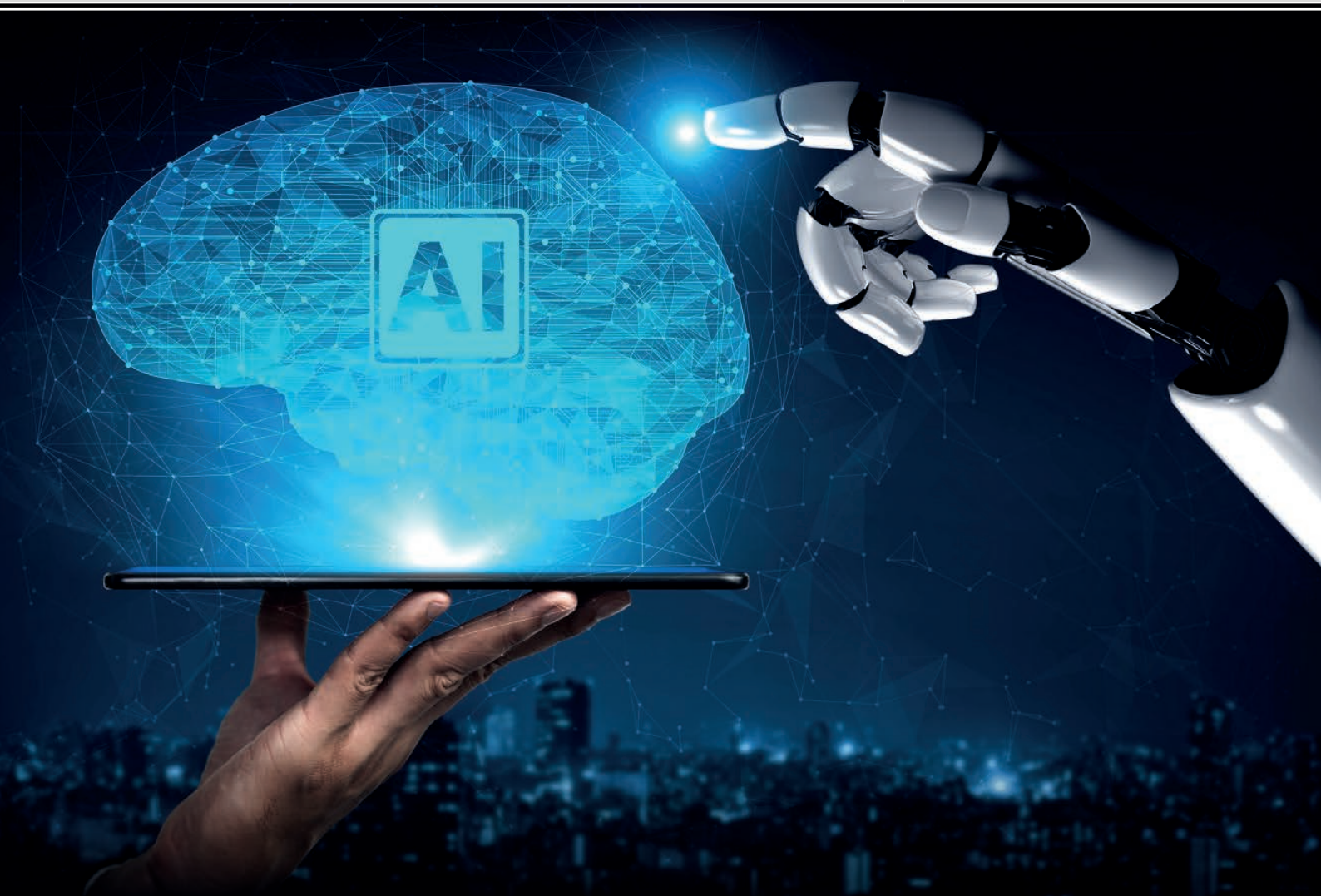
Korporativna varnost

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

Letnik 2025, februar • št. 37



Slovensko združenje korporativne varnosti
vključujoča platforma sodelovanja

Tradicionalna 16. mednarodna konferenca
Dnevi korporativne varnosti
Brdo pri Kranju, 19-20. maj 2025

ELES

RAZVIJAMO PRENOSNO OMREŽJE PRIHODNOSTI

Postavljamo nov mejnik v slovenski elektroenergetiki. Z raziskovalno-inovativnim delom se kot operater kombiniranega prenosnega in distribucijskega elektroenergetskega omrežja usmerjamo v njegov trajnostni, sistematični in napredni razvoj. Strateške inovacije nam bodo omogočile izpolnitev našega poslanstva tudi v prihodnosti – skrbeti za varen, zanesljiv in neprekinjen prenos električne energije 24 ur na dan.
To bomo dosegli z inovativnimi razvojnimi in tehnološkimi projekti in v sodelovanju z raznolikimi partnerji tako v domačem kot mednarodnem okolju. Za električno energijo na dosegu vaše roke danes in jutri.

www.eles.si

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.

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:
februar 2025

Izvod revije je brezplačen

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

ISSN 2232-6170

Korporativna varnost vedno bolj postaja pomembna tema in to ne samo znotraj organizacijskih okolij, temveč se o tej dejavnosti vedno bolj razpravlja tudi na nacionalnem in mednarodnem nivoju. Korporativna varnost, kot dejavnost, postaja pomemben deležnik celovitega sistema upravljanja s tveganji in obvladovanja kriznih dogodkov, brez katere si težko predstavljamo celovitost pristopov. Kritična infrastruktura in kritične storitve predstavljajo tisto stično točko, kjer je potreba po sodelovanju med nacionalnimi varnostnimi organi in korporativno varnostjo še posebej izražena. Vedno večje potrebe po strokovnem in kompetenčnem kadru v tej dejavnosti, nakazujejo podobne probleme, ki smo jim priča tudi v drugih sorodnih dejavnostih. Izobraževalni sistem namreč močno zamuja s prilagajanjem na zahteve in potrebe trga dela oz. dinamičnega varnostnega okolja. Na žalost na kadrovskem področju pri zagotavljanju ustreznih strokovnjakov s potrebnim kompetenčnim nivojem znanj ne moremo ubirati bližnjic. V določenem delu družbe se pojavlja prepričanje, da te vrzeli lahko zapolnijo predstavniki iz različnih varnostnih struktur, ki pa žal brez dodatnih znanj niso zadosti kompetenčni za delovanje na tem zahtevnem delovnem procesu. Če pa so ti prehodi kadrovskega potenciala povezani z nekritičnim razumevanjem kompetenčnih potreb in osebe v to dejavnost prihajajo z zavedanjem, da so že ustrezno usposobljene, potem imamo lahko velik problem. Brez potrebnih dodatnih znanj smo največkrat priča velikim strokovnim izzivom, ki se odražajo v nesistemskih pristopih in visoki stopnji fluktuacije na teh pomembnih delovnih mestih. Če k zmesi teh problemov dodamo še politično kadrovanje in vpliv na to dejavnost, potem imamo v tej družbi resne težave. To postaja vedno bolj izpostavljeno, saj smo v operativnem okolju korporativne varnosti priča pogostim menjavam, ki se na teh funkcijah dogajajo ob menjavi strateškega vodstva v organizacijah. To, poleg izraženih izzivov varnostnega okolja, na drugi strani pušča organizacije v nezavidljivem položaju za ustrezno sistemsko načrtovanje in izvajanje potrebnih ukrepov.

V prvi letošnji številki revije Korporativna varnost smo izpostavili različne posameznice in posameznike, da nam z deljenjem njihovih strokovnih izkušenj pomagajo bolje razumeti učinkovitost pristopov na področju korporativne varnosti. Skozi izbrane intervjuje, ponujamo možnost slišati tako strateški nivo odločevalcev, kakor tudi strokovnjake, kateri neposredno izvajajo aktivnosti v okviru svojih operativnih okolij. Poleg navedenega smo želeli v tokratni številki revije vsebinsko osvetliti tudi dovolj širok spekter ostalih strokovnih vsebin, ki bodo strokovni javnosti v pomoč pri iskanju potrebnih rešitev in strateške modrosti za ustrezno upravljanje varnostnih tveganj, s katerimi smo dnevno soočeni. V uredništvu revije upamo, da boste tudi v 37. številki revije našli ustrezne strokovne vsebine, ki vam bodo pomagale pri vašem zahtevnem delu.

izr. prof. dr. Denis Čaleta
Glavni urednik

INTERVJU
mag. Tadej Stergar,
direktor Korporativne varnosti, Telekom Slovenije

KORPORATIVNA VARNOST POSTAJA EDEN OD KLJUČNIH PROCESOV V ORGANIZACIJI

INTERVJU
mag. Katja Kraškovic,
dekanja GEA College - Fakultete za podjetništvo

ISKANJE USTREZNIH ODGOVOROV ZA ZAGOTAVLJANJE KOMPETENČNIH KADROV NA PODROČJU KIBERNETSKE VARNOSTI

KOLUMNA

ČLOVEK KOT KLJUČNI VARNOSTNI DEJAVNIK V DIGITALNI DOBI: ZAVEDANJE OMEJITEV IN IZZIVOV

VESOLJSKE INDUSTRIJE IN PRILOŽNOSTI ZA SLOVENSKE ORGANIZACIJE

V prispevku želimo podrobneje predstaviti korake, ki jih Republika Slovenija in preko tega tudi slovenske organizacije, izvajajo na področju sektorja vesoljske industrije.

UMETNA INTELIGENCA POMEMBEN IZZIV ZA KIBERNETSKO VARNOST

Umetna inteligenca (UI) je postala ključni element sodobne digitalne preobrazbe. Njena zmožnost hitre obdelave podatkov, generiranja vsebin in učenja na podlagi velikih količin informacij je revolucionarna, a hkrati prinaša tudi številne nevarnosti.

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

INTERVJU
mag. Tadej Stergar, direktor Korporativne varnosti, Telekom Slovenije*

KORPORATIVNA VARNOST POSTAJA EDEN OD KLJUČNIH PROCESOV V ORGANIZACIJI

Varnost je v Telekomu Slovenije strateška prioriteta, zato ji na vseh nivojih posvečajo velik pomen. To je edini način za zagotavljanje ustreznega delovanja tega zahtevnega poslovnega sistema. O sistematičnem načrtovanju novih rešitev in celovitih pristopov na področju korporativne varnosti nam je, v smeri njihove dolgoročne uveljavitve, nekaj ključnih misli zaupal mag. Tadej Stergar.

Pred dobrim letom ste prevzeli pomembno funkcijo korporativno varnostnega managerja oz. direktorja Korporativne varnosti v Telekomu Slovenije. Nam lahko pojasnite, katera so ključna področja vaših pristojnosti?

Ključne aktivnosti so usmerjene v zagotavljanje korporativne varnosti v celotni Skupini Telekom Slovenije. Pri tem so ključna naslednja področja: splošna varnost, varovanje informacij in neprekinjeno poslovanje, storitve varnostno-nadzornega centra ter izvajanje določenih zakonskih obveznosti.

Na področju splošne varnosti gre za več aktivnosti:
- redno izvajanje in spremljanje ocene tveganj;
- vpeljava in upravljanje varnostnih politik in postopkov;
- izobraževanje in usposabljanje zaposlenih ter ozaveščanje in širjenje varnostne kulture;
- varovanje ljudi in premoženja ter nadzor dostopov do naše infrastrukture;
- ustrezen odziv in obravnava varnostnih incidentov;
- preventivno delovanje, npr. preprečevanje prevar;
- stalno spremljanje novih trendov groženj, novih oblik varovanja, tehničnih sredstev ...

Področje varovanja informacij in neprekinjenega poslovanja pa vsebuje:
- redno izvajanje in spremljanje ocene tveganj na področju informacijske varnosti,
- vpeljava in upravljanje varnostnih politik ter politik neprekinjenega poslovanja in postopkov, ki iz tega izhajajo;
- analize vpliva na poslovanje, načrtovanje neprekinjenega poslovanja ter načrtovanje obnove po nesrečah in drugih izrednih dogodkov;
- redno izvajanje testiranja načrtov, vzpostavitev ustreznih komunikacijskih protokolov in drugo, kar je povezano s preverjanjem in z nadgradnjo le-teh;
- izobraževanje in usposabljanje zaposlenih s področja varovanja informacij in neprekinjenega poslovanja ter informacijske varnosti;
- ustrezen odziv in obravnava varnostnih incidentov;
- skrb za implementacijo ustreznih preventivnih ukrepov, kot so npr. nadzor dostopov do informacijskih sredstev, šifriranje, redno posodabljanje, varnostno kopiranje itn.

V Telekomu Slovenije imamo tudi nov Varnostno-nadzorni center, za katerega smo prejeli pomemben mednarodni certifikat DIN EN 50518:2020. Center primarno uporabljamo za prenos alarmnih signalov in video nadzora naših objektov, dodatno pa storitve centra (skupaj še z drugimi storitvami) zagotavljamo tudi za trg. Med njimi so tudi storitve upravljanja videonadzora in nadzora dostopov, ki jih naši naročniki oz. poslovni uporabniki potrebujejo na področju zasebnega varovanja.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Zato je pomembno, da smo operaterji v dobri kondiciji ter vedno pripravljeni, 24 ur na dan, 7 dni na teden, 365 dni v letu. Marsikdo to opazi šele, ko pride do izrednega dogodka in potrebuje našo pomoč.

Nenazadnje pa so tukaj še zakonodajne obveznosti. Kot družba, ki deluje na področju telekomunikacijskih storitev, smo podvrženi zelo strogi regulaciji, zato imamo veliko zakonskih obveznosti, ki jih moramo seveda dosledno izpolnjevati.

Sedaj že lahko z gotovostjo naredite kratko primerjavo v oceni dinamike korporativnega okolja glede na pretekle izkušnje okolij, kjer ste prej opravljali svojo profesionalno pot.

V preteklosti sem v različnih vlogah sodeloval s številnimi družbami, med drugim tudi s kritično infrastrukturo. Pridobil sem ogromno izkušenj in znanja. Sem v stalnem poslovnem stiku z vodji korporativne varnosti drugih družb, s čimer imam dober vpogled v samo področje, hkrati pa sem tako seznanjen tudi z izzivi in načini reševanja le-teh. Sicer je vsaka panoga nekakšen svoj ekosistem, s svojimi posebnostmi, povsod pa so izzivi, med seboj zelo različni in zahtevni. Področje korporativne varnosti je zelo pestro in dinamično okolje s pojavnimi oblikami različnih groženj kot tudi s stalnim prizadevanjem za uvajanje mehanizmov za zmanjševanje tveganj, povezanih s temi grožnjami.

V Telekomu Slovenije smo glede na povedano resnično med (naj)boljšimi na področju korporativne varnosti. Varnost je naša strateška prioriteta, zato ji na vseh nivojih dajemo velik pomen, k rešitvam pristopamo načrtno, celovito in dolgoročno. Pri tem pa ves čas preverjamo, ali so naše rešitve ustrezne, tako z internimi kot eksternimi presojami.

Pomembno je, da je varnost na visokem nivoju, saj je treba poskrbeti za zaščito v vseh pomenih, ranljivosti pa ustrezno nasloviti in sistemsko urediti na ravni podjetja. Npr., v nekaterih družbah povsem nekritično dopuščajo administratorske pravice na delovnih postajah, marsikje nimajo niti ustrezne zaščite končnih točk z EDR-sistemi (Endpoint Detection and Response – zaznavanje končnih točk in odzivanje nanje). Prav tako v nekaterih podjetjih še vedno podpirajo in dopuščajo politiko BYOD (bring your own device – prinesi svojo napravo) ter nimajo ustreznih mehanizmov za neprekinjeno poslovanje in odzivov na varnostne incidente.

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

Priča smo skorajda eksponentnemu razvoju na področju informacijskih tehnologij in s tem tudi hitremu razvoju ter spreminjajoči se naravi samih groženj. Kibernetski napadi postajajo vse bolj sofisticirani in ciljno usmerjeni, prav tako so vedno bolj pogosti. Na drugi strani pa se ves čas soočamo z

vedno večjo odvisnostjo od tehnologij zaradi samih procesov, ki so vse bolj digitalizirani. Pa tudi s pomanjkanjem strokovnjakov za kibernetsko varnost, z nenehnim spreminjanjem in zaostrovanjem zakonodajne regulative ter s tem tudi z vedno večjimi stroški za zagotavljanje skladnosti z normativnimi zahtevami.

Sodobno družbeno življenje je namreč informacijsko in komunikacijsko medsebojno zelo tesno povezano in prepleteno, zato se panoga telekomunikacij, glede na pomembnost, postavlja praktično takoj za energetiko. Brez telekomunikacij ni povezljivosti, ni gospodarskega povezovanja in razvoja, ni dostopa do informacij. Ogrožena je marsikatera varnostna storitev, pri čemer so zelo pomembni tudi vplivi na inovacije, tehnološki napredek in družbeno povezanost. In ravno ta izredna pomembnost telekomunikacijskega sektorja ima za posledico zelo rigorozno normativno ureditev, ki smo ji podvrženi vsi operaterji - podobno, kot so banke podvržene strogi regulaciji na svojem področju.

Skratka, vse navedeno nas sili k nenehnemu spremljanju novosti, novih pojavnih oblik groženj in hitremu prilagajanju ter uvajanju sprememb, kar pa je seveda finančno in kadrovsko zelo izčrpajoče. Zato je pomembno, da smo operaterji v dobri kondiciji ter vedno pripravljeni, 24 ur na dan, 7 dni na teden, 365 dni v letu. Marsikdo to opazi šele, ko pride do izrednega dogodka in potrebuje našo pomoč.

Pred vsemi nami je implementacija več pomembnih evropskih direktiv, ki so ali še bodo prenesene v nacionalni pravni red. Naj omenimo samo nekatere kot na primer NIS-2 in CER direktiva, ki je že vnešena v nov Zakon o kritični infrastrukturi. Kako zahtevni so ti koraki prilagajanja tem zahtevam v tako kompleksnem sistemu kot je Telekom Slovenije?

V Telekomu Slovenije smo se že v okviru obstoječe področne zakonodaje, predvsem Zakona o elektronskih komunikacijah (ZEkom-2), prilagajali in stalno nadgrajevali ter izboljševali svoje procese varovanja informacij in neprekinjenega poslovanja. To dokazujemo tudi z vzpostavljenim sistemom upravljanja varovanja informacij (SUVI) in sistemom upravljanja neprekinjenega poslovanja (SUNP), ki ju imamo certificirana po ISO 27001 in ISO 22301. Posebej slednjega smo kot prva družba v Sloveniji pridobili že pred devetimi leti.

Tako prilagajanje in izboljševanje SUVI in SUNP vidimo kot stalnico in tudi v primeru prilagajanja novemu zakonodajnemu okvirju ne bo drugače. Zelo zahtevno bo prilagoditi posamezne postopke in dodatne ukrepe. Namreč, SUVI in SUNP sta vključena v vse nivoje organizacije in v vse procese družbe.

V sistemu ustreznega obvladovanja tveganj ima Varnostno nadzorni center v Telekomu Slovenije izredno pomembno vlogo. Nam lahko zaupate kako pomembna je centralizacija podatkov in varnostnih signalov vezano na fizično in tehnično varovanje vaše razpršene infrastrukture?

Centralizacija podatkov oz. varnostnih dogodkov na enem mestu je ne samo stroškovno učinkovitejša rešitev, temveč je ključna tudi za hiter in učinkovit odziv na posamezne incidente. Več kot imamo podatkov na enem mestu, bolj kakovosten in seveda bolj ustrezen je lahko naš odziv.

V preteklih letih ste bili med prvimi predlagatelji uporabe virtualne resničnosti v zahtevnih sodnih primerih pri pregledu krajev, kjer so se storila določena dejanja. Menite, da so te tehnologije že dovolj tehnološko zrele, da se aktivno uvedejo v sistem zagotavljanja korporativne varnosti?

Svojo poslovno pot sem začel v policiji in sem bil priča velikim izzivom pri pripravi gradiva, skic, posnetkov s krajev kaznivih dejanj, sodišča pa so se soočala s kupom dokumentacije (različna forenzična poročila, skice, fotografije, videoposnetki).

V preteklosti sem sodeloval z družbo, ki se je prva lotila področja virtualne resničnosti v Sloveniji in kasneje tudi razširjene (obogatene) resničnosti ter mešane resničnosti. Ob tem sem bil seveda tudi sam poln inovativnih idej, ki sem jih že 10 let nazaj predlagal Ministrstvu za pravosodje, npr. uvedbo elektronskih dražb, ki jih danes sicer uporabljajo. Za takšne oblike resničnosti, ki bi lahko bile v pomoč pri samih postopkih, takrat žal ni bilo posluha.

Še danes menim, da bi vse te omenjene resničnosti, predvsem pa dobra platforma, omogočile lažji pregled nad gradivom, soočanjem s samim krajem kaznivega dejanja ter tudi dobro vizualizacijo posameznega primera. Ob tem obstajajo tehnologije, ki so na trgu že dlje časa in so primerne za uporabo. Glede same varnosti pa je enako kot z ostalimi aplikacijami – pomembno je varovanje aplikacij, strojne opreme, podatkov, ki se v njih nahajajo, itn.

Kibernetska tveganja v zadnjem obdobju postajajo vedno večji izziv za vse organizacije. Vaš Center kibernetske varnosti in odpornosti zagotavlja varnost tudi vašim informacijskim in tehnološkim sistemom. Je pa jasno dejstvo, da je človeški faktor še vedno najšibkejši člen celovitega varnostnega sistema. Kako pristopate k dvigovanju varnostnega zavedanja zaposlenih v Telekomu Slovenije?

Vsak zaposleni prejme jasne, uporabne smernice glede varne uporabe tehnologij, ki jih redno posodabljamo glede na nove grožnje. Periodično se sestaja interna skupina, ki pregleduje novosti glede tehnologij, ter skladno s tem predlaga ukrepe varnostnemu kolegiju v naslednjem ciklu: zaščita informacij, zmanjševanje tveganj, skladnost in standardi (ZVOP, ISO 27001), zavedanje in stalne izboljšave.

Menim, da si bodo v prihodnosti le redke organizacije lahko privoščile delovanje brez takšne ali drugačne oblike umetne inteligence. Večja verjetnost je, da bodo umetno inteligenco uporabljale kar vse, morda ne povsem neposredno, saj bodo proizvajalci module umetne inteligence vključili že v svoje aplikativne rešitve.

Strokovna združevanja so zelo koristna za izmenjavo znanj in izkušenj, dostop do določenih virov in orodij, kot tudi za izkušnje za uporabo le-teh, pa medsebojno sodelovanje in mreženje ter posledično lažje skupno reševanje izzivov.

Redno izvajamo izobraževanja in delavnice, namenjene različnim vidikom kibernetske varnosti. Udeležujemo se mednarodnih vaj s področja kibernetske zaščite, zaposlene izobražujemo na posameznih certifikacijskih izobraževalnih institucijah. Sodelujemo pa tudi v mednarodnih projektih in smo člani mednarodne organizacije CERT. Prek internih komunikacijskih kanalov (intranet, e-pošta, novice) zaposlene obveščamo o novih grožnjah in varnostnih priporočilih za njihovo preprečevanje, saj je pomembno, da se varnostnih tveganj zavedamo vsi – najšibkejši člen je še vedno človek, zato je interno in eksterno izobraževanje in ozaveščanje del naših rednih aktivnosti. Organiziramo tudi simulacije t. i. phishing (spletno ribarjenje) napadov, ki pomagajo zaposlenim prepoznati potencialne nevarnosti v realnih scenarijih. Na podlagi rezultatov teh simulacij prilagodimo nadaljnje izobraževanje. Redno pa izvajamo tudi operacije kibernetske zaščite in odpornosti.

Ozaveščanje, obveščanje in izobraževanje zaposlenih o phishing napadih oz. napadih socialnega inženiringa se mi zdi izredno pomembno, pravzaprav nujno.

Kako bo nagel razvoj umetne inteligence vplival na zagotavljanje korporativne varnosti v naših organizacijskih okoljih?

Menim, da si bodo v prihodnosti le redke organizacije lahko privoščile delovanje brez takšne ali drugačne oblike umetne inteligence. Večja verjetnost je, da bodo umetno inteligenco uporabljale kar vse, morda ne povsem neposredno, saj bodo proizvajalci module umetne inteligence vključili že v svoje aplikativne rešitve.

Vsekakor pa na področju korporativne varnosti pričakujem velik vpliv na naslednji področjih:
- izboljšano odkrivanje groženj,
- avtomatizacija varnostnih procesov,
- napredne oblike analize tveganj,
- lažje in hitrejše prilagoditve varnostnih rešitev,
- pomoč pri pripravi ukrepov za skladnost z zakonodajo.

V katero smer se bo v prihodnosti razvijala profesija korporativne varnosti? Katere bodo tiste strokovne kompetence, ki jih bodo potrebovali strokovnjaki na tem področju, da bodo lahko uspešno parirali varnostnim izzivom prihodnosti?

Pričakujem povečane aktivnosti v smeri hibridnih groženj in znotraj tega močan porast kibernetskih napadov z uporabo vseh najnaprednejših tehnik, ki bodo imele močno podporo v umetni inteligenci. Skladno s tem bomo v boju proti tem grožnjam v vedno večji meri uporabljali podporo umetne inteligence. Poleg strokovnjakov za kibernetsko varnost bomo tako potrebovali tudi strokovnjake za analize ogromnih količin podatkov, strokovnjake za strojno učenje, inženirje in razvijalce ter t. i. implementatorje algoritmov umetne inteligence, inženirje za razvoj sistemov za obdelavo in razumevanje jezikov itn. Na drugi strani pa bomo na področju splošne varnosti imeli opravka s takšnimi in drugačnimi oblikami dronov, ki so cenovno zelo dostopni in v vsesplošni rabi.

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?

Strokovna združevanja so zelo koristna za izmenjavo znanj in izkušenj, dostop do določenih virov in orodij, kot tudi za izkušnje za uporabo le-teh, pa medsebojno sodelovanje in mreženje ter posledično lažje skupno reševanje izzivov.

Izmenjava primerov dobrih praks in medsebojno sodelovanje sta tisto, kar nam omogoča, da se lahko kot stroka razvijamo in postavljamo enotne standarde. ■

Foto: arhiv Telekom Slovenije d.d.

Ste pripravljeni na skladnost z NIS2, ISO 27001:2022 in Zakonom o kritični infrastrukturi?

Skladnost ni le formalno izpolnjevanje zahtev – ključni so učinkoviti procesi in celovit pristop k informacijski varnosti.

Kako zagotovimo skladnost?

Zahteve se pri analizi tveganj nekoliko razlikujejo, zato podjetja pogosto iščejo najučinkovitejši pristop. Pomembno vprašanje pa je tudi, kako lahko vse postopke in podatke pri upravljanju informacijskih tveganj obdelujemo na enem mestu.

Kaj morate urediti?

- Analiza informacijskih tveganj – prepoznavanje in ocenjevanje groženj
- Obvladovanje tveganj – uvajanje ukrepov za zmanjšanje izpostavljenosti
- Upravljanje neprekinjenega poslovanja – pripravljenost na izpade in motnje
- Obravnavanje varnostnih incidentov – hiter odziv in preprečevanje ponovitev

Kako vam lahko pomagamo?

- Izobražujemo in svetujemo za skladne in uporabne rešitve
- Uvajamo informacijski sistem Silver Bullet Risk (SBR) za celovito upravljanje tveganj

Kontaktirajte nas na info@silverbulletrisk.com in skupaj bomo poiskali optimalno rešitev!

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
mag. Katja Kraškovic, dekanja GEA College - Fakultete za podjetništvo

ISKANJE USTREZNIH ODGOVOROV ZA ZAGOTAVLJANJE KOMPETENČNIH KADROV NA PODROČJU KIBERNETSKE VARNOSTI

Izobraževanje strokovnjakov s področja kibernetske varnosti postaja eden od najpomembnejših izzivov kako zagotavljati ustrezen kompetenčni model kadrovskega potenciala za učinkovito upravljanje zahtevnih varnostnih tveganj. Za podroben vpogled v to tematiko smo se pogovarjali z mag. Katjo Kraškovic, dekanjo izobraževalne institucije, ki s svojimi programi zagotavlja izobraževanje novih strokovnjakov s področja kibernetske varnosti.

GEA College je ena od najstarejših zasebnih izobraževalnih institucij v Republiki Sloveniji. Nam lahko glede na prehojeno pot, zaupate, kateri so tisti izzivi na izobraževalnem področju, ki bodo po vaši oceni najbolj zaznamovali prihodnje obdobje?

GEA College že več kot tri desetletja sledi razvoju gospodarstva in potrebam posameznikov v Sloveniji. Prihodnost bo zaznamovalo predvsem prilagajanje hitrim tehnološkim spremembam, kot so umetna inteligenca, digitalizacija in avtomatizacija. Klasični modeli predavanj vse bolj prepuščajo prostor hibridnemu, fleksibilnemu in personaliziranemu učenju. Prav tako je pomembno, da programi sledijo globalnim spremembam, saj se trg razvija izjemno hitro, znanja in veščine pa morajo biti relevantne tudi v prihodnosti. Spodbujanje podjetniškega razmišljanja ostaja brezčasna prioriteta, saj gospodarstvo potrebuje inovatorje, ki znajo kritično razmišljati in ustvarjati nove priložnosti. Zato neprestano razvijamo rešitve, posodabljamo programe in krepimo sodelovanje z gospodarstvom doma in v tujini, da lahko ponudimo kakovostno izobraževanje za prihodnost.

Na GEA College - Fakulteti za podjetništvo ste pred časom akreditirali in začeli izvajati visokošolski program Informacijske in kibernetske varnosti. Nam lahko zaupate izkušnje po končanih prvih generacijah študentov?

Povpraševanje po strokovnjakih na tem področju je izjemno visoko, zato smo v sodelovanju s podjetji iz IT sektorja oblikovali program, ki povezuje teorijo s prakso. Prva generacija študentov trenutno zaključuje tretji letnik in se pripravlja na diplomski izpit. Kljub zahtevnosti programa smo z izvedbo zelo zadovoljni, saj študenti pridobivajo ključna znanja o zaščiti podatkov, analizi groženj in obvladovanju tveganj. Povratne informacije so odlične, saj študenti cenijo praktično usmerjenost, po kateri je GEA College poznan. Na odzive delodajalcev bomo morali še nekoliko počakati, vendar smo prepričani, da bodo naši diplomanti hitro našli mesto na trgu dela.

*avtorica je članica Slovenskega združenja korporativne varnosti

Da bi kibernetsko varnost približali mlajšim generacijam, smo poleti 2024 skupaj s Sekcijo za kibernetsko varnost pri GZS ZIT organizirali Cyber kamp za dijake in dijakinje. Tam so lahko spoznali osnove kibernetske varnosti in se naučili, kako se zaščititi pred tveganji. Zaradi izjemnega odziva pripravljamo podoben kamp tudi v letu 2025, saj verjamemo, da je ključno mladim pokazati, da kibernetska varnost ni le tehnično zahtevna, ampak tudi zanimiva in družbeno pomembna karierna izbira.

Kako uravnavate študijski program, da je v njem dovolj praktičnih vsebin, ki so za dvigovanje kompetenčnega okvira na tem zahtevnem področju ključne za učinkovit sistem izobraževanja?

Preplet teorije in prakse je temelj izobraževanja na GEA College. Že pri oblikovanju programa smo se zavedali, da mora biti praktično naravnan. Aktivno ga sooblikujejo strokovnjaki iz gospodarstva, ki predavajo, izvajajo delavnice in mentorirajo študente pri praktičnih projektih. Študenti tako delajo na resničnih primerih in simulacijah, kjer razvijajo ključne veščine, kot so zaščita informacijskih sistemov in odzivanje na kibernetske napade. S takim pristopom študenti ne pridobijo le teoretičnega znanja, ampak postanejo kompetentni strokovnjaki, ki lahko svoje veščine takoj uporabijo v praksi.

Bi se strinjali z ugotovitvijo, da imajo strokovnjaki na področju informacijske varnosti premalo strateške širine in, da so zelo fokusirani v določeno specifično kompetenčno področje znotraj te široke profesije? Dajete na vaši fakulteti dovolj pozornosti tudi grajenju strateškega kritičnega mišljenja, kot dopolnitvi specifičnih tehničnih kompetenc?

Informacijska varnost je izjemno kompleksno področje, kjer strokovnjaki pogosto delujejo znotraj ozkih kompetenčnih področij. Prav zato smo na GEA College oblikovali interdisciplinarni program, ki združuje tehnična znanja s širšim razumevanjem poslovnih in varnostnih kontekstov. Študenti skozi študije primerov povezujejo tehnična in poslovna znanja, analizirajo etične in družbene vidike kibernetske varnosti ter razvijajo celosten pristop k reševanju problemov. Naš cilj je ponuditi ravnovesje med tehničnimi znanji in strateško širino, ki jo nadgradijo z izkušnjami v praksi.

Že pri oblikovanju programa smo se zavedali, da mora biti praktično naravnan. Aktivno ga sooblikujejo strokovnjaki iz gospodarstva, ki predavajo, izvajajo delavnice in mentorirajo študente pri praktičnih projektih. Študenti tako delajo na resničnih primerih in simulacijah, kjer razvijajo ključne veščine, kot so zaščita informacijskih sistemov in odzivanje na kibernetske napade.

Vse analize in ugotovitve kažejo, da je na področju informacijske in kibernetske varnosti izredno veliko pomanjkanje ustreznih strokovnjakov. Praktično vsi, ki imajo ustrezne kompetence na tem področju so zelo zaposljiv kader. Kaj bi bilo potrebno po vašem storiti, da bi približali ta poklic z zaposlitvenimi priložnostim mlajši generaciji, ki prihaja v procese srednješolskega in dodiplomskega izobraževanja?

Potrebujemo aktivne ukrepe, da to področje približamo mladim, vključno z dekleti. Ozaveščanje se mora začeti zgodaj, v osnovnih in srednjih šolah, s tekmovanji, poletnimi šolami, zgodbami o uspehu in promocijo perspektivnih poklicev. Ključno je tudi povečati dostopnost programov ter ponuditi štipendije, ki bi mladim omogočile lažji vstop v to področje. Pobude, kot je Women4Cyber Slovenija, prav tako pripomorejo k spodbujanju raznolikosti in mentoriranju mladih talentov. S temi ukrepi lahko mlade navdušimo za področje, ki ponuja veliko možnosti za karierno rast in prispevek k digitalni varnosti. Na GEA College mladim približujemo kibernetsko varnost s poletnimi šolami, kot je Cyber kamp, ki ga bomo ponovno organizirali poleti 2025. Na teh dogodkih pokažemo, da kibernetska varnost ni le tehnično zahtevna, ampak tudi dinamična, zanimiva in družbeno pomembna karierna izbira.

Kakšne izkušnje imate z ustreznimi nacionalnimi institucijami, kot so NAKVIS in samo Ministrstvo za visoko šolstvo, znanost in inovacije? Ali ustrezno razumejo izzive na tem področju in ali so dovolj agilni, da se ustrezno prilagajajo potrebam realnega okolja?

Institucije se zavedajo izzivov, a naslavljanje teh vprašanj zahteva širše sodelovanje. Verjamemo, da institucije prepoznavajo izzive, vendar pogosto manjkajo dolgoročne analize in jasne strateške smernice. Brez proaktivnih akcijskih načrtov izgubljamo konkurenčnost v primerjavi z državami, ki se sistemsko lotevajo teh vprašanj. Za učinkovito prilagoditev izobraževalnega sistema je potrebno dolgoročno sodelovanje vseh deležnikov in večja prilagodljivost sistema.

Podeljevanje koncesij zasebnim izobraževalnim institucijam ima v tej državi že dolgo brado. Menite, da so tukaj mehanizmi za podeljevanje

koncesij na deficitarnih študijskih smereh pravilno razumljene in ali država realno sledi kadrovskim potrebam v realnem sektorju?

Koncesije bi morale biti strateško orodje za reševanje deficitarnih poklicev, ne zgolj administrativni postopek. Pri podeljevanju koncesij gre pogosto za napačna prepričanja o njihovem namenu, ki jih včasih podpihujejo tudi nekateri deležniki ali mediji. Ključno je razumeti, da koncesije niso vprašanje lastništva (javno ali zasebno), temveč učinkovitega reševanja ključnih kadrovskih vrzeli v gospodarstvu. Koncesije omogočajo, da se zasebne institucije vključijo v reševanje izzivov na področjih, kjer je javni sistem prepočasen ali omejen. Pogosto zasebne institucije hitreje razvijejo programe, ki naslovijo deficitarne poklice, medtem ko javne institucije zaostajajo. Pomanjkanje razpisov za financiranje teh področij preko koncesij neposredno škoduje razvoju države in družbe.

Država bi morala podeljevanje koncesij uporabljati kot strateško orodje za reševanje družbenih in gospodarskih izzivov, s čimer bi omogočila večjo sinergijo med izobraževalnim sistemom in realnim sektorjem. Država sicer prepoznava ključna deficitarna področja, vendar so ukrepi pogosto prepočasni in premalo usklajeni s potrebami trga dela. Pomanjkanje strateške usmeritve, premajhna povezava z gospodarstvom, premalo promocije perspektivnih poklicev in štipendij ter prepočasna implementacija sprememb zavirajo razvoj.

S pospešenimi in pravičnejšimi procesi bi država lahko učinkoviteje podprla razvoj deficitarnih študijskih programov in tako bolje odgovorila na potrebe gospodarstva ter prihodnosti mladih.

Primer podiplomskega študijskega programa Upravljanje s tveganji in korporativna varnost je verjetno tipičen primer nerazumevanja realnih potreb trga s strani države, da bi se uredilo ustrezno koncesioniran program, ki je bil edinstven v tistem trenutku akreditacije v Republiki Sloveniji in tudi širšem regijskem prostoru. Imate kakšno oceno in idejo, kaj bi v takih primerih pričakovali s strani odgovornih državnih institucij?

Programi, kot so Upravljanje s tveganji in korporativna varnost (danes Krizni management), Digitalni marketing ter Informacijska in kibernetska varnost, so nastali kot odgovor na realne potrebe gospodarstva. Ker takšnih programov pogosto ni na javnih institucijah, bi morali uživati večje priznanje in podporo države.

Osnutek novega Zakona o visokem šolstvu, ki predvideva ukinitev vseh koncesij v visokem šolstvu do leta 2029, povzroča negotovost. Celo programi, ki so polno zasedeni in kakovostni, se soočajo s tem, da bodo ukinjeni, kar lahko negativno vpliva na razvoj celotnega izobraževalnega sistema.

Ministrstvo bi moralo podpirati vse izobraževalne ustanove – javne in zasebne – in omogočiti razpise za koncesije, kjer lahko zasebni sektor hitro in učinkovito odgovori na deficitarne potrebe trga dela. Prava rešitev so razpisi za financiranje deficitarnih poklicev, s katerimi bi zagotovili stabilno in dolgoročno usmerjeno izobraževanje, ki bi naslavljalo potrebe gospodarstva in družbe ter omogočalo vključujoč in prožen izobraževalni sistem.

V zadnjem obdobju je veliko naporov usmerjeno tudi v vključevanje ženskega dela populacije na področje informacijske in kibernetske varnosti. V tem delu se verjetno skriva kar nekaj kadrovskega potenciala, ki bi ga s pravilnimi pristopi lahko usmerili na to področje, kjer kronično primanjkuje ustreznih kadrov. Katere korake v tej smeri izvajate vi osebno in katere izobraževalna institucija, ki jo vodite?

Vključevanje žensk na področje informacijske in kibernetske varnosti je izjemno pomembno, saj raznolikost prinaša nove perspektive in izboljšuje reševanje kompleksnih izzivov. Na GEA College že vrsto let podpiramo žensko podjetništvo, zdaj pa enako pozornost usmerjamo tudi v tehnične smeri.

Preko sodelovanja v iniciativi Women4Cyber ozaveščamo, organiziramo dogodke in mentoriramo mlade ženske, ki jih zanima to področje. S promocijo ženskih vzornic in mentorstvom želimo spodbuditi večje zanimanje za tehnične poklice.

Na GEA College organiziramo tudi poletne šole in izbirne predmete, ki dekletom omogočajo prvi stik s kibernetsko varnostjo. Na našem Cyber kampu 2024 je bilo že 9 deklet od skupno 40 udeležencev, kar je dober začetek, vendar si želimo, da bi bilo to število še večje.

Prav tako razmišljamo o dodatnih spodbudah, kot so štipendije ali finančna pomoč za dekleta, ki se odločijo za študij informacijske in kibernetske varnosti. S celostnim pristopom in podporo ženskam na tehničnih področjih gradimo prihodnost, kjer bo raznolikost ključni del razvoja informacijske in kibernetske varnosti. ■

Foto: arhiv GEA College - Fakultete za podjetništvo

> Ozaveščanje se mora začeti zgodaj, v osnovnih in srednjih šolah, s tekmovanji, poletnimi šolami, zgodbami o uspehu in promocijo perspektivnih poklicev. Ključno je tudi povečati dostopnost programov ter ponuditi štipendije, ki bi mladim omogočile lažji vstop v to področje. S temi ukrepi lahko mlade navdušimo za področje, ki ponuja veliko možnosti za karierno rast in prispevek k digitalni varnosti.

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.

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.

sbr
Mestna občina Ljubljana
GASILSKA ZVEZA LJUBLJANA
Občina Slovenska Bistrica
Melamin
Mercator
CAA
SMART COM
URSIV
telemach
SIEMENS
Onkološki inštitut Institute of Oncology Ljubljana
ELEKTRONČEK
Ministrstvo za infrastrukturo
GEN SKUPINA
Javni medobčinski stanovanjski sklad Maribor
Telekom Slovenije
Pošta Slovenije
DARS
PETROL
Energija za življenje
AKRAPOVIČ
interblock
LUXURY GAMING PRODUCTS
triglav
Informacijske storitve in inženiring, d.o.o.
INFORMATIKA
otpbanka
SPICA
tenzor
Elita i.b. d.o.o.
ZARJA ELEKTRONIKA
UNISTAR PRO
smartis
PAMETNI INFORMACIJSKI SISTEMI
LON
CINKARNA
Slovenske železnice
energetika ljubljana

www.ics-institut.si

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

KOLUMNA

ČLOVEK KOT KLJUČNI VARNOSTNI DEJAVNIK V DIGITALNI DOBI: ZAVEDANJE OMEJITEV IN IZZIVOV

Pred kratkim sem bil na predavanju priznanega slovenskega športnega pedagoga, filozofa in dihalnega terapevta, dr. Milana Hoste, ki je podal zanimivo ugotovitev. Dejal je, »da v sodobnem olimpizmu, kjer cilj opravičuje sredstva, človeško telo pri planiranju višjih ciljev, postaja ovira«.

Ta misel mi je dala odlično iztočnico za razmišljanje, kako je z vlogo človeka v procesih upravljanja z varnostnimi tveganji, kjer ima vse večjo vlogo digitalizacija procesov, uporaba najsodobnejših tehnologij in tehničnih rešitev ob podpori umetne inteligence in strojnega učenja. Najnovejši dosežki na področju generativne umetne inteligence spreminjajo svet, naše življenje in delo že danes. Uporabnost umetne inteligence (kot je npr.: ChatGPT) je postala splošno prepoznana v družbi, hkrati pa se je drastično povečala kompleksnost in velikost modelov generativne umetne inteligence. Umetna inteligenca zelo hitro napreduje in v tem napredku že ustvarja tudi lastno obliko inteligence – strojno inteligenco – z velikim vplivom na človeško življenje. Iz tega razloga je preprosto nujno, da družba oblikuje nov pogled na svet. S hitrim napredkom umetne inteligence se spreminjajo tudi naši poslovni modeli in struktura delovnih mest. Strah, da bo umetna inteligenca prevzela delovna mesta, je pogost, vendar pa obstajajo tudi napovedi, da bo umetna inteligenca v prihodnosti ustvarila nova delovna mesta in omogočila večjo produktivnost. Vse to pa odpira vprašanje, kako se prilagoditi in kako se razvijati v tehnološkem okolju, kjer bodo človek in stroj, bolje rečeno človek in programi, delovali v sinergiji.

Čeprav napredne varnostne rešitve, kot so umetna inteligenca ter avtomatizacija in šifriranje, igrajo ključno vlogo pri zaščiti digitalnih sistemov, ostaja človek najpomembnejši dejavnik pri njihovem upravljanju. Da bi ljudje lahko sledili temu razvoju in ga obvladovali, je potrebna zadostna stopnja digitalne pismenosti in poudarjanje pomena človeka pri upravljanju varnostnih tveganj.

Digitalna transformacija, digitalne kompetence in digitalna pismenost

Digitalna transformacija je omogočila hitrejši razvoj družbe, povečala dostop do informacij in izboljšala učinkovitost poslovnih procesov. Vendar pa je digitalna doba prinesla tudi številna varnostna tveganja, ki segajo od kibernetskih napadov, zlorabe osebnih podatkov, nepravilne uporabe digitalnih rešitev, pa vse do napačne interpretacije sprejetih podatkov

*avtor je član Slovenskega združenja korporativne varnosti

in informacij, ki nam jih posredujejo digitalne rešitve. Čeprav napredne varnostne rešitve, kot so umetna inteligenca ter avtomatizacija in šifriranje, igrajo ključno vlogo pri zaščiti digitalnih sistemov, ostaja človek najpomembnejši dejavnik pri njihovem upravljanju. Da bi ljudje lahko sledili temu razvoju in ga obvladovali, je potrebna zadostna stopnja digitalne pismenosti in poudarjanje pomena človeka pri upravljanju varnostnih tveganj.

Vse bolj spoznavamo, kako pomembno je, da se digitalna preobrazba osredotoča predvsem na posameznika (Krovna strategija digitalne preobrazbe Slovenije do leta 2030). Digitalna pismenost vključuje razumevanje, kako delujejo informacijske tehnologije, kako se zaščititi pred spletnimi grožnjami in kako uporabljati varnostna orodja. Po podatkih Evropske komisije iz leta 2022 ima kar 44 % prebivalcev EU nizko digitalno pismenost, kar pomeni, da ne poznajo osnovnih varnostnih praks, kot so uporaba dvofaktorske avtentikacije, prepoznavanje phishing napadov in drugih vrst kibernetskih groženj. V Sloveniji je stopnja digitalne pismenosti med odraslimi relativno nizka, kar pomeni, da veliko ljudi ni dovolj usposobljenih za varno uporabo digitalnih orodij. To postaja še večji problem v podjetjih, kjer zaposleni pogosto uporabljajo zastarele prakse in miselnost, kot so zapisovanje gesel na papir, uporaba enakega gesla za več računov ipd.

Statistični urad RS v eni izmed svojih analiz ugotavlja, da je imelo leta 2021 v RS zelo dobro razvite digitalne veščine 20 % prebivalstva. Razmeroma majhen je delež prebivalstva z vsaj osnovnimi digitalnimi veščinami. Ta znaša 50 %. Povprečje v EU je 54 %. Delež oseb brez digitalnih veščin je bil največji v starostni skupini 65 so 74 let, znašal je 45 %, kar je nad povprečjem EU, ki znaša 41 %. V Sloveniji je 18,4 % odraslih izjavilo, da nima izkušenj z računalniki ali nima osnovnega računalniškega znanja. Med odraslimi, ki imajo izkušnje z računalnikom, je bilo 49,2 % takih, ki so dosegli največ prvi novo ali manj v procesu reševanja izzivov v tehnološko naprednih okoljih. Na prvem nivoju so bili odrasli sposobni uporabljati le splošno razširjene rešitve, kot so e-pošta in spletni brskalniki, ter reševati probleme, ki so enostavni, z uporabo preproste logike in z minimalnimi prehodi med programi.

Ko govorimo o digitalnih kompetencah, govorimo o sposobnostih posameznika, da kompetentno in varno uporablja ter soustvarja digitalne tehnologije, rešitve in storitve. Digitalne kompetence spadajo v evropski referenčni okvir osmih ključnih kompetenc vseživljenjskega učenja. DigComp 2.2 razčlenjuje digitalne kompetence na pet ključnih področij to so: informacijska in podatkovna pismenost, komuniciranje in sodelovanje v okviru digitalnih tehnologij, ustvarjanje digitalnih vsebin, varnost in kompetence reševanja problemov. To so ključna področja, ki zahtevaj svoj prostor v sodobnih izobraževanih programih, ki zagotavljajo ustrezen nivo digitalnih kompetenc.

Človek kot najšibkejši člen ali ključni varnostni dejavnik?

Raziskave kažejo, da je več kot 80 % kibernetskih napadov povezanih s človeško napako (Verizon, 2023). Slaba gesla, pomanjkljivo razumevanje nevarnosti in neustrezno ravnanje z osebnimi podatki so glavni razlogi, zakaj napadalci uspejo. Primer iz leta 2020, ko so hekerji s pomočjo socialnega inženiringa prevzeli nadzor nad več Twitter računi kaže, da so tudi tehnološka podjetja ranljiva zaradi človeškega dejavnika.

Toda človek ni zgolj najšibkejši člen, ima tudi ključno vlogo pri zaznavanju in preprečevanju groženj. Varnostni strokovnjaki, etični hekerji in zaposleni, ki so ustrezno izobraženi, lahko bistveno zmanjšajo tveganje kibernetskih napadov.

Digitalna doba prinaša številne varnostne izzive, pri katerih ima človek ključno vlogo. Kljub napredku umetne inteligence in avtomatiziranih varnostnih sistemov in rešitev ostaja človeški dejavnik nepogrešljiv pri upravljanju varnostnih tveganj.

Pomembno je, da organizacije vlagajo v izobraževanje zaposlenih in razvijajo varnostno kulturo, ki spodbuja odgovorno ravnanje s podatki, tehnologijami in varnostnimi izzivi.

Vloga umetne inteligence pri upravljanju varnostnih tveganj

Umetna inteligenca se tudi na področju upravljanja z varnostnimi tveganji vse bolj uporablja za zaznavanje varnostnih groženj in avtomatizacijo odzivov. Napredni algoritmi lahko analizirajo ogromne količine podatkov in prepoznajo sumljive vzorce, ki bi jih človeški varnostni analitiki morda spregledali. Vendar pa uporaba umetne inteligence prinaša tudi nove izzive, kot npr.:

- Pomanjkanje razumevanja delovanja umetne inteligence. Uporabniki namreč pogosto ne razumejo, kako umetna inteligenca sprejema odločitve, kar lahko vodi do nezaupanja v sistem, v rešitve ali napačne interpretacije rezultatov.
- Zavajajoči podatki, ki jih producira umetna inteligenca. Kadar umetna inteligenca temelji na napačnih ali pristranskih podatkih, lahko sistem naredi napake, ki imajo lahko resne varnostne posledice, saj odločitve in delovanje sistemov lahko temelji na napačnih predpostavkah, podatkih in informacijah.
- Napačno konfigurirani sistemi s strani neustrezno usposobljenih strokovnjakov. Obstaja nevarnost, da organizacije in posamezni strokovnjaki ne razumejo, kako pravilno nastaviti, integrirati in uporabljati napredne in digitalne tehnološke rešitve ter umetno inteligenco, kot podporo obstoječim varnostnim rešitvam, s tem pa lahko ti sistemi postanejo neučinkoviti, nevarni ali celo škodljivi.

Glavni izzivi pri uporabi naprednih varnostnih rešitev

Kljub napredku tehnologije in vse večjem zavedanju, obstajajo resni izzivi pri implementaciji varnostnih rešitev v obstoječe sisteme, procese in organizacije, ki se kažejo predvsem v naslednjih pojavih:

- Pomanjkanje digitalne pismenosti zaradi neustreznega ali nezadostnega usposabljanja zaposlenih. Mnoge organizacije ne vlagajo dovolj sredstev in resursov v digitalno opismenjevanje in varnostno izobraževanje, zaradi česar so zaposleni bolj ranljivi in dovzetni za napade nanje in napake pri delu.
- Kompleksnost in digitalizacija varnostnih rešitev. Vse več se uvaja naprednih digitalnih orodij, kot so sistemi za zaznavanje vdorov, brezpilotni letalniki, pametna očala in napredne programske rešitve (tudi umetna inteligenca). Ta orodja ali rešitve so lahko preveč zapletene za povprečne uporabnike, kar vodi do njihove nepravilne uporabe ali celo strahu pred uporabo.
- Nizka stopnja digitalne pismenosti pri starejših uporabnikih. Le-ti imajo pogosto težave pri prilagajanju na nova varnostna pravila in nove varnostne tehnologije, kar povečuje njihovo ranljivost in učinkovitost.
- Pomanjkanje ali pa neskladnost regulativ in standardov. Na nivoju EU se sprejema nove in nove regulative na različnih področjih povezanih tudi z varnostjo (kibernetska varnost, kritična infrastruktura, umetna inteligenca ipd.), a še vedno obstajajo pomanjkljivosti pri njihovi implementaciji v državne regulative in dalje pri integraciji v organizacije.

Kakšne so možne rešitve in izboljšave?

Da bi zmanjšali razkorak med razvojem digitalnih kompetenc posameznika in globalnim tehnološkim razvojem, da bi dvignili digitalno pismenost in s tem z digitalizacijo varnostnih rešitev dejansko bolj učinkovito obvladovali varnostna tveganja, je ključno sprejeti več ukrepov kot npr.:

- Večji poudarek na izobraževanju in ozaveščanju zaposlenih. Lastniki, poslovodstva in drugi odločevalci se morajo zavedati, da bo v bodoče potrebno še več vlagati v usposabljanja zaposlenih o kibernetski ter fizični in tehnični varnosti in prilagajati programe usposabljanj za dvigovanje digitalne pismenosti zaposlenih in konkretnim rešitvam v praksi (on the job training).
- Uvajanje varnostnih standardov v varnostne procese in varnostne rešitve. Implementacija varnostnih standardov in uveljavljenih (dobrih) praks lahko bistveno poenoti in izboljša varnostne rešitve in procedure in s tem zagotavlja učinkovitejše obvladovanje varnostnih izzivov.
- Uvajanje enostavnih varnostnih orodij in rešitve. Razvijalci novih tehnologij in rešitve morajo ustvarjati uporabniku prijazne varnostne tehnologije in rešitve, ki jih lahko razume tudi nekdo brez tehničnega znanja.
- Povezovanje človeka in umetne inteligence. Čeprav umetna inteligenca lahko bistveno pripomore k hitrejšim odločitvam in učinkovitejšim varnostnim rešitvam, pa mora biti pri izvedbenih procesih vedno prisoten človek, ki zna ustrezno interpretirati, upravljati in nadzirati pridobljene podatke, informacije in določitve umetne inteligence.

Zaključek

Digitalna doba prinaša številne varnostne izzive, pri katerih ima človek ključno vlogo. Kljub napredku umetne inteligence in avtomatiziranih varnostnih sistemov in rešitev ostaja človeški dejavnik nepogrešljiv pri upravljanju varnostnih tveganj. Da bi zmanjšali varnostne grožnje, je nujno vlagati v digitalno pismenost, izboljšati regulative in spodbujati odgovorno ravnanje z digitalnimi orodji. Le s celostnim pristopom bomo lahko zagotovili varno digitalno prihodnost na način, da človek pri tem ne bo ovira, temveč učinkovita podpora. ■

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 LPT MASTER CERTIFIED · EC-Council CHFI CERTIFIED · EC-Council CPENT CERTIFIED · EC-Council CEH MASTER CERTIFIED · EC-Council ECIH CERTIFIED · OffSec OSCP

ISO 27001

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

BUREAU VERITAS

DPO

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Gregor Kovač, mag., vodja korporativne varnosti in organizacijski vodja heliporta v Splošni bolnišnici Celje*

SPLOŠNA BOLNIŠNICA CELJE PREDSTAVLJA POMEMBNO REGIJSKO ZDRAVSTVENO USTANOVO

Zdravstvene organizacije so poleg svoje osnovne dejavnosti vedno bolj pod vplivom varnostnih izzivov. Celovito upravljanje varnostnih tveganj postaja ključno za odpornost zdravstvenih organizacij. O vzpostavitvi varnostnega sistema in izzivih pri zagotavljanju varnosti v Splošni bolnišnici Celje smo se pogovarjali z Gregorjem Kovačem, vodjo korporativne varnosti.

Splošna bolnišnica Celje predstavlja pomembno regijsko zdravstveno institucijo v Republiki Sloveniji. Nam lahko prosimo pojasnite umeščenost in vlogo Službe za korporativno varnost v Splošni bolnici Celje? Kateri so tisti glavni dosežki, ki bi jih bilo potrebno izpostaviti?

Gre za vzpostavitev tako imenovanega integralnega varnostnega sistema v zavodu, kjer z varnostno politiko, vzpostavitvijo sistema upravljanja varnostnih tveganj in izrednih dogodkov ter z uvajanjem varnostnih standardov učinkovito obvladujemo varovanje in zaščito svojih lokacij, zgradb, sredstev, opreme, poslovnih in logističnih procesov, osebja, podatkov, informacij, poslovne dokumentacije in pogodbenih izvajalcev.

Posnetek in analiza stanja z oceno stopnje ogroženosti je bila izdelana po lastni metodologiji, na podlagi podatkov, informacij in dokumentov varovanja, ki so bili pridobljeni na vpogled za potrebe izdelave posnetka in analize stanja ter na podlagi operativnega posnetka stanja lokacij, zgradb ter ključnih procesov.

Organizacije, med njimi Splošna bolnišnica Celje so stalno podvrženi raznim oblikam notranjih in zunanjih nevarnosti, ogroženosti in tveganj. Gre za realne, potencialne in prikrite nevarnosti, ki v najširšem pomenu pomenijo ogroženost organizacije, materialno in moralno neugodno vplivajo na poslovne procese in poslovne rezultate ter neugodno vplivajo tudi na zaposlene in na ugled ter dobro ime organizacije. Zaradi tega je bilo smiselno, ekonomsko in poslovno koristno v našo bolnišnico uvesti varnostno funkcijo, ki prispeva k organizacijskemu redu, poslovni etiki in poslovnim rezultatom zavoda.

Korporativno oziroma poslovno varnost lahko opredelimo kot varnostni sistem v Splošni bolnišnici Celje ali sistem za zagotavljanje notranje varnosti v naši bolnišnici. Je celota pravnih, organizacijskih, funkcionalnih, tehničnih in kadrovskih ukrepov za ohranitev reda, spoštovanje zakonov in internih predpisov ter varnosti ljudi in premoženja v bolnišnici.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Obstoj sistema upravljanja z varnostjo je izrednega pomena, saj se občasno tudi naša bolnišnica nahaja v bolj ali manj (ne) stabilnem okolju.(tekst za okvir) Na nas vplivajo različni dejavniki ogrožanja, kot na primer najrazličnejša kazniva dejanja, različne nesreče, državni predpisi in ostala oblastna ravnanja, konkurenca, ipd. Notranja varnost je za poslovni uspeh v bolnišnici vitalnega pomena. Za nemoteno delovanje bolnišnice je izrednega pomena tudi varnost globalne dobavne verige. V bolnišnici imamo vzpostavljen ustrezen in učinkovit varnosti sistem s katerim lahko zagotovimo učinkovito upravljanja z varnostjo, kjer se naslanjamo na zagotavljanje skladnosti z mednarodno priznanim standardom ISO 28000:2022.

Pred dvema letoma ste v operativno uporabo dobili novo helikoptersko ploščad, ki na področju hitrega odzivanja in nujne zdravniške pomoči predstavlja pomemben dejavnik. Kakšne so izkušnje operativnosti delovanja v tem začetnem obdobju?

Izpostaviti gre strateško odločitev ob izgradnji heliporta, ki predstavlja trajnostni razvoj bolnišnice kot regionalne zdravstvene ustanove, razvoj stroke s sprejemom težkih poškodovancev in hitre oskrbe bolnikov, kjer helikopterski prevoz v terciar predstavlja izboljšano preživetje. Upravičenost investicije se je pokazala ob poplavah leta 2023, kjer je bilo v enem dnevu 12 priletov HEMSa.

Ob analizi delovanja našega heliporta smo ugotovili določene možnosti izboljšave delovanja in stabilizacije delovanja heliporta. Vsled ugotovitev smo pripravili 1. posvet o delovanju bolnišničnih heliportov z vabilom širokemu spektru udeleženih pri izvajanju delovanja bolnišničnih heliportov.

Na posvetu o delovanju bolnišničnih heliportov smo s predstavniki več deležnikov (CAA, piloti SV in policije, reševalci, MZ, Ministrstvo za infrastrukturo, MORS ...) prikazali izzive s katerimi se srečujemo ob delovanju heliportov z namenom dogovarjanja stroke-izvajalcev in organizatorjev-managementa. Prikazali smo več različnih izzivov od financiranja delovanja do poenotenja standardov delovanja bolnišničnih heliportov. Združenje, ki je bilo ustanovljeno v letošnjem letu je odgovor na zastavljena vprašanja in izzive.

Naloge Združenja bolnišničnih heliportov so: poenotenje sistema delovanja bolnišničnih heliportov od obveščanja, aktivacije, najave do sprejema poškodovancev, spremljanje, beleženje in spremljanje delovanja heliportov in posredno HEMSa, beleženje indikacij helikopterskih reševalnih prevozov, register morebitnih incidentov in neljubih dogodkov, povečanje varnosti delovanja heliportov, organizirati redna strokovna srečanja upravljalcev bolnišničnih heliportov, z drugimi deležniki organizirati redna usposabljanja osebja, ki izvajajo delovanje in vzdrževanje heliportov, oblikovati klinične poti za helikoptersko reševanje od aktivacije do sprejema poškodovancev, sprotno reševanje poročanja in reševanje novih izzivov.

V letu 2024 smo zabeležili skupno 104 prilete, primarnih in sekundarnih priletov s strani plovil Slovenske vojske in Policije . Aktivacijski čas celotne ekipe - piloti, tehniki in reševalci je bil v povprečju 11.4 minute vključno z aktivacijo sekundarnih (medbolnišničnih) transportov, kjer ni visoka stopnja nujnosti ter čas aktivacije DCZ in odobritve OpC SV.

V naši bolnišnici imamo ustrezno podporo s strani vodstva naše bolnišnice. Človeški viri so ključni kapital in naša bolnišnica se tega vse bolj zaveda. Dobrih kandidatov ni lahko najti. V prihodnosti bomo soočeni še z večjim pomanjkanjem delovne sile, zato je za našo bolnišnico izredno pomembno, da bomo znali zadržati kvalitetne kadre v svoji sredini.

V zadnjem obdobju smo priča vedno novim informacijam o nasilju uporabnikov bolnišničnih storitev nad zaposlenimi. Posebej je tukaj izpostavljen urgentni center. Kako se v SBC spoprijemate s to zahtevno problematiko?

Korporativna varnost v najširšem pomenu besede je dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v naši bolnišnici. Varnost pojmujemo kot stanje, kjer lahko posameznik uveljavlja svoje pravice in tudi dolžnosti, poenostavljeno pa lahko rečemo, da varnost predstavlja red. Varnost v zdravstvu je pomemben element kakovosti in pomeni odsotnost kakršnih koli posledic za paciente, zaposlene ali druge zaradi varnostnih odklonov. Cilj je stanje v katerem je varnostno tveganje znižano na minimalno možno raven. V zadnjem času varnost zagotavljajo različni subjekti tako javni kot korporativni. Ravno sodelovanje med slednjimi je bilo v preteklosti zagotovo bistvenega pomena tudi v Splošni bolnišnici Celje.

S sistemom za spremljanje opozorilnih nevarnih dogodkov, sporočamo t. i. najhujše nevarne dogodke tudi Ministrstvu za zdravje. V bolnišnici imamo vzpostavljen tudi interni sistem upravljanja z varnostnimi odkloni. Cilj vzpostavitve sistema je bil (1) Izdelati vzročno posledično analizo, prepoznavanje vzrokov, tako strukturnih kot procesnih, ter ustrezno ukrepanje za zmanjševanje posledic pri pacientu in preventivno delovanje, (2) Izboljšati kakovost in varnost oskrbe pacientov, (3) Izboljšati znanje o opozorilnih nevarnih dogodkih in boljše preventivno delovanje in (4) Obdržati zaupanje ljudi v našo bolnišnico.

SBC je ena izmed ključnih regijskih organizacij tudi na področju zagotavljanja neprekinjenega delovanja kritične infrastrukture in izvajanja bistvenih storitev. Ima v teh procesih Služba korporativne varnosti v SBC pomembno mesto? Kje je to najbolj izraženo?

Splošna bolnišnica Celje je tretja največja bolnišnica v Sloveniji, je medregijska bolnišnica, v skladu z zakonskimi pooblastili opravlja zdravstveno dejavnost na sekundarni ter deloma na primarni in terciarni ravni: specialistično ambulantno dejavnost in specialistično bolnišnično dejavnost. Edina v Savinjski regiji zagotavlja tudi nepretrgano specialistično pomoč. K njej gravitira do 300.000 prebivalcev širše celjske regije, kar predstavlja med 12 in 15 % slovenske populacije. Opravlja tudi določene dele tržne dejavnosti. Zaradi vsega naštetega je njena vloga, ki jo izvaja v skladu z javnimi pooblastili in pristojnostmi na sekundarni ravni, zelo pomembna, še posebej zato, ker izvaja del svoje dejavnosti tudi na terciarni ravni, čeprav storitev na tej ravni nima priznanih. S svojo dejavnostjo bistveno vpliva na dostopnost, kakovost in učinkovitost zdravstvenih storitev v Savinjski regiji in širše, v celotni državi.

Zdravstvena dejavnost Splošne bolnišnice Celje je organizirana v okviru 32 bolnišničnih oddelkov. Glede na dejavnost, ki jo opravljajo, so razdeljeni na operativne oddelke, neoperativne oddelke in oddelke skupnega medicinskega področja.

Zaradi velikosti, kompleksnosti, specifičnosti dejavnosti in razpršenosti lokacij smo se izgradnje integralnega varnostnega sistema Splošne bolnišnice Celje najprej lotili na strateškem nivoju. S posnetkom in presojo obstoječega stanja upravljanja z varnostnimi tveganji na korporativnem nivoju smo ugotovili, kako se na tem nivoju upravlja z varnostnimi tveganji in kako se sistemske rešitve upravljanja z varnostnimi tveganji prenašajo iz strateškega na operativni nivo, torej na nivo posameznih oddelkov. Posnetek in analiza stanja z oceno stopnje ogroženosti je bila izdelana po lastni metodologiji, na podlagi podatkov, informacij in dokumentov varovanja, ki so bili pridobljeni na vpogled za potrebe izdelave posnetka in analize stanja ter na podlagi operativnega posnetka stanja lokacij, zgradb ter ključnih procesov.

Splošna bolnišnica Celje poleg upravljanja z varnostnimi odkloni sprotno identificira in izvaja tudi vse potrebne sis-

temske ukrepe za obvladovanje varnostnih tveganj tudi na področju informacijske varnosti.

V sklopu članstva Splošne bolnišnice Celje v Inštitutu za korporativne varnostne študije združujemo in razvijamo nova znanja, izkušnje, spoznanja, potrebe ter uveljavljamo interese na področju korporacijske varnosti v nacionalnem in mednarodnem okolju.

Glede na dejstvo, da je SBC pomemben segment v zdravstvenem sektorju ima verjetno pomembno mesto tudi pri usklajevanju z ostalimi deležniki. Nam lahko osvetlite kvaliteto in obseg sodelovanja z ostalimi državnimi institucijami pri zagotavljanju neprekinjenosti delovanja zdravstvenega sistema?

Najizrazitejša kvaliteta sodelovanje je v naši bolnišnici izražena v sodelovanju s policijo, PGE Celje ter GRS. Splošna bolnišnica Celje je v sodelovanju s Slovensko policijo v Urgentnem centru Celje in na bolnišničnem heliportu Izvedla vajo "Amok dogodek in protiteroristični napad". V vaji so sodelovali Celjska bolnišnica, Letalska policijska enota, Specialna enota, Mobilna kriminalistična enota ter Center za varnost in zaščito slovenske policije. Scenarij vaje je predvideval napad na varovano osebo, ki je bila ob tem poškodovana. Osebo so predali v oskrbo, vaja pa se je nadaljevala s prikazi na bolnišničnem heliportu in v kletnih prostorih, kjer so pristojni aretirali storilce z uporabo posebne taktike Specialne enote.

Takšne vaje so izjemnega pomena za pripravo in usposobljenost ekip, saj nam omogočajo, da preizkušamo protokole, izboljšamo odzivnost in okrepimo sodelovanje med različnimi službami v kritičnih situacijah. Z njimi zagotavljamo boljšo pripravljenost na izredne dogodke ter večjo varnost za paciente, zaposlene in širšo skupnost.

Glede na to, da ste operativno vpet tudi v delovanja heliporta imate tudi v Celju take izzive, kot jih v medijih poslušamo glede UKC Ljubljana in njihovega heliporta?

Heliport Celje je redno vzdrževan in servisiran. Vsako leto je naš heliport podvržen tudi pregledu Agencije za civilno letalstvo. Nedelovanje heliporta Ljubljana ne morem komentirati, saj ne poznam podrobnosti.

Za učinkovit razvoj Službe za korporativno varnost je nujno potreben ustrezen strokovno usposobljen kadrovski potencial z različnimi kompetencami znanj. Je kadrovska politika na tem področju ustrezno načrtovana in ali imate s strani strateškega vodstva SBC ustrezno podporo?

V naši bolnišnici imamo ustrezno podporo s strani vodstva naše bolnišnice. Človeški viri so ključni kapital in naša bolnišnica se tega vse bolj zaveda. Dobrih kandidatov ni lahko najti. V prihodnosti bomo soočeni še z večjim pomanjkanjem delovne sile, zato je za našo bolnišnico izredno pomembno, da bomo znali zadržati kvalitetne kadre v svoji sredini.

Aktivno sodelujete v EU projektu CEDAR, kjer je projekt usmerjen v preprečevanje pojavnih oblik korupcije s tem, da se poskuša integrirati določene že obstoječe podatke in s pomočjo različnih tehnologij lažje identificirati korupcijska tveganja. Posebej ste usmerjeni v analizo področja nabav male vrednosti. Menite, da je lahko ta pilotni model dobra podlaga za uporabo teh pristopov tudi v ostalih zdravstvenih ustanovah?

Zaradi zmanjševanja in preprečevanja korupcijskih tveganj z uvajanjem umetne inteligence v procese naročanja se je Splošna bolnišnica Celje na podlagi razpisa EU, štev. CL-4-2023-DATA-01-02 in vabila Inštituta za korporativno varnostne študije, katerega člani smo, vključila v mednarodni projekt, konzorcij CEDAR - Common European Data Spaces and Robust Artificial Intelligence for Transparent Public Governance.

CEDAR bo v pomembnem delu vključeval proces transparentnosti v smeri zmanjševanja korupcijskih tveganj v različnih segmentih tudi v Splošni bolnišnici Celje. Projekt je za EU zelo pomemben zato je umeščen v okvir projektov (Research and Inovation), ki so s strani komisije financirani v obsegu 100%.

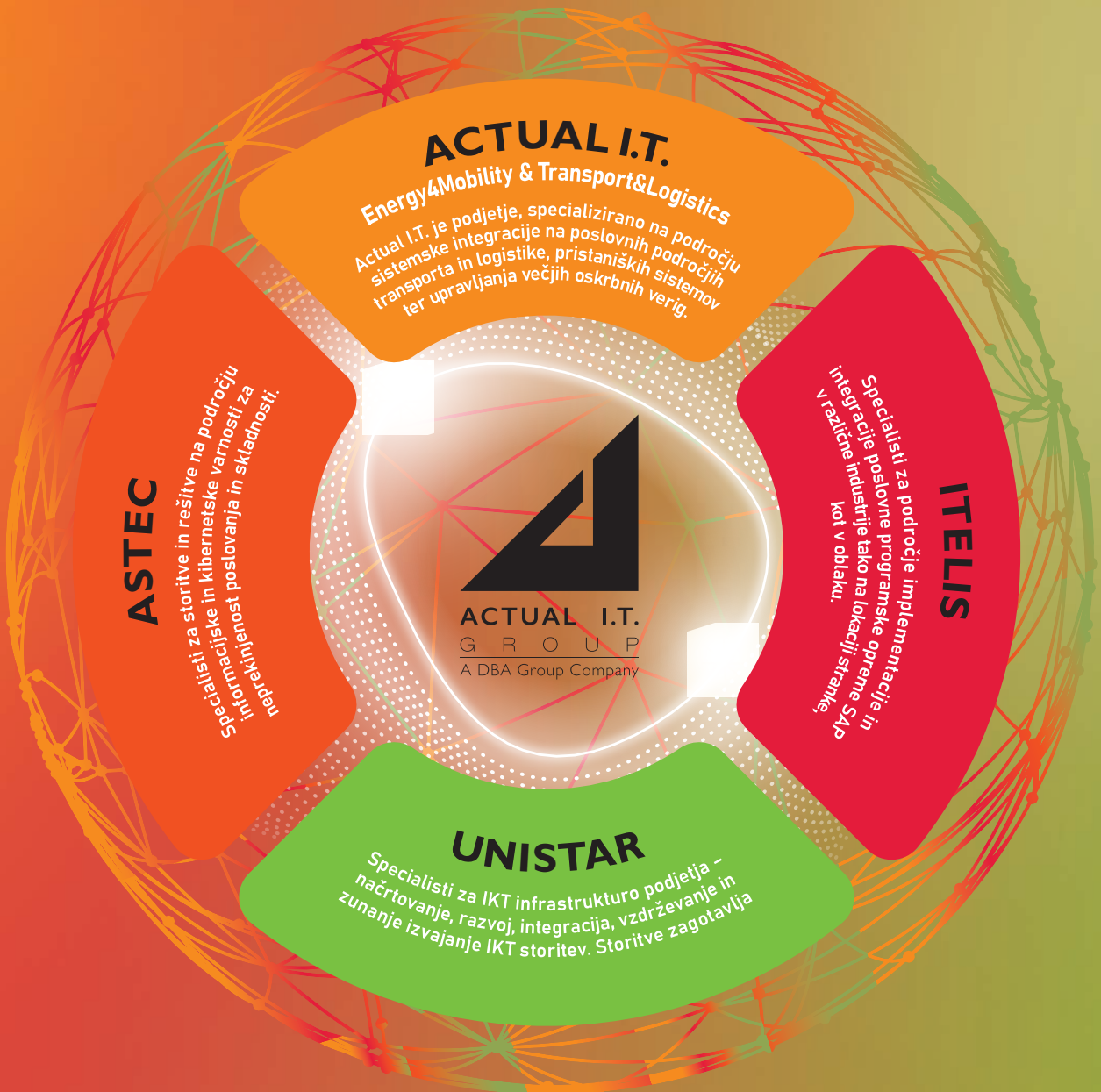
V okviru mednarodnega konzorcija je organizirano 5 pilotov, ki bodo vsak s svojega stališča obravnavali pomembne vidike uvajanja umetne inteligence v procese preprečevanja korupcijskih tveganj z izpostavljanjem določenih analiz in indikatorjev, ki organom na vseh nivojih predstavlja pomembne podatke za izvedbo nadaljnjih ukrepov za preprečevanje tovrstnih tveganj. Slovenski pilot (v SBC je določen vodja projekta), bo usmerjen na področje preprečevanja korupcije v zdravstvenem sistemu. V slovenskem pilotu so udeležene naslednje organizacije ICS Ljubljana – koordinator slovenskega pilota, Splošna bolnišnica Celje, Slovenska policija, Ministrstvo za digitalno preobrazbo, Ministrstvo za zdravje in podjetje SNEP – razvoj rešitev na področju strojnega učenja in AI. V okviru svetovalnega odbora projekta pa je vključena tudi predstavnica Komisije za preprečevanje korupcije KPK.

Po 36 mesecih, ki so namenjeni delovanju projekta, bo končni produkt dobra podlaga za uporabo teh pristopov tudi v ostalih zdravstvenih ustanovah.

Večina upravljalcev pomembne infrastrukture je združena v Slovenskem združenju korporativne varnosti. Vključeno je tudi nekaj pomembnih organizacij s področja zdravstvenega sektorja. Vam te povezave znotraj združenja olajšujejo operativno komunikacijo v realnem okolju?

V okviru poslanstva Slovenskega združenja korporativne varnosti se Splošna bolnišnica Celje združuje s pomembnimi organizacijami s področja zdravstvenega sektorja. Poleg lažje operativne komunikacije nam to povezovanje omogoča razvijanje novega znanja, izkušenj, spoznanj, potreb ter uveljavljanje interesov na področju korporativne varnosti v nacionalnem in mednarodnem okolju. ■

Foto: arhiv Splošne bolnišnice Celje



ACTUAL I.T. UNISTAR PRO astec ITELIS

www.actual-it.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Roman Fortuna, vodja Mestnega redarstva Ljubljana*

ZAGOTAVLJANJE VARNOSTI GLAVNEGA MESTA PREDSTAVLJA POSEBEN IZZIV

Specifike glavnih mest v vsaki državi pred tiste, ki zagotavljajo ustrezne procese varnosti, postavljajo posebne izzive. Te posebnosti je potrebno ustrezno razumeti in jih upoštevati pri zagotavljanju celovitega pristopa zagotavljanja varnosti. Mestno redarstvo Ljubljana v prakso prinaša nove modele zagotavljanja varnosti. Ti pristopi lahko v prihodnosti spremenijo razumevanje vloge organizacij, ki v glavnem mestu zagotavljajo varnostne procese na različnem nivoju pristojnosti. O novih pristopih in izzivih smo se pogovarjali z g. Romanom Fortuno, vodjo Mestnega redarstva Ljubljana.

Glede na to, da že vrsto let vodite Mestno Redarstvo v Ljubljani lahko z gotovostjo podate oceno varnostnih izzivov s katerimi se sooča naše glavno mesto?

Glede na razpoložljive podatke in informacije ocenjujemo, da so varnostne razmere v Ljubljani še vedno stabilne in ugodne. To potrjujejo Poročila o varnostnih razmerah Policijske uprave Ljubljana, Poročila o delu Mestnega redarstva ter Ocene varnostnih razmer v Mestni občini Ljubljana. Poleg tega javno dostopni podatki globalne baze Numbeo kažejo na nizek indeks kriminalitete in visok indeks varnosti v Ljubljani. Pri spremljanju stanja zaznavamo določena odklonska ravnanja, ki povzročajo nelagodje med občani in zmanjšujejo občutek varnosti. K temu prispevajo tudi včasih pristranska poročanja medijev o posameznih varnostnih tematikah, ki vplivajo na občutek ogroženosti in padec občutka varnosti. Posledično beležimo večje število pobud občanov, ki zahtevajo naše ukrepanje ali večjo prisotnost na terenu.

> Že več kot desetletje redarstva uspešno uporabljajo del policijskih pooblastil, česar pa ne odraža samo poimenovanje službe. Po vzoru iz tujine bi bilo smiselno razmisliti o formalnem preimenovanju službe v lokalno policijo, kar bi odražalo dejanski obseg nalog in pooblastil.

Katera so tista glavna težišča razvoja mestnega redarstva, ne samo v Ljubljani temveč v vseh večjih urbanih okoljih v Sloveniji. Mestno redarstvo Ljubljana je v mnogočem tisti prvi znanilec sprememb, katere uvajate na to področje.

V zadnjem desetletju opažamo pluralizacijo policijske dejavnosti, kar pomeni, da različni javni in zasebni subjekti, skladno s pristojnostmi, izvajajo določene (policijske) naloge, povezane z zagotavljanjem varnosti. Redarstvo je v tem kontekstu edinstveno, saj se po pooblastilih in nalogah najbolj približa

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

policiji. Že več kot desetletje redarstva uspešno uporabljajo del policijskih pooblastil, česar pa ne odraža samo poimenovanje službe. Po vzoru iz tujine bi bilo smiselno razmisliti o formalnem preimenovanju službe v lokalno policijo, kar bi odražalo dejanski obseg nalog in pooblastil.

Z decentralizacijo, ki je bila posledica dejstva, da država potrebuje partnerstvo pri zagotavljanju varnosti v lokalnem okolju, se je povečala vloga občin oz. lokalne skupnosti pri zagotavljanju varnosti na njihovem območju. Občine bi na področju lokalne varnosti delovale učinkovito le z moderno organizacijo, ki se je sposobna prilagajat varnostnim razmeram v lokalnem okolju. Potrebne so korenite spremembe krovne zakonodaje (Zakona o občinskem redarstvu), ki bi omogočile funkcionalno in organizacijsko prestrukturiranje službe, da bi lahko učinkoviteje opravljala svoje delo na področju zagotavljanja prometne in splošne javne varnosti v lokalnem okolju.

Prav tako obstaja veliko prostora in možnosti za izboljšanje povezljivosti in sodelovanja z drugimi službami s področja zagotavljanja javne in osebne varnosti in sistema zaščite ter reševanja, saj trenutno zakonodaja predvideva zgolj sodelovanje redarstva in policije. Poleg sodelovanja z drugimi institucijami, bi bilo potrebno formalno predvideti tudi sodelovanje redarstev s skupnostjo in preventivno delo, ki izhajajoč iz »v skupnost usmerjenega policijskega dela« prinaša pozitivne rezultate na področju varnosti v lokalnem okolju v smislu izmenjave informacij z občani, višanja občutka varnosti in zmanjšanja števila kršitev.

Poleg tega so tehnološki razvoj, digitalizacija in optimizacija delovnih procesov ključna vodila pri razvoju redarskega dela. Na trgu so na voljo preizkušene tehnologije, ki jih v tujini že dalj časa uporabljajo na področju zagotavljanja javne in prometne varnosti. Tehnološke rešitve imajo v praksi tako represivne kot tudi preventivne učinke, kar lahko najbolje ponazorimo s primerom stacionarnih samodejnih merilnih naprav, ki doprinesejo k zmanjšanju hitrosti na kritičnih cestnih odsekih z doslednim sankcioniranjem prekoračitev. Poleg tega, pa delujejo tudi preventivno, saj se hitrost na kritičnem odseku zmanjša tudi v času, ko sama samodejna merilna naprava ni nameščena v ohišju. Z uvedbo podobnih rešitev tudi na drugih področjih redarskega dela lahko bistveno zmanjšamo vpliv pomanjkanja kadra na

naše delo. Hkrati lahko s sodobno tehnologijo zagotovimo učinkovitejši pristop k urejanju in nadzoru prometa ter zagotavljanju splošne javne varnosti. Poleg tega lahko prispevamo k večji pravni varnosti strank v postopkih, zmanjšamo možnosti prekoračitve pooblastil, optimiziramo delovne procese ter izboljšamo prometno in splošno javno varnost v mestu. V praksi smo že uvedli avtomatizirano obdelavo fotografij prekoračitev hitrosti, ki jih zaznamo s pomočjo samodejnih merilnih naprav in spletni vpogled v prekrške, kar kršiteljem omogoča hiter, enostaven in pregleden dostop do informacij.

Mesto Ljubljana ima že zaradi dejstva, da je glavno mesto, določene varnostne specifike, ki jim morate naslavljati tudi v okviru delovanja Mestnega redarstva Ljubljana. Katere so tiste posebnosti, ki vas v tem okviru ločujejo od ostalih mestnih redarstev?

Zakon o glavnem mestu nas zavezuje, da zagotavljamo nemoteno delovanje državnih in mestnih institucij ter posebej skrbimo za javno varnost. Ker je Ljubljana pomembno prometno, gospodarsko, kulturno, politično in izobraževalno središče, to povzroča povečano gostoto pro-

meta in ljudi ter s tem povezana tveganja za prometno in javno varnost. V Ljubljani se na dnevni ravni nahaja preko pol milijona ljudi, kar predstavlja približno četrtino prebivalcev Slovenije, in preko 100.000 vozil. Na območju Ljubljane deluje tudi ključna kritična infrastruktura ter institucije državnega pomena. Poleg tega moramo upoštevati možnost naravnih in drugih nesreč, ki lahko bistveno vplivajo na stanje varnosti. Zaradi teh dejavnikov se soočamo z večjim obsegom dela in raznolikimi zahtevami oz. pričakovanji občanov ter institucij. Z namenom zagotavljanja karseda nemotenega delovanja zgoraj navedene infrastrukture in kvalitete življenja občanov je, v primerjavi z ostalimi redarstvi, količina in raznovrstnost dela v Ljubljani večja, kot je večja tudi potreba po naši prisotnosti na terenu. Raznolikost nalog in pričakovanj občanov ter institucij zahteva stalno prilagodljivost, strateško načrtovanje in učinkovito sodelovanje z drugimi službami. Kljub našemu dobremu delu pa smo pogosto tarča neupravičenih kritik laične javnosti, ki izhajajo iz nepoznavanja delovanja in pristojnosti redarstva.

V dobi, kjer je tehnološki razvoj izredno hiter, je verjetno tudi v vaši paradigmi usmeritev po ustreznem uveljavljanju novih tehnoloških rešitev za izboljšanje učinkovitosti vašega dela. Ali imate v načrtu na tem področju uvajati nove tehnološke rešitve in kakšni izzivi se vam pojavljajo na tej poti?

V Mestni občini Ljubljana je varnost prepoznana kot ena najpomembnejših vrednot in ena izmed prioritet trajnostnega razvoja. Na Mestnem redarstvu si z vso predanostjo prizadevamo za zagotavljanje reda in varnosti v Ljubljani, pri čemer nas usmerja slogan: »V službi mesta.«

Tehnološki razvoj ponuja številne možnosti za optimizacijo dela, predvsem razbremenitev kadra, tako redarstva kot tudi drugih varnostih subjektov, ki skrbijo za javno in prometno varnost. Na področju tehnološkega razvoja zaostajamo za sosednjimi državami. Ključni predpogoj za uvedbo tehnoloških rešitev je ustrezna zakonska podlaga, ki bo na eni strani zagotavljala varstvo vseh pravic posameznikov in nam na drugi strani omogočala razširitev možnosti uporabe tehničnih sredstev, kot pripomočka pri doseganju zastavljenih ciljev, na področju prometne kot tudi splošne javne varnosti. Načrtujemo širitev uporabe podobnih tehnoloških rešitev, ki bodo omogočile optimizacijo delovnih procesov, povečale učinkovitost ter zmanjšale delovne obremenitve naših zaposlenih. Izkušnje z uporabo tehničnih rešitev na področju meritev hitrosti kažejo, da je v praksi to mogoče in da lahko z ustreznimi varovalnimi mehanizmi preprečimo zlorabe tehnologije. Ključni izzivi pri uvajanju novih tehnologij so torej pomanjkanje ustrezne zakonske podlage, ki bi omogočila širšo uporabo tehničnih rešitev, in zagotavljanje varstva osebnih podatkov. Intenzivno se zavzemamo za spremembe in izboljšanje predpisov, saj bi z uvedbo tehničnih sredstev lahko bistveno izboljšali oziroma optimizira-

li prakso izvajanja urejanja, nadzora in preventive v cestnem prometu.

Za učinkovito delovanje tako pomembnega organa, kot je Mestno redarstvo je potrebna ustrezna podpora s strani strateškega vodstva v mestu Ljubljana. Menite, da imate ustrezno podporo s strani Župana in ostalih ključnih mestnih institucij?

V Mestni občini Ljubljana je varnost prepoznana kot ena najpomembnejših vrednot in ena izmed prioritet trajnostnega razvoja. Na Mestnem redarstvu si z vso predanostjo prizadevamo za zagotavljanje reda in varnosti v Ljubljani, pri čemer nas usmerja slogan: »V službi mesta.« Župan izkazuje velik posluh za potrebe mesta in meščanov na področju varnosti. Transparentno delo, podprto z argumenti, rezultati in sodelovanjem, predstavlja temelj podpore vodstva in ključnih institucij pri izvajanju naših nalog.

Mestna redarstva za učinkovitost dela potrebujejo tudi ustrezno partnerstvo in podporo raznovrstnih državnih institucij, predvsem Policije. Je ta nivo partnerstva na vseh nivojih ustrezen ali menite, da je možno tukaj še storiti kakšen korak k izboljšanju tega partnerstva? Predvsem tukaj referiramo tudi na podporo pri zakonskih rešitvah na določenih pomembnih področjih delovanja mestnih redarstev.

Sodelovanje med različnimi subjekti je ključno za zagotavljanje varnosti na lokalnem nivoju. Najbolj intenzivno Mestno redarstvo sodeluje s Policijsko upravo Ljubljana, natančneje policijskimi postajami, s katerimi odlično sodelujemo na področju izmenjave informacij in tudi v obliki mešanih patrulj na terenu v sestavi redar – policist. Na področju prometne varnosti in pri reševanju varnostnih vprašanj pa vključujemo tudi druge institucije in deležnike, kot so Agencija za varnost prometa, Svet za preventivo in varnost v cestnem prometu Mestne občine Ljubljana in Četrtne skupnosti. Poleg omenjenega operativnega sodelovanja, odlično sodelujemo tudi z akademsko skupnostjo in raziskovalnimi inštituti, predvsem s Fakulteto za varnostne vede Univerze v Mariboru, ICS - Inštitutom za korporativne varnostne študije, IVSR – Inštitutom za varnost in strateške raziskave in IPO – Internacionalno policijsko organizacijo. Ne smemo pozabiti tudi dolge prakse mednarodnega sodelovanja s predstavniki tujih služb, ki skrbijo za javno varnost na lokalnem nivoju. Kljub dobrim praksam vsekakor obstajajo priložnosti za izboljšanje, predvsem z jasno zakonsko opredelitvijo partnerstev in razširitvijo sodelovanja z drugimi institucijami na področju javne varnosti, ob predpogoju kadrovskih popolnitev.

Sodelovanje med različnimi institucijami je ključno za doseganje sinergijskega učinka. Pomembno je tudi vključevanje predstavnikov korporativne varnosti, saj kritična infrastruktura omogoča nemoteno delovanje družbe, hkrati pa predstavlja varnostno tveganje.

Kadrovski izzivi so verjetno tudi pri vas trenutno pereča tematika. Kakšno je stanje in predvsem ali imate kakšne predloge rešitev, ki bi bili lahko zanimivi tudi za ostalo varnostno skupnost?

Pomanjkanje kadra je izziv za vse subjekte, ki zagotavljajo varnost. V Ljubljani, kot glavnem mestu, se ta izziv še posebej izraža zaradi specifičnih varnostnih potreb. Rešitve vidimo v dodatnem vlaganju v zaposlovanje, izobraževanje, nagrajevanje, prilagoditvi pogojev dela in uvedbi tehnoloških rešitev za razbremenitev kadrovskih virov. Vzpostavljanje navedenih mehanizmov pomembno prispeva k motivaciji in ohranjanju kakovosti dela, vendar bi bilo potrebno tovrstno problematiko nasloviti na sistemski ravni. Vse, ki jih zanima dinamično in odgovorno delo mestnega redarja ter si želijo pridružiti naši ekipi pri zagotavljanju reda in miru v Ljubljani, vabimo, da se obrnejo na tajništvo Mestnega redarstva, kjer jim bomo z veseljem posredovali dodatne informacije.

Korporativna varnost postaja pomemben deležnik pri zagotavljanju varnosti, predvsem ključnih organizacij, ki upravljajo s kritično infrastrukturo in bistvenimi storitvami. Glede na dejstvo, da je pomembno število te kritične infrastrukture lokacijsko umeščeno v glavno mesto, je verjetno tudi v vašem strateškem interesu, da se to partnerstvo širi tudi na predstavnike korporativne varnosti. Menite, da je predvsem v lokalnih okoljih za ustrezno zagotavljanje varnosti širšega okolja potrebno vzpostaviti delujoče tripartitno partnerstvo med Policijo, Mestnim redarstvom Ljubljana in predstavniki korporativne varnosti v organizacijah?

Sodelovanje med različnimi institucijami je ključno za doseganje sinergijskega učinka. Pomembno je tudi vključevanje predstavnikov korporativne varnosti, saj kritična infrastruktura omogoča nemoteno delovanje družbe, hkrati pa predstavlja varnostno tveganje. Mestno redarstvo je v preteklosti že sodelovalo s predstavniki kritične infrastrukture v okviru evropskega projekta Precinct, kjer smo na podlagi scenarijev kaskadnega dogodka potrdili našo medsebojno povezanost in soodvisnost.

Mestno redarstvo je preko mesta Ljubljane tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja različnih varnostnih strokovnjakov lahko učinkovita platforma za iskanje ustreznih varnostnih odgovorov na zahtevne varnostne izzive?

Združevanje različnih varnostnih strokovnjakov omogoča obravnavo varnostnih problematik z različnih vidikov. Vključevanje v Slovensko združenje korporativne varnosti nam omogoča dostop do strokovnih znanj, izkušenj in dobrih praks, kar pripomore k učinkovitejšemu delu in večji prepoznavnosti Mestnega redarstva.

Kaj bi za konec sporočili bralcem revije Korporativna varnost?

Varnost je pomembna dobrina, ki jo moramo, glede na aktualne dogodke v naši bližini, še bolj ceniti. Naša naloga je, da proaktivno delujemo in se ne zadovoljimo z občutkom trenutne varnosti. Ljubljana je prepoznana kot varno mesto, kar pomembno prispeva k njeni privlačnosti tako kot turistične destinacije tudi kot kakovostnega okolja za življenje. Ob nenehnem povečevanju gostote ljudi in prometa pa se soočamo z izzivom, kako to varnost ohraniti. Pomembno je, da sledimo razvoju, uvajamo sodobne tehnološke rešitve in zaposlimo dodatne kadre, ki bodo tudi v prihodnje omogočali učinkovito zagotavljanje varnosti v našem mestu. ■

doorcloud

www.doorcloud.com

Odprite vrata od kjerkoli

Door Cloud je napredna rešitev za kontrolo pristopa, ki temelji na računalniškem oblaku in organizacijam omogoča, da na daljavo in v realnem času upravljajo ter spremljajo dostop do svojih prostorov.

Brez kartic, brez čitalcev

Vrata lahko odprete od kjerkoli s pomočjo pametnega telefona (iOS ali Android) ali Apple pametne ure. Čitalci kartic na račun napredne tehnologije za lociranje niso več potrebni. Identifikacija obiskovalca poteka preko mobilne aplikacije, vrata pa so izbrana s pomočjo lokacije pametnega telefona. Če so identifikacijske kartice kljub vsemu še vedno potrebne, je mogoče čitalec kartic in mobilni dostop uporabiti skupaj na katerihkoli vratih.

Večja varnost

Door Cloud temelji na novi generaciji krmilnikov namenjenih delovanju v oblaku po najsodobnejših varnostnih standardih in protokolih. Enako velja tudi za gostiteljsko platformo (Microsoft Azure) in mobilno maplikacijo (Android, iOS). Mnoge raziskave ugotavljajo, da so tako zgrajeni sistemi kontrole pristopa bolj varni pred vdori (hacking) od klasičnih lokalnih sistemov.

Povezava za odklepanje vrat

Uporabniki storitve Door Cloud lahko drugim osebam omogočijo dostop tako, da jim pošljejo povezavo za odklepanje vrat. Ker je povezava za odklepanje vrat običajna spletna povezava, zanjo ne potrebujemo aplikacije, zato lahko vsi, ki imajo pametni telefon in internetno povezavo, do nje dostopajo neposredno iz brskalnika.

Brezžične ključavnice

Door Cloud lahko uporabljate s splošnimi odpirali za vrata, z drugimi žičnimi električnimi ključavnicami ali pa z brezžičnimi ključavnicami Aperio podjetja Assa Abloy. Ključavnice Aperio lahko odprete s karticami ali z mobilnim telefonom prek mobilne aplikacije Door Cloud. Ključavnice Aperio in vrata se lahko prosto kombinirajo.

SPICA

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

INTERVJU
Peter Ceferin, direktor tehnike, Smart Com d.o.o.*

SLOVENSKO ZDRUŽENJE ELEKTROENERGETIKOV DEL POMEMBNE MEDNARODNE POVEZAVE

Slovensko združenje energetikov je polnopravni član pomembne mednarodne asociacije CEGRE-CIRED. Ob dejstvu, da tudi v elektro energetske sisteme vedno bolj prodira potreba po uvajanju informacijskih podpornih sistemov, se samo po sebi odpira vprašanje izzivov, ki jih prinašajo kibernetska tveganja. O delovanju tega pomembnega mednarodnega združenja in izzivih s področja kibernetske varnosti smo odprli razpravo z g. Petrom Ceferinom.

V zadnjem obdobju ste prevzeli pomembne dolžnosti v okviru Slovenskega združenja elektroenergetikov CIGRE-CIRED. Nam lahko zaupate osnovno poslanstvo te mednarodne asociacije, katere del je tudi Slovenija?

Slovensko združenje elektroenergetikov je strokovna organizacija, ki temelji na prostovoljnem, samostojnem in nepridobitnem delu fizičnih in pravnih oseb. Njegov glavni namen je izmenjava izkušenj in strokovnih znanj s področja elektroenergetike ter aktivno soustvarjanje na področju razvoja elektroenergetskih sistemov. Poslanstvo združenja je usmerjeno k stalnim izboljšavam elektroenergetskih sistemov, pri čemer ključno vlogo igra strokovno delo različnih ekspertov s tega področja.

Slovensko združenje CIGRE-CIRED je polnopravni član Mednarodnega sveta za velike elektroenergetske sisteme CIGRE (kratica izhaja iz francoskega poimenovanja »Conseil International des Grands Réseaux Electrique«) s sedežem v Parizu in predstavlja eno najstarejših strokovnih združenj nasploh, saj je bilo ustanovljeno že davnega leta 1921. Ravno tako je slovensko združenje CIGRE-CIRED polnopravni član Mednarodne konference za distribucijo električne energije CIRED (kratica izhaja ravno tako iz francoskega poimenovanja »Congrès International des Réseaux Electriques de Distribution«), s sedežem v Liegeju. Ker se tematike CIGRE in CIRED dopolnjujejo, smo v Sloveniji s konferenco leta 2001 pričeli delovati kot združenje in izvajati aktivnosti z obeh področij.

Danes strokovnjaki na skoraj vseh področjih elektroenergetike uporabljajo IKT sisteme kot nepogrešljiva orodja za izvajanje osnovnih procesov in nalog. Lahko govorimo o dveh vzporednih, a tesno prepletenih infrastrukturah: elektroenergetski infrastrukturi in informacijsko- komunikacijski infrastrukturi.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Moje delovanje v okviru slovenskega združenja sega že v obdobje prvih konferenc, kjer sem od leta 1995 dalje začel objavljati članke in aktivno sodelovati. Hkrati sem se strokovno poglabljal v področje informacijsko-komunikacijskih tehnologij (IKT) v elektroenergetskih sistemih, tako v teoriji, kot praksi, kar mi je omogočilo vključitev v bolj poglobljeno strokovno delovanje na področju IKT znotraj strukture slovenskega združenja CIGRE – CIRED, v zadnjem obdobju še posebej na področju kibernetske varnosti v elektroenergetiki. Od leta 2023 sem tudi redni član mednarodnega študijskega komiteja D2 CIGRE, ki naslavlja izzive informacijskih sistemov in telekomunikacij, kjer se aktivno vključujem v izmenjavo informacij med mednarodnim in slovenskim študijskim komitejem D2. Eno od področij mojega trenutnega dela je vodenje, koordinacija in izvajanje strokovnih recenzij člankov, ki jih avtorji z vsega sveta pripravljajo za glavne konference in simpozije CIGRE. Pri tem uporabljajo zelo stroga strokovna merila, da se zagotovi visoka kakovost objavljenih člankov.

V preteklosti je znotraj energetike veljalo prepričanje, da so ključni energetski sistemi popolnoma ločeni od informacijskega okolja. Razvoj informacijske tehnologije je to paradigmo postavil na popolnoma drugačne temelje. Lahko ocenite, ali je sploh še možno govoriti o delovanju energetskih sistemov brez informacijske podpore?

Delovanje elektroenergetskih sistemov brez informacijske podpore si danes skoraj ni več mogoče predstavljati. T. i. pametna omrežja (ang. Smart Grids), ki se intenzivno razvijajo najmanj zadnji dve desetletji (marsikje pa tudi že prej), temeljijo na vpeljavi in močni podpori informacijsko-komunikacijskih tehnologij. Industrija na tem področju in elektroenergetski sistemi so v tem času vpeljali vrsto tehnoloških inovacij in izboljšav. Danes strokovnjaki na skoraj vseh področjih elektroenergetike uporabljajo IKT sisteme kot nepogrešljiva orodja za izvajanje osnovnih procesov in nalog. Lahko govorimo o dveh vzporednih, a tesno prepletenih infrastrukturah: elektroenergetski infrastrukturi in informacijsko-komunikacijski infrastrukturi. Procesni (OT) segmenti elektroenergetskega sistema so močno prepleteni s t. i. sekundarnimi sistemi, ki vsebujejo programsko opremo in komunikacijske vmesnike. Zaradi tega nastajajo številne nove možnosti, saj so na voljo ogromne količine podatkov iz operativnih sistemov. Ni presenetljivo, da je področje obdelave velikih podatkov (ang. big data) in vpeljava umetne inteligence v procese doživela velik razmah tudi v elektroenergetiki.

Tudi v preteklosti je bil znotraj t. i. OT področij procesnih sistemov prisoten velik delež informacijskih in komunikacijskih sistemov. Vendar se je v zadnjih letih skokovito povečala potreba po povezovanju teh sistemov z IT domenami, hkrati pa se tudi dinamika razvoja znotraj OT povečuje. Ta trend se bo v prihodnosti le še okrepil, saj že sedaj opažamo porast novih tehnologij znotraj elektroenergetskega sistema. Razmere se z množičnim uvajanjem razpršenih virov, prehoda ogrevanja na električno energijo in pohodom e-mobilnosti zelo hitro spreminjajo.

S porastom vpetosti informacijskih tehnologij v energetskem sektorju je tudi kibernetska varnost dobila visoko prioriteto. Kaj so tisti osnovni cilji, ki jih znotraj združenja elektroenergetikov CIGRE-CIRED zasledujete pri dvigovanju zavedanja o pomenu kibernetske varnosti v sistemu elektroenergetike?

V zadnjem obdobju pa je zaradi spremenjenih razmer in izzivov, povezanih z digitalizacijo, avtomatizacijo in povezovanjem različnih akterjev v elektroenergetskih sistemih, pomen kibernetske varnosti močno porastel.

Na področju kibernetske varnosti v elektroenergetskih sistemih je mednarodno združenje CIGRE opredelilo več ciljev, ki so skladni z njihovim poslanstvom - spodbujanjem izmenjave znanja in sodelovanje v elektroenergetiki. Pri tem so vključeni vrhunski strokovnjaki s področja kibernetske varnosti, osredotočeni na izzive, povezane z elektroenergetskimi sistemi. Te cilje preko sodelovanja v slovenskem združenju CIGRE-CIRED prenašamo v slovenski elektroenergetski sistem, s čimer zagotavljamo vpeljavo najboljših praks in izboljšujemo odpornost sistema proti kibernetskim grožnjam. Najpomembnejši cilj pobud CIGRE je krepitev odpornosti na kibernetske grožnje. Ključnega pomena pri tem je ozaveščanje o pomenu kibernetske varnosti, ki ga uresničujemo z različnimi aktivnostmi:

- aktivnosti za stalno povečevanje ozaveščenosti deležnikov v elektroenergetskih podjetjih o pomenu kibernetske varnosti;
- izpostavljanje potencialnih tveganj in ranljivosti elektroenergetskih sistemov, povezanih s kibernetskimi grožnjami;
- osveščanje o nastajajočih kibernetskih grožnjah, značilnih za energetsko infrastrukturo;
- omogočanje izmenjave znanja in najboljših praks;
- spodbujanje sodelovanja med deležniki in ostalimi ekspertnimi organizacijami na mednarodni in nacionalni ravni;
- spodbujanje vključevanja ukrepov kibernetske varnosti v načrtovanje, delovanje in vzdrževanje elektroenergetskih sistemov;
- podpora oblikovanju politik in predpisov z zagotavljanjem tehnično-strokovnega znanja oblikovalcem politik.

Na mednarodnem nivoju CIGRE deluje s podporo celega niza strokovnih odborov, ki delujejo na različnih področjih. Kako je s področjem kibernetske varnosti? Je temu posve-

Dve področji sta izrazito močno zaznamovani z delom slovenskih strokovnjakov: prvo je področje izmenjave informacij in podatkov za omogočanje prihodnje interoperabilnosti prenosa in distribucije, kjer delujejo trije slovenski strokovnjaki, drugo pa področje kibernetske varnosti, kjer delujeta dva slovenska strokovnjaka. Poleg tega me veseli dejstvo, da smo bili prepoznani tudi na področju varnostno-operativnih centrov.

čen poseben odbor na mednarodni ravni?

Delovanje mednarodne CIGRE je organizirano znotraj 16 strokovnih domen oz. študijskih komitejev, ki združujejo strokovna znanja s posameznih področij, ključnih za elektroenergetske sisteme. Enaka organizacija velja tudi za slovensko združenje CIGRE-CIRED, z eno izjemo - dodan je namreč še en študijski komite, osredotočen na gradnike energetske preobrazbe. Že prej omenjen študijski komite - D2 se ukvarja izključno z IKT, ki so del elektroenergetskih sistemov že dlje časa. V zadnjem obdobju pa je zaradi spremenjenih razmer in izzivov, povezanih z digitalizacijo, avtomatizacijo in povezovanjem različnih akterjev v elektroenergetskih sistemih, pomen kibernetske varnosti močno porastel. Zato je tudi študijski komite D2 razširil svoje področje in spremenil ime v »Informacijsko komunikacijske tehnologije in kibernetska varnost«. S tem združuje tri povezane segmente: področje informacijskih tehnologij, telekomunikacijske sisteme in kibernetsko varnost. Ker so ta področja medsebojno izjemno prepletena, je njihovo združevanje znotraj ene skupine najbolj smiselno. Poleg tega komite D2 intenzivno sodeluje tudi z ostalimi študijskimi komiteji, saj so IKT in kibernetska varnost ključne za večino vsebinskih sklopov elektroenergetskih sistemov.

Slovensko znanje in strokovnjaki so v okviru globalne mednarodne organizacije CIGRE zelo cenjeni. Kje so tista glavna težišča, kjer ste predstavniki iz Slovenije še posebej aktivni?

Slovenski strokovnjaki so aktivno vključeni v delovanje mednarodnega združenja CIGRE in prisotni v skoraj vseh študijskih komitejih, kjer je slovensko znanje visoko cenjeno. Enako velja tudi za študijski komite D2, kjer je v različnih delovnih skupinah (ang. Work Groups - WG), bodisi znotraj domene D2 bodisi mešanih delovnih skupinah z ostalimi študijskimi komiteji, aktivnih 10 slovenskih strokovnjakov. Ti delujejo v okviru 16 trenutno aktivnih delovnih skupin. Dve področji sta izrazito močno zaznamovani z delom slovenskih strokovnjakov: prvo je področje izmenjave informacij in podatkov za omogočanje prihodnje interoperabilnosti prenosa in distribucije, kjer delujejo trije slovenski strokovnjaki, drugo pa področje kibernetske varnosti, kjer delujeta dva slovenska strokovnjaka. Poleg tega me veseli dejstvo, da smo bili prepoznani tudi na področju varnostno-operativnih centrov. V nedavno ustanovljeno delovno skupino, posvečeno implementaciji varnostno-operativnih centrov v elektroenergetiki, smo vključili slovenskega strokovnjaka.

Glede na kompleksnost varnostnega okolja je zelo težko zagotoviti, da vsako združenje ali organizacija za sebe integrira dovolj znanja in izkušenj za uspešno soočanje z varnostnimi izzivi, ki vplivajo na naše organizacije. Menite, da se tukaj kaže potreba po tesnejšem sodelovanju med ekspertnimi organizacijami? Ali lahko kot primer izpostavimo sodelovanje med Slovensko CIGRE-CIRED in Slovenskim združenjem za korporativno varnost?

Sodelovanje med različnimi ekspertnimi skupinami je izredno pomembno. Eden od osrednjih ciljev mednarodnega združenja CIGRE in slovenskega združenja CIGRE-CIRED je prav sodelovanje z ostalimi ekspertnimi organizacijami, ki imajo in razvijajo poglobljena strokovna znanja na področju kibernetske varnosti, še posebej tistimi, ki imajo tudi domenska znanja o kritičnih sistemih in korporativni varnosti. Kibernetska varnost v elektroenergetskih sistemih je namreč preplet različnih strokovnih področij, kar zahteva usklajeno delovanje na področju procesov, virov in tehnologij. Slovensko združenje za korporativno varnost se osredotoča prav na ta področja, zato je sodelovanje med združenjem CIGRE-CIRED in Slovenskim združenjem za korporativno varnost pomembno. Takšno sodelovanje bi bilo smiselno razvijati tudi v prihodnje.

Kaj bi z vašega strokovnega stališča sporočili bralcem revije kot pomembna napotila za leto 2025?

Glede na izredno hitro dogajanje na obeh straneh, ki vplivata na odpornost organizacij na kibernetske grožnje – na eni strani grožnje s strani napadalcev, hekerjev in drugih akterjev s slabimi nameni, na drugi pa hiter razvoj tehnologij in vedno bolj sofisticirani pristopi za krepitev odpornosti - bo nujno potrebno spremljati aktualne trende, tehnološki napredek in prepoznavati nove izzive, s katerimi se soočamo na področju kibernetske obrambe.

Pričakovati je porast groženj, ki jih poganja umetna inteligenca, avtomatizirani napadi in prilagodljive zlonamerne programske opreme. Po drugi strani pa bo uporaba umetne inteligence in avtomatizacije v kibernetski obrambi ključnega pomena. Takšni izzivi bodo zahtevali ustrezen odziv organizacij, ki ne bo vključeval zgolj tehnoloških rešitev, temveč tudi vzpostavitev ustreznih organizacijskih struktur in procesov. Ena izmed rešitev bo povezovanje znotraj elektroenergetike v enovit varnostnooperativni center, ki bo omogočil učinkovitejšo obrambo pred kibernetskimi napadi. Posebno pozornost bo treba posvetiti krepitvi kibernetske zaščite v OT in IoT segmentih, kjer še vedno obstajajo vrzeli, ki jih bo treba zapolniti. Eno od ključnih načel bo vpeljava kibernetske varnosti v poslovne procese, s t. i. pristopom »Security by Design«. Zelo pereč pa je tudi problem pomanjkanja visoko usposobljenih kadrov, zaradi česar moramo organizacije s tega področja še bolj podpirati razvoj prihodnje generacije mladih inženirk in inženirjev na tem področju. ■

Foto: arhiv Smart Com d.o.o.

Zagotovite varno in skladno poslovanje v digitalni dobi

Naredite prve korake za prilagoditev nivoja kibernetske varnosti vaše organizacije skladno z zahtevami evropske direktive NIS 2.

- Izdelava analize vrzeli med trenutnim stanjem in zahtevami direktive NIS 2
- Dopolnitev ali izdelava ocene informacijskih tveganj
- Dopolnitev ali izdelava analize poslovnih učinkov
- Ocena varnostne zrelosti organizacije
- Načrt procesnih in tehnoloških prilagoditev

bit.ly/3X8BvnV

Skupaj do skladnosti

SMART COM

UDEJANJAMO VAŠE VIZIJE

www.smart-com.si

Avtorica: Tanja Permozer / vodja Slovenske vesoljske pisarne in vodja delegacije RS pri Evropski vesoljski agenciji

VESOLJSKE INDUSTRIJE IN PRILOŽNOSTI ZA SLOVENSKE ORGANIZACIJE

V prispevku želimo podrobneje predstaviti korake, ki jih Republika Slovenija in preko tega tudi slovenske organizacije, izvajajo na področju sektorja vesoljske industrije. Prehojena pot predstavlja odlično odskočno desko za razširitev sodelovanja in izvajanja smelejših korakov na tem zahtevnem in visoko konkurenčnem področju. Republika Slovenija je namreč postala polnopravna članica Evropske vesoljske Agencije, kar prestavlja nove priložnosti za še močnejše sodelovanje skozi cel niz projektov usmerjenih v vesolje.

Področje vesoljske industrije je zelo obsežno in vanj se lahko vključijo podjetja iz najrazličnejših sektorjev: od prehrane, energije, telekomunikacij in navigacije, novih materialov in 3D tiskanja, kontrolnih sistemov, obdelave in hrambe velikih količin podatkov, novih načinov obdelave materialov, medicine, obrambe in številnih drugih.

Poleg tega ima sektor zaradi visoke stopnje inovativnosti tudi nadpovprečne učinke prelivanja. Primeri takega prelivanja so na primer uporaba laserske tehnologije razvite na področju vesoljske tehnologije za izvedbo očesnih operacij, uporaba infrardečih kamer prvenstveno razvitih za uporabo na satelitih za pametne naprave, uporaba inovativnih materialov razvitih za vesoljske objekte v letalski in avtomobilski industriji itd.

Tudi z vidika digitalnega gospodarstva ima vesolje vedno večjo vlogo, kar je prepoznal tudi Evropski parlament. Podatki, pridobljeni iz vesolja, lahko pomagajo okrepiti vodilno vlogo industrije na področju interneta stvari in avtomatizirane vožnje ter natančneje spremljati emisije toplogrednih plinov, kar bo povečalo učinkovitost podnebnih ukrepov. Tudi razvoj sodobnega, varnejšega, učinkovitega in trajnostnega prometa je tesno povezan z razvojem vesoljske tehnologije. Z navigacijskim sistemom in opazovanjem Zemlje so prometne storitve učinkovitejše. S tem se efektivno zmanjšujejo emisije. Razvoj vesoljskih tehnologij lahko pomaga pri spopadanju s podnebnimi spremembami, izboljšujejo se dostavne in poštne storitve, z boljšimi sistemi sledenja letalom pa se zmanjšuje hrup in število preklicanih letov.

Podatki, pridobljeni iz vesolja, lahko pomagajo okrepiti vodilno vlogo industrije na področju interneta stvari in avtomatizirane vožnje ter natančneje spremljati emisije toplogrednih plinov, kar bo povečalo učinkovitost podnebnih ukrepov.

Ministrstvo za gospodarstvo, turizem in šport je vključilo področje vesolja med svoje prioritete in je na tem področju zelo aktivno. Ustanovilo je **medresorsko delovno skupino**, namenjeno usklajenemu delovanju vseh akterjev, vključenih v to meddisciplinarno področje. V tej delovni skupini so vključeni predstavniki vseh ključnih ministrstev in agencij, ki so posredno ali neposredno povezana z vesoljem.

Sodelovanje z Evropsko vesoljsko agencijo - ESA

ESA ima 23 držav članic. Nacionalni organi, odgovorni za vesolje v teh državah, sedijo v upravnem svetu ESA: Avstrija, Belgija, Češka, Danska, Estonija, Finska, Francija, Nemčija, Grčija, Madžarska, Irska, Italija, Luksemburg, Nizozemska, Norveška, Poljska, Portugalska, Romunija, Španija, Švedska, Slovenija, Švica in Združeno kraljestvo. Kanada je tudi članica sveta in sodeluje pri nekaterih projektih v okviru sporazuma o sodelovanju. Slovaška, Latvija in Litva so pridružene članice. Štiri druge države EU imajo sporazume o sodelovanju z ESA: Bolgarija, Hrvaška, Ciper in Malta.

Slovenija z ESO sodeluje od leta 2009, ko je podpisala Sporazum evropske sodelujoče države (angleško The Plan for European Cooperating States - PECS). V letu 2016 je sodelovanje nadgradila s podpisom pridružitvenega sporazuma, s čimer je postala pridružena članica ESE. Leta 2020 pa je Slovenija podpisala še okrepljeni pridružitveni sporazum, ki se je iztekel 31. decembra 2024.

Slovenija je postala polnopravna članica 1. januarja 2025, ko so bile listine o njenem pristopu deponirane pri vladi Francoske republike kot depozitarju.

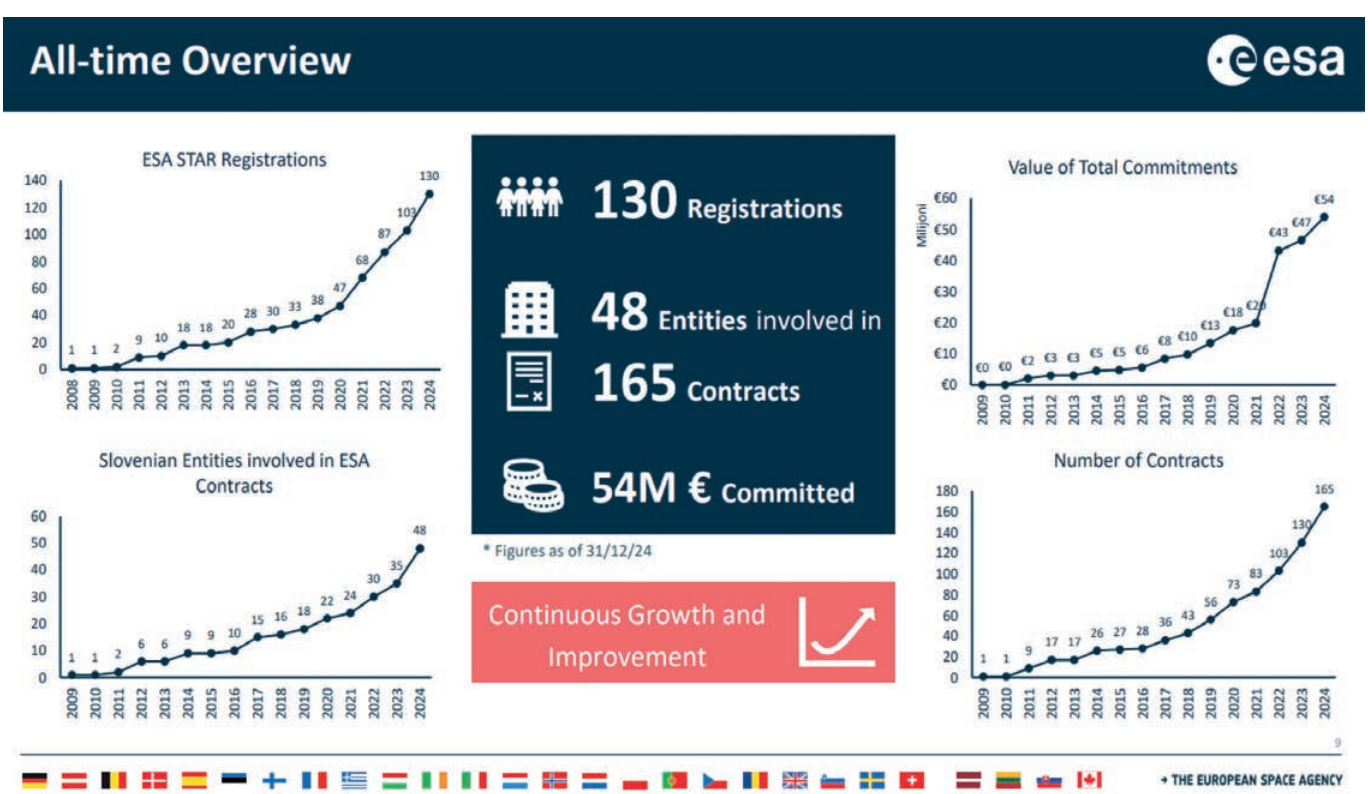
Primeri zelo uspešnega delovanja v vesoljskem sektorju so mnoga visokotehnološka podjetja, prav tako pa so sredstva iz ESE uspešno pridobila tudi podjetja iz lesarske industrije, zlatarne, tekstilne industrije in mnogi drugi. Polnopravno članstvo bo prineslo še dodatne možnosti za slovensko industrijo tako pri sodelovanju v programih, pri katerih do zdaj nismo sodelovali, kot pri črpanju sredstev, pa tudi pri povezovanju z mednarodnimi podjetji.

Slovenija je na ministrskem zasedanju Sveta ESA „CM22“, ki je potekalo v Parizu 22. in 23. 11. 2022, povečala finančni prispevek v programe ESA v naslednjih treh letih, in sicer s 3 milijonov EUR na 5,8 milijonov EUR letno.

Slovenija prispeva sredstva tudi v osnovno dejavnost Evropske vesoljske agencije. Osnovne dejavnosti (Basic Activities) so v bistvu del „članarine“ ESA, vendar ta naložba prinaša solidne koristi za države članice, njihove znanstvenike in njihove industrije, pa tudi izbirne programe ESA. Slovenija je na CM22 potrdila sodelovanje v štirih izbirnih programih, v katerih je sodelovala do sedaj (GSTP – splošne tehnologije, EO – opazovanje Zemlje, E3P3 – človeške in robotske raziskave, znanstveni program Prodex) ter dodatno potrdila sodelovanje v programih (Digitalni dvojček Zemlje, InCubed), programu telekomunikacij (Artes) ter Civil Security for Space za katerega je predviden finančni prispevek v višini: 1.760.000 EUR.

Naslednje ministrsko zasedanje Sveta ESA »CM25« bo potekalo novembra 2025.

V zadnjih skoraj 15 letih (od podpisa listine PECS leta 2010) je Evropska vesoljska agencija podpisala 165 pogodb z 48 slovenskimi deležniki v vrednosti več kot 54 milijonov evrov (vir: ESA). V sistemu za razpise (ESA Star) je registriranih 130 deležnikov, s tem, da se beleži stalna rast.



Slika: ESA pregled aktivnosti

ESA je maja 2024 objavila peti razpis v višini 1,5 mio EUR namenjen samo slovenskim deležnikom (v angleščini Requesting Party Activity - RPA) za zbiranje okvirnih predlogov projektov na temo različnih tipov aktivnosti, ki izhajajo iz razpisa.

RPA razpis za zbiranje predlogov projektov je namenjen samo podjetjem in akademskim in raziskovalnim organizacijam s sedežem v Sloveniji. Namen tega razpisa je krepitev slovenskega vesoljskega sektorja in spodbujanje vključitve novih podjetij in organizacij. Slovenski deležniki se lahko povežejo tudi s tujimi partnerji iz drugih držav članic ESA, vendar tuj delež ne sme presegati 20 % skupne cene projekta. ESA razpis RPA načrtuje tudi v letu 2025.

Članstvo Slovenije v ESA bo odpiralo tudi nove možnosti za sodelovanje slovenskih podjetij in raziskovalnih institucij z ESA – zlasti v okviru področja temeljnega tehnološkega raziskovalnega programa (Basic Technology Research Programme – TRP) in znanstvenega programa (Science Programme), kjer je ključna tudi komercialna komponenta. področji v ESI, v katerih slovenski vesoljski sektor doslej ni mogel sodelovati.

V okviru programa TRP gre za zgodnje razvojne faze na vseh področjih storitev in tehnologije ter preizkus njihove primernosti za vesoljske aplikacije.

Znanstveni program je temeljna podlaga za druge programe v okviru ESE (gre tudi za preizkus tehničnih zmogljivosti v vesolju) in za ustvarjanje »flight heritage«, ki kaže na zrelost vesoljskega sektorja.

Članstvo v okviru ESE pa Sloveniji omogoča tudi priložnosti za naslednje generacije. Študentje ter mladi bodo lahko sodelovali pri izobraževalnih programih, s katerimi bodo pridobili nova znanja in izkušnje na področju vesolja. To bo posledično pripomoglo k nadaljnjemu razvoju našega gospodarstva, saj slovenska podjetja tako lažje pridobivajo visoko usposobljene in izobražene kadre.

S podporo in koordinacijo Slovenske vesoljske pisarne tako mala in srednje velika podjetja dobijo priložnost, da v okviru programov ESA sodelujejo z nosilnimi podjetji (prime) in tako razvijajo nove izdelke ali rešitve. Nosilna podjetja iščejo rešitve na področju elektronike do precizne mehanike, IKT rešitev, 3D tiska in drugo.

Pomembno je poudariti, da se vesoljske tehnologije ne uporabljajo samo v vesolju, temveč da si v Slovenski vesoljski pisarni in v ESA prizadevajo za čim večjo uporabo tehnologij, razvitih za področje vesolja, tudi v vsakodnevnem življenju. Vesoljski sektor tako za slovenska podjetja predstavlja dobro poslovno priložnost, hkrati pa lahko pomembno prispeva k doseganju ciljev zelenega digitalnega prehoda in doseganju klimatskih zavez.

Slovenska vesoljska strategija 2030

Vlada je dne 3.11. 2023 na dopisni seji sprejela prvo slovensko vesoljsko strategijo in odločitev za prošnjo za polnopravno članstvo v Evropski vesoljski agenciji.

Vlada je sprejela prvo slovensko vesoljsko strategijo 2030 pod sloganom »Majhni na Zemlji, veliki v vesolju«, ki določa usmeritve in aktivnosti za povečanje konkurenčnosti slovenske vesoljske industrije in vzpostavitev vodilne vloge na vesoljskih področjih, kjer se odlikujejo slovenski deležniki.

Vesoljski sektor je eden izmed najhitreje rastočih sektorjev, tudi v Sloveniji. Zanj so značilni veliki multiplikativni učinki na gospodarsko rast in zaposlovanje. Zaradi digitalizacije družbe so aktivnosti tega sektorja vse bolj pomembne v vsakodnevnem življenju ljudi, obenem pa zaradi velikega vložka v raziskave in razvoj prinašajo številne prebojne rešitve. Vesoljska tehnologija se koristi v prometu, kmetijstvu, energetiki, gospodarstvu, varnosti, zdravstvu, izobraževanju in na številnih drugih področjih.

Zaključek

Naše gospodarstvo mora ostati konkurenčno na svetovnem trgu, k čemur vesoljske tehnologije veliko pripomorejo. Ključnega pomena, tudi pri vključitvi v polnopravno članstvo v Evropski vesoljski agenciji (v nadaljevanju: ESA), je dejstvo, da v vesoljskem sektorju obstaja prostor za vse. Primeri zelo uspešnega delovanja v vesoljskem sektorju so mnoga visokotehnološka podjetja, prav tako pa so sredstva iz ESE uspešno pridobila tudi podjetja iz lesarske industrije, zlatarne, tekstilne industrije in mnogi drugi. Polnopravno članstvo bo prineslo še dodatne možnosti za slovensko industrijo tako pri sodelovanju v programih, pri katerih do zdaj nismo sodelovali, kot pri črpanju sredstev, pa tudi pri povezovanju z mednarodnimi podjetji. ■

Avtor: Žiga Podgoršek / Institut za korporativne varnostne študije*

UMETNA INTELIGENCA POMEMBEN IZZIV ZA KIBERNETSKO VARNOST

Umetna inteligenca (UI) je postala ključni element sodobne digitalne preobrazbe. Njena zmožnost hitre obdelave podatkov, generiranja vsebin in učenja na podlagi velikih količin informacij je revolucionarna, a hkrati prinaša tudi številne nevarnosti.

V zadnjem obdobju smo priča drastičnemu porastu kibernetskih napadov, pri katerih se napadalci vse bolj opirajo na UI. Video posnetki z globokimi ponaredki (deepfake), generativni jezikovni modeli in glasovna kloniranja odpirajo vrata napadom, kjer napadalci poskušajo resnico zamegliti z uporabo digitalnih manipulacij in širjenjem dezinformacij.

Izredno zanimivo se mi zdi, kako UI širi paleto kibernetskih napadov, kakšne grožnje to predstavlja za podjetja in posameznike, ter kakšni so mogoči obrambni ukrepi.

Evolucija socialnega inženiringa - od klasičnega phishinga do z UI podprtih napadov

Socialni inženiring je že leta ena izmed najbolj učinkovitih metod kibernetskih napadalcev. Klasični phishing napadi, kjer napadalci pošiljajo lažna e-poštna sporočila, ki poskušajo prevarati uporabnike, so se skozi čas razvijali. Z napredkom umetne inteligence so postali bolj prepričljivi, težje prepoznavni in pogosto prilagojeni posamezniku ali organizaciji, kar povečuje njihovo uspešnost.

Novi napadi socialnega inženiringa ne vključujejo več zgolj klasičnih phishing e-poštnih sporočil, temveč tudi sofisticirane oblike manipulacije, kot so klici lažne tehnične podpore, kompromitacija poslovne e-pošte (BEC - Business Email Compromise) ter napadi z uporabo umetne inteligence.

Lažni klici tehnične podpore

Ena od vse pogostejših taktik je uporaba umetne inteligence pri simuliranju pristne tehnične podpore. Napadalci pokličejo žrtev in se izdajajo za predstavnike znanih podjetij, kot so Microsoft, Google ali ponudniki bančnih storitev. Pogosto jim uspe prepričati žrtev, da jim omogoči oddaljen dostop do računalnika ali vnese gesla v ponarejeno aplikacijo.

Kompromitacija poslovne e-pošte (BEC)

Napadalci uporabljajo umetno inteligenco za generiranje zelo prepričljivih ponarejenih e-poštnih sporočil, ki posnemajo stil pisanja vodstvenih kadrov podjetja. V teh napadih hekerji pogosto ukradejo dostop do e-poštnega računa ali ustvarijo e-poštni naslov, ki je skoraj identičen pravemu. Cilj je, da zaposleni izvedejo finančne transakcije ali delijo občutljive informacije, nevede, da ne komunicirajo s svojim nadrejenim ali poslovnim partnerjem.

Napadalci izkoriščajo umetno inteligenco za obvode tradicionalnih varnostnih mehanizmov, kar pomeni, da klasične metode odkrivanja groženj, kot so protivirusni programi in požarni zidovi, pogosto niso več dovolj učinkovite. Zmožnost UI za hitro prilagajanje obrambnim ukrepom ter generiranje napadov v realnem času pomeni, da so organizacije prisiljene razmišljati korak naprej.

*avtor je član Slovenskega združenja korporativne varnosti

Ponarejene spletne strani in avtomatizacija napadov

Z uporabo umetne inteligence lahko napadalci hitro ustvarijo realistične kopije spletnih strani, kjer od žrtev pridobijo podatke za prijavo ali osebne informacije. Poleg tega lahko UI avtomatizira in prilagodi phishing sporočila v realnem času glede na odziv tarče, kar pomeni, da napadi postajajo vedno bolj personalizirani in težko prepoznavni.

Napadi prek družbenih omrežij

Umetna inteligenca omogoča generiranje lažnih profilov na družbenih omrežjih, ki posnemajo resnične osebe. Ti profili lahko pridobivajo zaupanje tarč, jih prepričajo v klik na zlonamerne povezave ali iz njih izvabijo občutljive podatke, ki jih nato napadalci uporabijo pri nadaljnjih napadih.

Socialni inženiring je s pomočjo umetne inteligence dosegel novo raven prepričljivosti in nevarnosti. Organizacije in posamezniki morajo biti izjemno previdni pri preverjanju pristnosti komunikacije, saj tradicionalni znaki phishing napadov, kot so slovnične napake ali nenavadne povezave, niso več zanesljivi indikatorji goljufij.

Deepfake in glasovna kloniranja

Ena izmed največjih nevarnosti umetne inteligence so deepfake videi in glasovna kloniranja. Napadalci lahko danes s pomočjo UI ustvarijo realistične video posnetke, kjer znane osebe (npr. direktorji podjetij ali politiki) govorijo stvari, ki jih v resnici nikoli niso izrekli. Podobno lahko s pomočjo glasovne sintetične tehnologije napadalci posnemajo glasove ljudi in s tem prepričajo žrtve, da ukrepajo v skladu z navodili lažne osebe.

Generativni modeli in avtomatizacija phishing napadov

Novi generativni modeli UI omogočajo avtomatizacijo prepričljivih phishing sporočil. Klasični phishing pogosto trpi zaradi slovničnih napak, ki so bile eden glavnih prepoznavnih znakov prevare. Z umetno inteligenco pa lahko napadalci generirajo brezhibna, personalizirana sporočila, ki se prilagajajo tonu in slogu podjetja ali posameznika. Tovrstni napadi so bolj učinkoviti in imajo višjo stopnjo uspešnosti.

Napredne grožnje in avtomatizacija zlonamerne programske opreme

UI omogoča napadalcem tudi avtomatizacijo ustvarjanja zlonamerne programske opreme. S pomočjo UI lahko napadalci hitro razvijejo in prilagodijo zlonamerno kodo, ki se izogiba odkrivanju s strani tradicionalnih varnostnih rešitev. To pomeni, da se lahko zlonamerna programska oprema dinamično prilagaja okolju v katerem deluje, kar otežuje njeno zaznavanje in odstranjevanje.

Napadi na kritično infrastrukturo - Nova dimenzija groženj

Poleg klasičnih kibernetskih napadov igra umetna inteligenca vse pogosteje ključno vlogo pri napadih na kritično infrastrukturo. Napadalci lahko z uporabo UI analizirajo omrežne vzorce, prepoznavajo ranljivosti in avtomatizirajo napade na ključne sektorje, kot so elektroenergetski sistemi, vodovodna omrežja,

bolnišnice podprte z industrijskimi nadzornimi sistemi (ICS/SCADA).

Napadalci lahko izkoriščajo UI za avtomatizirano prepoznavanje ranljivosti, načrtovanje napadov in prilagajanje strategij v realnem času, kar otežuje odkrivanje in odzivanje na grožnje. Ti napadi lahko povzročijo motnje v oskrbi z elektriko, vodo ali zdravstvenimi storitvami, kar ima lahko resne posledice za družbo in gospodarstvo.

Kako se organizacije lahko zaščitijo?

Zaradi naraščajočih groženj UI-podprtih napadov je ključno, da organizacije prilagodijo svoje varnostne strategije in sprejmejo proaktivne ukrepe.

1. Uporaba umetne inteligence za obrambo
UI ni samo orožje napadalcev – lahko je tudi močno orodje obrambe. Napredni sistemi za zaznavanje groženj, ki temeljijo na umetni inteligenci, lahko analizirajo vzorce omrežne aktivnosti, prepoznajo anomalije in sprožijo pred nastavljene in avtomatizirane varnostne ukrepe.

2. Izobraževanje zaposlenih in ozaveščanje
Napadi, ki uporabljajo UI, pogosto temeljijo na manipulaciji človeške psihe. Ena ključnih obramb pred socialnim inženiringom ostaja izobraževanje zaposlenih. Redni treningi kibernetske varnosti, vključno s prepoznavanjem deepfake vsebin in naprednih phishing tehnik, so nujni.

3. Preverjanje pristnosti komunikacije
Podjetja bi morala uvesti strožje postopke preverjanja identitete v občutljivih komunikacijah. Razmišljam v smeri, da bi glasovna potrdila in videoklici, ki temeljijo na biometričnih preverjanjih, lahko preprečila prevare, povezane z deepfake tehnologijo.

4. Varnostna politika „zero trust“
Koncept „zero trust“ (ničelno zaupanje) temelji na predpostavki, da noben uporabnik ali sistem ni avtomatično zaupanja vreden. Organizacije bi morale striktno uvesti več faktorsko preverjanje na vseh nivojih in se držati zero trust varnostnega koncepta.

Brez proaktivnih ukrepov, kot so uporaba naprednih rešitev za zaznavanje groženj, izvajanje rednih varnostnih testiranj in predvsem izobraževanje zaposlenih o sodobnih taktikah napadalcev, bo kibernetska varnost postala vse bolj neobvladljiva. Vprašanje ni več, ali bo organizacija postala tarča napada, temveč kdaj – in kako dobro bo nanj pripravljena.

Nova realnost kibernetske varnosti

Umetna inteligenca je prinesla temeljito revolucijo v načinu izvajanja kibernetskih napadov in obenem postavila nova pravila igre v svetu digitalne varnosti. Od prefinjenih lažnih video posnetkov (deepfake), avtomatiziranih phishing napadov in naprednih oblik socialnega inženiringa do samoučečih se zlonamernih programskih orodij – sodobne grožnje postajajo vedno bolj prilagojene, prepričljive in težje zaznavne.

Napadalci izkoriščajo umetno inteligenco za obvode tradicionalnih varnostnih mehanizmov, kar pomeni, da klasične metode odkrivanja groženj, kot so protivirusni programi in požarni zidovi, pogosto niso več dovolj učinkovite. Zmožnost UI za hitro prilagajanje obrambnim ukrepom ter generiranje napadov v realnem času pomeni, da so organizacije prisiljene razmišljati korak naprej.

Hkrati se digitalna krajina nenehno spreminja – vedno več naprav je povezanih v omrežje, meje med fizičnim in virtualnim svetom se brišejo, občutljivi podatki pa krožijo skozi kompleksne ekosisteme. To pomeni, da morajo organizacije zavzeti celosten pristop k varnosti, ki vključuje tako tehnološke kot organizacijske in človeške dejavnike.

Brez proaktivnih ukrepov, kot so uporaba naprednih rešitev za zaznavanje groženj, izvajanje rednih varnostnih testiranj in predvsem izobraževanje zaposlenih o sodobnih taktikah napadalcev, bo kibernetska varnost postala vse bolj neobvladljiva. Vprašanje ni več, ali bo organizacija postala tarča napada, temveč kdaj – in kako dobro bo nanj pripravljena.

V tej novi realnosti kibernetske varnosti ni prostora za pasivnost. Le s kombinacijo najsodobnejših tehnoloških rešitev, premišljene varnostne strategije in ozaveščenih uporabnikov lahko organizacije zagotovijo svojo odpornost proti vedno bolj sofisticiranim napadom, ki jih omogoča umetna inteligenca. ■

ohranite neprekinjeno delovanje kritične infrastrukture

Zaščitite svojo kritično infrastrukturo s celovitimi varnostnimi rešitvami ALCEA. Sodelujte z nami za zaščito po meri: alceaglobal.com

ALCEA

ASSA ABLOY

Avtor: Matic Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Matjaž Tavčar, predstavnik UKC Ljubljana* v EU projektu SUNRISE

IZKUŠNJE EVROPSKIH PROJEKTOV PRI UPRAVLJANJU BODOČIH PANDEMIJ

Ob pojavljanju vedno novih kriz je pomembno, da se iz preteklih izkušenj kriznega upravljanja nekaj naučimo in to znanje prenašamo v nove ukrepe za povečanje odpornosti in pripravljenosti naših organizacij. Evropski projekti med drugim predstavljajo tudi pomemben del učenja iz izkušenj, ki predvsem na področju kritične infrastrukture, pomenijo pomembno podlago za iskanje učinkovitejših rešitev. O odprtih izzivih na področju upravljanja kriz, povezanih s pandemijo in iskanju potrebnih rešitev, smo se pogovarjali z g. Matjažem Tavčarjem, predstavnikom UKC Ljubljana v mednarodnem projektu SUNRISE s področja krepitve odpornosti kritične infrastrukture med pandemijami.

Imate bogate izkušnje iz večjih pomembnih procesov znotraj zdravstvenega sistema. Nam lahko kratko opišete svojo pomembno vlogo na EU projektu SUNRISE in ali vam pretekle izkušnje pomagajo pri upravljanju procesov sodelovanja v tem zelo pomembnem mednarodnem projektu?

V Univerzitetnem kliničnem centru Ljubljana sem zaposlen od leta 2013. Prvih sedem let kot poslovni direktor največje klinike UKCL, Kirurške klinike, kjer sem spoznal praktično vse procese temeljene zdravstvene dejavnosti. V dejavnost Kirurške klinike sodi tudi urgentna kirurška dejavnost (Urgentni kirurški blok), ki deluje v okviru Urgence UKCL ter transplantacijska dejavnost. S tem sem pridobil vpogled v delovanje in vodenje ustanove tako vertikalno kot horizontalno. Od leta 2019 sem prevzel vodenje Službe za korporativno varnost, vključujoč nekdanjo Službo za obrambo in zaščito. Pomen te službe se je izkazal v času pandemije COVID-19. S prijavo v konzorcij partnerjev na projektu SUNRISE, na vabilo ICS, sem prevzel vodenje tega projekta v okviru UKCL.

Kako bi ocenili, da je pandemija Covid19 vplivala na operativno odpornost zdravstvenih sistemov in s katerimi posebnimi izzivi ste se soočili v UKC?

Strategija v okviru projekta SUNRISE na podlagi pilotnih izkušenj šele nastaja in bo pomembno vplivala na samo zagotavljanje neprekinjenega delovanja izvajalcev bistvenih storitev. Pomembno bo vplivala na povezovanje teh iz različnih sektorjev kritične infrastrukture ter s tem preprečitvi »domino efekta« ne samo v primeru pandemij.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Nacionalni načrti odzivanja na krizna stanja se v zdravstvu v glavnem končajo v UKCL, ki naj bi ob vseh nesrečah zagotovil vso potrebno oskrbo poškodovancev, kar seveda ni realno. Tu pride do izraza državno in meddržavno sodelovanje in vključevanja kapacitet bolnišnic iz sosednjih držav (Trst, Celovec, Gradec, Zagreb, Reka).

Prav po sami vzpostavitvi Službe za korporativno varnost nas je marca 2020 doletela pandemija COVID-19. Zaradi migracijskih procesov smo se že poleti 2019 zavedali nevarnosti prenosa nalezljivih bolezni (npr. tuberkuloza, garje, ošpice). Takrat pristojne službe temu niso pridajale velikega pomena. Zdravstvene ustanove smo imele izdelane načrte za primer epidemije gripe, vendar je bil pojav SARS-CoV 2 oz. COVID-19 pospremljen z izdatno dozo strahu in nepoznavanja bolezni. Sama operativna odpornost ni bila posebej ogrožena, ker so bili precej hitro sprejeti zaščitni ukrepi, kot je prepoved obiskov, ukinitev nenujnih posegov in osamitev zaposlenih s ciljem preprečevanja širjenja okužb. Prav zaradi prej omenjenih tveganj prenosa bolezni, januarja 2020, smo izdelali tudi prvo oceno tveganj po Zakonu o kritični infrastrukturi na podlagi metodologije Ministrstva za zdravje, smo imeli na zalogi potrebno količino osebne varovalne opreme (maske, plašči,...). Svoje izkušnje smo vzporedno delili z drugimi deležniki, kot je Policija, Slovenska vojska in druge zdravstvene ustanove, ki so nam pomagali pri preprečevanju incidentov in zagotavljanju dodatnih zmogljivosti.

Ali lahko opišete tehnologije oziroma orodja, pri katerih razvoju sodelujete v okviru EU projekta SUNRISE, kašne so vaše izkušnje z že implementiranimi pilotnimi testi ter kako si predstavljate njihovo vključitev v operativno delovanje?

Eden prvih ukrepov po razglasitvi epidemije COVID-19 je bila omejitev dostopa v UKCL. Tako za paciente, obiskovalce kot zaposlene. Pogoji za dostop so se sčasoma dopolnjevali. Od začetnega merjenja telesne temperaturi, preko mask in kasneje potrdil o testiranju ali cepljenju. Vse te pogoje je bilo potrebno preveriti na vstopnih točkah. Od potrebne opreme smo imeli sčasoma na razpolago nekaj IR kamer, mobilnih telefonov z aplikacijo za preverjanje QR kod (testiranje, cepljenje). Za vse to pa varnostnika, zdravstvenega delavca in študente zdravstvene in medicinske fakultete. Torej vsaj tri ljudi, ki so preverjali pogoje za vstop. Tako je ena ključnih tehnologij, ki jo preverjamo v okviru projekta SUNRISE orodje RiBAC (Risk Based Access Control)., ki združuje preverjanje vseh potrebnih atributov za vstop (nošenje zaščitne opreme, preverjanje temperature in ustrezne QR kode).

Kako ocenjujete razvoj strategije upravljanja pandemičnih kriz v okviru EU projekta SUNRISE ter njeno uporabnost glede usklajevanja med različnimi deležniki za prihodnje krize?

Strategija v okviru projekta SUNRISE na podlagi pilotnih izkušenj šele nastaja in bo pomembno vplivala na samo zagotavljanje neprekinjenega delovanja izvajalcev bistvenih storitev. Pomembno bo vplivala na povezovanje teh iz različnih sektorjev kritične infrastrukture ter s tem preprečitvi »domino efekta« ne samo v primeru pandemij. Pomemben del bo prevzem strategije in njena uporaba tako v nacionalnih okvirih, kot v okvirih Evropske unije. Žal nimamo izkušenj kako se odločevalci (ministrstva, organi v sestavi) seznanjajo z rezultati dela na podobnih projektih ter kako, če sploh, jih vključujejo v nacionalne odzivne načrte. V projektu SUNRISE od vladnih organov sodeluje Ministrstvo za infrastrukturo, ostalih nosilcev sektorjev kritične infrastrukture zaenkrat ne čutimo.

Ali po vašem mnenju lahko rezultati EU projektov, kot je SUNRISE ter produktivno nacionalno in mednarodno sodelovanje, izboljšajo tudi vidike kakovosti oskrbe pacientov kot odgovor na bodoče potencialne pandemije?

Vsekakor. Sploh če pogledamo nabor sorodnih projektov v okviru Evropskega klastra za zagotavljanje varnosti kritične infrastrukture (ESCI). Nacionalni načrti odzivanja na krizna stanja se v zdravstvu v glavnem končajo v UKCL, ki naj bi ob vseh nesrečah zagotovil vso potrebno oskrbo poškodovancev, kar seveda ni realno. Tu pride do izraza državno in meddržavno sodelovanje in vključevanja kapacitet bolnišnic iz sosednjih držav (Trst, Celovec, Gradec, Zagreb, Reka). Podrobnih dogovorov na to temo (še) ni in o vsakem takem nujnem sodelovanju mora odločati Vlada Republike Slovenije. V kolikor bi bilo to vključeno v državne načrte bi postopki potekali hitro in bi jih pri svojem odločanju lahko upoštevala tudi Dispečerska služba zdravstva. In to ne samo v primeru pandemije. Projekt SUNRISE gradi strategijo na podlagi izkušenj iz pandemije COVID-19, ki bo uporabna tudi za druga krizna stanja.

Katere spremembe so po vašem mnenju potrebne za okrepitev pripravljenosti zdravstvenega sektorja na prihodnje pandemije ter kako lahko pozitivno izkoristimo izkušnje, pridobljene v času pandemije Covid19?

Ministrstvo za zdravje ima v svoji organizacijski strukturi Sektor za krizno medicino in nujno medicinsko pomoč. Ta bi moral biti aktiven nosilec priprave vseh načrtov odziva na krizne razmere in povezovalni člen z drugimi ustanovami v tujini. Nacionalni krizni center upravljanja (NCKU) pri Ministrstvu za obrambo pa koordinator delovanja vse kritične infrastrukture v kriznem stanju. Žal smo po petih letih oz. treh od pandemije COVID-19 marsikaj pozabili.

Kakšne so izkušnje vaše organizacije z uvajanjem zdravja na daljavo in telemedicine? Ali lahko taki pristopi v času pandemij zmanjšajo fizični pritisk pacientov na zdravstvene ustanove?

Telemedicina se je v UKCL vzpostavila v okviru projekta TELEKAP, ki ga je vodila prof. dr. Žvan. Ob pandemiji pa je izkušnje iz tega projekta uspešno razširila dr. Oroszy in nastal je praktično center za telemedicino. Zaradi omejitev fizičnega dostopa do zdravstvenih ustanov je bila to več kot dobrodošla rešitev.

Za konec kakšni bi bili vaši osnovni strateški predlogi za izboljšanje odpornosti najpomembnejše zdravstvene institucije, ki jo predstavlja UKC Ljubljana?

V UKCL je zbranega ogromno znanja in izkušenj, ki ga je potrebno ustrezno ubesediti in umestiti v načrte delovanja v kriznih razmerah. Pri tem je ključnega pomena sodelovanje Ministrstva za zdravje, ne toliko zaradi znanja, kot zaradi koordinacije z drugimi ministrstvi in predvsem zagotavljanja finančnih sredstev. V času COVID-19 so bila dovolj hitro zagotovljena potrebna finančna sredstva za prilagoditve (ureditev COVID-19 intenzivnih terapij,...), žal na podlagi osebnih znanstev in ne nacionalnih načrtov delovanja. Zaradi vojne v Ukrajini in potencialnih nevarnosti, med drugim tudi radiološke nesreče, intenzivno urejamo ustrezna zaklonišča in opremo za diagnosticiranje in zdravljenje posledic sevanja. Posebne odzivnosti pristojnih za finančno podporo ureditvi ni zaznati, kar bi lahko v primeru dejanske krize bilo zelo drago in to ne samo v denarju. Izrednega pomena pa je tudi redno izvajanje vaj ter s tem krepitev pripravljenosti in odpornosti izvajalcev bistvenih storitev. ■

VARNOSTNI PREHODI ZA KONTROLO DOSTOPA V NADZOROVANA OBMOČJA

Visoka in nizka vrtljiva vrata ter hitri avtomatizirani prehodi kot dodatna kontrola točka za vstop v omejena območja.

Primerno za zunanjo ali notranjo namestitev in za območja z velikim pretokom uporabnikov.
Možnost integracije z obstoječimi VNC sistemi in uporabo enega medija znotraj kompleksa.
Zvočni in svetlobni alarmi v primerih neavtoriziranega prehoda.
Možnost avtomatiziranih plačljivih prehodov ter dodatnih modulov po meri naročnika
(biometrija, ticketing – avtomatizirano preverjanje vstopnic, štetje obiskovalcev,...).

ID SHOP – ZANESLJIV PARTNER ZA ZAGOTAVLJANJE KONTROLE PRISTOPA V VAŠIH OBJEKTIH

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

- Nižji stroški fizičnega varovanja.
- Bolj kontroliran pretok ljudi.
- Večja izkoriščenost varnostno-nadzornega centra.
- Učinkovita integracija z obstoječo kontrolo pristopa v stavbi.
- Doseganje višjih varnostnih standardov.

ID Shop zagotavlja celovite rešitve za zagotavljanje kontrole pristopa:

Mehanski sistemi zaklepanja • Elektronski sistemi zaklepanja (pametne ključke, digitalni cilindri, mehatronske komponente) • Varnostni prehodi (visoka, nizka vrtljiva vrata, hitri prehodi in zapore)

IDealni partner za identifikacijo in varnost

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

cominfo By GUNNEBO Entrance Control

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

ENDURANCE – STRATEGIJE IN ORODJA ZA ZAGOTAVLJANJE USTREZNE ODPORNOSTI IN SODELOVANJA V EVROPI

Projekt ENDURANCE predstavlja enega izmed najpomembnejših poskusov EU pri iskanju ustreznih strategij in orodij za zagotavljanje učinkovite odpornosti kritičnih subjektov. V omenjenem projektu imajo ključno vlogo tudi organizacije iz Slovenije, kjer se bo odvijal eden izmed najpomembnejših pilotnih testiranj. Pomembna pričakovanja pa se polagajo tudi na pripravo ustreznega predloga strategije za zagotavljanje odpornosti kritičnih subjektov v EU.

Motivacija za izvedbo projekta

Sredi vse bolj medsebojno povezanega in kompleksnega sveta ostaja zagotavljanje osnovnih storitev ključnega pomena za blaginjo evropskih državljanov in nemoteno delovanje notranjega trga. Vendar pa nenehno razvijajoče področje tveganj, od kibernetskih groženj, fizičnih napadov in človeških napak do naravnih nesreč, zahteva proaktiven in sodelovalen, vseevropski pristop za zagotavljanje odpornosti proti motnjam. Zato projekt ENDURANCE poganja kritična potreba po okrepitvi bistvenih evropskih storitev proti morebitnim motnjam, ki presegajo izključno osredotočenost na osnovna kritična sredstva.

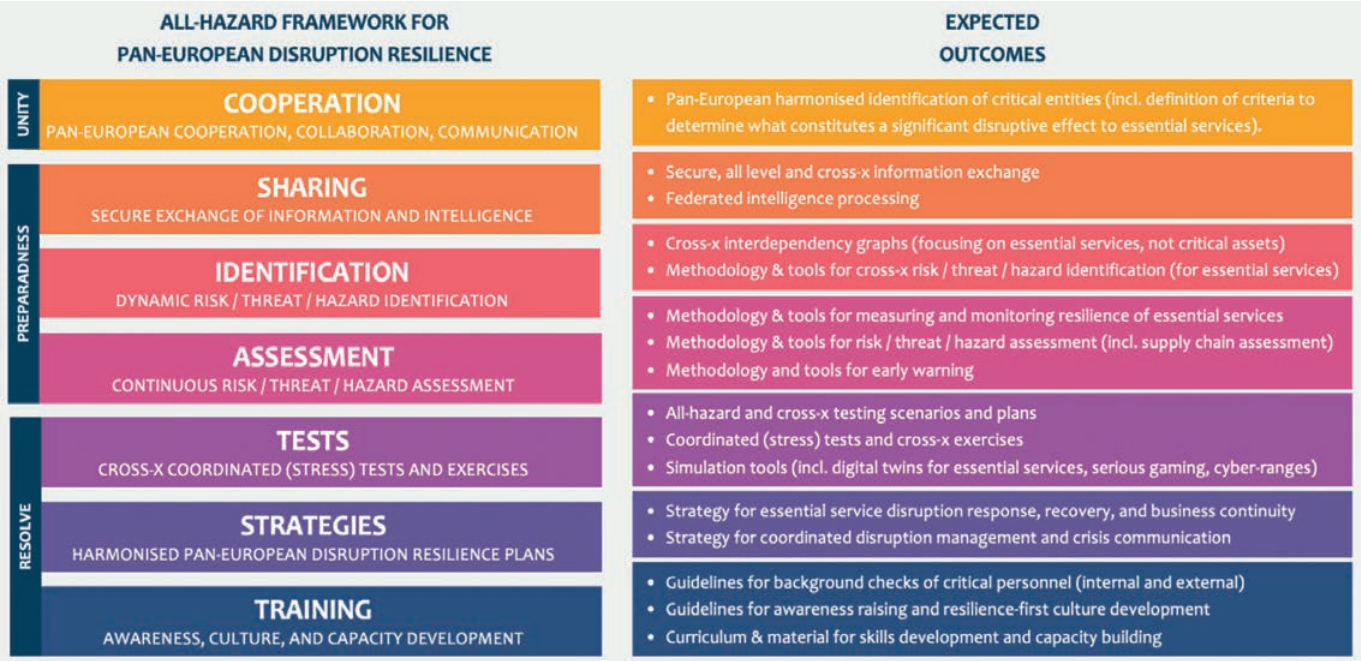
Ob priznavanju pomena direktiv CER in NIS 2 pri postavljanju temeljev za odpornost in, vzporedno, trenutnega silosnega pristopa k odpornosti kritične infrastrukture (KI) in neprekinjenosti poslovanja bistvenih storitev, ki jih zagotavljajo, bomo pomagali organom KI po vsej EU pri popolnem razumevanju in usklajenem izvajanju obeh direktiv. S celovitim razumevanjem in s pripravo na zahteve teh zakonodajnih ukrepov (in njihovega nacionalnega izvajanja) želimo opolnomočiti države članice EU, oblasti in operaterje KI z znanjem in izkušnjami, metodologijami, storitvami in strategijami, ki so potrebne za učinkovito krmarjenje v kompleksni odpornosti na motnje.

Z ekipo devetih odličnih raziskovalnih, tehnoloških in poslovnih organizacij (vse z bogatimi izkušnjami v projektih INFRA) in s sedmimi organi držav članic EU in šestimi operaterji KI, ki predstavljajo 6 kritičnih sektorjev in 4 države članice EU, bo ENDURANCE: (i) izboljšal strateško sodelovanje in sodelovanje med deležniki KI na vseh ravneh. (ii) razvil nabor podatkov, registrov, metodologij, tehnologij in storitev (TRL6-7) za varno skupno rabo in zvezno obdelavo podatkov, pomembnih za CER, skupno oceno ustreznih tveganj, odpornosti in obsežno stresno testiranje pripravljenosti. (iii) Zagotovil usklajeno in pragmatično strategijo za kontinuiteto med seboj povezanih bistvenih storitev.

Obseg

Za učinkovito načrtovanje in razvoj okvira projekta ENDURANCE, ki naslavlja nevarnosti za vseevropsko odpornost na motnje, je projekt razdeljen na 7 dopolnjujočih in prepletenih stebrov.

*avtor je član Slovenskega združenja korporativne varnosti



KLJUČNO PODROČJE 1: ENOVITOST

*Vse nivojsko, pan-Evropsko **SODELOVANJE**, usklajevanje in komunikacija.*

Z aktivnim sodelovanjem različnih deležnikov KI na vseh ravneh in prek različnih lokacij, organizacij, sektorjev in meja bomo zbrali in združili znanje in izkušnje ter usklajeno opredelili merila za določitev, kaj predstavlja pomemben moteč učinek na bistvene storitve v smislu fizičnih, kibernetskih dogodkov in dogodkov, povezanih s človekom, in s tem podpora organom KI pri identifikaciji kritičnih subjektov po vsej EU. S tem delom bomo podprli deležnike KI pri učinkoviti implementaciji direktiv CER in NIS 2.

KLJUČNO PODROČJE 2: PRIPRAVLJENOST

***VARNA IZMENJAVA** ustreznih informacij in obveščevalnih podatkov, dinamično **IDENTIFIKACIJO** in stalno **OCENJEVANJE** ustreznih znanih in nastajajočih tveganj, groženj in nevarnosti.*

Zagotovili bomo rešitve za varno izmenjavo obveščevalnih podatkov in celovito analizo informacij, potrebnih za podporo KI organom, operaterjem in drugim deležnikom pri dinamičnem in neprekinjenem prepoznavanju in ocenjevanju različnih tveganj, groženj in nevarnosti, ki se nanašajo na notranje izzive posameznih organizacij (npr. starajoča se infrastruktura, organizacijska tveganja) in/ali izvirajo iz zunanjih odvisnosti (npr. varnost dobavne verige, sistemska tveganja, naravne nevarnosti, sabotaža). To delo bo temeljilo na analizi medsebojnih povezav in soodvisnosti različnih bistvenih storitev v različnih krajih, organizacijah, sektorjih in mejah. Če združimo vse skupaj, bomo zagotovili rešitve in smernice za uporabniku prijazno, skladno s CER / NIS 2 ter stalno kvalitativno in kvantitativno merjenje odpornosti proti motnjam.

KLJUČNO PODROČJE 3: REŠITVE

*Usklajeni **TESTI**, usklajene **STRATEGIJE** in **USPOSABLJANJE** po meri.*

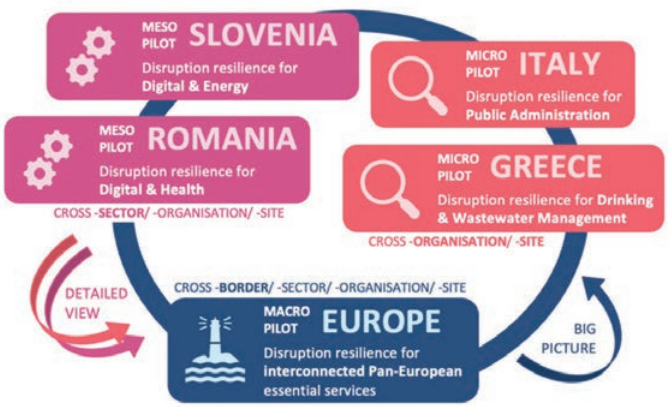
Na podlagi znanja, pridobljenega z mednarodnim sodelovanjem različnih strokovnjakov in praktikov, bomo oblikovali in izvajali scenarije in načrte za usklajene, mednarodne, medsektorske, obsežne teste in vaje, da bi zagotovili, da so razvite metodologije, strategije in orodja za pripravljenost na motnje učinkovita in pragmatična. Testi bodo usklajeni z „Načrtom za incidente in krize KI“ Evropske komisije in bodo vključevali različna simulacijska orodja, ki bodo služila tudi kot sredstvo za usposabljanje kritičnega osebja. Rezultat scenarijev in vaj bo strategija za povečanje odpornosti na motnje, ki bo vključevala smernice za sprejemanje novih modelov za usklajeno (1) krizno upravljanje in neprekinjeno poslovanje, (2) odziv na motnje in (3) komunikacijo, usklajeno s pomembnimi premiki v naši družbi zaradi pandemije, političnih konfliktov, gospodarske krize in naravnih nesreč. Končno bodo vsa ustvarjena znanja in izkušnje uporabljena za pripravo smernic za ozaveščanje in razvoj kulture varnosti na prvem mestu v organizacijah ter kurikuluma in gradiva za usposabljanje in izpopolnjevanje/preusposabljanje zaposlenih za izgradnjo celovite varnostne zmogljivosti.

Aplikativna področja

ENDURANCE bo preverjen na naslednjih področjih uporabe, ki so najbolj pomembna za evropsko družbo, gospodarstvo in okolje:

- **MAKRO pilot**: Pilot je strateško usmerjen in se ukvarja z visokimi čezmejnimi izzivi.
- **MESO pilot – Slovenija** : Izboljšanje odpornosti bistvenih storitev na katastrofe v **digitalno-telekomunikacijskem-energetskem** ekosistemu v **Sloveniji**.

- **MESO pilot – Romunija** : Izboljšanje odpornosti bistvenih storitev na nesreče v **zdravstvenem-telekomunikacijskem-transportnem** ekosistemu v **Romuniji.**
- **MIKRO pilot – Italija** : Izboljšanje odpornosti bistvenih storitev na nesreče v ekosistemu **digitalnega zdravja, prostora in javne uprave** v **Italiji.**
- **MIKRO pilot – Grčija**: Izboljšanje odpornosti bistvenih storitev na nesreče v ekosistemu **upravljanja s pitno in vodo** v **Grčiji**.



V MAKRO pilotu se bomo osredotočili predvsem na vrednotenje storitve ocenjevanja strategije ter ocene tveganja in odpornosti, da bi neposredno podprli KI pri izvajanju direktive CER. Pilota MESO SLOVENIJA in ROMUNIJA bosta opredelila, analizirala in obravnavala medsektorske izzive na lokalni, regionalni in nacionalni ravni, v Sloveniji znotraj in med sektorji digitalne energije oziroma v Romuniji digitalnega zdravja. V teh dveh pilotnih projektih se bomo osredotočili predvsem na vrednotenje digitalnega dvojčka, da bi prikazali in natančno analizirali medsektorske soodvisnosti.

Pilota MICRO ITALIJA in GRČIJA bosta poskušala prikazati posebnosti posameznih držav, regij in sektorjev ter se osredotočila na vidike med subjekti, lokacijami in regijami v Italiji in Grčiji v sektorjih javne uprave oziroma upravljanja (pitne in odpadne) vode. V teh dveh pilotnih projektih se bomo osredotočili predvsem na vrednotenje storitve simulacije in usposabljanja, da bi ocenili vidike uporabnosti.

Konzorcij je sestavljen iz 23 partnerjev iz 7 EU držav. Slovenski partnerji projekta so AKOS, URSIV, ELES, Telekom Slovenije, Silver Bullet Risk in Institut za korporativne varnostne študije, ICS-Ljubljana.

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

Avtor: pred. mag. Marko Potokar / Slovensko združenje za korporativno varnost*

ZAŠČITA INDUSTRIJSKIH INFORMACIJSKIH SISTEMOV

Zaščita operativne tehnologije pred kibernetskimi grožnjami zahteva proaktiven in večplasten pristop, ki, tako kot pri zagotavljanju varnosti poslovnih informacijskih sistemov, združuje tehnične kontrole, organizacijske politike in ozaveščenost zaposlenih.

Uvod

Leto je za nami in morda se bomo v luči zadnjih dogajanj v zvezi z odločanjem naroda o gradnji dodatnega modula jedrske elektrarne, varnostni managerji letos ponovno dobili v naši jedrski lepotici. Pa si prikličimo v misli naš zadnji obisk, ko smo stali v komandni sobi postrojbe in v miru poslušali predstavitev tamkajšnjih strokovnjakov o delovanju sistemov. Nič posebnega se ni zgodilo, čeprav si z malo domišljije z vsakim dihom lahko čutil energijo, ki jo je proizvajal sistem. Operaterji na dolžnosti so spokojno sedeli za delovnimi postajami in suvereno spremljali dogajanje na kopici zaslonov, nameščenih po stenah in mizah. Obisk smo zaključili v vedrem razpoloženju, predvsem pa pomirjeni, da v naši elektrarni vse lepo teče.

Pa si zamislimo scenarij, da v trenutku našega obiska v sobo vstopi oseba brez identifikacijske priponke, odrine enega izmed operaterjev in prične na videz naključno premikati miško in tipkati po tipkovnici delovne postaje. Nastane zmeda, nekdo kliče varnostnike, preostali zaposleni skočijo na vsiljivca in ga odvlečejo proč od konzole. Ko varnostniki odpremijo nepoklicano osebo, vsi v sobi pričnejo napeto zreti čez ramena operaterja, ki je spet za svojim komandnim pultom in poskuša ugotoviti posledice dejanj. Eno je gotovo: za nas se na tem mestu obisk konča. Preden pa odidemo vseeno poskusimo zadostiti poklicni radovednosti in vprašamo gostitelja: 'Videli smo, da je neznanec nekaj tipkal po tipkovnici in premikal miško. Kakšen pa je sprejemljiv čas nenadzorovanega upravljanja vašega procesa? Kaj pa RTO, RPO? Kakšno je še sprejemljivo tveganje? Testirate backupe? A požarni zid je nove generacije?' V sobi nastane tišina, vse oči zaposlenih se obrnejo proti nam. Gostitelj se odkašlja: 'Oprostite, ne razumem teh vprašanj. Pravo vprašanje je, kako je oseba prišla do komandne sobe in kaj bomo naredili, da se to nikoli več ne ponovi.'

Odkrivanje vdora v sistem zahteva čas. Odločitev, da opozorila in drugi dokazi, ki jih imamo pred seboj, res predstavljajo situacijo, ki je vredna preiskave, zahteva čas. Za premeščanje ekipe za odzivanje na incident je potreben čas. Da ekipa ugotovi, ali gre res za vdor in ne za nekakšen lažni alarm, potrebuje čas. In ko ekipa ugotovi, da je prišlo do vdora, je potreben čas za obravnavanje vdora. Ves ta čas ima naš nasprotnik nadzor nad nekaterimi ali vsemi računalniki v našem industrijskem omrežju. V mnogih industrijskih sistemih je to nesprejemljivo.

Operativna tehnologija

Izraz ***operativna tehnologija*** (Operational Technology; OT) se nanaša na strojno in programsko opremo, ki se uporablja za spremljanje in nadzor fizičnih naprav, procesov in infrastrukture v različnih panogah, kot so proizvodnja, energetika, transport in zdravstvo. Proizvodni in distribucijski sistemi energije, telekomunikacijska infrastruktura, finančne storitve, vodovodni in kanalizacijski sistemi, varnostne storitve, zdra-

> Veliko sistemov kritične infrastrukture, ki so bili v preteklosti sestavljeni izključno iz fizičnih elementov in izoliranih industrijskih krmilnih sistemov, so s procesom digitalizacije postali obvladljivi in sledljivi s pomočjo informacijskih in komunikacijskih tehnologij.

*avtor je član Slovenskega združenja korporativne varnosti

vstvene storitve in prevozne storitve so glavne panoge kritične infrastrukture. Elementi kritične infrastrukture so fizični in numerični sistemi, ki so med seboj odvisni in so potrebni za pravilno delovanje družbenega življenja. Zakon o kritični infrastrukturi (ZKI-1, 2024) definira kritično infrastrukturo kot: 'Kritična infrastruktura Republike Slovenije je sredstvo, objekt, oprema, omrežje ali sistem oziroma njegov del, ki je nujen za oziroma omogoča opravljanje bistvenih storitev.'

Industrijski krmilni sistemi, imenovani SCADA (Supervisory Control and Data Acquisition), se že vrsto let uporabljajo za upravljanje in nadzor sistemov kritične infrastrukture. SCADA je ena od razpoložljivih rešitev za sisteme za zajemanje podatkov, spremljanje in nadzor, ki pokrivajo velika geografska območja. Nanaša se na kombinacijo zajemanja podatkov in telemetrije. Sistem prikaže prejete podatke z oddaljenih mest na zaslonih v centru in omogoča izvedbo potrebnih nadzornih dejanj na oddaljenih terminalskih enotah.

Sodobni sistemi SCADA nadomeščajo ročno delo pri izvajanju nalog distribucije npr. električne energije in ročne procese v distribucijskih sistemih z avtomatizirano opremo. SCADA maksimira

učinkovitost sistema za distribucijo z zagotavljanjem funkcij, kot je pogled v realnem času, beleženje podatkov, vzdrževanje želenih napetosti, tokov in faktorjev moči, generiranje alarmov, izvaja avtomatski nadzor, varovanje in krmiljenje različne opreme v distribucijskih sistemih z uporabo inteligentnih elektronskih naprav ter obnavlja storitev napajanja med stanjem napake in tudi vzdržuje
želene pogoje delovanja.

SCADA sistemi, ki ne vključujejo informacijskih in komunikacijskih tehnologij ter niso povezani z drugimi omrežji ali so bili razviti posebej za določeno infrastrukturo v preteklosti, sedaj že, oziroma začenjajo vsebovati široko uporabljano, znano programsko in strojno opremo ter omrežne protokole. Poleg tega se je veliko SCADA sistemov, ki upravljajo in nadzorujejo sisteme kritične infrastrukture, začelo povezovati s korporativnimi omrežji in internetom, na katerih slonijo poslovni informacijski sistemi (IT). Posledično so SCADA sistemi postali veliko bolj ranljivi za kibernetske napade, obstoječe varnostne kontrole pa vprašljive z vidika zagotavljanja ustreznega nivoja varnosti.

OT vs. IT

Veliko sistemov kritične infrastrukture, ki so bili v preteklosti sestavljeni izključno iz fizičnih elementov in izoliranih industrijskih krmilnih sistemov, so s procesom digitalizacije postali obvladljivi in sledljivi s pomočjo informacijskih in komunikacijskih tehnologij. Kritična infrastruktura in informacijske tehnologije se prepletajo na mnoge načine. Ti preseki jasno kažejo pomembnost informacijske tehnologije. Za razliko od informacijske tehnologije, ki se osredotoča na obdelavo podatkov in komunikacijo (IT), se OT ukvarja predvsem z operativnimi vidiki sistema. Ena od ključnih razlik med OT in IT je kritičnost sistemov, ki jih upravljata. Sistemi OT se pogosto uporabljajo v okoljih, kjer ima lahko vsaka motnja ali okvara resne posledice, kot so izpadi električne energije, okvare opreme ali celo ogrožanje življenja. Zaradi tega so sistemi OT glavna tarča kibernetskih groženj, kjer lahko napadalci poleg kraje občutljivih podatkov, poskušajo motiti delovanje ali povzročiti fizično škodo.

Že ob hitrem razmisleku lahko navedemo vrsto razlik med IT in OT sistemi: v omrežjih OT je težje nameščati popravke, prav tako je težje osveževanje protivirusne zaščite, omrežja OT uporabljajo zelo stare protokole in računalnike, ljudje, ki ta omrežja upravljajo, pa imajo dostikrat ogromen odpor do sprememb. Vse te razlike pa so le površinske. Temeljna razlika med tema dvema vrstama omrežij so posledice: največkrat se najhujše posledice kibernetskih napadov močno, kvalitativno, razlikujejo v omrežjih IT in OT.

Kakšna je razlika? Izsiljevalska programska oprema zadene naše IT omrežje in kaj storimo? Zaznamo, se odzovemo in obnovimo. Identificiramo prizadete računalnike in jih izoliramo. Posnamemo forenzične slike za varnostne analitike in izbrišemo opremo. Obnavljamo iz varnostnih kopij. Ponavljamo. To je stalo časa in truda. Napadalec je morda ukradel intelektualno lastnino in/ali osebne podatke, zaradi česar smo utrpeli tožbe. Vse to so poslovne posledice. Povedano drugače, v omrežjih IT je cilj obvladovanja kibernetskega tveganja preprečiti poslovne posledice z zaščito informacij: varovanje zaupnosti, celovitosti in dostopnosti (poslovnih) informacij.

V omrežjih OT pa so najhujše posledice ogrožanja zelo pogosto fizične. Eksplozije ubijejo ljudi, industrijske okvare povzročijo okoljske katastrofe, luči ugasnejo, letala padejo z neba ali pa je naša pitna voda onesnažena. Cilj obvladovanja kibernetskega tveganja v OT omrežjih je na splošno zagotoviti pravilno, neprekinjeno in učinkovito delovanje fizičnega procesa. Cilj ni »zaščita informacij«, ampak bolj zaščita fizičnega delovanja pred informacijami, natančneje pred kibernetskimi napadi, ki so lahko vgrajeni v informacije. To je temeljna razlika med omrežji IT in OT: niti človeških življenj, niti poškodovanih turbin ali okoljskih katastrof ni mogoče obnoviti iz varnostnih kopij.

Za razliko od sistemov IT se sistemi OT pogosto zanašajo na podedovane tehnologije, ki morda nimajo vgrajenih varnostnih funkcij ali rednih posodobitev programske opreme, zaradi česar so bolj ranljivi za kibernetske napade. Za zaščito sistemov OT pred kibernetskimi grožnjami morajo organizacije uvesti robustne varnostne ukrepe, prilagojene edinstvenim zahtevam okolij OT. To vključuje segmentacijo omrežja za izolacijo omrežij OT od omrežij IT, mehanizme nadzora dostopa za omejitev nepooblaščenega dostopa, šifriranje za zaščito podatkov med prenosom in hranjenjem ter stalno spremljanje in odkrivanje ter odzivanje na varnostne incidente v realnem času. Poleg tega bi morale organizacije izvajati redne ocene tveganja, varnostne revizije in usposabljanja zaposlenih za ozaveščanje o kibernetskih grožnjah in najboljših praksah za zaščito sistemov OT.

SEC-OT

Temeljni cilj varovanja operativne tehnologije pred kibernetskimi grožnjami, je zaščita fizičnih operacij pred napadi, vgrajenimi v informacije. Temelji na naslednjih elementih:

- Varnost: prva prioriteta je zagotovitev varnosti. Varnost je opredeljena kot preprečevanje nesprejemljivih tveganj žrtev na lokaciji, groženj javnosti v bližnjih skupnostih in okoljskih katastrof.
- Zanesljivost: druga prioriteta je zanesljivo delovanje fizičnega procesa. Zanesljivo delovanje vključuje pravilne, učinkovite in neprekinjene fizične operacije. Nenačrtovani izpadi, napake v kakovosti proizvodov in poškodbe opreme so primeri nizke zanesljivosti delovanja sistemov.
- Nadzor: industrijske operacije so računalniško vodene. Pravilno in pooblaščeno krmiljenje računalnikov, ki nadzorujejo fizični proces, je bistvenega pomena za varno in zanesljivo delovanje.
- Informacije: vsi napadi so informacije - cilj varovanja OT ni zaščititi informacije, temveč zaščititi fizične operacije pred napadi, vgrajenimi v informacije.

Ta vidik se razlikuje od koncepta varovanja informacij. Klasičen odziv informacijske varnosti na zaščito informacij »šifriraj vse« ima omejeno vrednost v varovanju OT - vsi kibernetski napadi so informacije in informacije o napadu je mogoče šifrirati prav tako enostavno kot legitimne informacije. Posledice ogrožanja IT so poslovne posledice, kot so škodovanje ugledu, tožbe in kompromitirani računalniški programi in podatki, ki jih je treba obnoviti iz varnostnih kopij. Posledice

Zaščita operativne tehnologije pred kibernetskimi grožnjami zahteva proaktiven in večplasten pristop, ki, tako kot pri zagotavljanju varnosti poslovnih informacijskih sistemov, združuje tehnične kontrole, organizacijske politike in ozaveščenost zaposlenih.

za OT pa so fizične posledice in jih na splošno ni mogoče 'obnoviti iz varnostnih kopij'. Filozofija informacijske varnosti 'naj informacije tečejo, kjer hočejo, dokler so informacije zaščitene', je neposredno v nasprotju s filozofijo varnosti OT, ki temelji na nadzorovanju pretoka napadov s temeljitim omejevanjem in nadzorom pretoka informacij.

Seveda pa so zasnove in najboljše prakse zaščite OT vedno nadgrajene s tehnologijami in pristopi IT varnosti, za zaščito poslovnih skrivnosti in tudi kot druga linija zaščite, ki temelji na programski opremi, za varno in zanesljivo delovanje fizičnih procesov.

Koncept zaščite OT sistemov lahko strnemo v naslednje postavke:

- Nič ni varno - varnost je kontinuum, ne binarna vrednost.
- V vsako programsko opremo je mogoče vdreti – vsaka programska oprema ima napake, nekatere napake pa so ranljivosti, ki jih je moč izkoristiti.
- Vsi kibernetski napadi so informacije in vsaka informacija je lahko napad.

Zaključek

Zaščita operativne tehnologije pred kibernetskimi grožnjami zahteva proaktiven in večplasten pristop, ki, tako kot pri zagotavljanju varnosti poslovnih informacijskih sistemov, združuje tehnične kontrole, organizacijske politike in ozaveščenost zaposlenih. Pri tem je bistveno razumevanje razlik med sistemi OT in IT ter izvajanjem ustreznih varnostnih ukrepov, saj lahko organizacije le tako ustrezno ublažijo tveganja, ki jih predstavljajo kibernetske grožnje in zaščitijo svojo kritično infrastrukturo pred morebitno škodo. Poleg razumevanja razlik med OT in IT je za zagotovitev celostnega pristopa h kibernetski varnosti bistveno tudi sodelovanje in dopolnjevanje znanja med ekipami obeh strokovnih področij.

Viri

- A. Direskeneli, B. Baskus (2017). *P_Cyber Warfare And Critical Infrastructure*. PowerGen Europe 2017 Conference, 27-29 June 2017, Luxembourg.
- A. Ginter (2023). *Engineering-Grade OT Security*. Abterra Technologies Inc., Calgary.
- Zakon o kritični infrastrukturi (ZKI-1). Uradni list RS, št. 102/2024. ■

STANISLAVU V SPOMIN IN SLOVO

Pred časom nas je pretresla novica, da nas je za vedno zapustil naš član Stanislav Veniger.

Gospod Stanislav je s svojim neumornim strokovnim delom v svoji več kot 40 letni karieri bistveno pripomogel k dvigovanju ugleda varnosti v slovenskem in mednarodnem okolju. V svoji dolgoletni karieri je opravljal pomembne funkcije v javnih organizacijah nacionalne varnosti med katerimi je potrebno posebej izpostaviti funkcijo Generalnega direktorja Policije. V zadnjem obdobju svoje strokovne poti je svoje bogate izkušnje iz javnega sektorja nadgrajeval z delom v mednarodnem in korporativno varnostnem okolju. Njegovo delo v zadnjem obdobju je najbolj zaznamovalo delo v DCAF Ljubljana (Geneva Centre for Security Sector Governance) in kasneje v Zavarovalnici Triglav, kjer je kot svetovalec direktorja postavil pomembne temelje za učinkovit sistem korporativne varnosti. Na tem področju je s svojimi pronicljivimi idejami in visokim strokovnim znanjem zagotavljal, da se je dejavnost razvijala v smeri potreb, ki jih je prinašalo novo poslovno in varnostno okolje. Hkrati je pomembno pripomogel tudi k razvoju kvalitete korporativne varnosti, kot krovne strateške dejavnosti. Stanislav je užival visok ugled tako v širšem nacionalnem kot tudi v mednarodnem okolju.

V zadnjem obdobju se je posvetil delovanju znotraj Slovenskega združenja za korporativno varnost, kjer je bil eden od pomembnih članov. S svojimi bogatimi izkušnjami je pomembno pripomogel k rasti ugleda omenjenega združenja in s tem posledično tudi korporativne varnosti kot profesije. Seveda pa je bil njegov neutrudni duh izražen tudi skozi družbene aktivnosti, ki so pokazale njegovo strokovno širino in pripravljenost razdajanja na različnih družbeno pomembnih področjih povezanih z varnostjo. Med drugim je bil tudi prejemnik nagrade za življenjsko delo na področju korporativne varnosti, ki jo podeljujeta Institut za korporativne varnostne študije in Slovensko združenje korporativne varnosti.

Naj počiva v miru.

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

SODOBNI PRISTOPI K PRENOSU ALARMNIH SIGNALOV V VARNOSTNO-NADZORNE CENTRE

Varnostno-nadzorni centri (VNC) predstavljajo hrbtenico sodobnih varnostnih sistemov, saj omogočajo centralizirano spremljanje, analizo in obdelavo alarmnih signalov v realnem času. Ključni dejavnik njihove operativne učinkovitosti je zanesljiv in visoko hitrostni prenos alarmnih podatkov, ki mora biti skladen z najnovejšimi regulativami, tehničnimi zahtevami in varnostnimi standardi.

Z nenehnim razvojem telekomunikacijskih tehnologij so se pojavile različne metode prenosa alarmnih informacij, ki se razlikujejo glede na odzivnost, robustnost, stroškovno učinkovitost in stopnjo integracije v sodobne varnostne arhitekture.

Tradicionalne metode prenosa alarmnih signalov

Ena izmed najstarejših in zanesljivejših metod prenosa alarmnih signalov je uporaba najetih vodov. Ta tehnološka rešitev zagotavlja izjemno hitro komunikacijo, saj se signal posreduje instantno. Kljub temu ima znatne omejitve, saj omogoča zgolj prenos osnovnih informacij, kot so aktivacija alarma, normalno stanje in prekinitev povezave. Visoki stroški vzdrževanja ter omejene funkcionalnosti so privedli do postopnega upadanja uporabe te metode v sodobnih varnostnih sistemih.

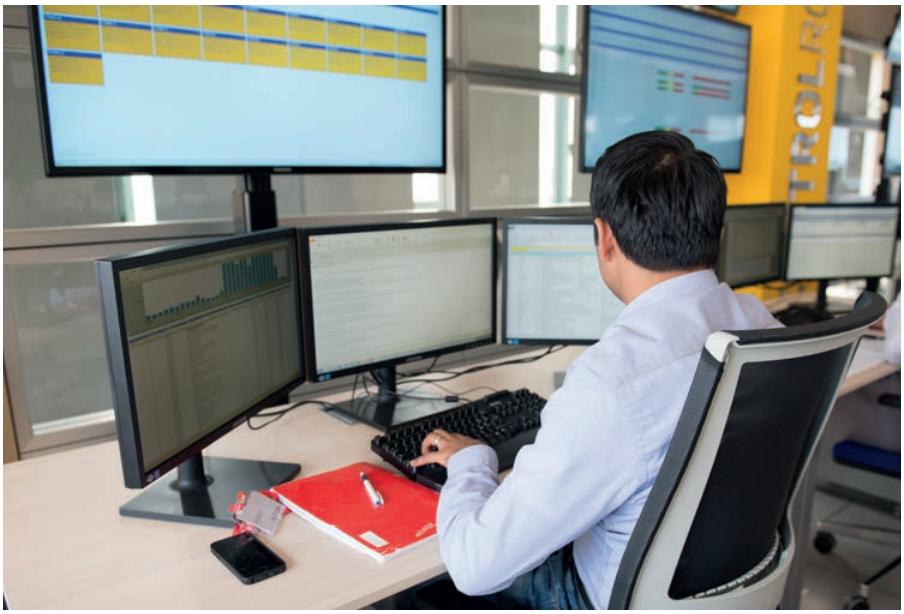
Druga široko uporabljena metoda je prenos prek klasične telefonske linije, ki se zaradi svoje enostavne implementacije in obstoječe infrastrukture še vedno pogosto uporablja. Ta sistem omogoča prenos podrobnih informacij o alarmnih dogodkih, vključno s podatki o particijah in sproženih conah. Kljub svoji priljubljenosti ima ta metoda več pomanjkljivosti, med katerimi so počasnejši prenos podatkov (več kot 15 sekund) ter omejen nadzor povezave, ki se izvaja v intervalih od štiri do štiriindvajset ur. To povečuje tveganje za pozno zaznavo napak v komunikaciji oziroma prekinitvi linije.

Najnovejši trendi v industriji varnostnih sistemov vključujejo implementacijo univerzalnih IP vmesnikov, katerih ključna značilnost je centralizirano upravljanje. Takšni sistemi ponujajo obsežne prednosti na področju vzdrževanja in nadzora, saj omogočajo enostavno in učinkovito obvladovanje širokega spektra naprav in komponent direktno iz samega varnostno-nadzornega centra.

Sodobne tehnologije prenosa alarmnih signalov

Z napredkom digitalnih komunikacijskih sistemov se vse pogosteje uveljavlja prenos alarmnih signalov prek internetnih omrežij. Ta metoda omogoča bistveno hitrejšo, zanesljivejšo in varnejšo komunikacijo, ob tem pa omogoča izboljšan nadzor nad celotno infrastrukturo. Internetni prenos omogoča, da se digitalni signali prenesejo v manj kot eni sekundi, medtem ko prenos prek ContactID protokola še vedno traja približno

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



15 sekund. Ena izmed ključnih prednosti te metode je neprekinjen nadzor povezave, ki poteka v nekaj sekundnih intervalih, kar omogoča hitro zaznavanje morebitnih anomalij in prekinitev povezave. Stroškovni vidik je prav tako ugodnejši, saj omogoča uporabo že obstoječe internetne infrastrukture, pogosto v kombinaciji z mobilnimi podatkovnimi povezavami (SIM karticami).

Vloga IP vmesnikov pri naprednem prenosu alarmnih signalov

Sodobni alarmni sistemi vse pogosteje vključujejo IP vmesnike, ki omogočajo prenos podatkov preko internetnega protokola (IP). Ti vmesniki se delijo na lastne rešitve proizvajalcev alarmnih naprav in na univerzalne rešitve, ki zagotavljajo širšo združljivost z različnimi varnostnimi sistemi.

IP vmesniki proizvajalcev alarmnih central so običajno zasnovani posebej za določene alarmne centrale, kar omogoča optimalno integracijo in hitro izmenjavo podatkov. Njihova uporaba je omejena na specifične ekosisteme, saj pogosto ne podpirajo univerzalnih standardov ali pa zahtevajo namenske sprejemnike alarmnih signalov proizvajalca. Poleg tega so tovarniški protokoli pogosto zaščiteni, kar onemogoča njihovo prilagoditev ali nadgradnjo zunaj okvirov določenega proizvajalca. Varnostne zahteve, ki jih določa slovenska zakonodaja, v mnogih primerih niso v celoti upoštevane, saj globalni proizvajalci pogosto ne prilagajajo svojih sistemov specifičnim trgom z manjšim obsegom uporabnikov.
Na drugi strani univerzalni IP vmesniki omogočajo večjo prilagodljivost, saj so združljivi z večino alarmnih central, ki podpirajo standardne protokole, kot sta ContactID in SIA-DC09. Prednost teh rešitev je v odprtosti sistema, ki omogoča povezovanje z različnimi nadzornimi centri in sprejemniki, ne glede na specifičnega proizvajalca. Številni univerzalni vmesniki vsebujejo dodatne digitalne vhode, ki omogočajo razširitev funkcionalnosti sistema in s tem povečanje varnostne redundance, kot tudi poenostavitev v primeru prenosa požarnih signalov, ki zahtevajo le prenos alarma in napake.

Najnovejši trendi v industriji varnostnih sistemov vključujejo implementacijo univerzalnih IP vmesnikov, katerih ključna značilnost je centralizirano upravljanje. Takšni sistemi ponujajo obsežne prednosti na področju vzdrževanja in nadzora, saj omogočajo enostavno in učinkovito obvladovanje širokega spektra naprav in komponent direktno iz samega varnostno-nadzornega centra. S pomočjo takšnega pristopa je mogoče izvajati konfiguracijo naprav na daljavo, kar bistveno zmanjša potrebo po lokalnih posegih, povečuje fleksibilnost in optimizira operativne procese.

Ena izmed ključnih prednosti teh sistemov je izboljšana odzivnost ob morebitnih napakah ali varnostnih grožnjah. Ko pride do težav, je možno takojšnje diagnosticiranje in popravilo napak iz centralne lokacije, brez potrebe po fizični prisotnosti tehnične podpore na terenu, kar prihrani čas in stroške. Prav tako ti sistemi omogočajo nemoteno nadgradnjo programske opreme ter optimizacijo delovanja sistema. To pomeni, da se programska oprema lahko posodobi brez potrebe po fizičnem dostopu do naprav, kar zmanjša tveganje za napake, povečuje varnost in zagotavlja nemoteno delovanje sistema.

S centraliziranim pristopom in uporabo IP tehnologije, kot na primer eAlarm.io, je mogoče zmanjšati kompleksnost obvladovanja infrastrukture ter povečati njeno učinkovitost, kar se odraža v višji ravni varnosti, zanesljivosti in prilagodljivosti sistema.

Sklepne ugotovitve

Prenos alarmnih signalov predstavlja ključno komponento sodobnih varnostnih sistemov, pri čemer je izbira ustrezne tehnologije odvisna od več dejavnikov, vključno z zanesljivostjo, hitrostjo, stroški in stopnjo prilagodljivosti. Medtem ko tradicionalne metode, kot sta prenos prek najetih vodov in telefonskih linij, še vedno ohranjajo določeno vlogo, se prihodnost varnostnih rešitev vse bolj nagiba k uporabi IP tehnologij. Univerzalni IP vmesniki z odprtimi standardi omogočajo višjo stopnjo prilagodljivosti, povečano varnost in optimizacijo delovnih procesov v varnostno-nadzornih centrih ter kompatibilnostjo z obstoječimi standardi, kar predstavlja temelj nadaljnjega razvoja na področju alarmnih sistemov.

Sistemska integracija naprednih metod prenosa alarmnih signalov zagotavlja celovito optimizacijo delovanja varnostnih centrov. Prihodnost varnostne industrije bo v veliki meri odvisna od zmožnosti implementacije inovativnih tehnologij, ki bodo omogočale še višjo stopnjo avtomatizacije, zmanjšanje operativnih tveganj ter izboljšanje odzivnosti na varnostne grožnje v realnem času. S tem se ustvarja bolj robusten in učinkovit varnostni ekosistem, ki bo v prihodnje še bolj prilagojen potrebam končnih uporabnikov in zahtevam regulativnih organov.

Več o taki rešitvi si lahko preberete na https://ealarm.io/ ■

PODELITEV NAGRAD

Slovenian Grand Security Award

Brdo pri Kranju, 20. maj 2025

16. mednarodna konferenca Dnevi korporativne varnosti

Podelijo se izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti. Nagrado podeljuje ICS-Ljubljana v sodelovanju s Slovenskim združenjem korporativne varnosti. Neodvisna komisija ocenjuje in izbira kvaliteto ter izvirnost prijavljenih udeležencev v naslednjih kategorijah:

- **Najbolj varno podjetje**
- **Najboljši prispevek s področja varnosti**
- **Najbolj varno mesto/občina**
- **Korporativno varnostni manager leta**
- **Najbolj inovativna varnostna rešitev**
- **Inovativna medijska promocija varnosti**

Več o nagradi in nagrajencih na spletni strani instituta www.ics-institut.si!

VAŠA 360° VARNOST 365 DNI V LETU

Odmevni kibernetski varnostni incidenti v preteklem letu so potrdili, da je tudi **Slovenija na radarju kibernetskih kriminalcev**. Ribarjenje oziroma phishing je najbolj razširjena oblika kibernetskega kriminala Zadnje statistike kažejo, da se število tovrstnih napadov tako po svetu kot v Sloveniji iz leta v leto povečuje.

Za vašo varnost in najvišjo stopnjo kibernetske zaščite naj skrbijo **naši visoko certificirani strokovnjaki** iz **Centra kibernetske varnosti in odpornosti**, ki **24 ur na dan in 365 dni v letu** spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske grožnje.

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

Telekom Slovenije, d.d., Ljubljana.

TelekomSlovenije
Vedno na boljše.

16. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 19. - 20. MAJ 2025

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