Korporativna varnost

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

Letnik 2024, februar • št. 34



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

Vloga Državnega sveta pomembnejša kot kadarkoli do sedaj

g. Marko Lotrič, predsednik Državnega sveta Republike Slovenije



VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

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

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

telekom.si/poslovni

TelekomSlovenije

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



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 2024

Izvod revije je brezplačen

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

ISSN 2232-6170

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

V zadnjem obdobju so informacijska tveganja ponovno odprla resno razpravo o tem, kako varni so tisti informacijski sistemi v organizacijah, ki upravljajo s kritično infrastrukturo. Čeprav smo za varnost informacijskih sistemov v organizacijah odgovorni predvsem sami, se vedno bolj krepi spoznanje, da je za učinkovito obvladovanje informacijskih tveganj vedno bolj pomembno vzpostaviti učinkovit ekosistem celega niza deležnikov. Le tako delujoč ekosistem lahko zagotovi celovitejše pristope in bolj sistemsko obvladovanje informacijskih tveganj. Primer HSE je ponovno izpostavil dejstvo, da tega v Sloveniji nismo v celoti razumeli, saj nismo sposobni strokovni skupnosti posredovati jasnih informacij, katere bi tudi ostalim deležnikom omogočile, da bodo pripravljeni na podobne kibernetske napade. Model deljenja je tisti model, pri katerem se znajdeš na različnih delih tega sistema, in sicer kot posredovalec informacij, v primeru, da si bil žrtev napadov ali kot odjemalec informacij. To bo v prihodnosti omogočilo, da se bomo lažje izognili takim napadom. Seveda je za učinkovito delovanje takega ekosistema potrebno postaviti trdne temelje, ki bodo temeljili na zaupanju in razumevanju, da je s skupnimi pristopi možno doseči višjo raven informacijske varnosti posameznih organizacij in družbe kot celote. Krepitvi tega ekosistema in izmenjavi dobrih praks iz različnih operativnih okolij v reviji Korporativna varnost namenjamo izredno veliko pozornosti. Nikakor pa ne smemo pozabiti tudi drugih varnostnih izzivov, ki so še vedno prisotni in si v svoji intenziteti pojavnosti samo podajajo prioritete.

Ravno tem vsebinam je v tokratni številki revije Korporativna varnost namenjena ustrezna strateška pozornost. Skozi izbrane intervjuje imamo možnost slišati tako strateški nivo odločevalcev, ki upravljajo pomembne nacionalne in lokalne organizacije, kakor tudi strokovnjake, ki neposredno izvajajo svoje aktivnosti v okviru procesa korporativne varnosti. Poseben del v tokratni številki namenjamo strateškim nivojem Republike Slovenije, in sicer skozi intervjuja s predsednikom Državnega Sveta Republike Slovenije in novim svetovalcem predsednika Vlade Republike Slovenije za nacionalno in mednarodno varnost. Poleg navedenega smo želeli v tokratni številki revije vsebinsko osvetliti tudi dovolj širok spekter ostalih strokovnih prispevkov in vsebin, ki bodo v pomoč strokovni javnosti pri iskanju potrebnih rešitev in strateške modrosti za ustrezno upravljanje varnostnih tveganj s katerimi smo dnevno soočeni. V uredništvu revije upamo, da bo tudi pričujoča številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi v bodoče.

izr. prof. dr. Denis Čaleta
Glavni urednik



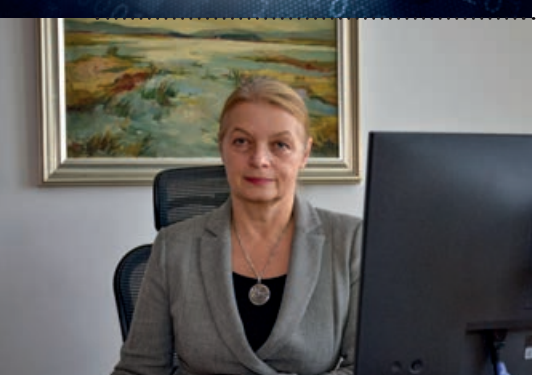
INTERVJU
g. Vojko Volk, veleposlanik, svetovalec predsednika Vlade RS za nacionalno in mednarodno varnost

DINAMIČNI VARNOSTNI IZZIVI REPUBLIKE SLOVENIJE 10



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

KAKŠNA JE DRUŽBENA VREDNOST STROKOVNJAKOV KORPORATIVNE VARNOSTI V SLOVENIJI? 15



INTERVJU
mag. Stanislava Zadravec Caprirolo,
direktorica Združenja bank Slovenije

BANČNI SEKTOR JE VSESKOZI USMERJEN V UČINKOVITO OBVLADOVANJE VARNOSTNIH TVEGANJ 20



INTERVJU
ga. Irena Španinger, dipl. ekon. spec., direktorica Javnega medobčinskega stanovanjskega sklada Maribor

JAVNE ORGANIZACIJE NA LOKALNI RAVNI SE SOOČAJO S SPECIFIČNIMI VARNOSTNIMI IZZIVI 25



SOOBLIKOVANJE STANDARDOV IN POLITIK ZA VEČJO ODPORNOST KRITIČNE INFRASTRUKTURE V EVROPI

Evropa se danes nahaja na prelomnici, kjer je potreba po dvigovanju odpornosti za neprekinjeno delovanje kritične infrastrukture bolj izpostavljena, kot je bila kadarkoli do sedaj. 51

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

INTERVJU
g. Marko Lotrič, predsednik Državnega sveta Republike Slovenije

VLOGA DRŽAVNEGA SVETA POMEMBNEJŠA KOT KADARKOLI DO SEDAJ

Republika Slovenija je bolj kot kadarkoli soočena s potrebo močnejšega povezovanja in ustreznega sodelovanja. Svoje misli o priložnostih za dvigovanje zavedanja o pomenu varnosti in tudi o varnostnih izzivih, pred katerimi se nahaja Republika Slovenija, nam je zaupal g. Marko Lotrič, predsednik Državnega sveta Republike Slovenije.

Državni svet Republike Slovenije je ena od najpomembnejših državnih institucij, ki predstavlja stičišče različnih interesnih okolij. Nam lahko prosim pojasnite težišča delovanja vašega tokratnega mandata?

Državni svet imenujemo tudi zgornji ali drugi dom slovenskega parlamenta. Je svetovalna in nadzorna institucija, katere temeljni smisel je, da prispeva k sprejemanju čim bolj kakovostne zakonodaje. Funkcije in pristojnosti Državnega sveta so vezane na delovanje Državnega zbora. Med pristojnostmi so širši javnosti najverjetneje najbolj znana mnenja, ki jih sprejemajo tako komisije Državnega sveta kot plenum Državnega sveta, in odložilni veto, ki ga je dr. Kristan, prvi predsednik Državnega sveta, opisal kot dobrodošli »time-out«, ki omogoča ponoven premislek o vsebini in posledicah določenega zakona, sprejetega v Državnem zboru. Državni svet lahko zahteva tudi parlamentarno preiskavo, sprejme zahtevo za presojo ustavnosti in zakonitosti predpisov in splošnih aktov ali vloži zakonodajno iniciativo.

V sedmem mandatu je od decembra 2022 do konca leta 2023 Državni svet sprejel 13 odložilnih vetov, vložil pet zahtev za presojo ustavnosti in zakonitosti predpisov in splošnih aktov ter dve zakonodajni iniciativi, konkretneje *Predlog zakona o dopolnitvah Gradbenega zakona* in *Predlog zakona o spremembah Zakona o volitvah v državni zbor*. Namen slednjega je v skladu z mednarodnimi standardi zagotoviti vsem invalidom pravno in dejansko uresničevanje volilne pravice, vključno z osebami s psihosocialno ali intelektualno oviranostjo.

Kot ste omenili v vprašanju, Državni svet predstavlja stičišče različnih interesnih okolij in mi radi rečemo, da smo prvi dom civilne družbe in v skladu s tem se čutimo poklicane, da negujemo povezanost s civilno družbo in ostajamo povezovalec med civilno družbo oziroma državljani in politiko. Prav zato tudi v tem mandatu nadaljujemo z organizacijo številnih posvetov, katerih namen je ponuditi široko platformo, prostor za izmenjavo mnenj in pogledov na aktualne družbene tematike. V okviru posvetov se ukvarjamo predvsem s tistimi tematikami, ki terjajo širok družbeni konsenz in poglobljeno večstransko razumevanje težav, s katerimi se soočajo posamezniki ali posamezne družbene skupine in se rešujejo s kulturo dialoga. V preteklem letu smo izvedli številne posvete z različnih področij, od kmetijstva, gospodarstva, do zdravstva, izobraževanja in še bi lahko našteval. Naj vas na tem mestu raje povabim k spremljanju posvetov, ki se bodo še odvili.

Zaradi nenehnih sprememb je treba vedno znova razumeti in iskati ustrezne odgovore in rešitve za nove oblike groženj, da se lahko ohrani nemoteno delovanje naših organizacij in širše družbene skupnosti.

*avtor je član Slovenskega združenja korporativne varnosti



Kot prvi dom civilne družbe se čutimo k podpori razprave poklicani in radi odpremo vrata vsem, ki želijo v naših prostorih razpravljati o perečih izzivih, pri tem pa jim nudimo tudi tehnično in komunikacijsko podporo. Varnostni procesi so ključni tako za posameznike kot za delovanje družbe na splošno, pa naj si gre za fizično ali informacijsko varnost, neprekinjeno poslovanje, upravljanje s tveganji in človeškimi viri ali varovanje ključnih informacij organizacij.

Drug močan fokus tega mandata je nadaljevanje dela prejšnjega sestava Državnega sveta na področju uvedbe druge ravni lokalne samouprave, pokrajin, ki so ena izmed še neuresničenih ustavnih določb. S tem namenom v okviru Državnega sveta deluje Delovna skupina za pripravo pokrajinske zakonodaje, ki jo vodim. V Državnem svetu menimo, da je vzpostavitev pokrajin edini način, da pride do decentralizacije. O decentralizaciji se sicer v Sloveniji pogovarjamo že dolgo, hkrati pa lahko opazimo, da se proces centralizacije pospešeno odvija sam od sebe. Da pokrajine potrebujemo, so pokazale tudi avgustovske vremenske ujme. Pokrajine bi lahko nase prevzele naloge, ki jih tako država kot manjše občine ne zmorejo optimalno opravljati: umeščanje v prostor, urejanje vodotokov, vodooskrba, odvoz in obdelava odpadkov, socialno varstvo, upravljanje regijskih bolnišnic, razvojni projekti ipd. Decentralizacija bi imela za posledico med drugim tudi to, da bi ljudje lažje našli službo v lokalnem okolju, kar bi razbremenilo avtoceste, okolje in ljudi.

Nedavne poplave so še bolj izpostavile zavedanje, da varnost predstavlja eno od osnovnih dobrin in predpogojev za nemoten razvoj in delovanje družbe. Kako lahko Državni svet pripomore k dvigovanju varnostnega zavedanja o pomenu varnosti v slovenskem okolju?

Res je, nedavne poplave so nas spomnile, da varnost ni samoumevna, kot so nas že nekatere naravne in industrijske nesreče pred tem. Pokazale so tudi, da imamo v Sloveniji izvrsten sistem civilne zaščite in požrtvovalne gasilce, med katerimi jih večina deluje na prostovoljni bazi. Menim, da moramo okrepiti sistemski način financiranja mreže, brez katere bi bila škoda po avgustovskih poplavah še veliko večja. Poplave so pokazale tudi, da so občine, tudi majhne, ključne za reševanje kriz, saj župani zaradi poznavanja terena, prebivalstva in služb lahko veliko prispevajo k usklajeni koordinaciji. In če grem še korak dlje, so poplave pokazale, da tudi v mirnih časih (če mir razumemo kot odsotnost vojne) potrebujemo sodobno opremljeno in usposobljeno vojsko. Druga, manj prijetna

stvar, ki so jo poplave pokazale pa je to, da z vodotoki v Sloveniji slabo gospodarimo. Prav tako marsikje tudi z gozdovi.

27. novembra 2023 se je v dvorani Državnega sveta v organizaciji Komisije Državnega sveta za državno ureditev, Instituta za korporativne varnostne študije (ICS) in Slovenskega združenja za korporativno varnost odvil posvet *Odpornost in neprekinjenost delovanja ključnih organizacij imperativ moderne družbe*, katerega namen je bil pretresti sisteme odzivanja na varnostne grožnje, s poudarkom na organizacijah, ki so ključne za delovanje širše družbene skupnosti. Na posvetu je bilo med drugim izpostavljeno dejstvo, da bo vremenskih neurij, vključno s poplavami, viharji in sušami v prihodnje še več, zato bomo morali razumevanje okolja postaviti na novo raven in se na prihajajoče izredne razmere bolje pripraviti. Potrebne bodo prilagoditve številnih zakonov, premisliti bo treba, kako v sistem zagotavljanja varnosti integrirati vse ključne akterje, kako okrepiti sodelovanje in kako še izboljšati osveščanje vseh akterjev in javnosti.

Še pred tem je oktobra lani Državni svet, kot soorganizator, skupaj s Slovenskim nacionalnim komitejem za velike pregrade, Slovensko inženirsko zvezo in Inženirsko akademijo Slovenije pripravil posvet *Zadrževanje voda in pregrade – pomemben gradnik okolja in družbe: znanje in izkušnje od včeraj in danes za uspešen trajnostni razvoj*. Vodilo nas je zavedanje, da moramo ne le učinkovito uvesti rešitve, ki bodo vodo takrat, ko je le-te preveč, zadržale za sušne čase, poskrbeti je treba tudi za to, da takrat, ko je vode res veliko, ta ne odnese s seboj domov, javne infrastrukture, gospodarskih objektov in življenj. Udeleženci posveta, ki so prišli iz različnih sfer, so se strinjali, da zaradi spreminjajočih se hidroloških oziroma podnebnih dejavnikov in vse bolj neenakomerne porazdelitve padavin, upravljanje vodotokov, ki temelji zgolj na ohranjanju trenutnih razmer, v prihodnje ne bo zadoščalo, ter da je učinkovite rešitve treba iskati v dialogu med vsemi deležniki, vključno z zakonodajalci in pristojnimi ministrstvi.

To sta le dva primera izmed številnih, katerih namen je bil dvigati varnostno zavedanje in hkrati pospešiti ukrepanje pristojnih v smeri zagotavljanja varnosti.

Ste izredno uspešen poslovnež, kar pomeni, da je pomen zagotavljanja obvladovanja tveganj vtkan v vaš način razmišljanja. Kako osebno ocenjujete razvoj dejavnikov kompleksnega varnostnega okolja, ki nas obdaja?

Gre za proces, ki se ga ne da ustaviti, zato se moramo nanj ustrezno odzvati, se prilagoditi. Z vedno večjo povezanostjo, tudi na račun hitrega tehnološkega napredka, bliskovitega vzpona umetne inteligence in globalizacijskih učinkov tako v fizičnem kot tudi virtualnem svetu, s prepletenostjo na vseh nivojih, se veča tudi kompleksnost varnostnega okolja, ki zahteva še močnejše in aktivnejše sodelovanje predvsem med javnim in gospodarskim sektorjem. Ali če poenostavim: tveganjem se ne da izogniti, se pa lahko nanje pripravimo, kar pa zahteva konstantno proaktivno delo.

Zaradi nenehnih sprememb je treba vedno znova razumeti in iskati ustrezne odgovore in rešitve za nove oblike groženj, da se lahko ohrani nemoteno delovanje naših organizacij in širše družbene skupnosti. Še posebej je to pomembno, ko govorimo o delovanju kritične infrastrukture, kot so energetika, promet, oskrba s hrano, pitno vodo, zdravstvo, delovanje



informacijsko-komunikacijskega omrežja in podobno, saj v teh primerih ne gre le za omogočanje ali onemogočanje načina življenja, kot smo ga vajeni, ampak je dobro delovanje pomembno tudi za dober odnos in zaupanje med državljani in vlado. Brez sodelovanja in predvsem vključevanja stroke v postopke odločanja, se kompleksnega varnostnega okolja ne da obvladati.

Državni svet Republike Slovenije je v preteklosti zelo močno podpiral odpiranje strokovne razprave o perečih družbenih izzivih. V tem so bile močno prisotne tudi teme, ki zadevajo varnostne procese. Bo tudi v prihodnje temu namenjeno dovolj prostora?

Kot prvi dom civilne družbe se čutimo k podpori razprave poklicani in radi odpremo vrata vsem, ki želijo v naših prostorih razpravljati o perečih izzivih, pri tem pa jim nudimo tudi tehnično in komunikacijsko podporo. Varnostni procesi so ključni tako za posameznike kot za delovanje družbe na splošno, pa naj si gre za fizično ali informacijsko varnost, neprekinjeno poslovanje, upravljanje s tveganji in človeškimi viri ali varovanje ključnih informacij organizacij. Tega se zavedamo, hkrati pa seveda nismo mi tisti, ki si bomo izmišljali rešitve. O tem morate spregovoriti tisti, ki se na to spoznate, naše delo pa je, da vam to omogočimo in zato vedno znova odpiramo vrata Državnega sveta.

Menite, da bi se moral Državni svet RS na podlagi izhodišč in zaključkov, ki jih prinaša taka strokovna razprava, močneje vključevati v zakonodajne procese ob nastajanju določenih zakonskih okvirov?

V povezavi s posveti, ki se odvijejo v soorganizaciji komisij Državnega sveta ali Državnega sveta, smo vpeljali prakso, da zaključke najprej obravnava pristojna komisija Državnega sveta, ki pripravi poročilo. Poročilo nato obravnava plenum Državnega sveta na eni izmed rednih sej in sprejme sklep, s katerim pozove Vlado Republike Slovenije in v njenem okviru pristojna ministrstva, da zaključke posveta proučijo in se do njih opredelijo.

Pristojne komisije prav tako bdijo nad zakonodajo, pripravljajo strokovno podkrepljena mnenja, ki so, tako verjamem, v pomoč odborom Državnega zbora. Pod črto: v Državnem svetu se trudimo, tako proaktivno z razpravami o perečih tematikah, kot z odzivanjem in opozarjanjem na morebitne pomanjkljivosti v predlogih zakona, ki so v postopkih, ali nenazadnje z odložilnimi veti in, v kolikor je to potrebno, zahtevami za presojo ustavnosti in zakonitosti, ko je zakon že sprejet, zakonodajo izboljšati. Na Vladi RS in Državnem zboru pa je nato odločitev v kolikšni meri naše materiale upošteva.

Gospodarstvo je interesno zelo močno zastopano v Državnem svetu. Katere bi bile po vaši oceni tiste priložnosti, ki bi ravno skozi te kanale gospodarstvu posredovale več informacij in znanj s področja boljšega obvladovanja varnostnih tveganj?

Državni svet sestavlja 40 članov, in sicer 22 predstavnikov lokalnih interesov, štirje predstavniki delodajalcev, štirje predstavniki delojemalcev, štirje predstavniki kmetov, obrtnikov in samostojnih poklicev in šest predstavnikov negospodarskih dejavnosti. Pomembno je tudi to, da so vse državne svetnice in svetniki aktivno vpeti v delo na področju, ki ga v Državnem svetu zastopajo, kar pomeni, da ima vsak izmed njih širok krog, ki ga lahko doseže in obvešča. Svoje delo odlično opravljajo tudi sekretarji komisij in interesnih skupin in služba za odnose z javnostmi. Dobro sodelujemo tudi z Gospodarsko zbornico Slovenije in Obrtno-podjetniško zbornico Slovenije, preko katerih lahko prav tako z obvestili dosežemo velik del gospodarskih subjektov.

Slovensko združenje za korporativno varnost predstavlja pomembno združbo organizacij in posameznikov s področja korporativne varnosti. Izmenjava dobrih praks in informacij na področju obvladovanja tveganj je rdeča nit delovanja omenjene asociacije. Menite, da je v stičišču z Državnim svetom RS lahko to ena izmed poti strokovne podpore širšemu sektorju gospodarstva?

Zagotovo. Da bi lahko svoje delo v prostoru namenjenemu izmenjavi mnenj in iskanju široko podprtih rešitev, kar Državni svet je, opravili kakovostno, potrebujemo informacije od vas, strokovnjakov z varnostnega področja. Potrebujemo vaše argumente, ki temeljijo na vpogledih in izkušnjah, ki jim mora prisluhniti na eni strani politika kot regulator, na drugi strani pa se bomo v okviru svojih zmožnosti trudili tudi za posredovanje informacij tako gospodarstvu kot ostalim družbenim skupinam.

Institut za korporativne varnostne študije in Slovensko združenje za korporativno varnost vsako leto podeljujeta prestižno nagrado Slovenian Grand Security Award. Nagrada je podeljena tudi v kategoriji najbolj varno mesto in najbolj varna občina. Menite, da to še dodatno stimulira lokalna okolja k boljšemu zagotavljanju varnosti?

Bom začel na drugem koncu. Prepričan sem, da so občine v Sloveniji pomemben nosilec razvoja. Doprinos občin je viden na vsakem koraku – poraba sredstev je smotrna, vlaganja so zelo ciljna, lokalne skupnosti so znane po tem, da vsak evro obrnejo vsaj dvakrat. To velja za vsa področja, tudi za področje zagotavljanja varnosti. Zagotovo nagrade, kot je Slovenian Grand Security Award, predstavljajo dodatno spodbudo za še boljše zagotavljanje varnosti, hkrati pa sam postopek in seveda tudi prireditev, na kateri se nagrade podelijo, prispeva k širšemu ozaveščanju javnosti o pomenu varnosti. To zagotovo velja za vse kategorije, ne le v kategoriji najbolj varno mesto in občina.

Je za konec še kakšna misel, ki bi jo posebej želeli posredovati strokovnemu okolju revije Korporativna varnost?

Zahvaljujem se vam za to priložnost, da sem lahko podrobneje predstavil delo Državnega sveta in vam želim uspešno delo tudi v prihodnje, ter se veselim nadaljnjega sodelovanja. Vsem bralcem pa želim, saj smo še vedno na začetku novega leta, predvsem zdravo, uspešno in varno leto 2024, s čim manj tveganji. ■

Foto: Benjamin Beci, Fixmedia

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

SMART COM

Zagotovite varno, zanesljivo in odgovorno digitalno prihodnost

NIS 2

https://bit.ly/skladnost-NIS2

- Smart Center upravljanih varnostnih in omrežnih storitev
- Kibernetska varnost v poslovnem in industrijskem okolju in okolju kritične infrastrukture
- Sodobna omrežja nove generacije za odlično uporabniško izkušnjo



Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
g. Vojko Volk, veleposlanik, svetovalec predsednika Vlade RS za nacionalno in mednarodno varnost

DINAMIČNI VARNOSTNI IZZIVI REPUBLIKE SLOVENIJE

Gospod Vojko Volk je v pogovoru z nami analiziral stanje in izzive na področju zagotavljanja nacionalne in mednarodne varnosti. V pogovoru je med drugim posebno smer svojih razmišljanj namenil varnostnim izzivom pred katerimi se nahaja nacionalna varnost Republike Slovenije.

Najprej nam dovolite, da vam čestitamo ob nastopu te pomembne funkcije. Svetovalec predsednika vlade za nacionalno varnost ima v večini držav izredno pomembno vlogo pri usklajevanju in koordinaciji aktivnosti na področju nacionalne varnosti. Kako si bosta s predsednikom Vlade RS zastavila vašo vlogo?

Delo, ki ga je dobro opravljal moj predhodnik dr. Andrej Benedejčič, je zastavljeno od prvega dne delovanja te vlade. Imel je reden in pogost stik z vsemi sodelavci iz različnih državnih resorjev, ki sestavljajo operativno skupino za nacionalno varnost in s tem pristopom jaz nadaljujem. Pri našem delu ves čas opravljamo določene prilagoditve, kar je nujno, ker se spreminjajo tudi tveganja. V zadnjem času je v ospredju kibernetska varnost, zato krepimo kadrovske in finančne zmogljivosti na tem področju, kjer so ključen izziv izsiljevalske hekerske skupine, posebej iz Rusije in Kitajske.

Na začetku pogovora se nikakor ne moremo izogniti varnostnim krizam, ki se odvijajo pred vrati EU in so močno zaznamovala evropsko in tudi svetovno varnostno okolje. Kaj bi iz vaše perspektive izpostavili kot ključne varnostne izzive pred katerimi se je znašla EU?

Dva krvava vojaška spopada, ki se odvijata v naši neposredni soseščini sta ključna varnostna izziva za vso Evropo. Gre za neposreden vpliv na obe ključni varnostni tveganji tega časa, ki sta ilegalne migracije in terorizem. Izziv pri migracijah je uravnotežiti humanitarno in varnostno razsežnost tega pojava ter dejstvo, da moramo v Evropi okrepiti legalne prihode ljudi, ker brez tuje delovne sile naša gospodarstva ne zmorejo več. Te množične migracijske tokove izkoriščajo tudi teroristi, da v Evropo tihotapijo nevarne posameznike in skupine. Njihov edini namen pri tem je sejanje terorja, ki služi za njihovo politično propagando in cilje. Zato smo že lani stopnjo teroristične ogroženosti Slovenije dvignili na srednjo in ta velja še zdaj.

Občutek imamo, da se zaradi drugih izpostavljenih konfliktnih situacij Ukrajinska kriza vedno bolj odmika v medijski zaton. Kakšno je vaše mnenje o dinamiki podpore Ukrajini?

Umik ukrajinske vojne na medijsko obrobje najbolj osrečuje Rusijo kot agresorja. Še bolj bo Rusija vesela, če bo pri vojaškem prisvajanju tujih ozemelj dobila posnemovalce, denimo v namerah skrajnežev iz Izraela do Palestine, Kitajske do Tajvana ali pa Venezuele do Gvajane. Si predstavljate kaj bi ostalo od Slovenije, če si naši sosedje zaželijo povrnitve „zgodovinskih ozemelj“? Povojna stabilnost sveta je bila utemeljena na dialogu in na mirnem reševanju sporov, zdaj pa Rusija znova uvaja srednjeveško metodo kraje ozemelj šibkejšim. Posebej sramotno je, da Rusija to počne kot stalna članica Varnostnega sveta ZN in krši čisto vsa temeljna načela zapisana v Ustanovni listini ZN, od prvega do zadnjega. Zato je odgovor na vaše vprašanje zelo preprost; nikoli se ne smemo vdati osvajalskemu nasilju močnejšega, ker nas to vrača v barbarstvo in bomo na koncu poraženci vsi, ne samo Ukrajina.

Nikoli se ne smemo vdati osvajalskemu nasilju močnejšega, ker nas to vrača v barbarstvo in bomo na koncu poraženci vsi, ne samo Ukrajina.

*avtor je član Slovenskega združenja korporativne varnosti



Zaradi Izraelsko-Palestinskega konflikta se ponovno dviguje raven teroristične ogroženosti v EU, med drugim pa prvič tudi v Sloveniji. Kaj lahko pričakujemo ob teh tveganjih?

Brez dvoma lahko pričakujemo povečan val migracij proti Evropi, ki se je že lani močno povečal. K nam je lani prišlo skoraj 60 tisoč prebežnikov, kar je dva in pol krat več kot prejšnje leto, po sredozemski poti v sosednjo Italijo pa 155 tisoč, kar je že povsem blizu rekordnim številkam iz let 2015 in 2016. To so učinki, ki se jih sovražniki Evrope in celotnega Zahoda veselijo vnaprej, ker vedo, da vprašanje migracij povzroča politične napetosti tako znotraj držav kot na ravni EU. V primeru Gaze je Hamas natančno vedel, kakšne bodo posledice njihovega napada na Izrael in pokola nedolžnih civilistov. Hamas pa podpira Iran, isti Iran, ki prodaja na tisoče dronov Rusiji za zločinsko bombardiranje ukrajinskih mest. Iran in Putin sta pobratena v sovraštvu do Zahoda. Tako Iran kot tudi Putin izvajata ideološko in politično propagando, da je Rusija v vojni z Zahodom, kar morajo širiti vsi Putinovi podporniki po svetu, ne manjka jih niti pri nas. Pri tem gre za svojevrstni politični rasizem, ker diskvalificirajo vse nas, ki pripadamo zahodu. Je pa res, da je Zahod strahotno moteč za vse diktature, tako verske kot politične, ker je demokratičen, ker temelji na človekovih pravicah in vladavini prava. Islamski teroristi sovražijo vse, kar je nam na zahodu najpomembnejše, svoboda posameznika in še posebej enakopravnost žensk. Pri boju zoper terorizem je zato ključno, da ne podležemo njihovemu cilju, ki je ta, da živimo v strahu. Zato na Zahod množično prihajajo ljudje z vseh koncev sveta medtem, ko v diktature ne gre nihče. Dejstvo je, da demokracija še nikoli ni napadla demokracije in to nam daje upanje, da bo s širjenjem demokracij v svetu tudi manj vojn in trpljenja.

Kako vidite nadaljnji razvoj nacionalno-varnostnega sistema v teh zahtevnih gospodarskih in družbenih okoliščinah? Je možno nekatere procese integrirati in jih poenostaviti ter s tem povečati učinkovitost delovanja?

Integriranje je načeloma pot k večji učinkovitosti, ne pa vedno. Zaenkrat vidim predvsem kadrovske pomanjkljivosti, potrebovali bi veliko več strokovnjakov na vseh področjih, ki bi se lahko tako v javni upravi kot v zasebnem sektorju ukvarjali zgolj z varnim delovanjem države in njenih podsistemov, ter seveda gospodarstva. To delo terja spremljanje dogajanj v svetu in seznanjanje s strokovno literaturo, v zadnjem času pa je potrebna predvsem sposobnost predvidevanja varnostnih razmer in dogajanj. Časi, ko se je pojem varnostnih inženirjev povezovalo s fizičnim varovanjem stavb in oseb so preteklost. Recimo, da se varnostna stroka digitalizira tudi v tistem delu, kjer so naše navade še vedno analogne.

Minili pa so tudi časi, ko so grožnje nacionalni varnosti odkrivali predvsem policija, obveščevalne agencije in mediji. Zdaj je to naloga domala vseh državnih organov in tudi velikih podjetij, ki se morajo znati tudi sama ubraniti pred sumljivimi ponudbami, transakcijami, posli, prevarami, fiktivnimi posli ali pa pred posredniškim pranjem denarja. V zadnjem času postaja Slovenija zanimiva za mafijske združbe z Balkana, ki jim je zaradi evropskih sankcij do Rusije vedno težje prati de-

Pri boju zoper terorizem je zato ključno, da ne podležemo njihovemu cilju, ki je ta, da živimo v strahu. Zato na Zahod množično prihajajo ljudje z vseh koncev sveta medtem, ko v diktature ne gre nihče. Dejstvo je, da demokracija še nikoli ni napadla demokracije in to nam daje upanje, da bo s širjenjem demokracij v svetu tudi manj vojn in trpljenja.

nar, pridobljen iz nelegalnih poslov in trgovine z drogo, zadnja leta pa tudi iz ilegalnih migracij. Ustanavljajo predvsem podjetja, kjer se v transakcijah obrača velik denar, to pa je predvsem trgovanje z nepremičninami. Po lanskih podatkih OZN je trgovina z ilegalnimi migracijami po obsegu zaslužkov prvič presegla raven svetovne trgovine z orožjem in količina denarja, ki ga morajo kriminalci oprati je vedno večja.

Ob zadnjih katastrofalnih poplavah se je pokazalo tudi nekaj vidikov, ki bodo v prihodnje potrebovali več pozornosti v smislu zagotavljanja neprekinjenega delovanja kritične infrastrukture. Kaj lahko pri novih predlogih na tem področju storite vi, kot pomembno koordinativno stičišče na področju nacionalne varnosti?

Pod to vlado smo v Sloveniji doživeli največji požar, kot tudi največje poplave, kar pomnimo. Sistem je deloval dobro, od CZ do gasilcev, od vojske do policije, državnih organov in prostovoljcev. Iz požara na Krasu smo dobili poduk, da moramo okrepiti sposobnost gašenja iz zraka in smo sprejeli odločitev o nabavi letal, ki bodo to nalogo lahko opravila. Iz poplav pa smo dobili potrditev, da mednarodna solidarnost deluje. Takoj smo dobili pomoč iz EU, najprej tehnično in materialno in zdaj še finančno. Naučili smo se, da je ob tako ogromnih posledicah poplav nujno potrebno imeti težko mehanizacijo in zaradi goratosti naše domovine predvsem velike helikopterje, ki jih imajo praviloma samo vojske.

Zato gredo naši predlogi v smeri tega, da se tako nacionalne vojske kot tudi sam NATO ustrezno odzovejo na dejstvo, da bo naravnih nesreč vedno več in da mora vojska pri tem prevzeti del bremena, ko gre za pomoč prizadetemu prebivalstvu. Naj pri tem omenim študijo EU iz katere izhaja, da je prav Slovenija med vsemi evropskimi državami daleč najbolj prizadeta s škodami po naravnih nesrečah, v prvi vrsti po poplavah. Medtem, ko je evropsko povprečje obsega škod 0.20 odstotka BDP na leto je v Sloveniji številka skoraj dvakrat višja, točneje 0.35 odstotka na leto, pri čemer rekordna škoda zaradi lanskih poplav sem še ni všteta. Med najbolj verjetnimi razlogi je vse bolj izrazito segrevanje Jadranskega morja, ki vpliva na vodonosnost oblakov nad Alpami in posledično obilnejše padavine.





A tako pri požaru kot pri poplavah je bilo skupno to, da smo v prvih urah delovali predvsem z vrha navzdol. Po domače povedano, vrh države in zaščitnih struktur je bil prvi dan ali dva ves čas na telefonih in se usklajeval, potem so šele stekli uteženi mehanizmi. Podobno je bilo ob kibernetskem napadu na HSE. Avtomatizmi pogosto odpovedo, ko ne gre za običajne dogodke. Nihče ni prvi dan požara ali poplav vedel, da bo tisto največji požar in bodo tiste poplave največje v zgodovini. Ko smo to zaslutili smo takoj ravnali preventivno, pri poplavah denimo takoj zaprosili za mednarodno pomoč, ki je potem prišla dobesedno takoj. Na koncu se je znova tudi potrdilo, da ljudje v tej državi še vedno hitro stopimo skupaj, ko je to potrebno.

Razvoj in odvisnost od informacijske tehnologije postavlja kibernetske grožnje v posebno perspektivo. Kateri so po vašem mnenju tisti koraki, ki jih lahko storijo manjše države, kot je Slovenija, za učinkovito zavarovanje pred temi kompleksnimi grožnjami? Primer napada na HSE je prišel na vašo mizo skoraj takoj po prevzemu te pomembne funkcije.

Kadrovska in finančna krepitev zaščite je nujna in o tem smo konkretne predloge na vlado že posredovali. Drugi segment je ustrezno obveščanje medijev in javnosti in naj povem, da se je hitra odločitev HSE, da o napadu seznani pristojne organe izkazala za pravilno in učinkovito. Tretji segment pa je širjenje znanja o pomenu kibernetske varnosti in tukaj nam še veliko manjka, tudi zato, ker pri digitalizaciji družbe zaostajamo, pa kot majhna in prilagodljiva družba ne bi smeli. Zgled nam morajo biti baltske države, ki so vodilne na tem področju in so novim časom prilagodile tudi šolske programe oz. kurikulume. To opravilo nas še čaka in upam, da bodo slovenski šolniki sposobni razumeti, da se časi spreminjajo hitreje kot nekoč. Moramo pa to storiti čim prej, če ne se bo naš razvojni zaostanek samo še povečal.

> Minili pa so tudi časi, ko so grožnje nacionalni varnosti odkrivali predvsem policija, obveščevalne agencije in mediji. Zdaj je to naloga domala vseh državnih organov in tudi velikih podjetij, ki se morajo znati tudi sama ubraniti pred sumljivimi ponudbami, transakcijami, posli, prevarami, fiktivnimi posli ali pa pred posredniškim pranjem denarja.

Slovenske organizacije so zelo aktivne na različnih EU projektih s področja kritične infrastrukture in kibernetske varnosti. Menite, da lahko operativno raziskovalna spoznanja pomagajo pri iskanju novih rešitev za izboljšanje normativnih in koordinativnih ukrepov v



Republiki Sloveniji? Postavlja se glavno vprašanje kako pravilno usmeriti in integrirati vso pridobljeno znanje v različne dele nacionalno-varnostnega sistema?

Drži, znanja nam ne manjka, vendar ga ne znamo pretočiti oziroma aplicirati na delovanje družbenih sistemov, ne samo varnostnih. Zdravstvo je tipičen primer tega, tam nam krošnjarijo privilegirani ponudniki, digitaliziranost naših bolnišnic pa ostaja sramotno razdrobljena in neučinkovita. Enako velja za področje dolgotrajne oskrbe, kjer smo v primerjavi z razvitimi državami še v srednjem veku. Če znamo vrhunsko voditi NEK in jo v vseh pogledih ustrezno varnostno zaščititi in če imamo vrhunske znanstvene ustanove, kakršen je Inštitut Jožef Štefan, bi morali znati ustrezno opremiti in zaščititi tudi ostalo proizvodnjo in distribucijo energije in seveda tudi samo državno upravo.

Strokovna združenja imajo pomembno mesto pri zagotavljanju uveljavljanja posamezne stroke. Slovensko združenje korporativne varnosti je tukaj izredno aktivno, kar s svojo vedno večjo včlanitvijo prepoznavajo tudi ključne državne institucije. Menite, da je ta strokovno-povezovalna pot lahko ena od možnosti tesnejšega sodelovanja vseh deležnikov pri iskanju učinkovitih rešitev za kompleksne grožnje, katerim je izpostavljena Republika Slovenija?

Združenja so pomembna za širjenje zavedanja o pomenu varnosti, tudi varnosti pri zaščiti naših dosežkov s področja znanja, prav posebej tudi v gospodarstvu. Pred 23 leti sem kot takratni vodja urada za varovanje tajnih podatkov koordiniral pripravo našega prvega zakona o varovanju tajnih podatkov in takratnemu PV Janezu Drnovšku podpisal prvo nacionalno varnostno preverbo. Tista leta je bilo moderno, da so se v medijih norčevali iz pojma zaščite „nacionalnih interesov“, češ da je to nekaj slabega in preseženega. Seveda je šlo pogosto za lobiranje za interese tujega kapitala, da pokupi slovensko srebrnino. Krona tega početja je bila, da smo ravno v času, ko se je hrana začela izkazovati za strateško nacionalno dobrino v nekaj letih tujcem, posebej hrvaškim podjetjem, prodali komplet slovenske prehranske industrije, na čelu z Mercatorjem in Drogo Kolinsko. Sam sem imel enako težavo, dopovedati poslancem, ki so morali glasovati o zakonu, da država pač mora ščititi svoje tajnosti in s tem svoje nacionalne interese, ker to počno vse države. Nek poslanec je zahteval, da to pojasnim in sem odvrnil, da „država brez nacionalnih interesov ni kaj več od krajevne skupnosti“. In nekaj časa smo pač bili krajevna skupnost, ceno tistega časa pa plačujemo še danes.

Podobno je danes s tistimi, ki se hitro navdušijo nad cenejšimi ponudbami azijskih ali kitajskih proizvajalcev IT storitev in opreme. Začetna nizka cena se lahko hitro obrne v škodo po tem, ko se rešitve izkažejo za problematične z vidika varnosti in zaščite znanja ter patentiranih tehnoloških rešitev. V takih primerih so strokovna združenja lahko ključnega pomena, še posebej v povezavi z mediji in javnim mnenjem. Da se najcenejše blago pogosto na koncu izkaže kot najdražje, pa so vedele že naše stare mame. ■

Foto: Žan Kolman, KPV

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



KOLUMNA

KAKŠNA JE DRUŽBENA VREDNOST STROKOVNJAKOV KORPORATIVNE VARNOSTI V SLOVENIJI?

Sodobno varnostno okolje ima vedno večji vpliv na neprekinjenost delovanja naših organizacij. Obvladovanje varnostnih tveganj je postal eden od glavnih procesov in pomemben predpogoj za učinkovito in uspešno delovanje organizacij. S tem povezanim dejstvom se nam logično odpre vprašanje, kakšna je družbena vrednost strokovnjakov korporativne varnosti, ki naj bi v organizacijah nosili težiščno breme načrtovanja in izvajanja ukrepov za obvladovanje varnostnih tveganj. V pričujoči kolumni želimo predvsem osvetliti poti in stranpoti v razvoju ugleda dejavnosti, ki jo pojmujemo s terminom korporativna varnost.

Živimo v času, ko se vrednotenje pomembnosti posameznih poklicnih skupin zrcali predvsem skozi indikatorje, ki predstavljajo družbeno pomembnost teh poklicev. Ti indikatorji so največkrat povezani z višino finančnih sredstev, ki jih zaposleni v določeni dejavnosti v povprečju prejemajo. Seveda so poleg materialno finančnih vidikov, ki se rezultirajo v višini osebnih prihodkov, nagrad, deležih v podjetjih in drugih finančno materialnih bonitet zrcalijo tudi skozi nematerialne vidike, kot so hierarhični položaj v organizacijah, zaznavnost pomembnosti in privlačnosti posameznega poklica v širšem družbenem okolju, medijska izpostavljenost in privlačnost ter drugi delovni pogoji.

Skozi navedene dejavnike bomo poskušali analizirati uspešnost razvoja korporativne varnosti v Sloveniji, od časa osamosvojitve države do današnjih dni, ter nakazati glavne smernice tega razvoja za prihodnost.

Najprej se dotaknimo organizacijske umeščenosti omenjene dejavnosti. Če smo v začetku devetdesetih in ob prehodu v 21. stoletje to dejavnost gledali predvsem skozi prizmo fizičnega in tehničnega varovanja, je bil položaj omenjenih strokovnjakov v organizacijah relativno odrinjen na marginalno obrobje pomembnosti. Nahajali so se na 4. ali 5. nivoju

Živimo v času, ko se vrednotenje pomembnosti posameznih poklicnih skupin zrcali predvsem skozi indikatorje, ki predstavljajo družbeno pomembnost teh poklicev. Ti indikatorji so največkrat povezani z višino finančnih sredstev, ki jih zaposleni v določeni dejavnosti v povprečju prejemajo.

*avtor je član Slovenskega združenja korporativne varnosti

organizacijske umeščenosti, največkrat nesistemsko umeščeni v Službe za podporo ali splošne zadeve. S tem povezana pa je bila tudi privlačnost te dejavnosti zelo nizka, kar se je odražalo tudi skozi nizke finančne prejemke in družbeno neprivlačnost te dejavnosti. Razumevanje izvajanja korporativne varnosti je temeljilo predvsem na tradicionalnem pogledu zagotavljanja varnostnih procesov, ki so izhajali iz rigidnih pogledov državnih struktur, policije, vojske in drugih državnih organov iz katerih so v večini prihajali kadri v takratno korporativno varnost. Ti pogledi niso bili usmerjeni v dinamičnost in prožnost prilagajanja zahtevnemu poslovnemu okolju, kjer je bil konstanten pritisk v smeri učinkovitosti in racionalnosti delovanja ter zagotavljanja maksimalnega dobička. S tem je bilo v prvih 15 letih delovanja po osamosvojitvi Slovenije največ izzivov, kateri so se največkrat odražali skozi nerazumevanje med zahtevami in pričakovanji strateškega managementa, ki je logično izhajal iz ekonomsko poslovnih vod in je v glavnem gojil poslovni vidik razumevanja. Na drugi strani pa kadri, ki so se znašli v dinamični poslovni situaciji s temeljem znanja in izkušenj, ki so jih pri tem včasih pomembno omejevali. To nerazumevanje obeh pomembnih struktur se je največkrat odražalo v tem, da so bili strokovnjaki korporativne varnosti izključeni iz strateškega nivoja odločanja in predvsem oblikovanja strateških pobud za nadaljnje razvojne korake. To pa je za organizacije pomenilo, da so pri razvoju in prodoru na določena tržišča v največji meri zanemarjala varnostne vidike obvladovanja tveganj, oz. so jih v svoje procese vključevala mnogo prepozno, kar je zmanjševalo njihovo kvaliteto in organizaciji prinašalo entropične vplive, tudi skozi povečevanje stroškov poslovanja ali v določenih primerih propadlih poslovnih načrtov. Na tej poti so se, počasi vendar odločno, začeli razvijati zametki novih izobraževalnih konceptov in strokovnega združevanja, ki je dejavnosti korporativne varnosti začelo dajati prve orise, kot jo poznamo danes. V tem okviru velja posebej izpostaviti dr. Milana Vrška in dr. Braneta Bertonclja[1], ki sta pomembna pionirja uvajanja novih poslovno varnostnih procesov, kot so bili razumevanje integralnega varnostnega sistema, razumevanje statusa, ki bi ga morali doseči strokovnjaki na tem področju, izobrazbene stopnje in družbene pomembnosti tega poklica znotraj organizacij. V takratnem obdobju so bili ti pionirji večkrat poimenovani s prispodobo »petelinov, ki prezgodaj pojejo«, saj niti družba kot celota, kakor tudi strateški management v organizacijah, nista bila sposobna dojeti pomena teh predlaganih poti. Roko na srce manjkala pa je tudi kritična masa strokovnjakov s tega področja, ki bi zadeve hitreje premikala naprej. Kljub izobraževalnim zametkom in vnašanju te vsebine v izobraževalne programe določenih izobraževalnih organizacij, so te vsebine zaradi slabega vpisa vedno bolj drsele na obrobje in v večini primerov tudi izpadle iz rednih izobraževalnih shem. Bili so tudi poskusi na področju interesnega združevanja, ki so bili storjeni v okviru Združenja varnostnih menedžerjev Slovenije, vendar je pobuda, zaradi pomanjkanja vizije razvoja in parcialnih interesov organizatorjev, zamrla. V tem delu ne želimo slovenski primer izpostavljati, kot primer, ki je popolnoma ločen od procesov, ki so se dogajali v širšem mednarodnem prostoru. Dejavnost se je tudi drugje ukvarjala s podobnimi izzivi in ovirami pri razvoju. Seveda jo je pa potrebno razumeti skozi drugačno širino potencialov, na finančnem in kadrovskem področju ter nenazadnje s pritiski globalnega mednarodnega okolja. Slovenija je bila v tem obdobju še vedno zelo obremenjena z dojemanjem samozadostnosti v svojih majhnih okvirih.

V začetku 21. stoletja je mednarodno varnostno okolje z vsemi pojavnimi oblikami groženj in tveganj, ki so imele zelo velik vpliv tudi na samo poslovanje organizacij, postalo tako obremenjujoče, da je iz tega logično sledila potreba po hitrejšemu razvoju dejavnosti korporativne varnosti.



V začetku 21. stoletja je mednarodno varnostno okolje z vsemi pojavnimi oblikami groženj in tveganj, ki so imele zelo velik vpliv tudi na samo poslovanje organizacij, postalo tako obremenjujoče, da je iz tega logično sledila potreba po hitrejšemu razvoju dejavnosti korporativne varnosti. V Sloveniji je glavno prelomnico ob koncu leta 2008 predstavljala ustanovitev Slovenskega združenja za korporativno varnost, ki je s podporo Instituta za korporativne varnostne študije dosegel visok nivo prepoznavnosti in pomembnosti te dejavnosti v širši družbeni skupnosti. Danes je v združenju integrirano zelo veliko število ključnih organizacij in posameznikov. Posebna vrednost tega združevanja pa je, da so poleg ključnih poslovnih organizacij, vrednost in pomembnost tega strokovnega združevanja na področju korporativne varnosti, prepoznale tudi ključne državne institucije, kar je to združevanje dvignilo še na mnogo višji nivo.

Nahajamo se na pomembni poti, kjer pa je pred nami še veliko ovir, ki jih bo potrebno uspešno premagati, da se bo dejavnost korporativne varnost še naprej razvijala z ustrezno dinamiko.

Prvi izziv vsekakor predstavlja finančni vidik te dejavnosti. Če lahko rečemo, da smo na področju organizacijske umeščenosti naredili potrebne korake v smeri dvigovanja korporativne varnosti direktno na ali v bližino strateškega nivoja, pa težje rečemo, da je to dojemanje sledilo tudi na področju finančne ovrednotenosti dela na teh delovnih mestih. Če

pogledamo primer direktorja službe za korporativno varnost in ga primerjamo s primerljivimi nivoji na globalnem mednarodnem okolju, lahko omenimo, da je ta dejavnost v Sloveniji še vedno primerjalno podcenjena. Po mednarodni raziskavi, ki jo vsako leto izvede Foushée Group in je usmerjena v »Security & Compliance Compensation Survey«[1] je povprečni dohodek globalnega direktorja za korporativno varnost (CSO – Chier Scurity officer) v letu 2022 znašal 348.153 USD. Na to pa je v povprečju CSO dobil še 209.460 USD za uspešnost, ki se največkrat izplačuje v delnicah podjetja. Predvsem v tej dodatni kategoriji je zaznano pomembno povečanje tudi na globalnem nivoju od predkoronskih let 2017, ko je višina teh dodatnih bonusov znašala v povprečju 142.486 USD. Če to stanje pogledamo še za drugo pomembno funkcijo v sistemu korporativne varnosti in sicer CISO (Chief Information Security Officer) vidimo, da 204.073 USD predstavlja osnovno plačilo v letnem obdobju in še dodatnih 57.781 USD kot nagrada, ki se največkrat izplača v delnicah podjetij. V Sloveniji bo potrebno podrobno analizo tega področja še opraviti, vendar z usmerjenimi intervjuji z najbolj izpostavljenimi direktorji korporativne varnosti v največjih slovenskih organizacijah lahko z gotovostjo trdimo, da močno odstopamo od navedenih primerjalnih vrednosti, ki jih dosega stroka na globalnem nivoju. V večini se sicer nahajajo v statusu sklepanja individualnih pogodb za svoje delo, kar jim omogoča višjo raven finančne ovrednotenosti njihovega dela, vendar so z drugega vidika tudi zelo vezani na prepogoste menjave strateških vodstev v slovenskem poslovnem okolju. Na žalost je finančni vidik še vedno tisti, ki v dobi potrošniškega dojemanja delovanja družbe tudi najbolj determinira uspešnost in privlačnost poklicev.

Naslednji izziv predstavlja izobraževalni sistem. Posledično se še vedno nezadostna privlačnost teh poklicev zrcali tudi v izobraževalnem programu, kjer so tisti redki programi, kateri ponujajo te specialistične vsebine, zelo slabo obiskani. To predstavlja dve bistveni težavi, in sicer, da v realni sektor ne prihaja dovolj visoko usposobljenega podmladka, na drugi strani pa to predstavlja pomanjkanje kritične mase, ki bi sistem pri svojem razvoju potiskala naprej. Na tem področju bo potrebno naredi resni premislek, kako narediti slovenski ekosistem na področju izobraževanja teh specifičnih profilov bolj prožen in atraktiven za višji vpis mladih kadrov.

Tretji pomemben izziv je krepitev strokovnega izobraževanja. Če vzamemo zdravnike, kot aktualno poklicno skupino, imajo preko svojega združenja FIDES in Zdravniške zbornice dve močni temeljni sidri za skupne nastope in pogajanja o ustreznem vrednotenju njihovega finančnega in materialnega statusa. Tudi na področju korporativne varnosti je potrebno še krepiti zavedanje, da je Slovensko združenje za korporativno varnost tisti strokovni interesni okvir, ki bo imel dovolj moči za spreminjanje širših sistemskih predpogojev za prepoznavnost in uspešnost korporativne varnosti. S tem pa posledično tudi dvig pomembnosti in finančne vrednosti vsakega posameznega dela te dejavnosti v vsaki posamezni organizaciji. Na tem delu imamo še veliko rezerve, saj si za aktivnejše delovanje znotraj te asociacije ne uspemo zagotoviti dovolj svojega časa. S tem je povezana tudi udeležba na ključnih strokovnih dogodkih, kot so Dnevi korporativne varnosti, kjer je včasih občutek, da si strateški management lažje oddvoji svoj dragoceni čas za udeležbo, kot sami strokovnjaki s področja korporativne varnosti. Ugotovitev se zdi sicer absurdna, temveč ni daleč od resnega zaznavanja realnega stanja.

Če bodo strokovnjaki na teh delovnih mestih uspeli dokazati visoko stopnjo profesionalnosti in strokovnosti, bo tok dogodkov sam poskrbel, da bodo omenjene dejavnosti postale neodtuljivi del vsakega organizacijskega ustroja, pa naj si gre za gospodarsko ali javno organizacijo.

Stopnja profesionalnosti na eni strani in višja samopodoba, kot dopolnilo tega, sta naslednja pomembna izziva. Dejstvo je, da so varnostni izzivi s katerimi se soočamo v moderni družbi najboljša reklama za to dejavnost. Če bodo strokovnjaki na teh delovnih mestih uspeli dokazati visoko stopnjo profesionalnosti in strokovnosti, bo tok dogodkov sam poskrbel, da bodo omenjene dejavnosti postale neodtuljivi del vsakega organizacijskega ustroja, pa naj si gre za gospodarsko ali javno organizacijo. S tem povezan je tudi problem, ki ga vse prevečkrat zapažamo pri Slovencih in to je nizko samovrednotenje. Dejstvo je, da je strokovni nivo večine predstavnikov dejavnosti v Sloveniji popolnoma primerljiv z mednarodnim okoljem in je s tega stališča potrebno zagotoviti samo kanček strokovne prednosti in prevzemanja odgovornosti, ki bo pomenil dodatni preskok naprej. Odgovornost želimo poudariti, kot enega izmed ključnih dejavnikov za dvigovanje strokovnega nivoja, tudi na področju korporativne varnosti. Ko bo management začel prevzemati odgovornost za svoja ravnanja ali ne ravnanja in se bo v nekaterih primerih začelo uveljavljati odškodninske in druge zahtevke od odgovornih, bo tudi na področju dejavnosti korporativne varnosti to predstavljalo velik korak v smeri dvigovanja potrebnih kompetenc za izvajanje te zahtevne dejavnosti.

V pričujočem prispevku smo poskušali kratko osvetliti nekaj ključnih izzivov, ki dejavnosti korporativne varnosti vodijo po poti nadaljnjega uveljavljanja v širšem družbenem okviru. Prehojena pot nam predvsem kaže na to, da so pred nami pomembe prelomnice, ki bodo korporativno varnost izstrelile v orbito uspešnih in cenjenih poklicev. Brez njih si družba ne more predstavljati svojega normalnega delovanja. S tem pa bodo prišli tudi drugi učinki, kot so finančna privlačnost dejavnosti in njena prepoznavnost.

1 Oba imenovana sta prejemnika najvišjega priznanja Slovenian Grand Security Award za življenjsko delo, ki ga podeljujeta Slovensko združenje za korporativno varnost in Institut za korporativne varnostne študije.
2 Podrobnosti o raziskavi Foushée Group dostopno na: https://www.securitymagazine.com/articles/98831-the-average-security-professionals-salary ■

Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

Združenje ima redne, korporacijske in častne člane.

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

Melamin, Mercator, telemach, SIEMENS, NIJZ Nacionalni inštitut za javno zdravje, ELEKTRONČEK, Telekom Slovenije, Pošta Slovenije, AKRAPOVIČ, AJPES, INFORMATIKA, novakbm, Elita i.b. d.o.o., ZARJA ELEKTRONIKA, UNISTAR PRO, CINKARNA, Slovenske železnice, GEN SKUPINA, Občina Slovenska Bistrica, Onkološki inštitut Institute of Oncology Ljubljana, CAA, SMART COM, URSIV, Ministrstvo za infrastrukturo, Javni medobčinski stanovanjski sklad Maribor, GENERALI, Mestna občina Ljubljana, PETROL Energija za življenje, interblock luxury gaming products, triglav, SPICA, DARS, smartis pametni informacijski sistemi, LON, energetika ljubljana

www.ics-institut.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
mag. Stanislava Zadravec Caprirolo, direktorica Združenja bank Slovenije

BANČNI SEKTOR JE VSESKOZI USMERJEN V UČINKOVITO OBVLADOVANJE VARNOSTNIH TVEGANJ

Dinamično delovanje bančnega sektorja je močno odvisno od učinkovitih procesov obvladovanja raznovrstnih varnostnih tveganj. Pospešeni procesi digitalizacije so postali realnost tudi v tem pomembnem sektorju. Zaradi navedenega ima Združenje bank Slovenije v pogledu izmenjave dobrih praks in usklajenih pristopov na področju obvladovanja vplivov zahtevnega varnostnega okolja izredno pomembno vlogo. O priložnostih in izzivih delovanja tega pomembnega združenja smo se pogovarjali z mag. Stanislavo Zadravec Caprirolo.

Bodite tako prijazni in nam na kratko predstavite glavna težišča delovanja Združenja bank Slovenije na področju povezanim z obvladovanjem tveganj.

Združenje bank v interesu svojih članic – bank, hranilnic in lizing družb, opravlja dejavnosti, ki so v povezavi z bančno in finančno dejavnostjo članic, kot na primer predstavljanje in zastopanje skupnih interesov članic Združenja pri državnih organih, monetarnih oblasteh, finančnih organizacijah ter drugih združenjih o vprašanjih, ki zadevajo urejanje razmerij iz makroekonomskih in denarnih politik, povezovanje z gospodarstvom, finančnimi organizacijami ter znanstvenimi, tehničnimi in drugimi institucijami zaradi pospeševanja razvoja trga denarja in kapitala ter uveljavljanja bančništva in drugih finančnih dejavnosti. Velik del aktivnosti je posvečen izobraževalnim aktivnostim, predvsem za potrebe članic, pa tudi na področju finančnega opismenjevanja mladih oziroma vseh starostnih skupin. Glavna težišča delovanja so strateška področja regulative in nadzora, poslovanja s komitenti (prebivalci in podjetji) povezano tudi s financiranjem prehoda na zeleno ekonomijo (ESG) in pa varstvom potrošnikov in podatkov, področje digitalne transformacije ter ne nazadnje ugleda. Z vidika področij upravljanja tveganj pa so poleg »tradicionalnih« tveganj, kot so področje kreditnega, kapitalskega,

Proces zagotavljanja neprekinjenega poslovanja je dinamičen proces tudi v povezavi z razvojem tehnologije, digitalizacijo, kibernetskim tveganjem in mu v okviru strokovnega dela delovnih teles Združenja in tudi v strokovnih razpravah namenjamo pomemben prostor.

*avtorica je članica Slovenskega združenja korporativne varnosti

likvidnostnega, obrestnega in operativnega (našteta so le nekatera), vedno bolj pomembna tudi »nova« tveganja, kot na primer tveganja povezana z geopolitičnimi tveganji in vojnami oziroma sankcijami, tveganja povezana z zelenim prehodom - ESG tveganja in pa, zaradi razvoja tehnologije, tudi vedno bolj pomembna z njo povezana tveganja, kot na primer kibernetsko tveganje. Le ta so zelo pomembna tudi z vidika ozaveščanja komitentov.

Za seboj imate bogato zgodovino opravljanja najodgovornejših funkcij v Slovenskem bančnem sistemu. Vam tovrstne izkušnje pomagajo pri opravljanju te zahtevne funkcije direktorice ZBS, kjer morate koordinirati različne interese članic kakor tudi zunanjih deležnikov?

Poleg neposrednih strokovnih izkušenj tudi vse navedene izkušnje, tako poznavanje delovanja državne uprave in oblikovanja ekonomskih politik ter delovanja zakonodajnih procesov, kakor tudi poznavanje delovanja regulatorja in nadzora, tako nacionalnih okvirov, kakor tudi skupnega evropskega (ter razumevanje razmejitev pristojnosti enega in drugega), in ne nazadnje poznavanje okvirov poslovanja bank in hranilnic, zagotovo koristijo pri delu na Združenju. Pomembna za takšno delo, pa je tudi zmožnost sodelovanja, in pa dobri, visoko strokovni sodelavci. Na Združenju je ekipa sicer majhna, ampak odlična. Zelo pomembna pa je za delo Združenja tudi vizija in strategija članic ter njihova podpora, saj je bančni sektor zaradi svoje vloge finančnega posrednika, eden izmed ključnih za delovanje in razvoj gospodarstva. Ključna načela delovanja Združenja so sodelovanje, strokovnost in spoštovanje vseh deležnikov.

Zahtevno varnostno okolje ima pomemben vpliv tudi na delovanje bančnega sektorja. Informacijska tveganja so v tem okviru še posebej izpostavljena. Kakšen pomen tem izzivom posvečate v okviru vašega združenja?

Tako članice, kakor tudi regulatorji ter nadzorniki, in pa seveda posledično tudi Združenje, posveča kibernetskim tveganjem zelo veliko pozornost. Upravljanje kibernetskega tveganja je eno izmed najpomembnejših področij delovanja. Tveganjem smo zaradi razvoja tehnologije vedno bolj izpostavljeni vsi. Pri upravljanju izpostavljenosti kibernetskemu tveganju je res izrazito pomembno tudi sodelovanje različnih institucij, tako Nacionalnega odzivnega centra za kibernetsko varnost (SI-CERT), policije in vseh, ki lahko pripomorejo k večji zaščiti. Zelo pomembno je sodelovanje pri preventivnih aktivnostih in eno izmed področij, ki mu članice in Združenje posvečamo veliko pozornosti, je tudi ozaveščanje javnosti.

Uspešno usposobljen in osveščen posameznik je verjetno garant za visoko stopnjo varnosti pri delovanju bančnega sektorja. Področju izobraževanja v vašem okviru namenjate posebno pozornost. Katera so tista težišča na področju izobraževanja, ki jim polagate posebno pozornost?

Res je, da pri finančnem poslovanju prebivalcev in podjetij največ za varnost svojih podatkov in finančnih sredstev lahko naredimo komitenti sami. Banke in hranilnice uporabljajo varnostne sisteme in mehanizme s katerimi do največje možne mere zaščitijo podatke strank, vendar pa ti mehanizmi in sistemi ne morejo preprečiti izpostavljenosti tveganjem v primerih, ko komitenti sami, nehote ali v nekaterih primerih tudi hote, posredujejo svoje podatke nekomu, ki jih potem lahko v nadaljevanju uporabi za goljufive ali druge nezakonite namene. Vsi razpoložljivi podatki kažejo na to, da do zlorab prihaja v največji meri zaradi ravnanj ljudi, bodisi zaradi nevednosti ali neozaveščenosti (Phishing),





Slovensko združenje za korporativno varnost ima zelo pomembno vlogo pri povezovanju in izmenjavi mnenj, znanj ter izkušenj in poslovnih praks, in zatorej pri delovanju na področju učinkovitega obvladovanja varnostnih tveganj.

bodisi zaradi malomarnosti (neskrbno ravnanje s podatki, kot so gesla, PIN-i itd., bodisi zaradi naivnosti (prevare pri spletnih nakupih ali ljubezenske prevare) ali zaradi želje po hitrih zaslužkih (investicijske prevare) in podobno. Razpoložljivi podatki kažejo, da je na splošno raven digitalne pismenosti relativno nizka, kljub temu, da je delež prebivalstva, ki dnevno uporablja tehnološko napredne aparate in aplikacije, velik. Zato je eno izmed pomembnih težišč izobraževanja tudi področje kibernetske varnosti ter že omenjeno ozaveščanje. Z namenom ozaveščanja so članice preko Združenja in s pomočjo zunanje agencije že v letu 2023 izvedle kampanjo o kibernetski varnosti PAZI.SE, ki je preko anketnih rezultatov in drugih pokazateljev imela dober učinek, vendar pa so rezultati hkrati pokazali, da je potrebno kampanjo ozaveščanja še nadaljevati in jo nadaljujemo tudi v letu 2024. Zelo si želimo, da bi se ji pridružile tudi druge inštitucije in gospodarske družbe, ter, da bi postala takšna kampanja v naslednjih letih skupen, tako rekoč nacionalni projekt, saj je ozaveščenost ljudi ključna pri učinkovitem zniževanju izpostavljenosti kibernetskim tveganjem.

Vaša cenjena publikacija Bančni vestnik je brana tudi izven bančnih krogov. Katere so tiste teme, ki jim v tej publikaciji namenjate največ pozornosti?

Bančni vestnik je edina slovenska strokovna revija s področja bančništva in financ in veseli smo, da se krog bralcev iz leta v leto vztrajno širi tudi izven bančnih krogov, saj so teme, ki jih naslavlja, relevantne v velikem delu tudi za tiste, ki ne delujejo neposredno v bančništvu. V publikaciji namenjamo veliko prostora različnim temam, ki se tičejo celotnega gospodarstva in družbe, vedno več pozornosti pa je namenjeno okolju, družbeni odgovornosti in družbeno odgovornemu upravljanju ter poslovanju, in pa vedno več razvoju tehnologije, digitalizaciji in kibernetski varnosti. V letu 2023 je bila septembra izdana posebna številka , ki je bila namenjena izključno različnim aspektom kibernetske varnosti. Tudi v letu 2024 bo predvidoma izdana posebna številka za to področje in pa tudi za področje umetne inteligence.

V zadnjem času je zaradi ekstremnih vplivov okolja na delovanje naših organizacij vedno bolj izpostavljen tudi proces zagotavljanja neprekinjenega poslovanja bančnega sektorja. Ali tudi temu področju v okviru ZBS namenjate prostor v strokovnih razpravah?

Proces zagotavljanja neprekinjenega poslovanja je dinamičen proces tudi v povezavi z razvojem tehnologije, digitalizacijo, kibernetskim tveganjem in mu v okviru strokovnega dela delovnih teles Združenja in tudi v strokovnih razpravah namenjamo pomemben prostor. V preteklosti je bil med drugim pripravljen, v sodelovanju s članicami, poseben pripomoček oziroma dokument z naslovom »Metodologija načrtovanja neprekinjenega poslovanja in vzpostavitev rezervnih zmogljivosti«.

Veliko vaših članic je vključenih tudi v delovanje Slovenskega združenja za korporativno varnost. Menite, da obstaja možnost za dodatno tesnejše sodelovanje obeh združenj, predvsem na področju učinkovitega obvladovanja varnostnih tveganj?

Slovensko združenje za korporativno varnost ima zelo pomembno vlogo pri povezovanju in izmenjavi mnenj, znanj ter izkušenj in poslovnih praks, in zatorej pri delovanju na področju učinkovitega obvladovanja varnostnih tveganj. Zelo pomembno vlogo ima tudi pri izobraževanju in ozaveščanju. Hiter razvoj tehnologije prinaša izjemne dobrobiti, hkrati pa tudi nova, drugačna tveganja in samo s sodelovanjem vseh deležnikov, ki lahko doprinesejo k širitvi zavedanja in obvladovanja teh tveganj, bo moč le ta učinkovito obvladovati. Možnosti za dodatno tesnejše sodelovanje (na področju izobraževanja, izmenjave strokovnih stališč in dobrih praks, priprave skupnih dogodkov in predstavitev novosti s področja spremljanja regulative, ozaveščanja javnosti,...), obstajajo in jih moramo izkoristiti.



Pred nami je implementacija dveh pomembnih EU direktiv v slovenski pravni red in sicer NIS 2 in CER. Menite, da lahko obe združenji skupaj naslovita pričakovanja in dobre prakse, ki bodo pomagale državnim institucijam pri tej implementaciji?

Januarja 2023 je pričela veljati nova EU direktiva o ukrepih za visoko skupno raven kibernetske varnosti v EU - direktiva NIS 2, s katero želi EU doseči visoko skupno raven kibernetske varnosti ter dodatno izboljšati kibernetsko odpornost in odzivnost v primeru varnostnih incidentov v vseh državah članicah EU. Med drugim določa kritične sektorje, ključne elemente, ki jih morajo deležniki upoštevati pri oblikovanju ukrepov kibernetske varnosti in poročanje o incidentih, kar naj bi vse pripomoglo k večji odpornosti v EU. Komplementarna je direktiva CER (Critical Entities Resilience Directive, december 2022), ki določa obveznosti držav članic EU, da sprejmejo posebne ukrepe za zagotovitev, da se bistvene storitve za vzdrževanje vitalnih družbenih funkcij ali gospodarskih dejavnosti na notranjem trgu zagotavljajo neovirano. Sodelovanje obeh združenj in tudi drugih, zaradi dosedanjih izkušenj in dobrih praks, lahko zelo pozitivno pripomore k implementaciji direktive v slovenski pravni red.

> Izziv zagotavljanja ustreznega kadrovskega potenciala, na področju informacijske varnosti oziroma na vseh področjih informacijske tehnologije je vedno izrazitejši, v tako rekoč vseh sektorjih gospodarstva.

Izzivi s katerimi so soočene organizacije pri zagotavljanju ustreznega kadrovskega potenciala na področju informacijske varnosti so vedno izrazitejše. Menite, da lahko obe združenji pomagata potisniti slovenski izobraževalni sistem k večji dinamiki spreminjanja in prilagajanja realnim potrebam?

Izziv zagotavljanja ustreznega kadrovskega potenciala, na področju informacijske varnosti oziroma na vseh področjih informacijske tehnologije je vedno izrazitejši, v tako rekoč vseh sektorjih gospodarstva. Če želimo v Sloveniji ohraniti konkurenčnost gospodarstva in zmožnost nadaljnje rasti produktivnosti in gospodarske rasti, moramo čim prej sprejeti vse ukrepe, ki bodo omogočili zagotavljanje ustreznega kadra. Eden od nujnih ukrepov je oblikovati izobraževalni sistem, ki bo pravočasno odziven realnim potrebam gospodarstva, poleg tega pa, zaradi naše demografske slike, sprejeti tudi druge dodatne ukrepe (predvsem tudi na področju davkov in prispevkov in ne nazadnje na področju administrativnih postopkov zaposlovanja tudi tujega kadrovskega potenciala), ki bodo zagotovili v nadaljevanju ohranjanje interesa domačega kadrovskega potenciala in tudi privabljanje tujega kadrovskega potenciala za delo v Sloveniji. Vsi moramo pomagati pri teh spremembah, ki so ključne, če želimo ohraniti ali povečati produktivnost in blaginjo. ■

Informacijske storitve in inženiring, d.o.o.

INFORMATIKA



Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

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

Vplivi kibernetskih napadov na različna področja v energetiki:

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

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

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

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

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

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

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

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

ČAS JE ZA ODLOČILEN KORAK

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

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

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

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

www.informatika.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
ga. Irena Španinger, dipl. ekon. spec., direktorica
Javnega medobčinskega stanovanjskega sklada Maribor*

JAVNE ORGANIZACIJE NA LOKALNI RAVNI SE SOOČAJO S SPECIFIČNIMI VARNOSTNIMI IZZIVI

Nenehno dinamično spreminjanje varnostnega okolja ima pomembne vplive tudi na javne organizacije, ki delujejo na lokalnih ravneh naše širše družbene skupnosti. Ravno ta kompleksnost pri zagotavljanju neprekinjenosti delovanja naših organizacij je izpostavila polno mero izzivov pred katerimi stojijo strateški voditelji javnih organizacij. Predvsem se to odraža na lokalnih okoljih, saj se na tej ravni soočamo z izrazitim pomanjkanjem razumevanja potrebnosti obvladovanja varnostnih tveganj, poleg tega pa smo soočeni z velikim pomanjkanjem ustreznih kadrovskih in finančnih virov pri upravljanju z varnostnimi tveganji. O vseh teh odprtih vprašanjih smo se pogovarjali z go. Ireno Španinger.

Bodite tako prijazni in nam na kratko predstavite delovanje Javnega medobčinskega stanovanjskega sklada Maribor.

Stanovanje sodi med osnovne človekove potrebe in pravica do primernega stanovanja je priznana, kot pomembna sestavina pravice do primerne življenjske ravni. Za zadovoljevanje teh pravic in potreb občanov ter za doseganje ciljev na stanovanjskem področju, so občine Duplek, Hoče – Slivnica, Miklavž na Dravskem polju, Rače – Fram, Starše in Mestna občina Maribor ustanovile skupni stanovanjski sklad – Javni medobčinski stanovanjski sklad Maribor (JMSS Maribor). JMSS Maribor, kot naslednik Stanovanjskega sklada občine Maribor, je bil kot neprofitna stanovanjska organizacija osnovan leta 1992, dejansko pa vpisan v sodni register leta 1994, kar pomeni, da kot takšen deluje že 30 let.

Sklad je pravna oseba javnega prava, s pravicami, obveznostmi in odgovornostmi, ki jih določajo Zakon o javnih skladih, Odlok o ustanovitvi javnega medobčinskega stanovanjskega sklada Maribor, statut in drugi predpisi.

S temeljitim upoštevanjem teh vidikov varovanja osebnih podatkov organizacija, ne le izpolnjuje zakonske zahteve, temveč tudi gradi zaupanje uporabnikov in strank. To postavlja organizacijo v boljši položaj za ustvarjanje in vzdrževanje zaupanja ter zagotavljanje varnosti podatkov v digitalnem okolju.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Organa sklada sta nadzorni svet in direktor oziroma direktorica. Notranjo organizacijo sklada narekuje dejavnost sklada ter posebni predpisi, v skladu s katerimi morajo delovati pravne osebe, ki imajo status javnega sklada ter se štejejo za neprofitne stanovanjske organizacije.

JMSS Maribor upravlja in razpolaga z namenskim premoženjem, ki ga sestavljajo stanovanja, stanovanjske hiše in zemljišča, ter drugo premoženje, ki so ga s Pogodbo o prenosu nepremičnin občine ustanoviteljice v letu 2001 prenesle na JMSS Maribor. Sklad razpolaga z 2.100 stanovanji, od tega jih ima dobrih 2.000 v lasti in okvirno 100 v upravljanju od občin ustanoviteljic. Večina stanovanj se nahaja na območju Mestne občine Maribor. Pretežno gre za neprofitna stanovanja, manjši delež pa predstavljajo stanovanja s tržno najemnino, začasne bivalne enote, ter službena in oskrbovana stanovanja.

Za seboj imate bogato zgodovino tudi na področju različnih aktivnosti povezanih z obvladovanjem varnostnih tveganj. Kako vam ta znanja pomagajo pri trenutnem izvajanju te zahtevne funkcije strateške voditeljice?

Tveganja so neločljivo povezana s poslovanjem vsakega podjetja in organizacije. Sistematično in predvsem učinkovito upravljanje tveganj je dejavnost, ki se pri nas šele razvija. Moja poslovna kariera, tako v zasebnem in javnem, kakor tudi v bančnem sektorju, je imela skupno točko, torej varnost. Največ znanj sem pridobila s priložnostjo delati v NKBM, v sektorju za upravljanje fizične in informacijske varnosti, pod vodstvom direktorja gospoda Božidarja Dajčmana, ki je eden vodilnih strokovnjakov s področja upravljanja z varnostnimi tveganji. Njegovo vodenje, pogledi in razumevanje le-teh so mi zagotovo veliko pomagali, dali osnovo, kakor tudi nadgradnjo razumevanju in izvajanju trenutne funkcije. Kot vemo, v bančnem sektorju varnostnih izzivov ne primanjkuje. Tako na področju informacijske, kakor tudi fizične varnosti. Tukaj torej lahko povlečem vzporednico z našim nepremičninskim sektorjem. Tudi naše poslanstvo in cilj je učinkovito zagotavljanje tako varnosti zaposlenih in poslovnih partnerjev, kakor tudi naših najemnikov. Varnost, ki je širok pojem, je eden izmed pomembnejših dejavnikov poslovne uspešnosti podjetja. Vemo, da je pogoj za dober temelj izgradnje varnostne kulture organizacije, zavedanje na nivoju uprave. Tu je moja dodana vrednost, ker lahko kot direktorica med zaposlenimi vzpodbujam, podpiram in gradim zavedanje o pomembnosti varnostne kulture. Zavedam se, da bi ne glede na znanje in voljo, brez dobrega sodelovanja in zaupanja zaposlenih, bila ta naloga še veliko težja.

Glede na to, da je več občin vaših ustanoviteljev je to verjetno zahteven zalogaj v smeri koordinacije aktivnosti. Je to problem tudi pri investicijah na področju zagotavljanja informacijske varnosti?

Lastništvo več občin ustanoviteljic je zagotovo eden večjih izzivov pri poslovanju sklada. Nenazadnje je potrebno za sprejem letnega poslovno finančnega načrta, v katerem se opredelijo in sprejmejo investicije, cilji in strategije poslovanja, med drugim tudi s področja infor-



macijske varnosti, pridobiti potrditev tako Nadzornega sveta JMSS Maribor, večinske lastnice Mestne občine Maribor in še vsaj ene občine ustanoviteljice. To z vidika načrtovanja in uresničevanja ciljev zagotovo pomeni, veliko predhodne koordinacije, usklajevanj in nenazadnje veliko mero sposobnosti, da deležnike prepričaš o pomembnosti projektov, ki jih želimo izvesti. Kar se tiče investicij s področja informacijske varnosti ugotavljamo, da je iz leta v leto opaziti vedno večjo podporo in naklonjenost, tako različnim vlaganjem v posodobitve informacijskih sistemov, kakor tudi zagotavljanju informacijske varnosti.

Pri svojem poslovanju obdelujete pomembne osebne podatke vaših uporabnikov storitev. Kakšno pomembnost v tem okviru posvečate informacijski varnosti v vaši organizaciji?

Varovanje osebnih podatkov je ključnega pomena v informacijski varnosti, še posebej v današnjem digitalnem svetu, kjer je zbiranje, shranjevanje in deljenje podatkov zelo pogosto. Ključni vidiki varovanja osebnih podatkov vključujejo spoštovanje zakonodaje, kot je Zakon o varstvu osebnih podatkov (ZVOP-2), in druge specifične zakonske okvire, kot je Stanovanjski zakon (SZ-1).

Pomembno je zbirati samo tiste podatke, ki so nujno potrebni za delovanje organizacije in so ustrezno zaščiteni z varnostnimi ukrepi. Dostop do podatkov je treba omejiti le na pooblaščene osebe z jasno določenimi pravicami in odgovornostmi. Nadzor nad tem, kdo lahko dostopa do katerega podatka in kdaj, predstavlja ključni element varnostne politike.

Uporaba ustreznih varnostnih ukrepov je ključnega pomena. To vključuje uporabo požarnega zidu, XDR zaščite, operativnega centra kibernetske varnosti v sodelovanju s pogodbenim partnerjem Telekomom, redne varnostne kopije ter sistematične nadgradnje sistemov.

Ob sodelovanju z zunanjimi partnerji ali pogodbeniki je ključno imeti jasno določene varnostne zahteve glede ravnanja z osebnimi podatki. Prenos osebnih podatkov je treba izvajati preko varnih komunikacijskih kanalov in šifriranih protokolov, kar je ključno za zagotavljanje varnosti podatkov med prenosom.

S temeljitim upoštevanjem teh vidikov varovanja osebnih podatkov organizacija, ne le izpolnjuje zakonske zahteve, temveč tudi gradi zaupanje uporabnikov



in strank. To postavlja organizacijo v boljši položaj za ustvarjanje in vzdrževanje zaupanja ter zagotavljanje varnosti podatkov v digitalnem okolju.

Kako motivirate svoje sodelavce, da tudi na področju varnostnega zavedanja naredijo korak naprej. Danes je namreč vsak posameznik lahko vstopna točka za varnost delovanja naših informacijskih sistemov.

Dejstvo, da je organizacija in njen varnostno informacijski sistem tako močan, kot je njen najšibkejši člen, kar pa so največkrat zaposleni, je sicer fraza, ki se veliko uporablja, vendar nenazadnje tudi drži. Pri nas se trudimo, da vodstvo prevzema vodilno vlogo pri spodbujanju varnostnega zavedanja med zaposlenimi. To pomeni aktivno podporo in promocijo varnostnih praks ter jasno izražanje prednosti varnosti podatkov.

Izvajamo redna usposabljanja in delavnice o varnosti podatkov, ki so ključnega pomena, saj omogočajo zaposlenim, da osvežijo svoje znanje, se seznanijo z novimi grožnjami in pridobijo večje razumevanje pravil ravnanja s podatki. Prav tako so simulacije varnostnih incidentov, kot je na primer preizkus phisinga, dragoceno orodje, ki omogoča zaposlenim pridobivanje praktičnih

Še posebej v primerih resnih kršitev, ki ogrožajo varnost ljudi in premoženja, bi bilo smiselno, da javni stanovanjski skladi pridobijo zakonsko pravico do enostranske odpovedi najemne pogodbe s hitrim postopkom izselitve. Sodni postopki za odpoved najemne pogodbe in izselitev so namreč običajno dolgotrajni postopki.



izkušenj. S tem se dviguje njihova pripravljenost in ozaveščenost o varnostnih tveganjih ter pomembnosti ustrezne zaščite podatkov.

Motiviranje zaposlenih za izboljšanje varnostnega zavedanja, ni le enkraten proces, temveč kontinuiran proces, ki zahteva veliko energije in napora, ne samo vodstva, temveč tudi vseh zaposlenih. Spodbujanje s strani vodstva je le delček v mozaiku do ustvarjanja kulture, ki ceni in spoštuje varnost delovnega procesa. Ustvarjanje pozitivnega delovnega okolja pa je osnova za zadovoljstvo zaposlenih, saj je poznano dejstvo, da nezadovoljni zaposleni lahko postanejo tudi velik varnostni problem.

V zadnjem obdobju se zelo aktivno trudite tudi na področju gradnje novih stanovanj in ne samo upravljanje obstoječih. Ali v fazi projektnega načrtovanja novih stanovanjskih objektov vključujete tudi segmente varnosti, ki bodo že v osnovi zagotavljali določene varnostne standarde?

Kot sem že povedala, je varnost zelo obsežen koncept. Danes se veliko govori in piše o pametnih mestih, pametnih objektih itd. S temi izrazi opisujemo območje, ki je v prostor in upravljanje vpeljalo širok spekter tehnoloških rešitev. Trenutno smo v fazi projektiranja objekta za mlade in mlade družine. Z arhitekti smo se dogovorili, da bomo vključili čim več tehnoloških rešitev, tako v objekt, kot tudi v urejanje okolice, ki bodo našim najemnikom in širši skupnosti zagotovila večjo varnost bivanja. Še posebej bi izpostavila videonadzor objekta in njegove okolice, požarno zaščito (uporaba materialov za gradnjo, ki imajo večjo požarno odpornost, oziroma niso gorljivi), različne protivlomne sisteme, upravljanje sistemov osvetlitve glede na prisotnost stanovalcev v objektu in še bi lahko naštevala. Vendar se kot investitorji zavedamo, da smo glede različnih predlaganih varnostnih rešitev zavezani, tako obstoječi zakonodaji kot tudi razpoložljivim finančnim sredstvom. Naša želja je, da bi v prihodnosti država in vse obstoječe institucije, ki vplivajo na ta razvoj, dejansko spodbujale tehnološki napredek na tem področju ter primerno sofinancirale takšne projekte.

Bi s strani državnih institucij pričakovali več strokovne pomoči na segmentih, ki so povezani z varnostjo upravljanja stanovanjskih nepremičnin?

Varnost in pravilno upravljanje stanovanjskih nepremičnin sta ključna faktorja za dobrobit stanovalcev in celotne skupnosti. Na JMSS Maribor se pri oddaji stanovanj srečujemo z vrsto izzivov, ki imajo neposreden ali posreden vpliv na varnost v naših najemnih enotah. Predvsem se ti izzivi nanašajo na spoštovanje hišnega reda, primernega ravnanja z najemnimi stanovanji ter urejenost večstanovanjskih stavb in njihove okolice.

Ob kršitvah najemnih pogodb s strani najemnikov ali uporabnikov imamo, kot lastniki stanovanj le možnost sodne odpovedi najemne pogodbe, kar je običajno dolgotrajen in kompleksen postopek. To pogosto vodi v neučinkovito reševanje problematičnih situacij.

Še posebej v primerih resnih kršitev, ki ogrožajo varnost ljudi in premoženja, bi bilo smiselno, da javni stanovanjski skladi pridobijo zakonsko pravico do enostranske odpovedi najemne pogodbe s hitrim postopkom izselitve. Sodni postopki za odpoved najemne pogodbe in izselitev so namreč običajno dolgotrajni postopki.

Z namenom zagotavljanja varnosti in zaščite pravic ter ustvarjanja varnega in prijetnega bivalnega okolja za vse stanovalce je treba preučiti možnosti posodobitve zakonodaje in postopkov, ki bi omogočili hitrejše in učinkovitejše ukrepanje v primerih resnih kršitev, ki ogrožajo varnost ljudi in premoženja v najemnih stanovanjih. S tem bi se povečala učinkovitost ukrepov in izboljšala varnost ter kakovost bivanja v stanovanjskih soseskah.

Ste dolgoletni člani Slovenskega združenja za korporativno varnost. Kaj vam v strokovnem pogledu prinaša članstvo v tej pomembni asociaciji?

Združenje je za naše podjetje pomembno, kot stična točka, kjer se srečujemo posamezniki, ki si želimo izmenjevati znanje in izkušnje. Ker je sklad del javnega sektorja, je združenje za nas toliko pomembnejše, saj se skozi njega prepleta, tako javni kot zasebni sektor, in nam s tem omogoča prepotrebno ohranjanje vezi z gospodarstvom. ■

Foto: arhiv JMSSM

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 14. MAJ 2024

15. 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!

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Janez Lencl, pomočnik direktorja za korporativno varnost in komuniciranje, UKC Maribor*

NEPREKINJENOST DELOVANJA V ZDRAVSTVENEM SEKTORJU POMEMBEN IMPERATIV

Univerzitetni klinični center v Mariboru predstavlja drugo največjo zdravstveno organizacijo v Republiki Sloveniji. Ob različnih tveganjih, ki se pojavljajo v zdravstvenem sektorju, je učinkovito obvladovanje varnostnih tveganj izredno pomemben proces za zagotavljanje nemotenosti delovanja te pomembne institucije. O izzivih in priložnostih smo se pogovarjali z g. Janezom Lenclom.

UKC Maribor predstavlja pomembno zdravstveno institucijo v Republiki Sloveniji. Nam lahko prosim pojasnite umeščenost in vlogo Službe za korporativno varnost v UKC Maribor? Kateri so tisti glavni dosežki, ki bi jih bilo potrebno izpostaviti?

UKC Maribor je javni zdravstveni zavod, ki opravlja specialistično dejavnost na sekundarni in terciarni ravni za prebivalce Maribora, okolice, severovzhodne Slovenije, kot tudi celotne Slovenije in tujine. Obenem je UKC Maribor učni zavod za vse poklice zdravstvenih in ne zdravstvenih delavcev, dodiplomskih in podiplomskih študentov. V UKC Maribor je zaposleno nekaj več kot 3700 oseb.

Služba za korporativno varnost je nova služba v okviru UKC Maribor, ki se organizacijsko in kadrovsko šele vzpostavlja. Prvič je v Statutu zavoda iz leta 2023 omenjeno področje varnosti in je navedeno, da varnostna služba spada neposredno pod pristojnost generalnega direktorja. Prav tako je omenjeno področje obrambe in civilne zaščite. To, da je dozorelo spoznanje, da tudi UKC Maribor potrebuje takšno službo je dosežek, ko zdravstvo pestijo druge težave, pomanjkanje kadra, zastarela oprema in zgradbe. Prav tako si kot dosežek štejem, da smo našli ter opremili prostore za upravno območje, ter pričeli urejati dokumente na tem področju.

Strokovna znanja s področja korporativne varnosti so specifična in plačni sistem javnih uslužbencev ni stimulativen za zaposlovanje na tem področju, še posebej ne na segmentu informacijske varnosti.

Ali bi lahko na tej točki potegnili nekatere splošne zaključke glede učinkovitosti spopadanja zdravstva z epidemijo, predvsem pa, kaj smo se iz tega naučili za ravnanje v podobnih izrednih razmerah?

Prav epidemija je pokazala, da mora tudi zdravstvo imeti vzpostavljene in organizirane službe oziroma osebe, ki pokrivajo področje Civilne zaščite, v skladu z zakonodajo, ki predvideva kako deluje država v izrednih razmerah. S tem mislim na štabe civilne zašite, na dobave iz blagovnih rezerv (maske, respiratorji, kontejnerji, šotori, postelje, idr.), pomoč vojske in njihovih kapacitet (bolnica ROLE...), kontaktne osebe in pa izdelane načrte delovanja v izrednih razmerah. Vodstva zavodov so ob tej situaciji spoznala pomen in vrednost tega segmenta.

Kriza korona virusa je družbo zdramila, da so nevarnosti pandemij več kot realno tveganje. Kakšni so glavni varnostno-organizacijski pristopi s katerimi kontinuirano zagotavljate

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

ustrezen nivo varnosti pred vnosom okužb v vašo zdravstveno institucijo?

V tem primeru gre za tesno sodelovanje več služb znotraj UKC Maribor. Konkretno z Enoto za obvladovanje bolnišničnih okužb, ki določi strokovne kriterije in potem izvedba vstopnih točk (info točke) ter omejitev gibanja. Običajno je potrebno izvesti tudi določene predelave prostorov, vrat, filtrov, itd. V ta namen imamo izdelan načrt, katerega skrbnik je pomočnik direktorja za korporativno varnost in komuniciranje.

Korporativna varnost že dolgo časa ni omejena samo na zagotavljanje fizičnega in tehničnega varovanja, temveč vedno bolj tudi na področje informacijske varnosti. Kakšne organizacijske in procesne spremembe se dogajajo na tem področju?

Kot informacijska družba, ki prehaja v digitalno, odpira vprašanja informacijske varnosti kot temeljne varnosti delovanja države oziroma družbe kot celote. V tem smislu je sprejet zakon o informacijski varnosti, ki nalaga obveznosti. Tako je sam proces informacijske varnosti prepoznan kot področje, ki ne zadeva zgolj informatike, ampak se obravnava širše v sklopu korporativne varnosti. Sprejeti je potrebno veliko ukrepov za zagotavljanje informacijske varnosti, ki niso vezani izključno na informatike in anti-virusne programe, požarne zidove, varnostne kopije, neprekinjeno napajanje, itd.

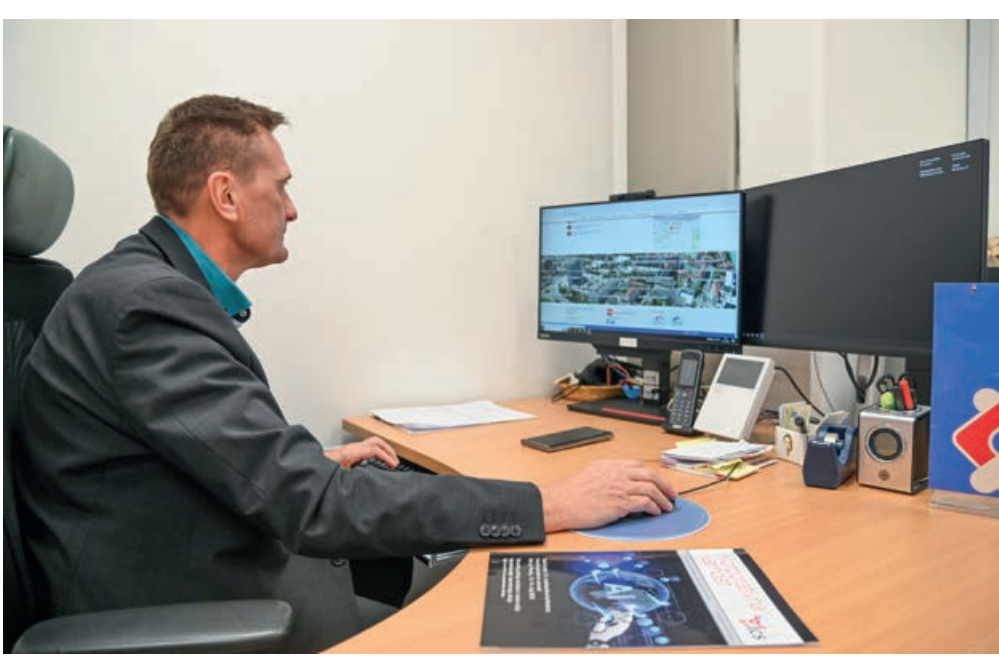
UKC-Maribor je ena izmed ključnih organizacij tudi na področju zagotavljanja neprekinjenega delovanja kritične infrastrukture in izvajanja bistvenih storitev. Ima v teh procesih Služba korporativne varnosti v UKC-Maribor pomembno mesto? Kje je to najbolj izraženo?

Zakon o kritični infrastrukturi nalaga, da mora UKC Maribor izvajati in skrbeti za neprekinjeno zdravstveno oskrbo ljudi. Zaradi tega izdelujemo letno oceno tveganja. V tem smislu je koordinator aktivnosti znotraj zavoda Službe za korporativno varnost. Vendar je na tem segmentu težko dobiti strokovne kadre, ki poznajo problematiko in se permanentno s tem ukvarjajo.

Glede na dejstvo, da je UKC-Maribor pomemben segment v zdravstvenem sektorju, ima verjetno pomembno mesto tudi pri usklajevanju z ostalimi deležniki. Nam lahko osvetlite kvaliteto in obseg sodelovanja z Ministrstvom za obrambo, Ministrstvom za



Služba za korporativno varnost je nova služba v okviru UKC Maribor, ki se organizacijsko in kadrovsko šele vzpostavlja. Prvič je v Statutu zavoda iz leta 2023 omenjeno področje varnosti in je navedeno, da varnostna služba spada neposredno pod pristojnost generalnega direktorja. Prav tako je omenjeno področje obrambe in civilne zaščite. To, da je dozorelo spoznanje, da tudi UKC Maribor potrebuje takšno službo je dosežek, ko zdravstvo pestijo druge težave, pomanjkanje kadra, zastarela oprema in zgradbe. Prav tako si kot dosežek štejem, da smo našli ter opremili prostore za upravno območje, ter pričeli urejati dokumente na tem področju.





zdravje, NIJZ in ostalimi bolnicami na področju zagotavljanja neprekinjenosti delovanja tega sistema?

Po zakonu o kritični infrastrukturi je za sektor zdravstva zadolženo ministrstvo za zdravje, ki daje usmeritve za zdravstvo. Obrambno ministrstvo nudi strokovno pomoč in izobraževanja, kakor tudi tehnično pomoč. Zelo aktiven je Urad vlade za informacijsko varnost, ki deluje zelo proaktivno na tem področju z informiranjem, izobraževanjem in pilotskimi projekti, ki jih organizira EU. Na dnevni bazi pa zaradi zdravstvene oskrbe prebivalstva sodelujemo bolnišnice na sekundarni in terciarni ravni. Veliko vlogo pri tem ima v zdravstvu dispečerski center, preko katerega se izvaja koordinacija in pretok informacij skupaj z Ekipami nujne medicinske pomoči.

Ste med samo krizo povezano z obdobjem korona epidemije zaznavali kakšne pomembne anomalije in zunanje grožnje za neprekinjeno delovanje vaših organizacijskih in informacijskih sistemov?

V času krize takšnih zunanjih groženj nismo zaznali.

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 UKC-Maribor ustrezno podporo?

Vsesplošno pomankanje kadra v zdravstvu, od zdravnikov do medicinskih sester, se širi tudi na upravno tehnične službe. Vodstva se pretežno ukvarjajo s kadrovsko problematiko zdravnikov in medicinskega osebja. Žal upravno tehnične službe niso deležne takšne pozornosti. Strokovna znanja s področja korporativne varnosti so specifična in plačni sistem javnih uslužbencev ni stimulativen za zaposlovanje na tem področju, še posebej ne na segmentu informacijske varnosti.

Kakšno stališče imate v UKC-Maribor vezano na sodelovanje v različnih evropskih projektih s področja obvladovanja tveganj in zagotavljanja neprekinjenosti delovanja? Menite, da lahko skozi take projekte pridete do nujno potrebnih novih znanj, ki bodo pripravljenost v vaši organizaciji postavila na višji nivo?

Vsekakor podpiramo evropske projekte in smo v njih že sodelovali, še posebej na področju informacijske varnosti. Smo del NATA in EU in kolektivna varnost je skupna odgovornost. Samo skupaj lahko zagotavljamo varno okolje. Informacijski sistem ne pozna državnih meja, niti mej med samimi organizacijami. Zato je na tem področju nujno sodelovanje.

Večina upravljalcev pomembne infrastrukture je združenih 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?

Kot uspeh in veliko zadovoljstvo si štejem, da sem uspel vodstvo UKC Maribor prepričati, da smo postali polnopravni člani Slovenskega združenja za korporativno varnost. To članstvo nam omogoča strokovno rast in zagotavlja biti v stiku z kompetentnimi ljudmi in organizacijami v Sloveniji, kot tudi v širšem mednarodnem okolju. ■

Foto: arhiv UKC Maribor

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



VARNOST, BREZ KOMPROMISOV

HUAWEI

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Alen Jamšek, direktor informacijske varnosti in skladnosti iz skupine Actual I.T.

BENCINSKI SERVISI V DIGITALNI DOBI: KLJUČ DO CELOVITE ZAŠČITE PRED NAPREDNIMI KIBERNETSKIMI NAPADI

V preteklih desetletjih so bencinski servisi prevladujoče veljali za preprosta mesta, namenjena zgolj oskrbi vozil z gorivom. Danes smo priča prelomnici, ko ti servisi postajajo pravo digitalno središče, prepleteno s kompleksnimi mrežami in najnovejšo tehnologijo. V tej dinamični transformaciji ima skupina Actual I.T. ključno vlogo, saj aktivno prenavlja IT okolje bencinskih servisov MOL v Sloveniji in jim s tem postavlja nove standarde za prihodnost maloprodaje. Napredna digitalizacija hkrati prinaša številne izzive, ki odpirajo novo poglavje na področju varnosti bencinskih servisov. Skupaj s strokovnjakom za kibernetsko varnost, Alenom Jamškom iz skupine Actual I.T., smo se pogovarjali, kako se prepletanje fizične in digitalne varnosti izkaže za ključno pri ohranjanju integritete poslovanja.

Bencinski servisi postajajo vse bolj povezani in digitalizirani, kar postavlja informacijsko varnost v središče, saj je ključnega pomena za ohranjanje nemotenega delovanja in zaščito tako digitalnih kot fizičnih vidikov poslovanja. Kako ta povezava med digitalizacijo in varnostjo vpliva na sodobne bencinske servise in kako vzpostavljate povezavo med fizično in digitalno varnostjo, ter zakaj je ta integracija ključna za celovito zaščito?

Transparentno obveščanje v primeru kibernetskih napadov je ključno za vzdrževanje zaupanja in omejitev negativnih vplivov na ugled podjetja.

Integracija med fizično in digitalno varnostjo je ključna za celovito zaščito, saj napadalci lahko izkoristijo različne poti in vrzeli za napad. Če na primer fizična varnost ni ustrezna, lahko napadalec neposredno dostopa do strojev ali naprav na bencinskem servisu, po drugi strani pa lahko pomanjkljiva digitalna varnost omogoči kibernetskim napadalcem, da prodrejo v omrežje in povzročijo škodo ali krajo podatkov. Zato je nujno vzpostaviti celovit pristop k varnosti, ki združuje tako fizične kot digitalne vidike ter uporablja napredne tehnologije in postopke za ohranjanje celovitosti, zaupnosti in razpoložljivosti informacij ter sistemov.

Kako bencinski servisi sistematično analizirajo specifične grožnje, vključno s kibernetskimi napadi, krajo podatkov in vandalizmom ter kakšen je sistemski pristop k varnosti, z izpostavljenimi elementi, kot so požarni zidovi, antivirusna zaščita in šifriranje podatkov,

*avtor je član Slovenskega združenja korporativne varnosti

in kako omogočajo celovito varnost in učinkovito zaščito pred temi grožnjami?

Ključni elementi tega pristopa vključujejo oceno tveganja, da se identificira potencialne grožnje in ranljivosti v svojem poslovnem okolju, identifikacijo ključnih sredstev in podatkov, ki jih je treba zaščititi in postavljanje varnostnih politik ter postopkov, ki določajo, kako se bo obravnavalo tveganja in kako se bodo izvajali ukrepi zaščite. Z implementacijo tehnoloških rešitev zaščitijo svoje sisteme, ti pa potrebujejo stalen nadzor, sistematično spremljanje in redno testiranje ter posodabljanje, ki vključuje simulacijo kibernetskih napadov, da se preizkusi učinkovitost varnostnih ukrepov. In nenazadnje redno izobraževanje zaposlenih o varnosti. Sistematičen pristop, ki združuje tehnične, organizacijske in človeške vidike varnosti, omogoča bencinskim servisom boljšo zaščito pred različnimi grožnjami. Požarni zidovi, antivirusna zaščita in šifriranje podatkov so le nekateri od ključnih elementov tega celostnega pristopa k varnosti, ki omogoča učinkovito zaščito pred različnimi grožnjami, tako digitalnimi kot fizičnimi.

S kibernetskimi napadi, kot je nedavni primer skupine Predatory Sparrow na iranske bencinske servise, postaja jasno, da so globalni izzivi na področju kibernetske varnosti resni. Kako bi opisali trenutni globalni položaj in izzive bencinskih servisov glede kibernetske varnosti, ter kako se ta globalna slika preliva v lokalni kontekst, zlasti pri MOL Slovenija?

Napadi postajajo vedno bolj sofisticirani in ciljani, grožnje pa segajo od klasičnih kibernetskih napadov, kot so ransomware in distribuirani napadi z odrekajočo storitvijo (DDoS), do bolj kompleksnih vohunskih operacij in napadov na industrijske nadzorne sisteme (Industrial Control Systems, ICS). Vzroki za takšne napade so lahko raznoliki, vključno z željo po finančni dobičkonosnosti, geopolitičnimi motivacijami, krajo občutljivih podatkov in celo terorističnimi motivi. Manjši operaterji bencinskih servisov morda težje vzdržujejo enako stopnjo kibernetske zaščite kot globalni velikani, saj nimajo enakih sredstev za investicije v visokotehnološke varnostne rešitve. Vendar je ključno poudariti, da sodelovanje z lokalnimi organi za kibernetsko varnost in deljenje informacij o potencialnih grožnjah lahko izboljšata sposobnost prepoznavanja in učinkovite obravnave napadov, kar je še posebej relevantno v lokalnem okolju, kjer so specifične značilnosti poslovanja pomembne. Celovit pristop h kibernetski varnosti, ki vključuje, tako tehnične ukrepe kot tudi izobraževanje zaposlenih, ter sodelovanje z lokalnimi organi, je ključen za obrambo pred vedno naprednejšimi kibernetskimi grožnjami.

Lokalno se lahko soočamo s specifičnimi izzivi na področju kibernetske varnosti, ki morda niso tako izpostavljeni v mednarodni javnosti. Ali opažate kakšne posebnosti ali trende na tem področju, ki so lokalno bolj izraziti, vendar ključni za razumevanje stanja?

Lokalni izzivi na področju kibernetske varnosti se kažejo v pomanjkanju sodelovanja med sektorji, kar ovira učinkovito deljenje informacij o grožnjah. Hkrati opažamo pomanjkanje ozaveščenosti o nevarnostih kibernetskih napadov, kar povečuje ranljivost lokalnih skupnosti. Različne regulativne zahteve predstavljajo dodaten izziv, saj podjetja težko sledijo lokalnim zakonodajam. Za obvladovanje teh izzivov je nujno medsektorsko sodelovanje, povečano ozaveščanje in stalno prilagajanje varnostnih praks lokalnim zahtevam. Razumevanje teh lokalnih specifičnosti je bistveno za razvoj učinkovitih strategij kibernetske varnosti. Lokalne organizacije in vlade pa morajo sodelovati pri spodbujanju ozaveščenosti, izmenjavi informacij in zagotavljanju potrebnih virov za izgradnjo in vzdrževanje robustnih varnostnih okvirov.



Nedavni napadi na bencinske servise po svetu, ki so povzročili zastoje na črpalkah, kažejo na naraščajoče kibernetske grožnje. Kako se bencinski servisi po svetu spopadajo z izzivi, ki izhajajo iz teh napadov, in kateri so najpogostejši načini napadov?

Spopadanje z izzivi kibernetskih napadov vključuje povečanje ozaveščenosti in izobraževanje zaposlenih, implemen-

Kibernetski napadi imajo lahko resne posledice na neprekinjeno poslovanje sistemov bencinskih servisov. Napadi na te sisteme prizadenejo različne vidike delovanja, vključno s plačilnimi sistemi, industrijskimi nadzornimi sistemi, komunikacijskimi omrežji in drugimi ključnimi infrastrukturnimi elementi.



tacijo varnostnih tehnologij, vzpostavitev jasnih varnostnih politik in postopkov ter redno posodabljanje programske in strojne opreme. Nadvse pomembno je izvajanje varnostnih pregledov, ki identificirajo ranljivosti in izboljšujejo celotno varnostno postavitev bencinskega servisa. Najpogostejši načini kibernetskih napadov na bencinske servise vključujejo ransomware napade, distribuirane napade DDoS, napade na plačilne sisteme, napade na nadzorne sisteme, socialni inženiring ter napade na komunikacijska omrežja.

Motivi za kibernetske napade se razlikujejo, od državnih do kriminalnih. Kako različni motivi in cilji vplivajo na to, da so bencinski servisi tarča napadov, in kakšna je razlika med napadi prek interneta in fizičnimi napadi na infrastrukturo?

Različni motivi in cilji kibernetskih napadov vplivajo na to, zakaj so bencinski servisi tarča napadov. Državni akterji lahko izvajajo vohunjenje ali sabotažo, medtem ko kriminalne združbe motivira zaslužek ali finančna goljufija. Na tej točki bi omenil še ideološke motive, ki vključujejo aktivizem. Glede na način napada se razlikujejo med spletnimi vdori in napadi prek interneta, ki vplivajo na digitalno infrastrukturo ter fizičnimi napadi na infrastrukturo, ki neposredno vplivajo na operativne procese bencinskih servisov. Kombinacija obeh predstavlja „kibernetsko-fizično grožnjo“, za katero je ključen celovit pristop k varnosti, ki vključuje tako kibernetske kot tudi fizične ukrepe zaščite. Razlika med napadi prek interneta in fizičnimi napadi na infrastrukturo se nanaša na način, kako napadalci dosežejo svoje cilje, pri čemer so lahko posledice obeh vrst napadov pomembne za delovanje bencinskih servisov.

Kako kibernetski napadi vplivajo na neprekinjeno poslovanje sistemov bencinskih servisov? Ali obstajajo konkretni primeri, kjer so napadi povzročili prekinitve storitev ali operativne težave, ki so jih bencinski servisi morali reševati?

Kibernetski napadi imajo lahko resne posledice na neprekinjeno poslovanje sistemov bencinskih servisov. Napadi na te sisteme prizadenejo različne vidike delovanja, vključno s plačilnimi sistemi, industrijskimi nadzornimi sistemi, komunikacijskimi omrežji in drugimi ključnimi infrastrukturnimi elementi. apad na Colonial Pipeline v ZDA, leta 2021 je privedel do zaustavitve cevovoda, povzročil pomanjkanje goriva in resno vplival na promet ter logistiko. Podobni primeri v Mehiki, Rusiji, Libiji in na Norveškem so prav tako pokazali, kako napadi lahko povzročijo prekinitve storitev, težave s plačilnimi sistemi, spremljanjem zaloge goriva in druge operativne težave na bencinskih servisih. Zaradi visoke odvisnosti od informacijskih tehnologij so bencinski servisi postali privlačna tarča za kibernetske napadalce, ki lahko izkoristijo ranljivosti v digitalnih sistemih, da povzročijo škodo tako na operativni kot gospodarski ravni.

Sistematične nadgradnje programske opreme potekajo prek interneta, kar prinaša določena varnostna tveganja. Kako se bencinski servisi spopadajo s temi tveganji, povezanimi z uporabo interneta za prenos posodobitev programske opreme?

Bencinski servisi se soočajo s varnostnimi tveganji pri prenosu posodobitev programske opreme prek interneta. Ključni pristopi za obvladovanje teh tveganj vključujejo uporabo varnostnih protokolov, kot je šifriranje podatkov, uvedbo varnostnih politik za posodobitve s poudarkom na avtentikaciji in digitalnih podpisih, omejitev dostopa do sistemov, redno vzdrževanje varnostnih ukrepov, nadzor omrežja, zaščito pred zlorabami, testiranje varnosti pred implementacijo posodobitev ter izvajanje usposabljanj zaposlenih o varnostnih praksah in tveganjih. S kombinacijo teh pristopov bencinski servisi zmanjšujejo tveganje za kibernetske grožnje, povezane s prenosi posodobitev programske opreme prek interneta, in zagotavljajo vzdrževane, varne sisteme.

Kako podjetja v tej industriji obravnavajo kibernetske napade, in kakšne konkretne ukrepe izvajajo za obnovitev sistemov ter zagotovitev neprekinjenega poslovanja?

Za dobro obravnavo je učinkovit odziv na kibernetske napade s celovitimi strategijami kibernetske varnosti. To vključuje uporabo omrežnih varnostnih rešitev, sistematično posodabljanje ter izvajanje varnostnih politik in postopkov. Pomemben del je tudi usposabljanje zaposlenih, izvajanje rednih varnostnih pregledov ter nadzor dostopa, vključno z identifikacijo in avtentikacijo. Načrti za obvladovanje incidentov in obnovo (IRM) so ključni za učinkovito obvladovanje posledic kibernetskih napadov, ki zajema tudi vzpostavitev varnostnih ukrepov za industrijske nadzorne sisteme in zračno ločevanje omrežij. Sistematična izvedba teh ukrepov je bistvena za

zmanjšanje tveganj in zagotavljanje neprekinjenega poslovanja bencinskih servisov v primeru kibernetskih napadov.

Transparentno obveščanje strank in poslovnih partnerjev v primeru kibernetskih napadov je ključno v krizni situaciji. Kako to vpliva na podjetja, glede na izjave podjetij v primeru napadov, in kako podjetja obvladujejo posledice ter ohranjajo zaupnost informacij?

Transparentno obveščanje v primeru kibernetskih napadov je ključno za vzdrževanje zaupanja in omejitev negativnih vplivov na ugled podjetja. Pomembni vidiki vključujejo hitro obveščanje, jasna sporočila brez tehničnega žargona, previdno upravljanje z informacijami, potrditev poteka preiskave, odgovornost, pomoč prizadetim strankam, sodelovanje z organi in načrte za obnovo ter zaščito pred dezinformacijo. Kljub temu morajo podjetja najti ravnotežje med transparentnostjo in ohranjanjem varnosti, zlasti pri občutljivih informacijah. Vzpostavitev učinkovitega načrta odziva na incidente, ki vključuje tudi komunikacijsko strategijo, je poglavitna za obvladovanje posledic kibernetskih napadov. Zgodnje in odgovorno obveščanje lahko pomaga zmanjšati škodo in ohraniti zaupanje deležnikov.

Vse bolj pogosti kibernetski napadi odpirajo vprašanja o pripravljenosti na podobne grožnje. Ali menite, da smo v Sloveniji dovolj pripravljeni na morebitne podobne kibernetske varnostne izzive, ki bi lahko prizadeli našo kritično infrastrukturo ter kako se lahko na potencialen napad dobro pripravimo?

Pripravljenost na kibernetske napade je dinamičen proces, ki zahteva nenehno izboljševanje in prilagajanje, pri čemer je potrebno sodelovanje, izobraževanje ter skupna odgovornost na državni ravni. V slovenskem kontekstu je pripravljenost na kibernetske varnostne izzive izjemno pomembna, saj so kritične infrastrukture vedno bolj povezane in digitalizirane. Kljub temu je težko dati natančno oceno pripravljenosti, saj je odvisna od mnogih dejavnikov, vključno z nenehnim spreminjanjem groženj, varnostnimi ukrepi posameznih organizacij in sodelovanjem med sektorji.

Izkušnje drugih držav z napadi nudijo priložnost za izboljšanje naših kibernetskih obrambnih strategij. Kako se lahko iz teh izkušenj učimo in izboljšamo svoje strategije za preprečevanje motenj v delovanju ključnih infrastrukturnih sistemov?

Iz izkušenj preteklih kibernetskih napadov na kritično infrastrukturo v tujini se lahko učimo prepoznavanja in obvladovanja podobnih groženj v lastnem okolju. Sodelovanje s tujimi agencijami za kibernetsko varnost ter študije primerov, omogočajo izboljšanje načrtov obvladovanja incidentov, povečujejo zavedanje in krepijo strategije za preprečevanje motenj v delovanju temeljnih infrastrukturnih sistemov. Hkrati pa je odločilnega pomena tudi stalno izobraževanje strokovnjakov, saj se kibernetske grožnje nenehno razvijajo, kar zahteva posodobitve znanja in spretnosti v varnostnem sektorju. Pomembno je, da se zavedamo, da so v vsaki državi in infrastrukturi specifične grožnje, zato je treba pridobljene informacije vzeti kot dragocene lekcije in jih prilagoditi lokalnim razmeram. Nenehna prilagajanja strategij in sodelovanje na mednarodni ravni bosta nepogrešljiva za izgradnjo odpornosti proti vedno bolj kompleksnim kibernetskim grožnjam.

Zaščita pred kibernetskimi grožnjami je dinamičen proces, ki zahteva nenehno pozornost in prilagajanje na nove izzive. Industrija bencinskih servisov se mora zavezati k stalnemu izboljševanju svojih pristopov h kibernetski varnosti, da bi zagotovila neprekinjeno poslovanje in zaščito pred vedno bolj naprednimi grožnjami.

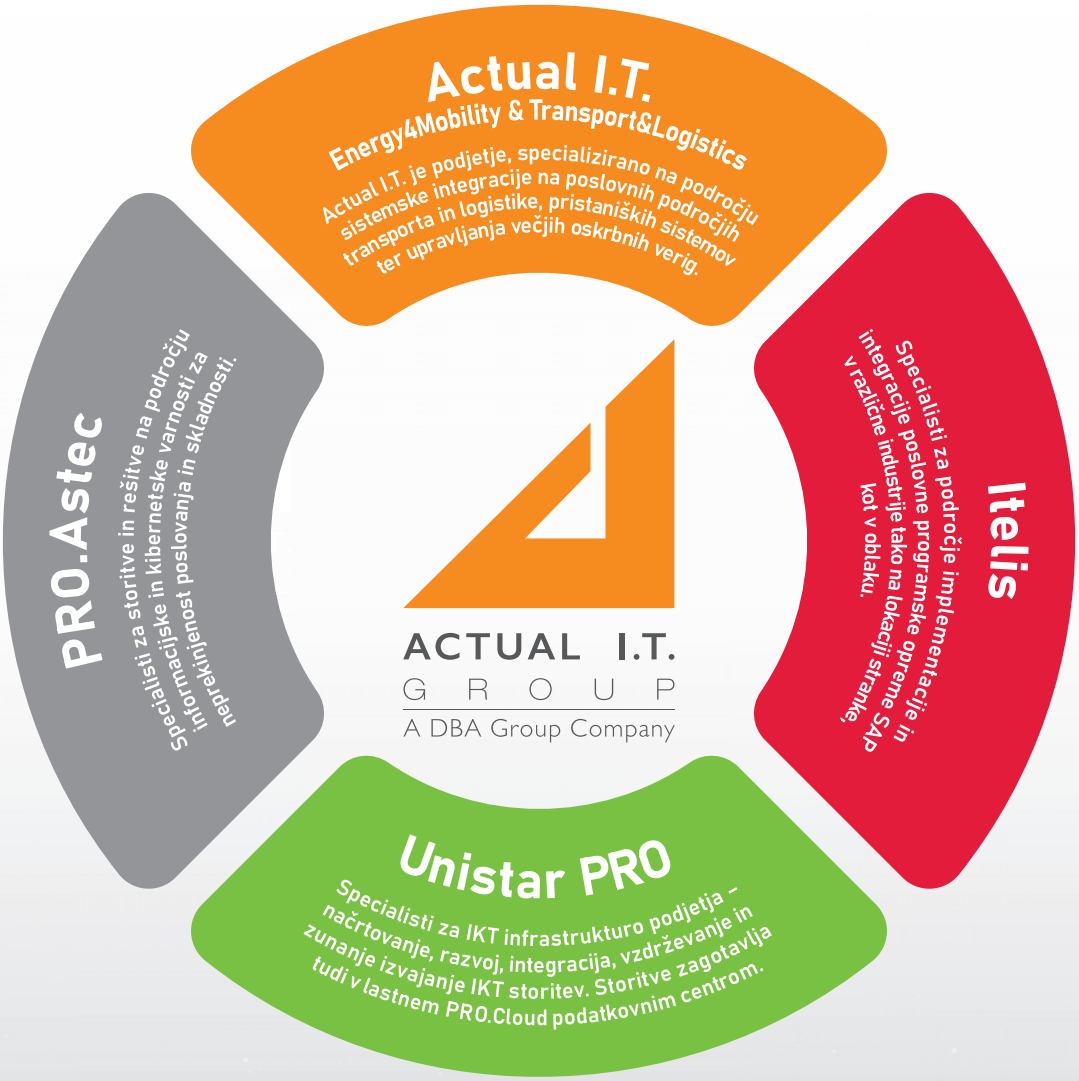
Nove informacijske tehnologije, kot so IoT, napredne analitike in umetna inteligenca tudi vplivajo na kibernetsko varnost bencinskih servisov. Kateri od teh tehnoloških trendov so trenutno ključni za izboljšanje varnosti?

Pomembno je razumevanje, da nobena tehnologija ni absolutno varna, zato je potrebno za kibernetsko odpornost kombinirati več pristopov in tehnologij za celovito kibernetsko varnost. Uporaba Interneta stvari (IoT) omogoča natančen nadzor nad fizičnimi elementi, kar predstavlja pomemben korak k hitremu odkrivanju in odzivanju na morebitne incidente. Poleg tega so napredne analitike in umetna inteligenca ključne za analizo podatkov, prepoznavanje vzorcev ter proaktivno preprečevanje kibernetskih napadov. Napredna blockchain tehnologija v kontekstu bencinskih servisov prispeva k integriteti podatkov in zagotavljanju varnosti transakcij. Razvoj posebnih varnostnih rešitev za industrijske nadzorne sisteme (ICS) odraža prizadevanja za zaščito operativne tehnologije pred kibernetskimi tveganji. Vzporedno se uveljavlja quantum-safe kriptografija, kot odgovor na prihajajočo dobo kvantnih napadov.

Industrija bencinskih servisov se mora iz vsakega kibernetskega incidenta nekaj naučiti. Kateri bi lahko bili naslednji koraki za izboljšanje kibernetske varnosti, zagotovitev neprekinjenega poslovanja ter učinkovite zaščite pred kibernetskimi grožnjami?

V ospredju je zagotovo sistematična ocena tveganj, ki ji sledi implementacija priznanih varnostnih standardov. Pomembni koraki vključujejo redno usposabljanje zaposlenih, uvajanje naprednih tehnoloških rešitev ter namenjanje posebne pozornosti k varnosti industrijskih nadzornih sistemov. Ključnega pomena je tudi integracija naprednih analitičnih orodij in umetne inteligence, redno testiranje varnostnih postopkov ter razvoj načrtov za obvladovanje incidentov. Aktivno sodelovanje s strokovnjaki v panogi in regulatorji predstavlja poglavitno vlogo, medtem ko širjenje ozaveščenosti med javnostjo omogoča ustvarjanje trdnega varnostnega okolja. Zaščita pred kibernetskimi grožnjami je dinamičen proces, ki zahteva nenehno pozornost in prilagajanje na nove izzive. Industrija bencinskih servisov se mora zavezati k stalnemu izboljševanju svojih pristopov h kibernetski varnosti, da bi zagotovila neprekinjeno poslovanje in zaščito pred vedno bolj naprednimi grožnjami. ■

Foto: arhiv Actual I.T.



ACTUAL I.T. astec ITELIS UNISTAR PRO

IT360°

www.actual-it.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Robert Kuzmič, glavni direktor Kontron, d.o.o. *

V DRUŽBI IN GOSPODARSTVU JE VEČINOMA VZPOSTAVLJENO ZAVEDANJE, DA JE INFORMACIJSKA VARNOST NUJNA ZA DELOVANJE DRUŽBE

Zavedanje o pomenu informacijske varnosti postaja vse močnejše in je praktično vključeno v vse poslovne in razvojne procese. To dejstvo, pa na drugi strani prinaša pomembe priložnosti za organizacije, ki s svojim razvojnim potencialom in visoko usposobljenimi strokovnjaki nudijo storitve na tem zahtevnem področju. O vseh izzivih smo se pogovarjali z g. Robertom Kuzmičem.

Preteklo obdobje je bilo zelo dinamično za vašo organizacijo. Prihajalo je do raznovrstnih sprememb, ki so na koncu pripeljale do tega dejstva, da je Iskratel prešel v tuje lastništvo in se združil s podjetjem S&T Slovenija. Postali ste največje slovensko IKT podjetje, ki deluje kot pomemben del mednarodne skupine Kontron AG. Nam lahko zaupate, katere so tiste strokovne sinergije, ki jih pričakujete od tega koraka?

Res je, slovenski Kontron je del avstrijske skupine Kontron AG, skupine, ki se uvršča med vodilne ponudnike pametnih rešitev na področju pametnih tovarn, železniških in komunikacijskih sistemov, komunikacijskih rešitev in pametnih rešitev za področje energetike. Med drugim nam to omogoča lažji prodor na tuje trge, predvsem zahodne, kamor smo močno usmerjeni. Imamo močnega lastnika, kar novim, predvsem tujim strankam, daje dodaten občutek varnosti in zanesljivosti, naša zaveza pa je, da strankam in partnerjem dostavimo, kar obljubimo.

Ste kljub vključitvi v mednarodno korporacijo uspeli zadržati določene slovenske specifike, ki so pomembne za vaše delovanje tudi v sedanjem obdobju?

Prenos lastništva in sprememba imena kranjskega podjetja v Kontron ni spremenila ključnih značilnosti naše družbe.

V vse bolj povezanem svetu varnostna tveganja v energetskih, logističnih, zdravstvenih, finančnih in drugih sistemih skokovito naraščajo. Z namenom, da zagotovimo varnost teh sistemov oz. zvišamo nivo kibernetske varnosti organizacij, moramo vpeljati ustrezne ukrepe.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Naša organizacijska struktura, predvsem pa portfelj rešitev in storitev ter odnos do kupcev in partnerjev se spreminja le, če se spreminja trg. V našem fokusu so – in to vedno bodo – stranke, ki jim zagotavljamo napredne, zanesljive, pametne in varne informacijske in komunikacijske rešitve. Tako z znanjem, odgovornostjo in inovativnim pristopom strankam nudimo celovite IKT-rešitve za reševanje najkompleksnejših izzivov in učinkovito podporo na njihovi poti digitalizacije. Prav tako je pomembno izpostaviti, da smo ohranili lastno proizvodnjo, ki jo še širimo in moderniziramo, zadržali pa smo tudi dolgoletno tradicijo znamke Iskratel, s katero poimenujemo svoje produktne družine. Kot primer, najhitrejši optični omrežni terminal na svetu še naprej nosi ime Iskratel Lumia T6.

Drži, z Iskratel produkti ste bili v preteklosti zelo uspešni na vzhodnih trgih, ki pa so sedaj nedostopni. Varnostno okolje ima namreč na poslovanje organizacije izredno močan vpliv. Kako ste naslovili izzive, ki so nastali z izpadom teh trgov?

Še več pozornosti smo usmerili na Balkan, ohranili poslovanje v vzhodnih državah, kjer je bilo to mogoče in veliko energije vložili v prodor na zahod. Prav pri vstopu na nove, zahodne trge nam je bila naša matična skupina Kontron AG v veliko pomoč, saj je bila s svojimi produkti in rešitvami že prisotna na trgih kamor smo želeli tudi mi. Naše (pred)prodajne aktivnosti so bile tako, tudi po zaslugi sinergij z ostalimi entitetami skupine Kontron AG, še hitreje uspešne na nemškem, britanskem, španskem in tudi avstrijskem trgu. Tako bo denimo slovenski Kontron z napredno dostopovno rešitvijo XGS-PON odigral ključno vlogo pri zagotavljanju hitrejšega in bolj zanesljivega internetnega dostopa naročnikom Speed Connecta po Spodnji, ruralni Avstriji. Takšni projekti delujejo kot odlična referenca, odskočna deska, če želite, in so za naše sodelavce dobra spodbuda, motivacija in energija za naprej.

Ste na tujih trgih prisotni tudi z drugim, pripojenim delom vašega portfelja, denimo z informacijskimi rešitvami?

Da, s pridruženim delom portfelja slovenskega Kontrona, torej informacijskimi rešitvami, ki jih je v preteklosti zagotavljal S&T Slovenija, smo našli sinergije tudi pri prej omenjenem projektu v Avstriji. Zelo lepo se namreč povežejo Iskratelove širokopasovne rešitve z zagotavljanjem zanesljivih, varnih in hitrih omrežnih povezav.

Na splošno so varnostni izzivi vedno pomembnejši dejavnik pri načrtovanju zanesljivega in neprekinjenega delovanja naših organizacij. Je to ob dejstvu, da se vodstva gospodarskih organizacij vedno bolj zavedajo teh izzivov, priložnost za vašo organizacijo?

Pomen kibernetske varnosti v družbi na splošno, še posebej pa v gospodarskih organizacijah, verjetno še nikoli ni bil večji in seveda to potrebo naslavljamo z našimi varnostnimi rešitvami.

V vse bolj povezanem svetu varnostna tveganja v energetskih, logističnih, zdravstvenih, finančnih in drugih sistemih skokovito naraščajo. Z namenom, da zagotovimo varnost teh sistemov oz. zvišamo nivo kibernetske varnosti organizacij, moramo vpeljati ustrezne ukrepe. V našem podjetju imamo širok nabor rešitev, kot tudi celotno ekipo strokovnjakov, ki delu-

jejo znotraj varnostno-operativnega centra (SOC). Le-ta ekipa bdi nad okolji naših naročnikov in ima primarno nalogo, da morebitno grožnjo pravočasno zazna in brez ustvarjanja panike sledi dogovorjenemu načrtu ravnanja za čimprejšnjo obveščanje, reševanje in povrnitev v prvotno stanje.

Je SOC primeren odgovor za vse tipe organizacij?

Podjetja se seveda tovrstnih izzivov lotevajo na različne načine. Najbolj zanesljivo pa je, da zagotovijo ustrezne sistemske rešitve, torej varnostne rešitve, rezervne lokacije in sisteme za neprekinjeno delovanje, interne procese ravnanja ali protokole in kompetenten kader za obvladovanje kibernetskih incidentov. A zaradi manjka slednjega, raste povpraševanje po najemu zunanjega izvajanja storitev informacijske varnosti.

Kadrovski izzivi so v zadnjem obdobju zelo izpostavljeni. Verjetno se temu ne morete izogniti niti v vaši organizaciji. Kako uspete zagotavljati zadostno število visoko strokovnih kadrov, ki jih potrebujete v zahtevnih procesih svojega delovanja?

Danes je več kot pomembno, da znamo obdržati kader. Kontron je stičišče visoko usposobljenih strokovnjakov, z različnih področij, ki so zaposleni v vseh poslovnih enotah znotraj podjetja. Mislim, da je za tak kader zelo pomembno, da mu delovno okolje nudi izzive, ki jih s svojim strokovnim znanjem in dolgoletnimi izkušnjami znajo nasloviti, in okolje, ki je spodbudno, tržno naravnano in inovativno. Tako zagotavljamo motivacijo in zavzetost zaposlenih pri nas.

Dodatno pa nam številčna ekipa visoko usposobljenih kadrov omogoča poprej omenjeno zagotavljanje zunanjega izvajanja storitev za naše stranke, tudi t.i. »informacijske varnosti kot storitev« (CSaaS – Cyber Security as a Service). Na ta način svojim strankam omogočamo, da lažje podprejo dinamiko poslovanja ter si zagotovijo boljšo kibernetsko varnost, brez, da bi za to morali zaposliti varnostnega strokovnjaka. Podjetja se tako ob hitrejši uvedbi novih storitev bolje in prej prilagodijo potrebam ter se hitreje odzivajo, oziroma pripravijo na nova tveganja.

Informatizacija in digitalizacija sta močno prodrli tudi v varnostni sektor. Kje vidite tiste priložnosti, na katere boste v naslednjem obdobju še posebej pozorni pri razvoju svojih rešitev?

> Namen sodelovanja znotraj Slovenskega združenja korporativne varnosti, katerega člani smo, je zagotovo združevati in usklajevati interese ter deliti dobre prakse uporabnikov kibernetske varnosti in ponudnikov kibernetskih varnostnih rešitev.

To je pravzaprav osnova za zagotavljanje naprednih informacijskih rešitev – da si kot ponudnik vedno na preži za najnovejšimi in še bolj učinkovitejšimi rešitvami. V Kontronovem varnostno-operativnem centru prav z uporabo napredne tehnologije in specifičnim znanjem pravočasno odkrijejo ranljivosti, jih analizirajo in odpravijo. Pri zagotavljanju kibernetske varnosti, denimo v SOC-u uporabljajo več kot 10 orodij, zagotovo pa bo – z vpeljavo novih tehnologij in rešitev – številka še rasla.

Med njimi so tudi takšne tehnologije, ki delujejo s pomočjo umetne inteligence, ki ni več samo prihodnost, temveč je postalo dejstvo sedanjosti. Umetna inteligenca je svetovni trend, ki podjetjem pomaga pri pridobivanju konkurenčne prednosti. Vendar po podatkih Statističnega urada Republike Slovenije (SURS), umetno inteligenco pri poslovanju uporablja le 12 odstotkov slovenskih podjetij.

Kako močno umetno inteligenco uvajate v svoje razvojne in poslovne procese?

V varnostnih rešitvah je umetna inteligenca, oziroma še bolj t.i. strojno učenje, prisotno že vrsto let, seveda tudi v naših rešitvah in pri izvajanju storitev SOC-a.





Pričakujemo, da se bo še v večji meri kot sedaj uporabljala pri optimizaciji poslovnih procesov. Podjetjem namreč, poleg kibernetske varnosti, pomaga pri avtomatizaciji in optimizaciji poslovnih procesov ter zmanjšanju stroškov.

Ste tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Katere so dodane vrednosti tega sodelovanja v tej strokovni asociaciji?

Namen sodelovanja znotraj Slovenskega združenja korporativne varnosti, katerega člani smo, je zagotovo združevati in usklajevati interese ter deliti dobre prakse uporabnikov kibernetske varnosti in ponudnikov kibernetskih varnostnih rešitev. S svojim delom tako združujemo gospodarstvo, javni sektor in državne institucije ter posamezne strokovnjake za skupen razvoj kibernetskih varnostnih zmogljivosti in tako spodbujamo digitalni razvoj gospodarstva v Sloveniji.

Menite, da v Sloveniji premalo cenimo razvojno znanje naših organizacij? Kaj bi bilo po vašem mnenju potrebno, da bi se tudi varnostne rešitve v večjem obsegu integrirale v operativno delovanje javnega in gospodarskega sektorja?

Osebno menim, da je znanje, še posebej na področju kibernetske varnosti, v Sloveniji izredno pomembna vrednota. V našem podjetju zagotovo je in zavedamo se, da so inovativnost, kompetentnost in strokovnost tiste lastnosti naših kadrov, ki nas postavljajo na mesto prve izbire naših kupcev. To in pa zanesljivost, seveda.

Menim pa, da je po večini v gospodarstvu vzpostavljeno zavedanje, da je vpeljava varnostnih rešitev nujna za zanesljivo in varno delovanje družbe, sedaj pa je potrebna čim hitrejša realizacija – v vseh panogah, na vseh nivojih. ■

Foto: Žiga Kalan

Avtorica: Mateja Mirtič / Skrbnica ključnih kupcev, ID Shop d.o.o.



KJE SE ZAČNE VARNOST VAŠIH POSLOVNIH PROSTOROV?

V omenjenem prispevku želimo predstaviti pristope, ki predstavljajo primere dobre prakse pri načrtovanju in integraciji tehničnih sistemov. Pomembno je, da pri tem upoštevamo tudi naročnikove želje in pričakovanja, ki morajo skupaj z zagotavljanjem varnosti omogočiti pozitivno uporabniško izkušnjo. Racionalizacija in povečanje učinkovitosti ter zagotavljanje visokega nivoja varnosti so tisti pomembni vidiki, ki jih nikakor ne smemo zanemariti v procesu načrtovanja in izvedbe projektov.

Pri načrtovanju tehničnega varovanja v novogradnjah, kot tudi v obstoječih poslovnih, proizvodnih, skladiščnih in drugih prostorih, moramo poznati prednosti in pomanjkljivosti različnih rešitev, ki so na voljo.

Naročniki po navadi vedo kaj lahko pričakujejo od kontrole pristopa in nemalokrat si želijo, da se ta integrira s katerim od ‚zunanjih sistemov', ki jih v organizaciji že uporabljajo ali vsaj, da lahko zaposleni uporabljajo isti medij za različne namene (kontrolo pristopa, kontrolo delovnega časa, plačevanje malic, odklepanje garderobnih omaric ipd.).

V kolikor so te želje zajete in predvidene že v fazi načrtovanja vzpostavitve vsaj enega od omenjenih sistemov, to za naročnika kasneje pomeni prihranek tako z vidika financ, kot tudi časa, ker dopušča večji izbor funkcionalnosti ter integracij, ki jih lahko med sistemi kasneje povežemo in uresničimo. Na ta način ne govorimo zgolj o zagotavljanju optimalnega varnostnega nivoja, temveč tudi o optimizaciji upravljanja, boljši uporabniški izkušnji ter bolj učinkoviti pregled nad dogodki.

Naš zadnji projekt je dober primer za prikaz poteka načrtovanja in izvedbe celovite kontrole pristopa v poslovnem objektu. Objekt obsega 6 nadstropij ter 2 nadstropji garaž. V spodnjem nadstropju je restavracija, ki je odprta tudi za zunanje obiskovalce, objekt pa vključuje še prostore za zaposlene za dejavnosti izven delovnega časa (fitnes, joga, savna ter učno-razvojni center).

Kako načrtovati učinkovito kontrolo dostopa?

Osnovni nivo varnosti se začne z mehanskim sistemom zaklepanja, vendar opažamo, da organizacije nemalokrat zanemarjajo njihovo pomembnost in jih pozabijo vključiti v načrtovanje že takoj ob gradnji objekta ali ob vselitvi v nove prostore, ker predvidevajo, da jim elektronska kontrola dostopa zagotavlja vso potrebno varnost. Ne zavedajo se, da lahko v primeru, če se nepooblaščena oseba dokoplje do ključa, z njim vstopi v prostor kljub elektronski kontroli dostopa brez, da bi se to kjerkoli zabeležilo! Na ta način je možno zaobiti varnostne elemente, ki naj bi jih elektronska kontrola dostopa zagotavljala.

1. Korak: Premišljen mehanski sistem zaklepanja, kot osnova za učinkovito zagotavljanje varnosti vseh ostalih sistemov zaklepanja.

Omenjeni praktični primer predstavlja dobro prakso možnih pristopov integriranja različnih tehnoloških rešitev in njihovo uskladitev z zahtevami naročnika. S tem se na eni strani pomembno dviguje varnost v organizacijah na višji nivo, na drugi strani pa zadovoljuje specifične potrebe naročnika, ki so na koncu tudi zelo pomembne za doseganje ustreznega nivoja zadovoljstva.



Pri končnih uporabnikih je pomembno zavedanje, da hkrati z elektronsko kontrolo pristopa obvezno uredijo tudi mehanski sistem zaklepanja in s tem zmanjšajo število ključev, uredijo dostope, poenostavijo upravljanje s ključi ter preprečijo njihovo nepooblaščeno kopiranje. Šele, ko vemo kje se nahajajo mehanski ključi, potem je lahko elektronski sistem zanesljiv in s polno funkcionalnostjo.
Kot primer dobre prakse, lahko navedemo primer, kjer je naročnik želel urejen mehanski sistem s čim manj ključi v obtoku, kljub temu, da bo objekt opremljen tudi s kontrolo pristopa.

Potrebovali so sistem zaklepanja, ki omogoča razvejane podsisteme in nudi čim boljšo zaščito, zato smo ponudili EVVA EPS cilindre. Poleg tehnične zaščite (poseben profil ključa z dodatnimi stranskimi narezi ter zaščite proti vrtanju in izvleku), jih odlikuje še patentna zaščita (zaščiten profil do leta 2041, ki omogoča izdelavo kopij le pri pooblaščenih ključavničarjih) in organizacijska zaščita (izdelava kopij je možna le ob predložitvi lastniške kartice).

Celoten sistem zaklepanja je obsegal več kot 160 EVVA EPS cilindrov. Poleg glavnega ključa za cel objekt imajo še 13 podsistemov, med drugim generalni ključ po nadstropjih, ključ za vse tehnične prostore, ključ za kuhinjo, ključ za jaške,... Glede na velikost objekta smo se srečali z vsemi vrstami vrat (požarna, kovinska, alu vrata, steklena ter lesena laminatna vrata) in ker so cilindri modularni, smo lahko dimenzije prilagodili kar ob sami montaži, predhodne izmere niso bile potrebne.

Naročnika so prepričale funkcionalnosti, ki jih ponuja EVVA EPS, poleg tega pa smo s sistemom lahko izpolnili tudi zahteve arhitektov, da so cilindri v črni barvi in se tako skladajo s celostno podobo notranjega dizajna.

2. Korak: Ustrezno izbrana elektronska kontrola pristopa, ki omogoča integracije z ostalimi sistemi, ki jih želi naročnik povezati med seboj.

Glavni namen elektronske kontrole dostopa je povečati varnost v objektu, omejiti dostop nepooblaščenim osebam na izbrana območja, zagotoviti pregled revizijske sledi ter pregledno in preprosto upravljanje s sistemom na daljavo, za uporabnika oz. zaposlenega pa enostavno uporabo.

Z naročnikom se je analiziralo različne možnosti, ki bi najbolje naslavljale njihove želje in nazadnje so se odločili za SALTO kontrolo pristopa, ki je lahko zadovoljila največ zahtev zaradi specifike objekta, kot same funkcionalnosti. Projekt je obsegal več kot 45 Salto XS4 ONE pametnih baterijskih ključuk na ščitu, več kot 50 čitalcev, programsko opremo Salto Space ter RFID kartice, ki jih uporabljajo tudi za identifikacijo.

Naročnik je želel zagotoviti nadzorovan dostop v vsa nadstropja, zato je vsako nadstropje opremljeno s čitalci. Zaposleni imajo že v naprej dodeljen dostop do določenega nadstropja, prav tako pa čitalci delujejo kot on line točka kar pomeni, da se z vsakim prehodom posodabljajo in prenašajo pravice in podatki o dostopih.

Na enak princip dodeljujejo pravice tudi obiskovalcem. Na recepciji so že v naprej sprogramirane kartice za vsako nadstropje, receptor pa na kartico doda le ime obiskovalca in časovni dostop. S tem so se izognili spremljanju obiskovalcev, kot so to imeli v prejšnjih prostorih, kjer je moral vsak obiskovalec počakati pri recepciji, da je prišel nekdo od zaposlenih in ga pospremil.

V vsakem nadstropju so tudi določeni prostori, ki potrebujejo dodaten nadzor in kamor lahko vstopajo samo določeni zaposleni, in sicer soba s strežniki, prostor za čistilko, vzdrževalca, fitnes, savna, kolesarnica v kleti, itd. Zato smo tam namestili baterijske pametne ključke.

Z vidika programske opreme smo naredili integracijo z njihovim »active directory«, da niso rabili vsakega zaposlenega ponovno vnašati v SPACE sistem. Prav tako so vsi domofoni, drsna vrata, dvižna zapornica in pa garažna vrata vezani na impulze od čitalca za enostavno upravljanje. SALTO kartice pa uporabljajo tudi za polnilnico električnih avtomobilov.

3. Korak: Dodana vrednost: Pametni sistem zaklepanja garderobnih omaric.

Z novimi koncepti delovnih mest, prihajajo v ospredje tudi »open floor« pisarne s skupnimi prostori za delo ali druženje. Takšni prostori pa morajo zagotavljati ustrezno opremo za varno shranjevanje osebnih predmetov in opreme. Ena od rešitev, ki sodi v tako zasnovane prostore je pametno zaklepanje garderobnih ali pisarniških omaric.

Naročnik je v svojem objektu načrtoval kar nekaj prostorov, kjer so potrebne garderobne omarice. Ker smo jim vzpostavili sistem kontrole pristopa, so imeli željo, da lahko tudi omarice odklepajo z obstoječimi mediji za kontrolo pristopa.

Stranki smo predlagali vgradnjo 32 Gantner ključavnic GAT ECO.Lock 7100 NW F/ISO (baterijske ključavnice) z osnovnim setom za upravljanje ključavnic (master mediji, MOLA mobilna aplikacija za upravljanje in dodatni mediji).

Omarice v garderobah delujejo kot »free locker«, kar pomeni, da niso dodeljene točno določenim osebam, ampak lahko omarico uporablja vsak, kadarkoli želi, v kolikor je ta takrat prosta.

Predali na recepciji so prav tako opremljeni z Gantner ključavnicami, vendar so tam ključavnice »dedicated«, torej imajo dostop točno določeni uporabniki, da lahko tam shranjujejo svoje osebne stvari (receptorka, varnostnik, ki pride popoldne, direktor, itd.).
Sistema zaenkrat nismo povezovali s kontrolo pristopa, ker v tej fazi to ni bilo potrebno. V kolikor bi naročnik v prihodnosti želel več »dedicated« omaric in koristiti dodatne funkcionalnosti (rezervacije, časovne omejitve ipd.), pa je sistem vedno možno povezati in upravljati v Salto programski opremi.

Specifično za Gantner omarice in kar je bilo arhitektom zelo pomembno je, da imajo ključavnice minimalističen dizajn in da so neopazne oz. »zlite« s samo omarico (»push-open« sistem).

Omenjeni praktični primer predstavlja dobro prakso možnih pristopov integriranja različnih tehnoloških rešitev in njihovo uskladitev z zahtevami naročnika. S tem se na eni strani pomembno dviguje varnost v organizacijah na višji nivo, na drugi strani pa zadovoljuje specifične potrebe naročnika, ki so na koncu tudi zelo pomembne za doseganje ustreznega nivoja zadovoljstva. Pri načrtovanju je potrebno izbrati najprimernejši sistem kontrole pristopa, naj gre za klasični mehanski sistem zaklepanja, mehatronsko ali digitalno zaklepanje, ali pa za varnostne prehode v nadzorovana območja v obliki vrtljivih vrat in hitrih prehodov. To je zagotovilo, da nameščen sistem deluje učinkovito in prinaša željene rezultate ter optimalno rešitev. ■

Foto: arhiv ID Shop d.o.o.





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



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

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

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



IDealni partner za identifikacijo in varnost

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

Gantner
www.gantner.com

Avtor: Jure Habbe / operativni direktor, Silver Bullet Risk



IZ TEORIJE V PRAKSO: ANALIZA KIBERNETSKIH TVEGANJ IN DIREKTIVA NIS 2

Lani je začelo veljati več predpisov EU na področju digitaliziranih dejavnosti, med katerimi je tudi Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS 2). Na njeni osnovi naj bi bila jeseni sprejeta nova slovenska regulativa za informacijsko varnost, kar je lepa priložnost za izboljšave nekaterih sedanjih pristopov.

V primerjavi z informacijsko varnostjo, ki poleg digitalnih, vključuje tudi druge oblike informacij, se kibernetska varnost osredotoča na zaščito informacijskih omrežij in sistemov pred digitalnimi napadi in nezakonitimi dostopi, kot so hekerski vdori, virusi, zlonamerna programska oprema, napadi DDoS in druge spletne grožnje.

Cilj kibernetske varnosti je zagotavljanje neprekinjenega in varnega delovanja digitalnih sistemov, vključno s celovitostjo, avtentičnostjo, razpoložljivostjo in zaupnostjo informacij.

Njen temelj pa je analiza tveganj, s katero organizacije sistematično prepoznavajo in ocenjujejo ter nato obvladujejo nevarnosti, ki jih ogrožajo na informacijskem področju.

To potrjuje tudi Direktiva NIS 2, ki v 2. točki 21. člena, kot prvi ukrep za zagotavljanje kibernetske varnosti navaja analizo tveganja in varnosti informacijskih sistemov.

Analiza kibernetskih tveganj na podlagi sredstev

Pri analizi kibernetskih tveganj večina organizacij uporablja pristop, ki temelji na sredstvih (ang. Asset Based Approach). Najdemo ga v smernicah Agencije Evropske skupnosti za kibernetsko varnost (ENISA), v standardu za obvladovanje informacijskih tveganj ISO/IEC 27005 in še marsikje.

Vendar izkušnje kažejo, da splošna razširjenost še ne pomeni najboljše možne rešitve. Kot vemo, pristop temelji na popisih informacijskih sredstev, ki jim pripišemo grožnje in ranljivosti glede na dejavnike celovitosti, razpoložljivosti in zaupnosti, katerim NIS 2 dodaja še avtentičnost.

Tveganje izračunamo kot produkt verjetnosti in vpliva uresničitve možne nevarnosti. Za ocenjevanje obeh faktorjev ISO/IEC 27005 predvideva kvalitativne in kvantitativne metode. Pri prvih tveganja vrednotimo opisno (npr. malo, srednje, veliko), pri drugih pa številčno (npr. od 1 do 3, 5 ali 10).

Rezultati takšnih analiz so seznami stotin in več informacijskih sredstev s številčnimi ocenami tveganj, za katere v organizacijah porabijo ogromno časa, vendar nimajo skoraj nobene uporabne vrednosti.

Analiza, ki sestoji iz prepoznavanja, ocenjevanja in razvrščanja informacijskih sredstev, je šele prvi korak k upravljanju in zagotavljanju kibernetske varnosti. Sledijo ukrepi za zmanjševanje tveganj in obvladovanje kibernetskih incidentov, če se zgodijo. Podatke o vseh teh procesih pogosto srečujemo v običajnih preglednicah ali preprostih lastnih aplikacijah, kar ima različne slabosti pri uporabnosti, sledljivosti in varnosti. Zaradi navedenega je potrebno iskati celovite rešitve. Ena od možnosti je vsekakor aplikacija SBR, ki omogoča celovito informacijsko rešitev za obvladovanje varnostnih tveganj.

Zato je marsikdo zagotovo že podvomil o njihovi smiselnosti ter pomislil, če je to zares edina možnost in ali poznamo bolj praktične metode.

Procesni pristop analize kibernetskih tveganj

Za odgovor najprej razmislimo, čemu so informacijska sredstva namenjena. Omrežja in sisteme uporabljamo, da z njimi opravljamo dejavnosti, ki so v poslovnem in delovnem okolju organizirane v procese. Vendar vsi procesi niso enako pomembni, zato jih delimo na primarne in podporne.

S primarnimi procesi, kot so proizvodnja, prodaja izdelkov in storitev ter podpora strankam, v gospodarstvu ustvarjamo prihodke, v negospodarstvu pa izvajamo temeljne dejavnosti, kot so zdravljenje bolnikov, varstvo in šolanje otrok, oskrba starejših občanov in podobno.

Omogočajo jih podporni procesi, kot so nabava, logistika, računovodstvo, informatika, ravnanje z zaposlenimi in vodenje.

Vsi procesi so stalno izpostavljeni različnim nevarnostim, da gre pri njihovem delovanju nekaj narobe, kar organizacijam povzroči manjšo ali večjo škodo. In kadar je nastala škoda lahko velika, govorimo o tveganjih.

Če takšno razmišljanje uporabimo za analizo kibernetskih tveganj in pri tem upoštevamo predpisane smernice, jo izvedemo v naslednjih korakih:

- **Ključni procesi:** V prvem koraku določimo ključne procese, kar običajno pomeni primarne poslovne procese, pri katerih motnje in izpadi povzročijo največjo škodo.
- **Skupine sredstev:** Za izvajanje procesov potrebujemo informacijska sredstva, ki jih najprej razdelimo v skupine, kot so kadri (zaradi katerih sredstva raje imenujemo viri), strojna in programska oprema, komunikacijski sistemi in podobno.
- **Sredstva:** V vsaki skupini določimo sredstva, ki so najbolj pomembna za nemoteno delovanje primarnih procesov. Pri tem ne navajamo vsake posamezne naprave, temveč jih združujemo v skupine z enakim pomenom, kot so na primer osebni računalniki in omrežna stikala.
- **Grožnje in ranljivosti:** Izdelamo seznama groženj in ranljivosti, pri katerih si lahko pomagamo z vzorci za posamezne dejavnosti. Praviloma upoštevamo, da so grožnje zunanji vplivi in ranljivosti notranje slabosti, čeprav srečujemo tudi drugačne razlage.
- **Prepoznavanje tveganj:** Za posamezna sredstva opredelimo grožnje in ranljivosti glede na dejavnike celovitosti, avtentičnosti, razpoložljivosti in zaupnosti.





- **Ocenjevanje tveganj:** Ocena tveganja je sestavljena iz verjetnosti (ali pogostosti) in vpliva uresničitve tveganja, kar pomeni nastale škode. Delimo jo na neposredno, ki predstavlja strošek, na primer popravila ali zamenjave informacijskega sredstva, in posredno, ki nastane zaradi zastoja primarnega procesa, kar v gospodarstvu večinoma lahko ovrednotimo s finančnimi ocenami.

- **Razvrščanje tveganj:** Na podlagi ocen sredstva razvrstimo po pomembnosti, pri čemer kot kriterij upoštevamo tveganja, ki lahko organizaciji povzročijo največjo škodo. Če imamo določeno lestvico s finančnimi kriteriji, lahko sredstva razvrstimo tudi glede na stopnje tveganja z ocenami na primer od 1 do 5.

Učinkovitost in skladnost procesnega pristopa

Če povzamemo, s procesnim pristopom pri analizi kibernetskih tveganj dosežemo dvojno korist.

Prvič, pridobimo uporaben seznam informacijskih sredstev, ki so najbolj izpostavljena različnim nevarnostim, na podlagi finančnih posledic. In drugič, z ocenami tveganj informacijskih sredstev v skladu s predvidenimi dejavniki zagotovimo skladnost z regulativnimi smernicami.

Procesni pristop niti ni revolucija, temveč je smiselna izboljšava analize kibernetskih tveganj, zato upamo, da najde pot tudi v posodobljene predpise za informacijsko varnost in prakso. ■

Učinkovite rešitve za analize in obvladovanje kibernetskih tveganj v vsaki organizaciji

Temelj za zagotavljanje kibernetske varnosti je upravljanje tveganj, ki organizacijam omogoča sistematično prepoznavanje in ocenjevanje ter nato obvladovanje nevarnosti, ki ogrožajo njihova informacijska omrežja, sisteme, naprave, podatke in druge informacijske vire.

Težava in rešitev

Pri analizi kibernetskih tveganj večina organizacij uporablja pristop, ki temelji na popisih in ocenah sredstev (ang. Asset Based Approach).

Rezultati takšnih analiz so seznami stotin in več informacijskih sredstev s številčnimi ocenami tveganj, za katere v organizacijah porabijo ogromno časa, vendar nimajo skoraj nobene uporabne vrednosti.

Učinkovita rešitev je procesni pristop in finančne ocene tveganj, s katerim pridobimo dvojno korist.

Prva je uporaben seznam informacijskih sredstev, ki so najbolj izpostavljena različnim nevarnostim, na podlagi možnih finančnih posledic. Druga pa so ocene tveganj za informacijska sredstva v skladu z regulativnimi smernicami, kot je standard ISO/IEC 27005.

Kako vam lahko pomagamo?

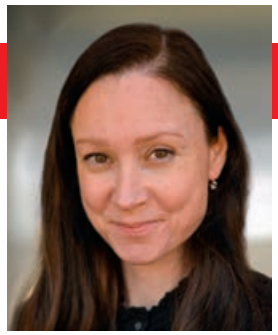
Vsem, ki ste odgovorni za kibernetsko varnost, lahko pomagamo:

- s svetovanjem pri pripravi metodologije za analizo kibernetskih tveganj v skladu s procesnim pristopom (prepoznavanje, ocenjevanje, razvrščanje),
- z izvedbo delavnic za analizo kibernetskih tveganj,
- z informacijsko rešitvijo Silver Bullet Risk (SBR) za celovito obvladovanje kibernetskih tveganj z vsemi ključnimi procesi in podatki na enem mestu.



Za več informacij ali predstavitev rešitve SBR nam pišite na naslov **info@silverbulletrisk.com**.

Avtorica: dr. Jolanda Modic / Institut za korporativne varnostne študije*



SOOBLIKOVANJE STANDARDOV IN POLITIK ZA VEČJO ODPORNOST KRITIČNE INFRASTRUKTURE V EVROPI

Evropa se danes nahaja na prelomnici, kjer je potreba po dvigovanju odpornosti za neprekinjeno delovanje kritične infrastrukture bolj izpostavljena, kot je bila kadarkoli do sedaj. Pomembno težišče pri iskanju ustreznih smeri razvoja imajo tudi predstavniki konzorcijev raziskovalnih projektov, ki so bili specifično financirani z namenom povečevanja varnosti delovanja kritične infrastrukture. ICS-Ljubljana ima v tem okviru posebej pomembno vlogo, saj je med vsemi slovenskimi organizacijami najbolj aktivno prisoten ravno na teh EU projektih s področja kritične infrastrukture.

ECSCI – Evropski grozd za zaščito kritične infrastrukture

Evropski grozd za zaščito kritične infrastrukture (*European Cluster for Securing Critical Infrastructures*) je mreža raziskovalnih projektov, financiranih s strani Evropske komisije, ki naslavljajo izzive s področja fizične in kibernetske varnosti kritične infrastrukture (KI). Grozd je bil ustanovljen na iniciativo treh projektov iz programa Obzorje 2020 (Horizon 2020), danes pa šteje že 34 zaključenih in tekočih projektov iz programov Obzorje 2020 in Obzorje Evropa (Horizon Europe), kot je razvidno iz Slike 1.



Slika 1. Projekti - člani grozda ECSCI.

*avtorica je članica Slovenskega združenja korporativne varnosti

Glavni cilj grozda je ustvarjanje sinergij med projekti, organizacijami in posamezniki ter spodbujanje skupnih oz. usklajenih raziskav in razvoja inovativnih rešitev za povečevanje odpornosti naše skupne evropske KI. Predstavniki projektov, ki so člani ECSCI grozda, temu cilju sledijo z organizacijo skupnih mednarodnih dogodkov, ki vključujejo, ne le predstavnike projektov, ampak tudi predstavnike Evropske komisije, oblikovalcev politik, ter zunanjih raziskovalcev in razvijalcev.



Slika 2. Perspektive, predstavljene na ECSCI-SPM delavnici.

Skupaj zmoremo več

Vsi projekti ECSCI grozda so si različni. Vsak od njih pokriva svoj sektor (npr. energetiko) ali njihove preseke, naslavlja specifične izzive (npr. analizo tveganj na medsektorskem in mednarodnem nivoju) in razvija določene tehnologije (npr. nove algoritme umetne inteligence za hitrejšo in natančnejšo zaznavo kibernetskih napadov). A vendar imajo vsi projekti skupni cilj – izboljšati nivo varnosti KI v Evropi.

Kot člani številnih projektov ECSCI grozda ter partnerji številnih upravljavcev KI v Sloveniji smo v ICS Ljubljana v lanskem letu v tem istem ekipnem duhu s predstavniki drugih projektov organizirali delavnico na temo sooblikovanja standardov in politik za povečevanje odpornosti evropske KI pod naslovom »*ECSCI-SPM Workshop for Collaborative Standardisation and Policy Making for Greater CI Resilience in Europe*«. Cilj delavnice je bil zbrati različne poglede na odpornost KI ter oblikovati skupno strategijo za učinkovito in uspešno sodelovanje pri oblikovanju prihodnjih standardov in politik za to področje.

Natančneje, kot je prikazano na Sliki 2, je bil cilj delavnice razumeti (i) dolgoročno vizijo Evropske komisije za povečevanje odpornosti KI, (ii) izkušnje in priporočila zaključenih projektov na temo oblikovanja politik in standardov, (iii) vrzeli v trenutnih standardih in potrebe pri oblikovanju politik ter (iv) priložnosti za sinergije pri naslavljanju teh vrzeli in potreb med aktivnimi projekti. Ti pogledi so sestavljali osnovo za pripravo naše skupne perspektive.

Ključni povzetki iz delavnice

Delavnica je potekala v spletni obliki, in sicer v torek, 5. decembra 2023. Organizirana je bila v obliki različnih sklopov, ki so bili usklajeni s petimi perspektivami, ki smo jih želeli zajeti. Agenda delavnice z naslovljenimi temami, njihovimi predstavitelji ter moderatorji je prikazana na Sliki 3.

Time	Session Title	Chair & Speakers
09:00 – 09:15	**Welcome speech by ECSCI**	Speaker: **Habtamu Abie**, Norsk Regnesentral (NRS)
09:15 – 10:00	**The EC Perspective** On the EC expectations towards the running ECSCI projects, on the vision for the future of the INFRA topic, and on the implementation of the CER Directive.	Chair: **Habtamu Abie**, NRS Speakers: • **Georgios Valsamos**, JRC, European Commission • **Max Brandt**, DG HOME, European Commission
10:00 – 11:05	**Closed ECSCI Projects' Perspective** *Presentations reflecting projects':* • *Activities and results.* • *Experience and lessons learnt.* • *Supporting active projects.*	Chair: **Fabio Bolletta**, RINA Speakers: • **Jenny Rainbird**, Inlecom (PRECINCT) • **John Soldatos**, Innov (FINSEC) • **Diego R. Lopez**, Telefonica (FISHY)
11:05 – 11:15	**Coffee Break**	
11:15 – 12:00	**The Standards & Policy Perspective** Talks reflecting current activities, gaps, and support needed for standardisation and policy making.	Chair: **Aleksandar Jovanović**, Steinbeis EU-VRi Speakers: • **Georgios Sakkas**, KEMEA Research • **Catherine Banet**, Scandinavian Institute of Maritime Law
12:00 – 13:00	**Lunch Break**	
13:00 – 15:05	**Active ECSCI Projects' Perspective** *Presentations reflecting projects':* • *Current activities.* • *Potential contributions.* • *Support needed.*	Chair: **Sebastian Serwiak**, DG HOME, European Commission Speakers: • **Antonio Alvarez Romero**, Atos (SUNRISE) • **Gabriele Giunta**, Engineering (ATLANTIS) • **Anas Husseis**, Ikerlan (CyberSEAS) • **Esteban Damian Gutierrez Mlot**, CIRCE (eFORT) • **Wissam Mallouli**, Montimage (DYNABIC, AI4CYBER) • **Sofia Tsekeridou**, Netcompany-Intrasoft (IRIS)
15:05 – 15:15	**Coffee Break**	
15:15 – 16:30	**The Joint Perspective** *Round table discussion on standardisation and policy making for greater CI resilience.*	Chair: **Stefan Schauer**, AIT Panelists: • **Sebastian Serwiak**, Policy Officer, Security Research and Innovation unit, DG HOME, EC • **Christian Després**, Director of Security Research, Ministry of Ecological Transition, Energies and Transportation, France • **Damjan Horvat**, Secretary, Ministry of Infrastructure, Slovenia • **Nina Jirouskova**, Head of Strategic Partnership, Resallience, Vinci Group, France
16:30 – 17:00	**Moving Forward & Closing Remarks** *Takeaways and steps forward.*	Speaker: **Habtamu Abie**, Norsk Regnesentral (NRS)

Slika 3. Agenda ECSCI-SPM delavnice.

Delavnico je s predstavitvijo trenutnih aktivnosti ECSCI grozda in pozdravnimi besedami otvoril koordinator grozda. Sledile so predstavitve predstavnikov Evropske komisije (natančneje, oddelka za raziskave ter oddelka za oblikovanje politik), ECSCI projektov ter strokovnjakov za standardizacijo in zakonodajo s področja varnosti in odpornosti KI.

Vse predstavitve so se vsaj deloma dotikale Direktive (EU) 2022/2557 Evropskega parlamenta in sveta o odpornosti kritičnih subjektov (t.i. CER Direktive). Predstavniki Evropske komisije so izpostavili pomembnost sodelovanja vseh nivojev (regij-

skega, nacionalnega in evropskega) pri njeni vpeljavi v prakso ter predvsem pomembnost obstoja usklajenih zakonskih instrumentov in standardov. V človeški naravi nam je namreč skupno to, da brez zunanjega pritiska, ki ga predstavljajo tudi zakoni, uredbe in standardi, ljudje večinoma težimo zgolj k izvajanju minimuma. Ko pa govorimo o varnosti KI, minimum še zdaleč ni dovolj.

Predstavniki projektov so predstavili izzive, ki so jih oz. jih še vedno naslavljajo, rezultate, ki so jih oz. jih bodo razvili in so osnova za sooblikovanje standardov, ter izkušnje, ki so jih pridobili pri oblikovanju priporočil za izboljševanje standardov in zakonov. Kot glavne izzive so izpostavili tanko mejo med potrebo po zaščiti občutljivih informacij (na primer, o ključnih ranljivostih in grožnjah v posamezni KI), ter potrebo po deljenju teh informacij za učinkovitejše in hitrejše reševanje povezanih izzivov.

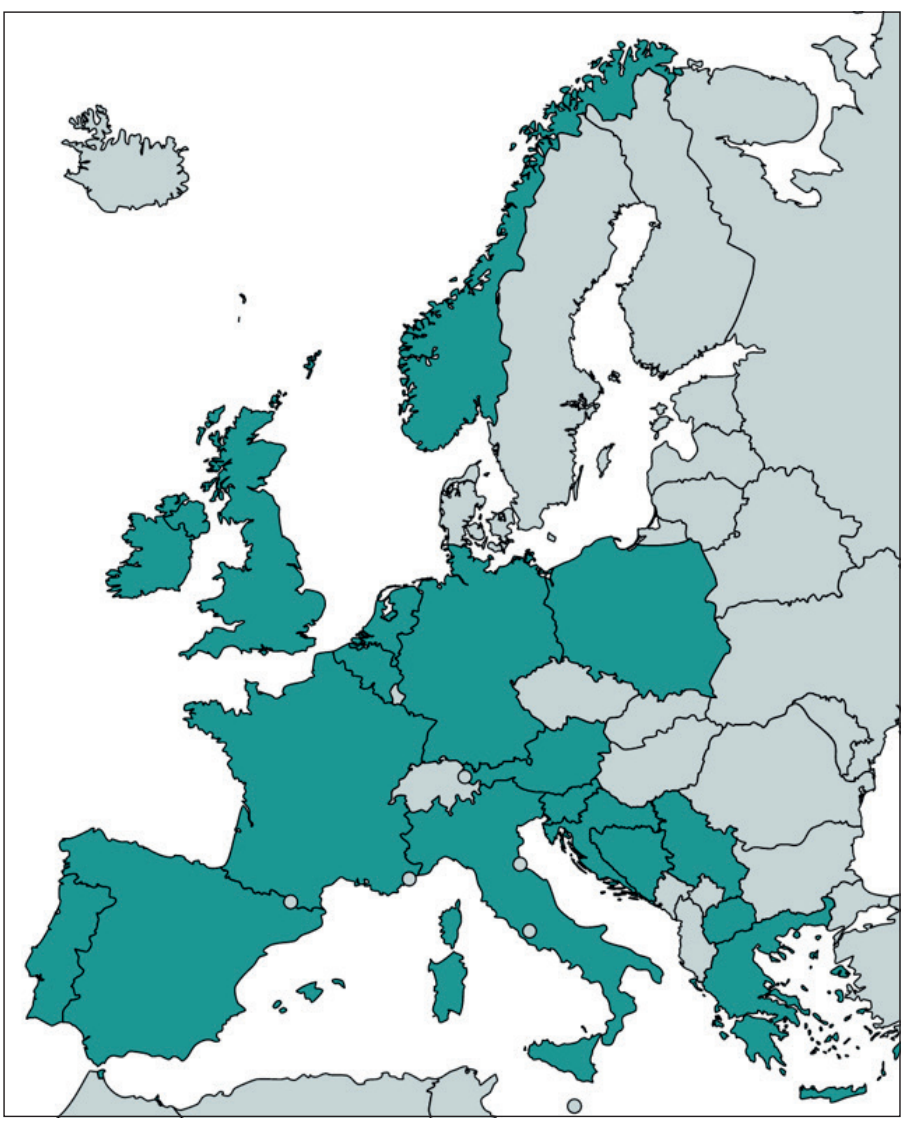
Strokovnjaki za področje standardizacije so povzeli aktualne in prihajajoče standarde s področja odpornosti KI ter povezane standardizacijske aktivnosti. Izpostavili so različne izzive, s katerimi se projekti običajno soočajo, ko želijo aktivno sodelovati pri sooblikovanju standardov. Standard običajno potrebuje 5 ali več let od ideje do sprejetja, medtem ko EU projekti običajno trajajo le 3 leta. Še tako ambicioznim raziskovalcem in perspektivnim idejam, prehitro zmanjka sredstev za financiranje svojih standardizacijskih aktivnosti. Dolgotrajno sprejemanje standardov je v današnjem hitro spreminjajočem se svetu izziv že sam po sebi.

Strokovnjaki so med drugim izpostavili tudi neusklajenost med interesi organizacij za standardizacijo, ki zagovarjajo stališče, da vsaka tehnologija ali proces ne potrebuje standarda, ter projekti, ki običajno želijo standardizirati kopico svojih rezultatov. Po letu 2006 je bilo razvitih več kot 300 standardov za področje KI in skoraj 400 standardov povezanih s področjem zaščite KI in kriznega upravljanja.

Govora je bilo tudi o sami definiciji in interpretaciji pojma »odpornost«, ki sta se vse do sprejetja CER Direktive močno razlikovali od sektorja do sektorja, od države do države. Stanje še vedno ni idealno, saj je pojem odpornosti še vedno pretežno vezan na splošen pojem tveganja (ne pa tudi na konkretnejše pojme povezane z npr. razpoložljivostjo ključnih virov za delovanje KI, učinkovitostjo podpornih tehnologij in varnostjo preskrbovalnih verig), a se izboljšuje. Ter tudi o tem, da morajo standardi podpreti upravljavce KI pri usklajevanju svojih procesov z zakoni, kar žal ni vedno praksa.

Dogodek smo zaključili z okroglo mizo, na kateri je med drugimi sodeloval tudi g. Damjan Horvat, sekretar na Ministrstvu za infrastrukturo Republike Slovenije, ki je s svojo udeležbo v ospredje postavil predvsem aktivnosti, izzive in načrte iz našega domačega okolja. Udeleženci okrogle mize so se sicer dotaknili razlik med zagotavljanjem odpornosti KI v zasebnem in javnem sektorju, ki izhajajo iz narave njihovega okolja. V zasebnem sektorju je večji poudarek na zaščiti podatkov in ustvarjanju poslovne vrednosti iz njihove analize. V javnem, pa se teži k (varnemu) deljenju in odpiranju podatkov, kjer je to le mogoče. Dotaknili so se tudi pomembnosti sodelovanja v EU projektih, ki služijo kot odlično izhodišče za usklajevanje pogledov na vseh nivojih (javnem in zasebnem, lokalnem in mednarodnem, ter znanstvenem in industrijskem), deljenje izkušenj in dobrih praks, ter inoviranje v tehnološkem in strateškem smislu.

Na delavnici pa niso sodelovali le zgoraj omenjeni predavatelji. Vključili smo tudi izkušnje in mnenja publike, ki jo je sestavljalo okoli 75 strokovnjakov iz področja, ki prihajajo iz različnih koncev Evrope (Slika 4). Gre za znanstvenike, predstavnike manjših in velikih podjetij, zasebnih in državnih upravljavcev KI, nevladnih organizacij ter različnih ministrstev.



Slika 4. Države, iz katerih prihajajo udeleženci ECSCI-SPM delavnice.



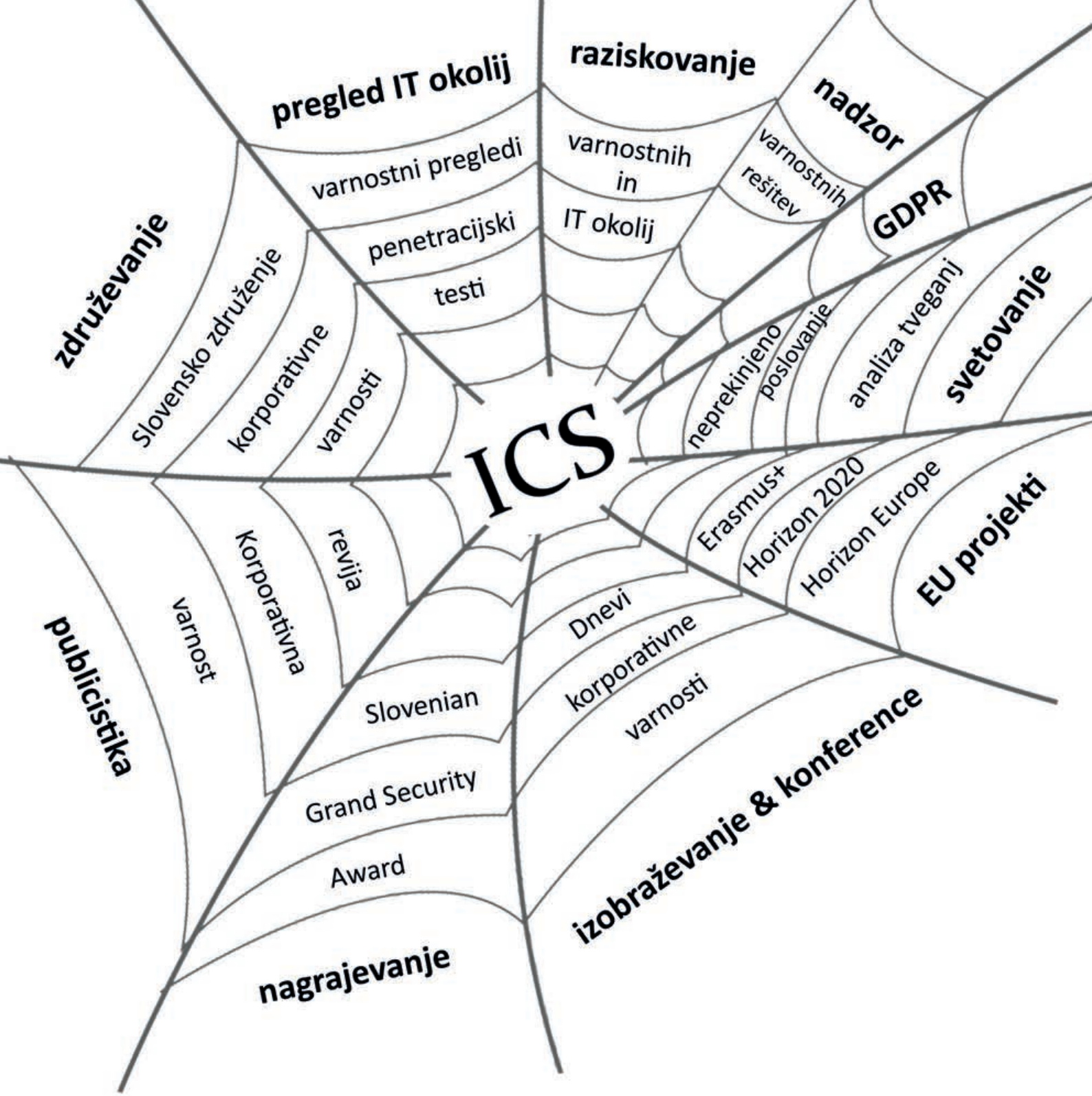
Med predstavitvami smo udeležencem zastavili nekaj vprašanj. Med njimi je bilo tudi naslednje: »*Kako bi prednostno razvrstili naslednja področja za razvoj novih standardov in politik za odpornost KI?*«, kjer je bilo možno izbirati med naslednjimi odgovori: (i) odgovornost in strukture upravljanja, (ii) javno-zasebno sodelovanje, (iii) centralizirana koordinacija, (iv) usklajene čezmejne dejavnosti, ter (v) raznolikost in vključenost. Udeleženci ankete so se strinjali (30% vseh glasov), da je usklajeno čezmejno sodelovanje s centralno koordinacijo ključnega pomena. V veliki večini (70% vseh glasov) so se udeleženci strinjali tudi, da bi morala biti odpornost KI ena izmed glavnih tem razprav na naslednjih evropskih parlamentarnih volitvah, ki bodo junija 2024.

Naslednji koraki

Dogodek smo zaključili s pregledom predlogov za bolj učinkovito sodelovanje med predstavniki vseh stebrov – Komisijo, organizacijami za standardizacijo ter EU projekti. Kot prvo nalogo smo si zadali pripravo skupnih priporočil Evropski komisiji za izboljšanje podpore EU projektom pri razumevanju (i) dolgoročne vizije in načrtov Komisije za krepitev odpornosti KI, (ii) vrzeli v obstoječih zakonih in standardih, ki bi jih EU projekti lahko pomagali nasloviti, ter (iii) rezultatov in izkušenj zaključenih EU projektov, ki lahko novim EU projektom služijo kot izhodišče za njihovo delo. ■

Evropski grozd za zaščito kritične infrastrukture (European Cluster for Securing Critical Infrastructures) je mreža raziskovalnih projektov, financiranih s strani Evropske komisije, ki naslavljajo izzive s področja fizične in kibernetske varnosti kritične infrastrukture (KI). ICS Ljubljana sodeluje v grozdu s tremi trenutno aktivni projekti in sicer CYBERSEAS, SUNRISE in ATLANTIS.

CyberSEAS ATLANTIS SUNRISE



ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

ISO 27001

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

DPO

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

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



NOVI PRISTOPI PREPREČEVANJA KORUPCIJE V DIGITALNI DOBI: VLOGA PROJEKTA CEDAR

Razvoj in vključitev naprednih tehnologij v javno upravo, kot so umetna inteligenca in strojno učenje, prinaša novo dobo transparentnosti in učinkovitosti v boju proti korupciji. V omenjenem projektu imajo slovenski partnerji še posebej pomembno vlogo. To dokazuje, kako je področje uvajanja novih tehnologij pomembno za strukturiranje ustrezne, na digitalnih rešitvah temelječe, družbe v Sloveniji.

V letošnjem letu je EU skozi raziskovalno-razvojni mehanizem izbrala in bo financirala pomemben projekt CEDAR (Common European Data Spaces and Robust AI for Transparent Public Governance). Projekt CEDAR je inovativen projekt, namenjen krepitvi transparentnosti in odgovornosti v evropski javni upravi. V obdobju, ko se Evropa sooča z vse večjimi izzivi v korupciji in pomanjkanju preglednosti, projekt CEDAR prinaša svež pristop k obvladovanju teh težav. Projekt se osredotoča na razvoj in uporabo sodobnih tehnologij, vključno z umetno inteligenco in strojnim učenjem. Cilj je zgraditi in deliti visokokakovostne baze podatkov, ki bodo vsebovale dragocene in uporabne informacije.

Projekt združuje multidisciplinarni pristop, ki vključuje pravo, etiko in družbene vede, s ciljem ustvarjanja neposrednih in merljivih učinkov na evropsko gospodarstvo, družbo in okolje. CEDAR s svojim inovativnim pristopom odpira nova obzorja v boju proti korupciji in zagotavljanju večje transparentnosti v javnem sektorju, kar obljublja pomembne spremembe v načinu delovanja javne uprave v 21. stoletju. V projektu sodeluje tudi pomembno število slovenskih partnerjev, ki prihajajo tako iz javnega kakor tudi zasebnega okolja. Slovenski konzorcij na projektu tvorijo Ministrstvo za digitalno preobrazbo, Ministrstvo za zdravje, Ministrstvo za notranje zadeve – Policija, Splošna bolnišnica Celje, tehnološki partner SNEP d.o.o. in Institut za korporativne varnostne študije, ki je tudi koordinator slovenskega pilota.

V središču projekta CEDAR je prizadevanje za inovativno obvladovanje korupcije in izboljšanje transparentnosti v javni upravi po vsej Evropi. Ta ambiciozni projekt se loteva te naloge z integracijo naprednih tehnologij in obsežnih podatkovnih zbirk.

Opis projekta CEDAR

V središču projekta CEDAR je prizadevanje za inovativno obvladovanje korupcije in izboljšanje transparentnosti v javni upravi po vsej Evropi. Ta ambiciozni projekt se loteva te naloge z integracijo naprednih tehnologij in obsežnih podatkovnih zbirk. Osrednja tema projekta CEDAR je upravljanje z velikimi količinami podatkov in izkoriščanje moči strojnega učenja za analizo in interpretacijo teh podatkov, kar omogoča bolj informirano in učinkovito odločanje v javni upravi.

V CEDAR so pilotne študije ključnega pomena, saj služijo kot testno okolje za preverjanje in demonstracijo učinkovitosti razvitih tehnologij in pristopov. Te študije potekajo v različnih evropskih državah, vključno z Italijo, Slovenijo in Ukrajino, kjer se osredotočajo na transparentno upravljanje sredstev. S tem praktičnim pristopom projekt zagotavlja, da

*avtor je član Slovenskega združenja korporativne varnosti

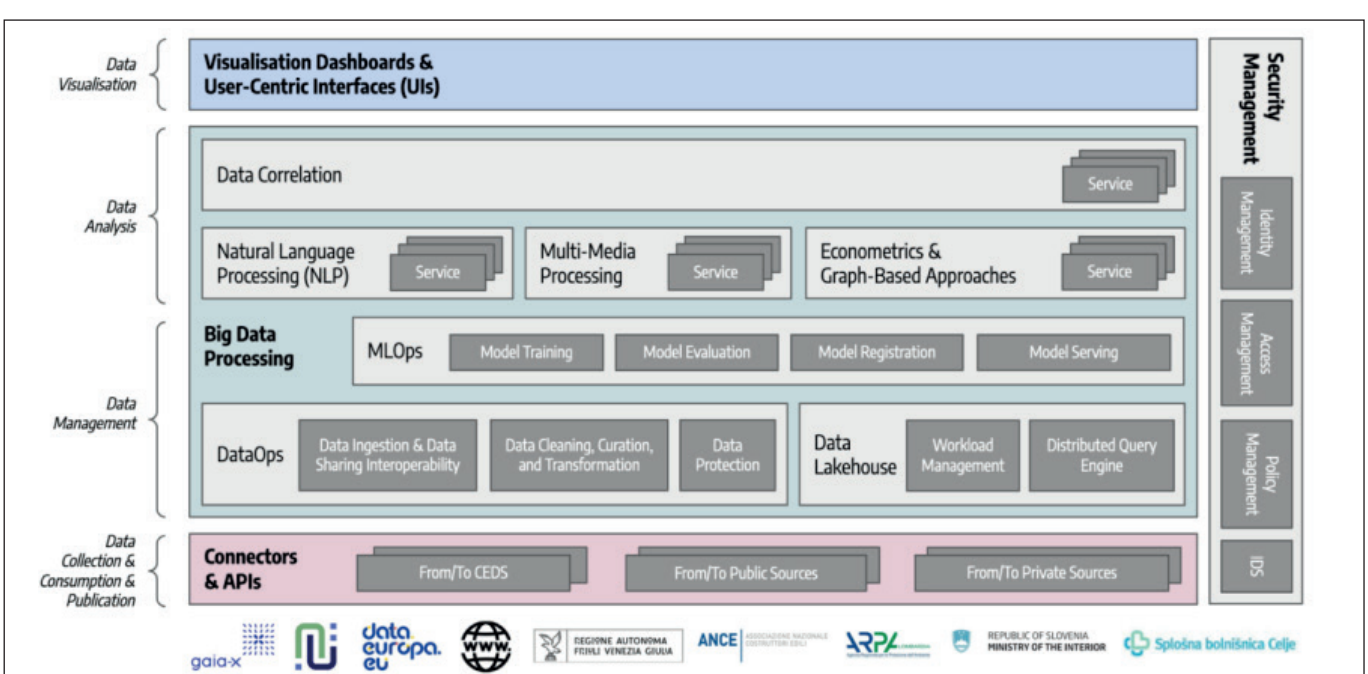


so tehnološke rešitve resnično prilagojene izzivom in potrebam realnega sveta.

Projekt CEDAR, kot že omenjeno, ne temelji zgolj na tehnoloških rešitvah, temveč upošteva tudi pravne, etične in družboslovne vidike. Ta multidisciplinarni pristop zagotavlja, da so tehnološke rešitve oblikovane in implementirane na način, ki spoštuje družbene norme in etična načela. S tem projekt CEDAR presega tradicionalne meje tehnoloških projektov in postavlja temelje za celovit pristop k reševanju družbenih izzivov.

Srce projekta CEDAR je uporaba najnovejših tehnoloških dosežkov, ki vključujejo napredno obdelavo podatkov in umetno inteligenco. Ta pristop omogoča temeljito analizo obsežnih informacij, s čimer se odpirajo vrata za globje razumevanje zapletenih vprašanj, s katerimi se sooča javna uprava. Takšna analitična moč je ključna za prepoznavanje in obdelavo skritih vzorcev ter trendov v podatkovnih zbirkah, kar bistveno prispeva k bolj premišljenemu in utemeljenemu procesu odločanja.

Poleg tega ima projekt CEDAR potencial za pomemben vpliv na evropsko gospodarstvo, družbo in okolje. S svojim poudarkom na transparentnosti in odgovornosti projekt prispeva k izboljšanju delovanja javne uprave, kar ima dolgoročne pozitivne učinke na družbo kot celoto.



Slika 1: Logična shema projekta

V odgovor na globalne izzive, kot so pandemija, konflikti, okoljske in energetske krize, se je povečalo nujno javno financiranje, kar je privedlo do ohlapnejših nadzornih mehanizmov in porasta vzorcev korupcije in goljufivih aktivnosti, ki imajo dolgoročne in pomembne negativne vplive na evropsko gospodarstvo, družbo, okolje in politiko.

Arhitektura na zgornji shemi vključuje povezovanje in API-je za pridobivanje podatkov iz različnih virov, podatkovno jezero za centralizirano shranjevanje, ter obdelavo in analizo podatkov. Predstavljeni so moduli za naravno obdelavo jezika, obdelavo večpredstavnostnih vsebin in različne metrične pristope. Varnostni sloj skrbi za zaščito podatkov skozi celoten cikel, od zbiranja do vizualizacije. Na koncu so podatki predstavljeni v uporabniku prijaznih nadzornih platformah za vizualizacijo, kar olajša razumevanje in sprejemanje ustreznih podlag za odločanje. Projekt združuje tehnologije DataOps in MLOps za upravljanje, modeliranje in dostavo podatkov, zagotavlja pa tudi orodja za analitiko in strojno učenje, ki so ključna za napredne uporabniške analize.

Poslanstvo projekta CEDAR

Projekt CEDAR, kot že omenjeno, se osredotoča na reševanje ključnih izzivov v javni upravi, s posebnim poudarkom na transparentnosti in boju proti korupciji. Vključuje napredne tehnologije in podatkovne analize, s ciljem ustvarjanja učinkovitejšega in odgovornejšega okolja v javnem sektorju.

Pilotne študije so razporejene med naslednjimi državami:
- Italija: Osredotoča se na upravljanje nacionalnih sredstev, predvsem tistih, ki so jih države dobile skozi mehanizem okrevanja po obdobju pandemije COVID-19. V tem primeru se bo predvsem usmerjalo v analizo tveganj, ki jih prinaša zloraba javnih sredstev s strani mafijskih organizacij.
- Slovenija: Projektna dejavnost se osredotoča na upravljanje javnih zdravstvenih sredstev. Slovenija ima med drugim pomembne izzive na področju korupcije v zdravstvu. Soočeni smo z odtekanjem javnih sredstev skozi različne oblike netransparentnih nakupov opreme in storitev.
- Ukrajina: Cilj je transparentno upravljanje tuje pomoči za obnovo države. Zaradi Ruske agresije na Ukrajino v državo priteka velika količina mednarodnih sredstev za pomoč in obnovo. V preteklem obdobju je bilo že javno izpostavljeno veliko korupcijskih izzivov neustreznega odtekanja denarja, ki ni bil porabljen za predviden namen.

Poslanstvo projekta CEDAR je oblikovanje in vzpostavitev napredne in vzdržne infrastrukture za obdelavo podatkov v javni upravi, ki se bo osredotočila na večjo transparentnost in odgovornost pri upravljanju z javnimi sredstvi v Evropi. Cilj projekta je zbrati, združiti, uskladiti, zaščititi ter deliti kakovostne in visoko vredne podatkovne nize, ki so ključni za zagotavljanje učinkovitega in odgovornega javnega upravljanja. Projekt se bo poslužil inovativnih in skalabilnih metodologij, algoritmov in programskih orodij, ki bodo omogočali učinkovito upravljanje z velikimi podatki in operacijami strojnega učenja (DataOps, MLOps). CEDAR bo preizkušal nove podatkovne nize in tehnologije v boju proti korupciji, s čimer se bo uskladil s strateškimi prednostnimi nalogami EU (digitalizacija, gospodarstvo, demokracija) in aktivno promoviral rezultate po vsej Evropi za zagotavljanje njihovega sprejetja in dolgotrajne uporabe ter generiranje pozitivnih, oprijemljivih in neposrednih učinkov.

V odgovor na globalne izzive, kot so pandemija, konflikti, okoljske in energetske krize, se je povečalo nujno javno financiranje, kar je privedlo do ohlapnejših nadzornih mehanizmov in porasta vzorcev korupcije in goljufivih aktivnosti, ki imajo dolgoročne in pomembne negativne vplive na evropsko gospodarstvo, družbo, okolje in politiko. Namen pa je skozi projekt razviti tudi metode in orodja za lažjo digitalizacijo obstoječih podatkov v javni upravi. Projekt se bo osredotočil na združevanje, usklajevanje in standardizacijo različnih podatkovnih virov, s čimer bo omogočil ustvarjanje novih visokokakovostnih in vrednih zbirk obsežnih podatkov.

Zaključek

Projekt CEDAR stoji na presečišču med tehnološko inovativnostjo in družbeno odgovornostjo, s ciljem oblikovati bolj transparentno in odgovorno prihodnost v javni upravi. Z združevanjem strokovnjakov iz različnih disciplin in uporabo najnovejših tehnoloških rešitev, CEDAR ne le naslavlja trenutne izzive v upravljanju in integriteti, ampak tudi postavlja nov standard za prihodnje generacije v upravljanju javnih sredstev. S svojim pristopom projekt odpira vrata za boljše razumevanje in obvladovanje kompleksnih družbenih izzivov, ki so pred nami, in s tem kaže pot k ustvarjanju bolj transparentne in odgovorne javne uprave za vse evropske državljane. ■

"CEDAR project has received funding by the European Union's Horizon Europe, under grant agreement no 101135577."



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 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 1828

DPO

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

15. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 13. - 14. MAJ 2024



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI