročene zaradi nesreče (npr. požar), motnje na trgu, motene dobave v oskrbovalni verigi ipd. Analiza se nanaša na cel spekter vplivov, ki so lahko finančni ali normativni (kazenska odgovornost, penali, ipd.).

Motnje lahko vplivajo na ugled podjetja, sprejem s strani kupcev, okolice ali družbe. Primer motnje v delovanju podjetja je večji požar. Zaradi nastale škode lahko proizvodnja v podjetju nekaj časa stoji. Zaradi tega lahko podjetje izgubi že sklenjen posel, plača zamudne obresti za kasnejšo dobavo izdelkov in izgubi zaupanje pri poslovnih partnerjih. V fazi analize vplivov mora podjetje določiti tudi ključne kadre in kritično infrastrukturo, nujno potrebno za neprekinjeno delovanje podjetja (prikazano na sliki 2). V fazi analize vplivov na poslovanje podjetja je potrebno opredeliti tudi dva pomembna merljiva dejavnika, in sicer: najdaljši dopustni čas ali obratovalni zastoj, ki si ga podjetje še lahko privošči in čas (ter s tem povezane stroške), ki ga podjetje rabi do ponovnega zagona. Na opredelitev najdaljšega dopustnega časa, ki si ga podjetje ob motnji lahko privošči, vplivajo že sklenjene pogodbe, razmerja med partnerji v oskrbovalni verigi, prisotnost konkurence ali npr. panoga v kateri podjetje deluje. V fazi opredelitve najdaljšega dopustnega časa, ki si ga podjetje ob motnji lahko privošči, si podjetje lahko zastavi enostavno vprašanje: »Koliko časa bo tržišče še toleriralo našo odsotnost?«

Analiza požarnih tveganj, podkrepljena s procesom zagotavljanja neprekinjenega poslovanja, lahko pokaže, da so ustrezna požarna zaščita strojne opreme plinasta gasila. Ta bodo požar pogasila, ob tem pa strojna oprema v prostoru ne bo poškodovana. Pri izdelavi načrta neprekinjenega poslovanja podjetja si mora podjetje kot cilj zastaviti, da je predviden čas do ponovnega zagona vedno krajši od najdaljšega dopustnega časa ne obratovanja. V nasprotnem primeru, ko predvideni čas do ponovnega zagona presega najdaljši dopustni čas ne obratovanja, se kdaj lahko zgodi, da konkurenca podjetje izpodrine ali pa mu odvzame tržni delež.

Kvalitetno narejena analiza vplivov prepoznanih tveganj na poslovanje podjetja je dobra osnova za načrtovanje neprekinjenega poslovanja podjetja in faz, ki sledijo. Hkrati omogoča analiza vplivov tudi dober vpogled v izvedeno varnost in tako dodatno podkrepi pomen varnosti v podjetju. S tem lahko rečemo, da je načrt neprekinjenega poslovanja podjetja navadno v podporo varnosti in kadrom, ki se na ravni podjetja ukvarjajo z varnostjo.



Slika 2: Ključni deli analize vplivov tveganja na poslovanje podjetja

Predviden čas do ponovnega zagona predstavlja čas, ko podjetje (proizvodnja linija ipd.) ne deluje ter čas, ki ga sistem potrebuje od zastoja do ponovnega zagona. Podjetje brez vgrajenega sistema za gašenje je lahko v primeru požara izpostavljeno daljšem času do ponovnega zagona. Požar lahko poškoduje objekt, stroje in drugo opremo, ki jo podjetje težko hitro nadomesti. S tem se podaljšuje čas do ponovnega zagona, kar hkrati vpliva tudi na povečevanje stroškov.

Fazi, ki sledita v izdelavi načrta neprekinjenega poslovanja podjetja, sta opredelitev ukrepov in načrt ukrepanj za zmanjšanje tveganj ter vzpostavitev skupine na ravni podjetja, ki bo skrbela za izdelavo, uvajanje in posodabljanje načrta neprekinjenega poslovanja podjetja. Pogosta praksa je, da vodstvo podjetja imenuje koordinatorja, ki bo skrbel za komunikacijo med vodstvom podjetja in skupino (pogosto odbor) za načrtovanje neprekinjenega poslovanja podjetja. Smernice in strategije načrtovanja neprekinjenega poslovanja podjetja morajo biti usklajene ter sprejete s strani vodstva podjetja.

Načrtovanje neprekinjenega poslovanja podjetja zahteva celovit pristop več služb na ravni podjetja, ki skupaj lahko realno ocenijo tveganja, politiko načrtovanja neprekainjenega poslovanja podjetja in sisteme, postopke in protokole, s katerimi se lahko podjetje izogne prekinitvi poslovanja, v primeru, da pride do prekinitve poslovanja, pa to v najkrajšem možnem času ponovno vzpostavijo.

Zadnja faza v procesu načrtovanja neprekinjenega poslovanja podjetja so neprestana testiranja, usposabljanje, priprave strategij in stalne dopolnitve načrta neprekinjenega poslovanja podjetja. Le na tak način v podjetju dosežejo, da zaposleni načrt poznajo, razumejo in se bodo znali odzvati hitro in učinkovito, ko bo to potrebno. V primeru, ko podjetja imajo načrt neprekinjenega poslovanja, so zato manj ranljiva, po motnji prej okrevajo in imajo navadno manjši negativen finančni vpliv v primeru tveganj.

Načrtovanje neprekinjenega poslovanja je postopek vzpostavitve mehanizmov prepoznavanja, preprečevanja in okrevanja v primerih, ko je podjetje izpostavljeno tveganjem. Poleg samega preprečevanja tveganj, je cilj načrtovanja neprekinjenega ravnanja podjetja predvideti in omogočiti tekoče poslovanje podjetja v času okrevanja. Kaže se, da imata v podjetjih z dorečeno politiko načrtovanja neprekinjenega poslovanja podjetja posebno mesto tudi varnost in zdravje pri delu, ter požarna varnost. Takšna podjetja se zavedajo, da bo lahko poškodovani ključni kader del kritične infrastrukture, od katerega je zelo odvisna izpolnitev že podpisane poslovne pogodbe. Tako dobi požarna varnost nov in s tem pomemben finančen pomen. ■

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

ZAKLJUČEK PROJEKTA PRECINCT IN KAJ SMO SE NAUČILI NA PRIMERU ŽIVEGA LABORATORIJA LJUBLJANA

V mesecu septembru se je z zadnjim sestankom v Bologni uspešno zaključil dvoletni evropski projekt PRECINCT, ki je bil financiran s strani Evropske komisije v programu HORIZON 2020 in je naslavljal varnostne izzive zaščite kritične infrastrukture, opredelitev možnih kompleksnih groženj za varnost te infrastrukture ter posledično razumevanje soodvisnosti in kaskadnih učinkov v primeru napada na posamezen sektor kritične infrastrukture.

V projektu je sodelovalo več kot 40 partnerjev iz 12 evropskih držav, ki so skozi štiri žive laboratorije (Living Labs oziroma krajše LL) preizkusili različna orodja in jih med seboj povezali v tako imenovano PRECINCT ekosistemsko platformo (PEP). Eden od laboratorijev je bil pozicioniran v Ljubljani, v njem pa so sodelovale naslednje organizacije: Slovenske železnice s podporo Prometnega instituta Ljubljana, Elektro Ljubljana (EL), Telekom Slovenije (TS), Ljubljanski potniški promet (LPP) in Mestna občina Ljubljana (MOL) z njeno službo Mestnega redarstva, vse skupaj pa je koordiniral Institut za korporativne varnostne študije (ICS).

Učinkovita komunikacija in sodelovanje med različnimi deležniki sta ključnega pomena za zagotovitev hitrega odziva in okrevanja med večjimi napadi. Celostni pristop, ki vključuje operaterje kritične infrastrukture, vladne organe, lokalne subjekte in državljane, je nujen za spopadanje s kompleksnostjo sodobnih groženj.

Za boljše razumevanje projekta bomo v tem odseku nekoliko osvetlili ozadje. Varno delovanje kritične infrastrukture je nepogrešljivo za normalno delovanje družbe. Medsebojna povezanost sektorjev in možnost kaskadnih učinkov zahteva celovit pristop, ki vključuje sodelovanje, komunikacijo in usklajevanje med različnimi deležniki. S sprejetjem celovite strategije, ki vključuje vse partnerje in poudarja pripravljenost, lahko družbe okrepijo svojo obrambo pred kibernetskimi in fizičnimi grožnjami ter zagotovijo neprekinjenost kritičnih storitev.

Pomemben izziv zaradi visoke soodvisnosti posameznih kritičnih infrastruktur so vsekakor možni kaskadni učinki, ki lahko nastanejo zaradi napadov ali motenj na kritični infrastrukturi. Ena sama krizna situacija lahko sproži učinek domin in razširi kaos na več sektorjev. To poudarja pomen usklajevanja med operaterji kritične infrastrukture za preprečevanje takšnih scenarijev. Učinkovita komunikacija in sodelovanje med različnimi deležniki sta ključnega pomena za zagotovitev hitrega odziva in okrevanja med večjimi napadi. Celostni pristop, ki vključuje operaterje kritične infrastrukture, vladne organe, lokalne subjekte in državljane, je nujen za spopadanje s kompleksnostjo sodobnih groženj. S spodbujanjem sodelovanja, odpravljanjem silosov in dajanjem prednosti odpornosti lahko krmarimo v razvijajoči se pokrajini kibernetskih in fizičnih groženj ter zagotovimo stabilno in varno družbo za prihodnje generacije.

LL Ljubljana z vsemi vključenimi akterji predstavlja zgleden primer kompleksnosti procesov in medsebojne povezanosti

*avtor je član Slovenskega združenja korporativne varnosti

različnih kritičnih infrastruktur. Izbrani operaterji kritične infrastrukture predstavljajo ravno tiste sektorje, ki so zaradi svoje dejavnosti najbolj izpostavljeni in predstavljajo osrednjo točko celotnega sistema kritične infrastrukture, in sicer oskrbo z električno energijo, telekomunikacije in transport. K temu dodajte še mesto Ljubljana z vso potrebno infrastrukturo in posredno vključenost služb prve pomoči. Vse to tvori skupek sodelujočih entitet, procesov in struktur medsebojnega prepletanja in sodelovanja, ki so bili ključni ne le za izvedbo aktivnosti LL Ljubljana, ampak za celoten projekt PRECINCT.

Velja posebej poudariti, da je specifičnost LL Ljubljana v tem, da je opravil pomembne analize in možne rešitve ter izvedbo pilotnih aktivnosti v pričakovanju bodočega koordinacijskega centra 3C (CI Coordination Centre), ki bi lahko nastal po dokončanju pomembnega prometnega vozlišča, ki se gradi v Ljubljani. To je dalo aktivnostim v okviru LL posebno težo, saj je namen tovrstnih projektov neposredno pridobljene izkušnje in dobre prakse preoblikovati v neposredno okolje delovanja. Ob že obstoječih organizacijskih in tehnoloških rešitvah se pojavljajo določene težave pri uvajanju novih pristopov, ki pogosto pomenijo spreminjanje starih, globoko zakoreninjenih vzorcev. Z nastankom popolnoma novih subjektov je ta prenos izkušenj in dobrih praks v neposredne projekte in kasneje operativne rešitve lahko učinkovitejši. Dejstvo, da bo vzpostavitev prometnega vozlišča v Ljubljani prinesla neposredno interakcijo delovanja različnih kritičnih infrastruktur, pomembnih za delovanje mesta in širše regije, je še kako pomembno z vidika rezultatov, ki jih prinaša LL preko projekta PRECINCT.

Testiranje orodij

Pri testiranju novih tehnoloških rešitev je bilo nekaj izzivov pri pravočasnem razvoju in pripravi le teh za proces testiranja. Na to je vplivalo predvsem zelo kratko trajanje tako kompleksnega projekta. Vendar je treba poudariti, da so vsi sodelujoči partnerji s svojim proaktivnim delovanjem poskrbeli, da so bili procesi testiranja in validacije na koncu uspešno zaključeni. V dveletnem obdobju je znotraj LL Ljubljana uspelo preizkusiti 14 orodij, ki jih lahko razdelimo v tri skupine:

- Digital Twin (DT), ki je povezal naslednja orodja: Unified PRECINCT Situational Awareness, Resilience Methodological Framework (RMF), Security and Privacy Monitoring tool, Cyber Range, Root Cause Analysis (RCA) in Test and Simulation (TaS), Complex Event Processing (CEP), Design Studio, Knowledge Graph (KG), Cascading Effects Simulation Engine (CESE), Data Mining Framework (DMF), Resilience Supervisory Control (RSC), Message Broker.
- Serious Game (SG), ki se uporablja za pomoč pri usposabljanju, simulaciji in napovedovanju kritične infrastrukture ter uporabi povratnih zank za povečanje učinkovitosti digitalnih dvojčkov.
- Cyber Range, ki je platforma za razvoj, dostavo in uporabo interaktivnih simulacijskih okolij. Simulacijsko okolje je predstavitev IKT, OT, mobilnih in fizičnih sistemov, aplikacij in infrastruktur organizacije, vključno s simulacijo napadov, uporabnikov in njihovih dejavnosti ter vseh drugih internetnih, javnih storitev ali storitev tretjih oseb, od katerih je lahko odvisno simulirano okolje.

V celotnem razvoju aktivnosti v LL Ljubljana lahko ugotovimo, da so rezultati presegli začetna pričakovanja. V celoti se je pokazalo, da zapletenih groženj, ki so jim danes izpostavljena mesta in njihova kritična infrastruktura, ni mogoče rešiti s silosnim pristopom reševanja vsakega deležnika zase.

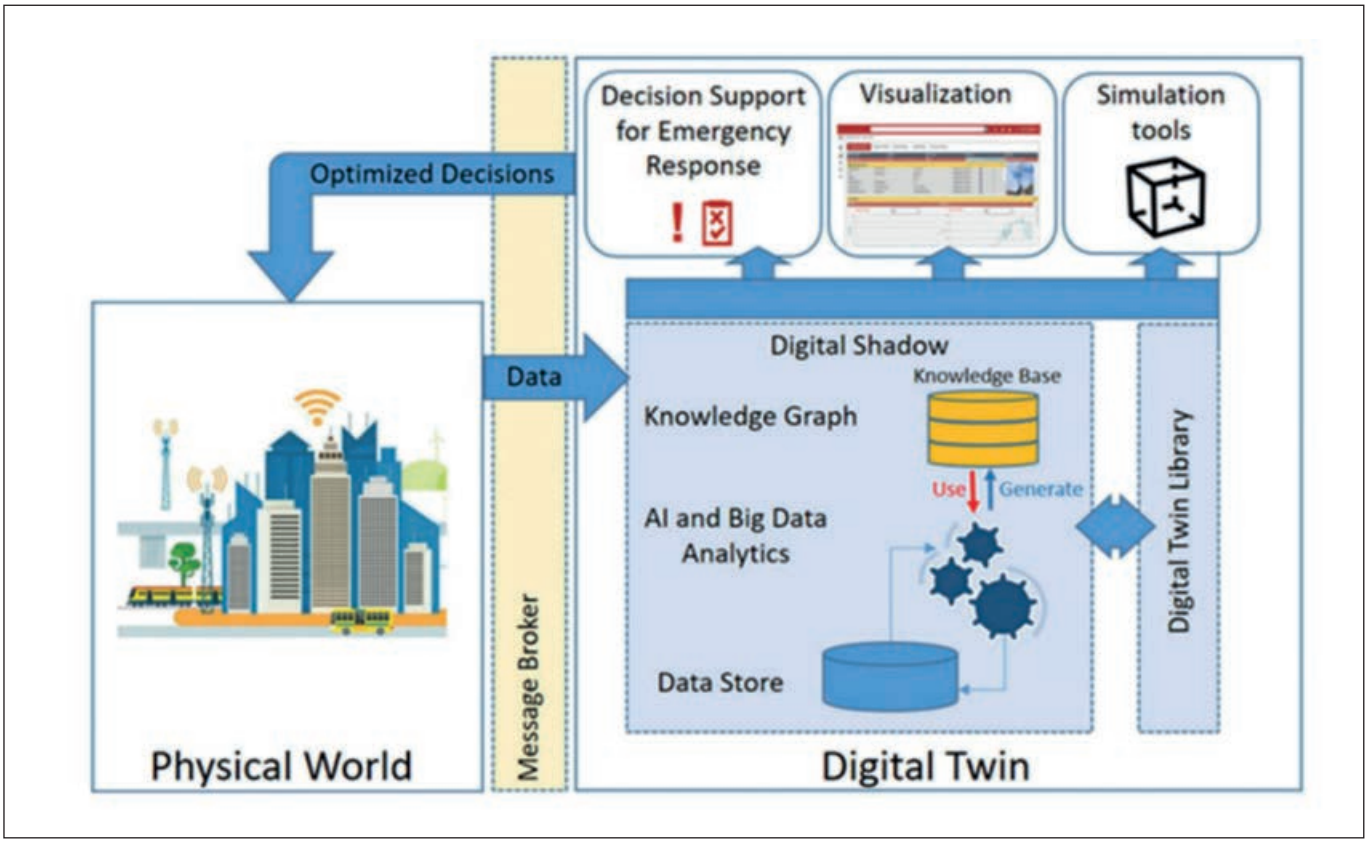
Zaključna faza projekta je bila namenjena testiranju teh orodij. Zaradi specifičnosti okolja so bila vsa testiranja izvedena v virtualnem okolju. Tako je bil pripravljen virtualni prostor za testiranje na Telekomu Slovenije, rezervni prostor pa je ponudil Inštitut za korporativne varnostne študije. V to okolje so se prenesla vsa orodja, hkrati je bil omogočen oddaljen dostop za vse partnerje projekta.

Glavno obdobje testiranja orodij PRECINCT je bilo od konca maja do začetka septembra 2023. Cilj je bil preizkusiti orodja skozi dva izbrana scenarija iz tako imenovane orodjarne PRECINCT, jih predstaviti končnim uporabnikom, deležnikom projekta ter pridobiti koristne povratne informacije.

Prvi scenarij je vseboval fizično grožnjo oz. bombni napad na kritično infrastrukturo, medtem ko je drugi scenarij vseboval kibernetski napad s hkratnimi DDoS napadi na kritične dele kritičnih industrijskih nadzornih sistemov (ICS) elektroenergetskih in komunikacijskih operaterjev, ki zagotavljajo pomembne storitve za neprekinjeno poslovanje transportnega vozlišča.

V okviru teh testiranj so sodelovali različni deležniki kritične infrastrukture, strokovnjaki varnostno operativnih centrov, varnostni menedžerji, odločevalci na nivoju kritične infrastrukture in nivoju lokalne uprave ter nekateri prvi posredovalci (npr. gasilci).

Testno obdobje je bilo razdeljeno na tri glavne faze. Prvi korak je bil namenjen usposabljanju, kjer so tehnični partnerji projekta predstavili nekatere zmožnosti orodij, ki so bila vkomponirana v skupni DT platformi. Drugi korak je bil namenjen testiranju dveh scenarijev v živem laboratoriju. Srečanje je bilo v obliki demonstracije, kjer smo pregledali vsa tri glavna orodja projekta PRECINCT - Digital Twin, Serious Games in Cyber Range Exercise. Zadnje orodje je bilo zasnovano in implementirano skupaj s Telekomom Slovenije. Z evalvacijo in diskusijo se se ugotovile pomanjkljivosti in dodatne zahteve, ki jih je bilo treba vključiti v rešitve. Po določenem času, potrebnem za posodobitev vseh orodij, je bil tretji korak namenjen predstavitvi končnih izdelkov. Za boljše razumevanje platforme PRECINCT je bil posebej predstavljen graf medsebojne odvisnosti in Cascading Effects Simulation Engine, ki sta najpomembnejši vgrajeni komponenti. Skozi ponovljeni fizični in kibernetski scenarij je test pokazal pomembne izboljšave na platformi DT.

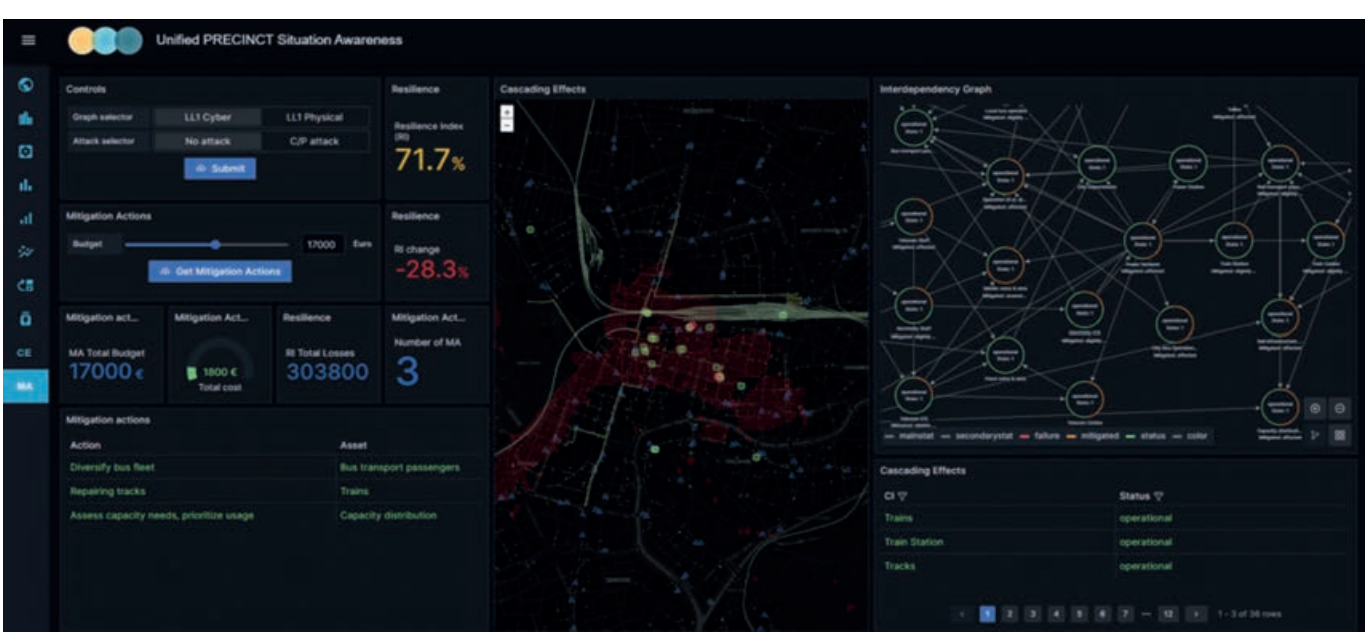


Slika 1: Arhitektura digitalnega dvojčka

Primer digitalnega dvojčka (DT)

Razvojni proces LL DT je vključeval sodelovanje različnih partnerjev. V sodelovanju z italijanskim partnerjem Engineering (ENG), ki je skrbel za tehnično podporo, so partnerji LL zbrali in zagotovili dragocene podatke, ki so bili ključni za izgradnjo natančne preslikave fizičnega sistema. V sliki 1 je predstavljena osnovna arhitektura digitalnega dvojčka.

Faza testiranja razvite rešitve za LL Digital Twin je vključevala aktivno vključevanje in sodelovanje s končnimi uporabniki. Ta pristop praktičnega testiranja je ENG-ju omogočil zbiranje dragocenih povratnih informacij od končnih uporabnikov, kar jim je omogočilo, da prepoznajo vsa področja izboljšave ali potrebne prilagoditve. Rezultat dela je bil integrirani DT LL. Na spodnji sliki je prikazan vmesnik, ki se integrira z orodjem za simulacijo kaskadnih učinkov (CESE), ki ga je razvil avstrijski partner AIT, super nadzorom odpornosti (RSC), ki ga je razvil partner BSC, in metodološki okvir odpornosti (RMF), ki ga je razvil partner RDS.



Slika 2: Integriran vmesnik DT platforme

Nekaj bistvenih izvlečkov projekta

V celotnem razvoju aktivnosti v LL Ljubljana lahko ugotovimo, da so rezultati presegli začetna pričakovanja. V celoti se je pokazalo, da zapletenih groženj, ki so jim danes izpostavljena mesta in njihova kritična infrastruktura, ni mogoče rešiti s silosnim pristopom reševanja vsakega deležnika zase. Kritična infrastruktura in nasploh družbeni procesi so se tako prepletli, da se ob vsakem malo večjem kritičnem dogodku takoj pojavi določen kaskadni učinek med soodvisnimi kritičnimi infrastrukturami. V primeru LL so bili vključeni najbolj izpostavljeni sektorji kritične infrastrukture, energetika, telekomunikacije in prometa ter mestne in državne institucije, ki so z aktivacijo prvih posredovalcev prvi porok za uspešen nadzor in obvladovanje kriznih dogodkov. Osnovne analize so pokazale zavidljivo raven organiziranosti posameznih sistemov znotraj posamezne kritične infrastrukture, nadaljnje analize pa so pokazale bistveno pomanjkanje koordinacije in komunikacijskih sistemskih pristopov za medsektorsko sodelovanje in sodelovanje na kompleksni ravni večjih urbanih območij.

Izbrani primeri scenarijev, še bolj pa točke izvedenih napadov, so bili skrbno izbrani in so pokazali, da lahko ciljani kombinirani napadi bistveno zmanjšajo delovanje celotnega nabora vključenih operaterjev kritične infrastrukture. Te analize so pripomogle k dvigu ozaveščenosti sodelujočih operaterjev na višjo raven, kar je bil tudi dober predpogoj za kasnejše aktivno sodelovanje pri vseh aktivnostih razvoja in testiranja tehnoloških zmogljivosti ter iskanju novih procesnih možnosti za izboljšanje koordinacije in učinkovitejšega upravljanja kriznih situacij.

Novi tehnološki pristopi so pokazali, da lahko služijo kot učinkovito orodje pri zagotavljanju ključnih aktivnosti, kot so boljše situacijsko zavedanje, vizualizacija in zgodnje odkrivanje incidentnih dogodkov, kar operaterjem na vseh ravneh omogoča boljše in hitrejše odločanje. Z dodatno možnostjo simulacij in napovedi je možno tudi dodatno usposabljanje sodelujočih strokovnjakov na vseh ravneh odločanja. Posebej velja izpostaviti izboljšanje situacijskega razumevanja s tem, da operaterji v posameznih centrih delovanja kritične infrastrukture prejemajo povratne informacije o aktivnostih, ki jih izvajajo v sosednjih soodvisnih kritičnih infrastrukturah. Prav zaradi vse močnejše medsebojne odvisnosti so te informacije ključne za ustrezen in pravočasen odziv, ki ima za posledico obvladovanje širših kriznih situacij, kot je obvladovanje kriznih dogodkov na lastni infrastrukturi.

Ustrezne primerjave in analize skozi aktivnosti LL so pokazale, da je v primeru izbranih lokacij v LL zelo velika verjetnost negativnih kaskadnih učinkov med različnimi infrastrukturami. Veliko teh izzivov je mogoče izboljšati z uvajanjem novih procesov in tehnoloških pristopov, ki so bili nakazani v LL in izvedeni preko ti 3C koordinacijskega centra.

V nadaljevanju si oglejmo nekatere bistvene ocene sodelujočih operaterjev, ki smo jih združili po posameznih sektorjih KI.

Prometni sektor

Združevanje dela več različnih služb na način, kot ga še ni bilo. S simulacijo fizičnih in kibernetskih napadov se je pridobilo prepotrebne izkušnje in znanje o sodelovanju z drugimi partnerji na lokaciji LL v izrednih razmerah. Predvsem pa je pomembno, da se s takim sodelovanjem vzpostavi in prepreči nadaljnja škoda in posledice v kriznih situacijah.

LPP se je pridružil projektu z zavedanjem, da so na varnostnem področju nepripravljeni. Do tega projekta so se srečevali z manjšimi incidenti v smislu izgredov na avtobusih. Pripravljenost na večje dogodke, ki bi močno posegli v samo obratovanje javnega potniškega prometa, pa je bilo omejeno. Skozi sam projekt PRECINCT in skozi posamezne korake, so spoznavali, kakšne so povezave in soodvisnosti med upravljalci kritične infrastrukture. Prav tako so spoznali, kakšne posledice ima lahko kibernetski napad na kritično infrastrukturo. V grafu soodvisnosti so se pokazale povezave in odvisnost od neoviranega delovanja ostale kritične infrastrukture. Fizičen napad in s tem prekinitev oziroma motnje v obratovanju so za LPP hujšega pomena, saj je s tem lahko onemogočeno izvajanje javnega potniškega prometa. Skozi projekt so spoznali, kako zelo pomembna je sistemska ureditev komunikacije med upravitelji kritične infrastrukture. Že sam vpliv različnih kritičnih infrastruktur na lokalnem ali državnem nivoju je stvar, ki ni bila ustrezno naslovljena. V sklopu projekta se je pod okriljem Mestnega redarstva postavilo temelje za razvoj sistemske komunikacijske platforme na podlagi katere so določene smernice, kako v prihodnje sistemsko in trajno urediti komuniciranje med deležniki – upravljalci kritične infrastrukture.

Z DT platformo in SG orodjem se je prikazal možen način simulacij izrednih dogodkov. S temi orodji si bodo v prihodnje lahko pomagali pri razvoju zaščite in prenovi postopkov v primeru izrednih dogodkov.

Energetski sektor

Glavna korist za Elektro Ljubljana je bila, da se je naučil izboljšati odziv v primeru fizičnega napada. Tudi analiza obstoječega odziva v primeru kibernetskega napada in primerjava s predlaganimi koraki projekta PRECINCT predstavlja zelo dobro izkušnjo. Projekt je omogočil ponovno odkritje medse-

Po koncu projekta lahko zaključimo, da je PRECINCT prinesel zelo pozitivne rezultate za LL v Ljubljani. S tako kompleksnim okoljem, ki vključuje veliko število operaterjev kritične infrastrukture iz različnih sektorjev, je res ponudil celo paleto možnosti za nadgradnjo razumevanja in pomena soodvisnosti in vplivov kaskadnih učinkov.

bojne povezanosti med drugimi lastniki KI in prvič specifičen odnos z Mestno občino Ljubljana. Projekt daje tudi potrditev, da so preventivni ukrepi Elektra Ljubljana proti kibernetskim napadom in načrt odzivanja v primeru kakršne koli fizične poškodbe omrežja v dobrem stanju.

Telekomunikacijski sektor

Eden glavnih izzivov Telekoma Slovenije predstavlja naraščanje grožnje kibernetskih napadov tako na samo podjetje in njegovo infrastrukturo kot na njegove stranke. S tem namenom je bil ustanovljen Operativni center za kibernetsko varnost (OCKV), ki nadzoruje tovrstne napade in analizira prihodnje grožnje. S pomočjo EU projekta PRECINCT je Telekom pridobil vpogled v dodatna orodja za spopad s tovrstnimi grožnjami, kot so na primer resne igre (Serious Games), digitalni dvojček (Digital Twin) in orodja za analizo odpornosti omrežja. Prvič se je obravnavalo tudi kombinirane in kaskadne napade, kjer se analizira možnost hkratnega kibernetskega in fizičnega napada in njunih posledic ter posledic napadov na druge upravljalce kritične infrastrukture, ki bi lahko vplivale na Telekomovo telekomunikacijsko omrežje.

Sektor mestne uprave

Projekt PRECINCT je imel številne pomembne vplive na Mestno občino Ljubljana. Pridobili so vpogled v trenutno stanje pripravljenosti mestnih služb in KI na kaskadne dogodke in možnosti za izboljšanje. V sklopu projekta so se povezale mestne službe, ki so zadolžene za upravljanje s KI in s tem pridobile vpogled v njihovo delovanje ter medsebojno povezanost. Poudariti je potrebno izjemno pomembno povezovanje, sodelovanje in izmenjavo informacij tako znotraj mesta, kot tudi z zasebnimi deležniki. Koncept 3C koordinacijskega centra predstavlja dobro izhodišče za morebitno nadaljnje delo in razvoj v smeri izmenjave informacij med javnim in zasebnim sektorjem, kar bi lahko posledično vodilo v izboljšanje zaznavanja in posredovanja v primeru kaskadnih dogodkov. Ljubljana je s preizkušanjem tehnoloških rešitev projekta PRECINCT pridobila dragoceno znanje, ki ga lahko mesto uporabi za izvajanje preventivnih ukrepov zaščite KI in oblikovanje odziva. Ugotovitve projekta bodo v pomoč pri oblikovanju digitalne platforme mesta in varnostno nadzornega centra Mestne občine Ljubljana. Poleg tega je s sodelovanjem v projektu mesto pridobilo nove kontakte ter izkazalo svoje prioritete, ki so usmerjene v razvoj pametnega mesta in trajnostnega razvoja, katerega prioriteta je večja varnost v mestu.

Zaključek

Po koncu projekta lahko zaključimo, da je PRECINCT prinesel zelo pozitivne rezultate za LL v Ljubljani. S tako kompleksnim okoljem, ki vključuje veliko število operaterjev kritične infrastrukture iz različnih sektorjev, je res ponudil celo paleto možnosti za nadgradnjo razumevanja in pomena soodvisnosti in vplivov kaskadnih učinkov.

Nadgradnja zavedanja upravljavcev kritične infrastrukture, da so pri zagotavljanju delovanja svoje infrastrukture v resnični soodvisnosti z drugimi kritičnimi infrastrukturami, je neprecenljiva. Na podlagi realnih scenarijev so bili dodatno vzpostavljeni novi procesni modeli sodelovanja, komuniciranja in skupnega reševanja določenih kriznih situacij, ki imajo medsektorski vpliv. S tovrstnim sodelovanjem se gradi in krepi mreža medsebojnih povezav tako na operativni kot strateški ravni, kar pomeni neprecenljivo dodano kakovost za hitrejše odzivanje v kriznih situacijah. Skozi projekt je bila izvedena tudi interakcija s ciljnimi okolji izven ožjega kroga projektnih partnerjev, kar je prispevalo k ozaveščanju o pomenu nekaterih ključnih ukrepov, ki so potrebni za zagotavljanje kontinuitete delovanja kritičnih družbenih vozlišč v mestu Ljubljana.

Kljub celemu nizu tehnoloških izzivov, ki se pojavljajo ob tako raznolikem naboru sodelujočih partnerjev iz različnih sektorjev KI, so se nekateri ključni pozitivni učinki pokazali tudi na tehnološkem področju. Tehnološke rešitve izboljšujejo potrebne informacije za boljše zavedanje situacije, hitrejše odzivanje ter učinkovitejšo komunikacijo in koordinacijo na vseh ravneh delovanja.

Kljub zahtevnemu časovnemu vidiku pri razvoju tehnologij, saj sta bili projektu namenjeni le dve leti, so bile vse tehnološke rešitve ustrezno testirane znotraj LL. Povratne informacije končnih uporabnikov so bistvena dodana vrednost za razvijalce tehnologij v procesu nenehnega izboljševanja tehnoloških rešitev. Z vidika uporabnika je možnost testiranja novih tehnologij zagotovo tista dodana vrednost, ki skozi tovrstne pilotne situacije, kot jih predstavlja LL, vodi do potrebnih informacij za morebitno uvedbo in nadgradnjo tehnologij, predvsem z namenom boljšega zavedanja situacije, hitrejšega reagiranja ter učinkovitejše komunikacije in koordinacije na vseh ravneh delovanja. ■

PRECINCT

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

Praktične rešitve za upravljanje tveganj na področju kritične infrastrukture in izvajanja bistvenih storitev

Zakon o kritični infrastrukturi in Zakon o informacijski varnosti s pripadajočimi navodili od upravljavcev kritične infrastrukture in izvajalcev bistvenih storitev med drugim zahtevajo, da analizirajo tveganja ter izvajajo ukrepe za njihovo obvladovanje in evidentirajo škodne dogodke.

V čem je težava?

V praksi je precej izzivov že pri analizi tveganj sredstev in virov v skladu z načeli celovitosti, razpoložljivosti in zaupnosti.

Nalogo dodatno otežujejo neskladja med navodili, ki se jim običajno pridružujejo še usmeritve in zahteve standardov za informacijsko varnost ISO/IEC 27000.

Nepriročno in varnostno vprašljivo pa je tudi obvladovanje podatkov v preprostih preglednicah in podobnih evidencah, na podlagi katerih poročamo in dokazujemo skladnost nadzornim organom.

Kako vam lahko pomagamo?

Upravljavcem kritične infrastrukture in izvajalcem bistvenih storitev lahko pomagamo na več načinov, kot so:

- Svetovalna podpora pri izdelavi analize tveganj in vzpostavitvi celovitega sistema upravljanja tveganj, ki upošteva zahteve predpisov in standarda ISO/IEC 27001.
- Informacijska rešitev Silver Bullet Risk za obvladovanje podatkov o tveganjih, ukrepih in škodnih dogodkih ter pripadajoča poročila na enem mestu.
- Sodelovanje pri načrtovanju in uvajanju sistemov neprekinjenega poslovanja v skladu s standardom ISO 22301.

Za več informacij ali pogovor nam pišite na naslov **info@silverbulletrisk.com**.

Avtor: Matic Čaleta / Certificirani etični heker, Institut za korporativne varnostne študije*

RAZVOJ UMETNE INTELIGENCE IN IZZIVI NA PODROČJU KIBERNETSKE VARNOSTI

Umetna inteligenca (UI) močno vpliva na kibernetsko varnost, saj prinaša revolucionarne metode za prepoznavanje in odzivanje na digitalne grožnje. Kljub njenim prednostim v obrambi, pa se UI lahko zlorabi za izvedbo naprednih in ciljanih kibernetskih napadov, kar postavlja varnostne strokovnjake pred nove izzive.

V sodobnem digitalnem okolju sta umetna inteligenca (UI) in kibernetska varnost postali neločljivo povezani. UI, ki posnema človeške sposobnosti razmišljanja, je v zadnjem času doživela velik napredek, zahvaljujoč napredkom v računalniški moči, algoritmih in dostopnosti do podatkov. Z razvojem digitalne tehnologije, pa se povečuje tudi število kibernetskih groženj. Zaščita pred temi grožnjami je postala nujna in tukaj UI ponuja nove priložnosti za detekcijo in preprečevanje napadov. S pomočjo umetne inteligence lahko hitro prepoznamo sumljive dejavnosti in se prilagodimo novim grožnjam. Seveda pa to prinaša tudi izzive, kot so zasebnost in etična vprašanja. Pričakovati pa je, da bo kljub tem izzivom vloga UI v kibernetski varnosti v prihodnje še bolj pomembna.

Umetna inteligenca v detekciji groženj

V današnjem digitalnem okolju, kjer se podatki kopičijo z eksponentno hitrostjo, je postalo skoraj nemogoče ročno spremljati in analizirati vse potencialne kibernetske grožnje v realnem času. V tem kontekstu je umetna inteligenca postala ne le koristna, ampak tudi nujna komponenta v boju proti kibernetskim grožnjam.

Tradicionalne varnostne rešitve, kot so protivirusni programi, imajo svoje omejitve. Te se večinoma zanašajo na podpisne baze, ki vsebujejo informacije o znanih grožnjah, kot so virusi in trojanski konji. Čeprav so te baze redno posodobljene, imajo ključno pomanjkljivost, in sicer nezmožnost prepoznavanja novih ali neznanih groženj, ki še niso bile dodane v bazo.

Tukaj pride na vrsto umetna inteligenca s svojimi pristopi, kot je strojno učenje. Ta tehnologija omogoča varnostnim sistemom, da se „učijo“ iz preteklih podatkov in prepoznajo sumljive vzorce, ki se lahko razlikujejo od znanih groženj. Na primer, če se aplikacija nenadoma začne obnašati drugače ali če se poveča količina omrežnega prometa iz določenega vira, lahko to kaže na potencialni varnostni incident.

Umetna inteligenca je v tem kontekstu postala nepogrešljivo orodje, saj omogoča avtomatizacijo odziva na incidente in s tem povečuje učinkovitost in hitrost varnostnih ekip.

Umetna inteligenca v odzivanju na incidente

V svetu kibernetske varnosti je hitrost odziva ključnega pomena. Ko se pojavi varnostni incident, je vsaka sekunda dragocena. Zamuda pri odzivanju lahko povzroči večjo škodo, izgubo podatkov ali celo finančne izgube. Umetna inteligenca je v tem kontekstu postala nepogrešljivo orodje, saj omogoča avtomatizacijo odziva na incidente in s tem povečuje učinkovitost in hitrost varnostnih ekip.

*avtor je član Slovenskega združenja korporativne varnosti

Avtomatizacija odziva na varnostne incidente s pomočjo UI

Tradicionalno odzivanje na varnostne incidente pogosto zahteva ročno posredovanje varnostnih strokovnjakov. To lahko vključuje analizo datotek, preverjanje sistema za znake vdora ali izvajanje ukrepov za izolacijo in odpravo groženj. Vendar pa je v velikih in kompleksnih omrežjih ročno odzivanje lahko počasno in neučinkovito. Z uporabo umetne inteligence je mogoče v procesu odzivanja na incidente avtomatizirati številne korake. Sistemi, ki temeljijo na UI, lahko samodejno zaznajo grožnjo in analizirajo njeno naravo. Avtomatizacija odziva na incidente pa s pomočjo UI prinaša številne prednosti, kot so hitrost, učinkovitost, natančnost in prilagodljivost.

Umetna inteligenca v analizi ranljivosti

Kibernetska varnost je nenehna tekma med napadalci in potencialnimi žrtvami. Medtem, ko na eni strani napadalci vztrajno iščejo nove načine za izkoriščanje sistemov, so na drugi strani tisti, ki se trudijo identificirati in odpraviti te ranljivosti, preden jih napadalci lahko izkoristijo.

Kako UI pomaga pri predvidevanju potencialnih točk napada

Ena izmed ključnih prednosti uporabe umetne inteligence v analizi ranljivosti je njena sposobnost predvidevanja. Namesto, da bi se osredotočala samo na znane ranljivosti, lahko UI analizira sisteme in njihovo vedenje, da bi predvidela, kje se lahko pojavijo nove ranljivosti. Na primer, UI lahko analizira način, kako se različne komponente sistema medsebojno povezujejo in prepozna potencialne točke napada, ki bi jih človeški analitik morda spregledal. Poleg tega lahko uporablja tehnike, kot so simulacija ali modeliranje, da bi „testirala“ sistem v varnem okolju in predvidela, kako bi se ta lahko odzval na različne vrste napadov.

Umetna inteligenca pri naprednih napadih

Ko govorimo o umetni inteligenci (UI) v kontekstu kibernetske varnosti, pogosto razmišljamo o njeni vlogi pri obrambi pred grožnjami. Vendar pa je UI dvostranski meč, saj jo lahko uporabljajo tudi napadalci za izvedbo naprednih in sofisticiranih napadov. Z razvojem tehnologije so se razvijale tudi metode napadov, ter postajale bolj zapletene in težje zaznavane. Napadalci uporabljajo umetno inteligenco za avtomatizacijo in optimizacijo svojih napadov. Na primer, s pomočjo UI lahko ustvarijo napredne phishing napade, kjer se sporočila prilagajajo posameznemu uporabniku in tako povečajo

verjetnost uspešnega napada. UI lahko analizira pretekle komunikacije in ustvari prepričljivo lažno sporočilo, ki se zdi legitimno. Poleg tega se UI uporablja tudi za avtomatizacijo napadov na več ciljev hkrati. Napadalci lahko uporabljajo algoritme, ki samodejno prepoznajo ranljive sisteme na spletu in jih napadejo brez človeškega posredovanja.

Vpliv UI na varnost odprtokodnih programov

Odprtokodni programi so postali temelj sodobne tehnološke infrastrukture. Mnoge organizacije in posamezniki se zanašajo na odprtokodne rešitve zaradi njihove prilagodljivosti, transparentnosti in skupnostne podpore. Vendar pa odprta narava teh programov prinaša tudi svoje varnostne izzive. Umetna inteligenca (UI) igra ključno vlogo pri obravnavi teh izzivov, hkrati pa poveča tveganje za varnost.

UI lahko pomaga pri izboljšanju varnosti odprtokodnih programov na več načinov:

- Avtomatizirano testiranje: UI lahko avtomatizira proces testiranja kode, da bi našla in odpravila potencialne ranljivosti. S pomočjo strojnega učenja se lahko sistemi „naučijo“ prepoznati sumljive vzorce v kodi, ki lahko kažejo na varnostne pomanjkljivosti.
- Analiza obnašanja: UI lahko analizira, kako se odprtokodni programi obnašajo v realnem okolju, da bi prepoznala nenavadne ali sumljive aktivnosti, ki bi lahko bile znak napada ali zlorabe.
- Skupnostna analiza: Ker so odprtokodni programi pogosto razvijani s pomočjo skupnosti, lahko UI analizira komunikacijo in sodelovanje med razvijalci, da bi prepoznala potencialne grožnje ali sumljive dejavnosti.

Kljub prednostim, ki jih UI prinaša, obstajajo tudi izzivi in tveganja, povezana z varnostjo odprtokodnih programov kot je npr. transparentnost kode. Medtem, ko je transparentnost odprtokodnih programov ena izmed njenih glavnih prednosti, lahko to tudi poveča tveganje. Napadalci lahko preučujejo kodo, da bi našli in izkoristili ranljivosti, pri čemer jim UI lahko v veliki meri pomaga.

Umetna inteligenca v spletnih prevarah

Spletne prevare so že dolgo del digitalnega sveta, vendar je z razvojem umetne inteligence (UI) postalo omogočeno ustvariti bolj prepričljive in sofisticirane napade. Posebej zaskrbljujoče je, kako se UI uporablja za ustvarjanje ponarejenih glasov, posnetkov in drugih medijskih vsebin, ki jih je težko ločiti od resničnih.

Uporaba UI za ustvarjanje ponarejenih glasov in posnetkov

Tehnologije, kot so „deepfakes“, uporabljajo napredne algoritme strojnega učenja za ustvarjanje zelo realističnih, a ponarejenih video posnetkov. Z uporabo velikih količin podatkov, kot so slike ali posnetki osebe, lahko ti algoritmi ustvarijo video, kjer ta oseba govori ali počne stvari, ki jih v resnici ni nikoli storila. Podobno pa se UI uporablja tudi za ustvarjanje ponarejenih glasov, kar se lahko uporabi za ustvarjanje lažnih telefonskih klicev ali sporočil. Take prevare lahko vodijo do izsiljevanja, širjenja lažnih novic ali celo lažnih navodil s strani vodilnega kadra v določenem podjetju.

Prihodnost umetne inteligence v kibernetski varnosti

Kot ena izmed najhitreje rastočih tehnologij v zadnjem desetletju, je umetna inteligenca (UI) močno vplivala na številna področja, vključno s kibernetsko varnostjo. Njena sposobnost obdelave ogromnih količin podatkov in avtomatizacije kompleksnih nalog je prinesla revolucijo v načinu, kako se soočamo s kibernetskimi grožnjami.

Kot ena izmed najhitreje rastočih tehnologij v zadnjem desetletju, je umetna inteligenca (UI) močno vplivala na številna področja, vključno s kibernetsko varnostjo. Njena sposobnost obdelave ogromnih količin podatkov in avtomatizacije kompleksnih nalog je prinesla revolucijo v načinu, kako se soočamo s kibernetskimi grožnjami.

Kaj lahko pričakujemo v prihodnosti?

V prihodnosti kibernetske varnosti bomo priča revolucionarnim spremembam, ki jih bo prinesla umetna inteligenca (UI). Sistemi kibernetske varnosti bodo postali bolj avtonomni, z zmožnostjo samostojnega učenja in prilagajanja novim grožnjam brez potrebe po človeškem posredovanju. Namesto tradicionalnega reaktivnega pristopa k obrambi se bo UI osredotočila na proaktivno iskanje in preprečevanje potencialnih napadov, še preden se zgodijo. Ta napredna tehnologija bo tesno integrirana z drugimi inovativnimi tehnologijami, kot so kvantni računalniki, blockchain in internet stvari (IoT), ki bodo skupaj zagotavljali celovito varnostno rešitev.

Uporaba umetne inteligence (UI) v kibernetski varnosti odpira kompleksna etična vprašanja, ki zahtevajo nujno pozornost. Na primer, kdo nosi odgovornost, če sistem, ki temelji na UI, napačno identificira kibernetsko grožnjo? Ali je etično sprejemljivo, da se UI uporablja za proaktivno iskanje potencialnih groženj, če to pomeni invaziven nadzor nad uporabniki? Poleg tega se poraja tudi vprašanje transparentnosti, kako odprti in jasni smo lahko glede delovanja teh algoritmov, ne da bi s tem ogrozili varnost?

Te etične dileme predstavljajo resne izzive za zakonodajalce, strokovnjake za kibernetsko varnost in končne uporabnike. Vsi vpleteni bodo morali skupaj najti uravnotežene rešitve, da se zagotovi etična uporaba umetne inteligence v okviru kibernetske varnosti.

Zaključek

V sodobnem digitalnem svetu, kjer se količina podatkov in povezav med napravami eksponentno povečuje, je kibernetska varnost postala ena izmed najpomembnejših tematik. Umetna inteligenca (UI) zavzema osrednje mesto v tej bitki za varnost, saj prinaša revolucionaren pristop k obvladovanju kibernetskih groženj. Grožnje se nenehno spreminjajo in razvijajo, zato morajo tudi varnostne rešitve ostati korak pred njimi. Umetna inteligenca, s svojo sposobnostjo učenja in prilagajanja, je idealno orodje za to nalogo. Vendar pa je pomembno, da se ne zanašamo izključno na tehnologijo. Človeški dejavnik ostaja ključnega pomena, bodisi pri razvoju in izvajanju varnostnih strategij, bodisi pri prepoznavanju in odzivanju na grožnje. Umetna inteligenca je močno orodje, vendar pa mora delovati v simbiozi s človeškimi strokovnjaki, da zagotovi najboljšo možno zaščito.

Za konec pa, umetna inteligenca je in bo še naprej igrala ključno vlogo v kibernetski varnosti. Z nenehnim razvojem in prilagajanjem bomo lahko zagotovili, da bodo naši digitalni svetovi varni in zaščiteni pred grožnjami, ki jih prinaša prihodnost.

Viri in literaura

Zhang, Z., Ning, H., Shi, F. *et al.* Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artif Intell Rev 55*, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0

Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN COMPUT. SCI.* 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

Rammanohar Das and Raghav Sandhane 2021 *J. Phys.: Conf. Ser.* 1964 042072

A. Ali *et al.*, „The Effect of Artificial Intelligence on Cybersecurity," *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ICBATS57792.2023.10111151 ■

Avtor: Aleš Ribič / direktor HSI d.o.o.*

PRENOS ALARMNIH SPOROČIL VSE PREVEČKRAT SPREGLEDAN DEJAVNIK POMEMBNOSTI

Prenos alarmnih sporočil je ključen gradnik alarmnega sistema. Le ta zagotavlja varen prenos sporočila od alarmne centrale do nadzornega centra. Da lahko zagotovimo zanesljiv in varen prenos sporočil, je potrebno pogledati širši vidik tega področja.

Na področju zagotavljanja ustreznega sistemskega pristopa upravljanja tehničnih sistemov varovanja je vse prevečkrat spregledana pomembnost prenosa alarmnih sporočil. Če želimo, da bodo omenjeni sistemi naročniku zagotavljali osnovno poslanstvo skozi učinkovit mehanizem varovanja premoženja, potem je potrebno razumeti vse njegove sestavne dele. Prenos alarmnih sporočil je eden od njih. Zahteva dovolj pozornosti, da je oblikovan v smeri varnega in hitrega prenosa alarmnih signalov na eni strani, na drugi strani pa dovolj enostavnega upravljanja, ki strokovnim osebam v organizacijah ne povzroča preveč operativnih težav pri nastavitvah in vzdrževanju. Za podrobnejšo razjasnitev postavljene teze je potrebno osvetliti nekaj pomembnih aspektov, ki bodo pomembno pripomogli k jasnejšemu razumevanju obravnavane problematike.

Zajem sporočil iz alarmne centrale

Proizvajalci alarmnih central že dolga leta nudijo telefonsko linijo kot primarni način prenosa alarmnih sporočil. Telefonska linija na strani ponudnika je skozi leta doživela kar nekaj preobrazb. Od klasične analogne linije, ISDN linije do VoIP linije. Slednji dve omogočata simulacijo klasične analogne linije s pomočjo posebnega vmesnika. Vsi ti vmesniki imajo, zaradi pretvorbe analognega v digitalni signal, določeno kompresijo, ki vpliva na kvaliteto prenosa alarmnega sporočila.

Problematika na tem področju je, da se analogne linije ne uporabljajo več, oziroma je po njih prenos iz dneva v dan bolj težaven. Pojavljajo se napake v prenosu, kar posledično pomeni daljši čas prenosa alarma na VNC, ali pa se celo zgodi, da dogodek sploh ni prenesen v VNC. V zadnjih letih se pojavljajo IP vmesniki, ki omogočajo prenos alarmnih sporočil preko interneta. Te vmesnike nudijo tako proizvajalci alarmnih central, kot tudi določena specializirana podjetja. Da tovrstni vmesniki delujejo z VNC-jem, mora proizvajalec zagotoviti tudi ustrezen sprejemnik alarmnih sporočil.

Pomanjkljivosti, ki jih imajo taki vmesniki so, da so kompatibilni samo z določenimi alarmnimi centralami znotraj istega proizvajalca. V večini imajo svoj protokol, ki ni javno dostopen, za programiranje in nastavljanje pa je potrebno ustrezno dodatno znanje.

Na področju zagotavljanja ustreznega sistemskega pristopa upravljanja tehničnih sistemov varovanja je vse prevečkrat spregledana pomembnost prenosa alarmnih sporočil.

Prenosna pot

Za prenosne poti so se v preteklosti uporabljale analogne linije in radijske frekvence. Le te so v zadnjih letih nadomestili z GSM omrežjem, nekatere pa tudi z LAN omrežji.

Pomanjkljivosti analognih linij so bile že omenjene v prejšnji točki, medtem ko je pri GSM in LAN omrežjih težava predvsem v poznavanju delovanja omrežij, TCP/IP protokolov. Tehnično osebje

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

varnostnih služb mora zagotavljati ustrezno usposobljenost svojih zaposlenih. Tehniki morajo dobro poznati delovanje obeh omrežij, kar pa je precejšen zalogaj. V primeru priklopa modula na LAN omrežje, se je potrebno dogovoriti z IT službo stranke, kar pa v nekaterih primerih dodatno otežuje implementacijo modula.

Specializirani in univerzalni vmesniki

Specializirani vmesniki so tisti, ki jih posamezni proizvajalec alarmnih sistemov proizvede za delovanje skupaj z njihovimi sistemi. Niso prenosljivi na alarmne centrale drugih proizvajalcev. Varnostni tehnik potrebuje posebno znanje za programiranje teh modulov, kot tudi znanje na področju GSM ali LAN omrežij.

Univerzalni vmesniki so na voljo že nekaj časa. Sama beseda pomeni, da jih lahko priklopimo na katerokoli alarmno centralo in niso vezani na posameznega proizvajalca. Kompatibilni so z večino sprejemnikov v VNC-jih. Za programiranje vseh teh modulov je potrebno imeti posebno namensko programsko opremo ter prenosnik, varnostni tehnik pa mora imeti dodatno znanje za programiranje univerzalnih vmesnikov. Vsak univerzalni vmesnik ima svojo specifiko, ki jo mora varnostni tehnik poznati in jo osvojiti.

Protokoli in podpora VNC

Na strani alarmne centrale se pošiljajo dogodki preko analogne linije, kjer se uporablja standardiziran ContactID protokol. Le ta je v uporabi že preko 30 let in se v tem času ni spremenil. Modul s simulacijo analogne linije tak dogodek sprejme iz alarmne centrale, ga ustrezno shrani, obdela, preuredi in pošlje v VNC v obliki SIA-DC09. Nadzorni center sprejme alarmni dogodek po standardu SIA-DC09, ki je v svetu zelo razširjen. Podpira tako TCP kot tudi UDP protokole, ter omogoča kriptirano pošiljanje podatkov. Dogodek se pošlje na primarni sprejemnik. Če primarni sprejemnik trenutno ni dosegljiv, se dogodek pošlje na sekundarni sprejemnik.

Oba omenjena protokola nista standardizirana, kar bi lahko jemali kot pomanjkljivost. Vendar se uporabljata v zelo široki paleti naprav, kar nam daje vedeti, da ni pričakovati sprememb, ki bi vplivale na potrebo po prilagoditvah.

Programiranje modulov

Programiranje modulov zahteva znanje in poznavanje tako alarmne centrale, kot tudi nastavljanje modula samega, kakor tudi omrežnih nastavitev. Če govorimo o GSM prenosu, moramo najprej zagotoviti ustrezno SIM kartico, ter nastaviti vse nastavitve v sam vmesnik. Če modul priklapljamo na LAN omrežje, moramo pridobiti ustrezne podatke od IT službe ter ob morebitnem nedelovanju uskladiti nastavitve modula oziroma požarne pregrade.

Lahko ugotovimo, da se tudi na področju varnega prenosa alarmnih signalov dogajajo določene spremembe in novi tehnološki pristopi, ki v prvi vrsti olajšajo ustrezno integracijo in nadgradnjo ter jo tako naredijo uporabniku bolj prijazno.

Programiranje modula se izvaja na lokaciji naročnika s prenosnim računalnikom ter posebno namensko programsko opremo. V nekaterih primerih pa tudi preko spletnega vmesnika, vendar vse na lokaciji naročnika.

Pomanjkljivosti so: potreba po fizični lokaciji, namensko znanje, namenska programska oprema, spremembe nastavitev pa je potrebno izvajati na lokaciji naročnika.

Spreminjanje nastavitev ali skupinsko spreminjanje parametrov

Skupinsko spreminjanje parametrov pomeni, da je potreba, da se na vseh modulih hkrati, oziroma v najkrajšem možnem času spremeni nek parameter.

Primer: Naročnik ima 100 modulov priklopljenih na najeti VNC. Ob podpisu pogodbe za nov VNC je potrebno spremeniti IP naslov sprejemnega centra na vseh 100-tih modulih. Potrebno bo obiskati vse lokacije modulov ter jim nastaviti nov IP. Če povzamem vse prej napisano, to pomeni, da mora varnostni tehnik obiskati vseh 100 lokacij, se dogovoriti s stranko za obisk, ter opraviti spremembe. Tovrstni postopki so časovno zelo zamudni in predvsem cenovno obremenjujoči.

Poslovni modeli

Dosedanji poslovni model temelji na nakupu opreme. Pod nakup se smatra nakup modula, montaža in priklop modula, ter priklop na VNC. Pri uporabi GSM omrežja zahteva tudi sklepanje naročnine za SIM kartico.

Pojavlja pa se nov poslovni model, ki temelji na storitvi prenosa. Le ta odpravlja vse zgoraj naštete pomanjkljivosti in znatno zniža stroške na dolgi rok.

Stranka preko varnostne službe najame storitev prenosa alarmnih sporočil saj storitev odpravlja potrebo po analogni liniji. Ni potrebno investirati v modul, ni potrebno imeti SIM kartice, ne potrebuje se LAN vmesnika, za montažo modula pa ni potrebnega nobenega predznanja, ne specializirane programske opreme, ker na objektu ni programiranja.

Storitev zajema prenos alarmnih sporočil od alarmne centrale do VNC-ja z minimalnimi stroški. Modul se NE programira na terenu ampak iz VNC-ja preko strežnika, nastavitve pa so zapisane v predlogi na strežniku. Le ta se v modul ob njegovi aktivaciji vanj samodejno naloži.

Modul ima že integrirano SIM kartico, ki omogoča, da preko varne VPN povezave modulu po potrebi kadarkoli spremenimo nastavitve. Prej omenjena težava z obiski lokacij in programiranjem posameznih modulov s tem odpade, kajti z nekaj kliki lahko spremenimo nastavitve na vseh modulih hkrati. Omogoča univerzalnost, enostavnost, hitro implementacijo, podpira standardne protokole in je skladen s prej omenjenimi standardi.

Zaključek

Lahko ugotovimo, da se tudi na področju varnega prenosa alarmnih signalov dogajajo določene spremembe in novi tehnološki pristopi, ki v prvi vrsti olajšajo ustrezno integracijo in nadgradnjo ter jo tako naredijo uporabniku bolj prijazno. Zaradi lažje integracije in posodobitev pa tudi zmanjšujemo možnost določenih napak, ki bi nastale na tem izredno pomembnem segmentu celotnega sistema tehničnega varovanja. Nikakor pa ne smemo spregledati tudi pomembnih prihrankov pri stroških ter obremenitvi strokovne delovne sile, ki v zadnjem obdobju postaja vse večji izziv. ■

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.

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

Kontakt: info@ics-institut.si / telefon: 05 90 54 300
spletna stran: www.ics-institut.si

EC-Council CHFI CERTIFIED
EC-Council CPENT CERTIFIED
EC-Council CEH MASTER CERTIFIED
EC-Council ECIH CERTIFIED
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

15. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 13. - 14. MAJ 2024

DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI