Korporativna varnost

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

Letnik 2025, maj • št. 38

Ministrstvo za notranje zadeve ima ključno povezovalno vlogo pri zagotavljanju odpornosti družbe
mag. Boštjan Poklukar, minister za notranje zadeve

Svečana podelitev prestižnih nagrad “Slovenian Grand Security Awards”
Brdo pri Kranju, 19-20. maj 2025

VAŠA 360° VARNOST 365 DNI V LETU

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

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

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

TelekomSlovenije
Vedno na boljše.

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:
maj 2025

Izvod revije je brezplačen

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

ISSN 2232-6170

Pred nami so Dnevi korporativne varnosti, ki predstavljajo praznik, festival korporativne varnosti in srečanje vseh, ki se v svojem profesionalnem okolju ukvarjajo z zahtevnimi procesi obvladovanja varnostnih tveganj. Varnostno okolje je postalo tako zahtevno in kompleksno, da upravljanje in obvladovanje tveganj ni več mogoče s parcialnimi pristopi. Celovitost pristopov in spoznanje, da lahko samo z vključevanjem vseh deležnikov v proces zagotavljanja varnosti in neprekinjenosti delovanja ključnih družbenih sistemov zagotovimo ustrezne rezultate, ki bodo zagotavljali pravo raven odpornosti družbe kot celote. V tem okviru je korporativna varnost kot proces postala neločljiv del tega celovitega sistema. Na tem mestu bomo izpostavili misel, ki je bila v tokratni številki revije zapisana pri prispevku predsednika Slovenskega združenja za korporativno varnost, da »korporativna varnost kot dejavnost ne sme zamuditi tega »zvezdniškega trenutka«, da se v vsem svojem obsegu delovanja pokaže kot eden izmed ključnih dejavnikov za zagotavljanje družbe. Korporativna varnost ima priložnost in odgovornost, da postane osrednji steber varnosti sodobne družbe. S svojim celostnim razumevanjem delovanja organizacij, sposobnostjo hitrega odziva in strateškega povezovanja lahko postane ključni igralec pri gradnji odporne, varne in stabilne prihodnosti.«

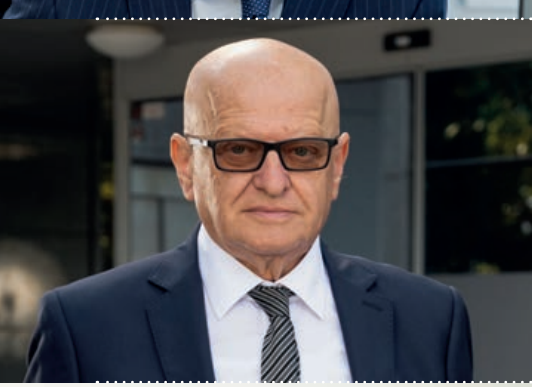
Odpornost je v zadnjem obdobju postala tista ključna vrednota, kateri na vseh nivojih namenjamo izredno veliko pozornost. Temu smo tudi v tokratni konferenčni številki revije namenili ključno pozornost in je vezna nit tokratne vsebine. Izpostavljeni strateški voditelji skozi ključna sporočila odkrivajo tiste pomembne korake, ki se ravno na področju zagotavljanja odpornosti celotne družbene skupine izvajajo v posameznih podsistemih.

Z izborom intervjujev in prispevkov smo omogočili vpogled v strateške perspektive ključnih odločevalcev ter hkrati v konkretne izkušnje strokovnjakov, ki izvajajo varnostne procese na operativni ravni. Poudarjamo, da je ravno preplet strateškega razmišljanja in operativne izvedbe ključen za oblikovanje učinkovitih varnostnih sistemov, ki bodo zmožni uspešno odgovarjati na dinamične spremembe v varnostnem okolju.

Poleg intervjujev smo v tokratni številki želeli celovito nasloviti tudi širši nabor aktualnih strokovnih vsebin, ki so nepogrešljive za učinkovito upravljanje sodobnih varnostnih tveganj. Predstavljene vsebine odražajo aktualna dogajanja na področju korporativne varnosti in so zasnovane tako, da bodo strokovni javnosti v podporo pri iskanju ustreznih rešitev, oblikovanju novih pristopov ter razvoju strateških usmeritev za doseganje večje odpornosti organizacij.

Prepričani smo, da bo predstavljena vsebina bralkam in bralcem nudila dodatno strokovno podporo ter jih spodbudila k nadaljnjemu razmisleku o pomenu usklajenega, sistematičnega in celostnega pristopa k obvladovanju varnostnih tveganj. S tem si želimo prispevati k dvigu splošne varnostne kulture ter krepitvi odpornosti organizacij in družbe kot celote v sodobnem ter izzivov polnem varnostnem okolju. V uredništvu revije upamo, da boste tudi v 38. številki revije našli ustrezne strokovne vsebine, ki vam bodo pomagale pri vašem zahtevnem delu.

izr. prof. dr. Denis Čaleta
Glavni urednik



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

INTERVJU
mag. Boštjan Poklukar, minister za notranje zadeve

MINISTRSVO ZA NOTRANJE ZADEVE IMA KLJUČNO POVEZOVALNO VLOGO PRI ZAGOTAVLJANJU ODPORNOSTI DRUŽBE

Zagotavljanje notranje varnosti je ključna komponenta nacionalno varnostnih sistemov. Kompleksnost varnostnih tveganj v luči zagotavljanja ustrezne odpornosti širše družbene skupnosti zahteva dobro delujočo koordinacijo celega niza deležnikov, ki imajo svoj vpliv na zagotavljanje varnosti. V tem okviru ima Ministrstvo za notranje zadeve ključno koordinativno in integrativno vlogo za vključujoče delovanje navedenih subjektov. O novih pristopih in bodočih korakih soočanja s temi izzivi smo se pogovarjali z ministrom za notranje zadeve mag. Boštjanom Poklukarjem.

V zadnjem obdobju je zelo aktualna tema zagotavljanje odpornosti v Republiki Sloveniji. Kako vi vidite ta pomemben proces na področju notranje varnosti?

Varnostne razmere v Sloveniji se trenutno ocenjujejo še vedno kot dobre in stabilne. Moramo pa se zavedati, da je naša država del širšega mednarodnega varnostnega okolja, ki postaja vedno bolj zahtevno.

Ministrstvo za notranje zadeve z organoma v sestavi (Policijo in Inšpektoratom Republike Slovenije za notranje zadeve) je nosilec podsistema notranje varnosti v nacionalno varnostnem sistemu Republike Slovenije. Zaradi dokaj nestabilnih varnostnih razmer v regiji in svetu si prizadevamo za povečanje odpornosti na področju notranje varnosti, zlasti delovanja Policije in njenega sistema v kriznih razmerah. To velja tako za zakonodajo, ki mora še naprej zagotavljati izvajanje policijskih pooblastil v spremenjenih varnostnih razmerah (bodisi ob naravnih in drugih nesrečah bodisi v krizi, izrednem stanju in vojni), kot za izvajanje ustreznih ukrepov za

> Lastno in skupno varnost ter obrambo gradimo preudarno in na različne načine. Tu imam v mislih zelo širok spekter različnih, a povezanih dejavnosti v okviru odpornosti države pred vsemi oblikami tveganj in groženj. Gradimo torej odporno, robustno in hkrati prilagodljivo nacionalno varnost.

*avtor je član Slovenskega združenja korporativne varnosti

zagotovitev kibernetske varnosti, preprečevanje terorizma in ekstremizma ter drugih oblik ogrožanja.

Zagotavljanje odpornosti v najširšem smislu pomeni vzpostavitev takih varnostnih struktur, ki so sposobne soočanja in prilagoditve sistema na negativne preizkušnje ali spremenjene varnostne razmere, ki se lahko zgodijo. Te spremembe na področju varnosti, tako mednarodne kot nacionalne in notranje, se izvajajo na podlagi preteklih izkušenj, aktualnih dogodkov in predvidenih varnostnih scenarijev.

Odpornost pa lahko krepimo samo na podlagi pravočasne zaznave in spremljanja groženj, izvajanja preventivnih aktivnosti, z ustreznim načrtovanjem odzivanja ter zadostno kadrovsko (tako številčno kot strokovno) in materialno popolnitvijo, usposabljanjem in opremljanjem za delo v spremenjenih razmerah.

Za zagotavljanje sistemskih korakov za odpornost celotne države je ključnega pomena sodelovanje in povezovanje z ostalimi družbenimi podsistemi. Kako čimbolj učinkovito zagotoviti ustrezno sodelovanje področja notranje varnosti z ostalimi podsistemi predvsem v smeri iskanja določenih sinergij?

Ministrstvo za notranje zadeve v okviru nacionalno varnostnega sistema Republike Slovenije izjemno dobro sodeluje z ostalima dvema podsistemoma – obrambnim podsistemom in podsistemom varstva pred naravnimi in drugimi nesrečami.

Ključnega pomena je usklajeno načrtovanje ukrepov, sodelovanje med resorji in razumevanje delovanja drug drugega. Usklajenost delovanja se nenehno preverja z vajami na državni, regijski in lokalni ravni, občasno tudi mednarodni ravni, tako v obrambnem sistemu kot v sistemu varstva pred naravnimi in drugimi nesrečami. Naša prednost je majhnost države, zato povezanost in prepletenost sistemov omogoča boljše poznavanje nalog in področij delovanja drugega. Seveda pa pri tem ne gre za sodelovanje izključno s podsistemi nacionalne varnosti, temveč tudi z vsemi drugimi deležniki, ki vsak na svojem področju zagotavljajo izvajanje dejavnosti iz svoje pristojnosti, da lahko država deluje neprekinjeno brez posebnih nihanj. Lastno in skupno varnost ter obrambo gradimo preudarno in na različne načine. Tu imam v mislih zelo širok spekter različnih, a povezanih dejavnosti v okviru odpornosti države pred vsemi oblikami tveganj in groženj. Gradimo torej odporno, robustno in hkrati prilagodljivo nacionalno varnost.

V zadnjem obdobju ste zelo jasno izrazil stališče, da je prišel čas, ko procesa, da bodo določena mestna redarstva prevzela delo in pristojnosti tako imenovane mestne policije, ni več mogoče ustaviti. Nam lahko zaupate glavne razloge za odločitev razvoja notranje varnosti in tesnejšega sodelovanja med Policijo in mestnimi redarstvi?

Sam kot minister za notranje zadeve in tudi na ministrstvu se zavzemamo za krepitev suplementarnih deležnikov na področju varnosti. To velja še zlasti na področjih, kjer policija v sodobnem času ne more biti vseprisotni represivni organ, in je glede na materialnopravno urejanje določenih pravnih področij z vidika načela zakonitosti in načela učinkovitosti smiselna ter nujna vključitev občinskih in mestnih redarstev. Občinska in mestna redarstva so eden izmed deležnikov, ki v sistemu notranje varnosti v lokalni skupnosti zagotavljajo

notranjo varnost. Nenazadnje sta med cilji Resolucije o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2024–2028 tudi cilja, da se vzpostavi proaktivno sodelovanje vseh deležnikov na področju varnosti z lokalno skupnostjo oziroma vzpostavi ustrezna partnerstva za doseganje skupnih ciljev. Torej še večjo varnost.

Že zdaj imajo ti varnostni deležniki svoje pristojnosti pri izvrševanju področne zakonodaje. Glede na razvoj lokalne samouprave in celotne družbe bo treba še okrepiti vlogo redarjev, saj mora biti delovanje policije prvenstveno usmerjeno v področja varnosti, ki so po vsebini najbolj zahtevna z vidika vzdrževanja varnosti, preprečevanja ogrožanja varnosti in pregon kršiteljev. Prvi pogoj pri krepitvi pristojnosti občinskih in mestnih redarjev pa seveda ostaja strogo spoštovanje načel zakonitosti in učinkovitosti.

Slovenija je ena redkih držav, ki področja protiterorizma nima jasno opredeljenega v enem krovnem zakonu, temveč se določeni nastavki, naloge in pristojnosti organov razdeljeni skozi več področnih zakonov. Menite, da je prišel čas za sprejem tega zakona in kakšne korake nameravate v tej smeri podvzeti na Ministrstvu za notranje zadeve?

Moramo se zavedati, da je na področju varnosti konec romantike. To je dejstvo, ki ga moramo sprejeti. Tudi pri nas obstaja določena stopnja teroristične ogroženosti države kot posledica vpetosti Slovenije v mednarodni prostor, članstva v EU in schengenskega območja (spomnite se le na nedavni teroristični napad v naši neposredni bližini v Beljaku v Avstriji). S tehnološkim razvojem v ospredje vse bolj prihajajo hibridne oblike ogrožanj, kibernetska ogrožanja, pa tudi dezinformacije. To vodi do destabilizacije sistemov in celo države. Sam sem prepričan, da bo prišel čas, ko bo tudi Republika Slovenija dobila protiteroristični zakon. Sodobnim in novim oblikam groženj se je namreč treba nenehno prilagajati na različne načine ter odpornost Republike Slovenije, njene družbe in njenih državnih institucij še povečati, da bi se lahko spopadli s prihodnjimi krizami in katastrofami.

Kritična infrastruktura in njeno neprekinjeno delovanje je ključnega pomena za delovanje države in družbene skupnosti. V tem segmentu imajo službe korporativne varnosti v teh organizacijah zelo pomembno vlogo pri zagotavljanju varnosti in neprekinjenosti delovanja te infrastrukture. Kako ocenjujete raven trenutnega sodelovanja med Policijo in predstavniki korporativne varnosti? Kaj bi lahko še naredili, da bi to delovanje dvignili še na višji sistemski nivo?

Zavzemamo se za to, da damo večji poudarek javno-zasebnemu partnerstvu. S prenosom določenih pristojnosti varovanja na zasebno varnostne subjekte se je varnostni sistem že nekoliko razbremenil. Menim, da bi država morala, še posebej v spremenjenih varnostnih razmerah, varnostne družbe in varnostnike ustrezno opredeliti kot ene izmed ključnih nosilcev dopolnjevanja izvajanja varnostnih nalog države.

Zakon o zasebnem varovanju določa zavezance za obvezno organiziranje varovanja, kar je izrednega pomena za zagotavljanje varnosti v podjetjih, objektih in na območjih, kjer imajo lahko nekateri nepredvidljivi in neljubi dogodki vpliv tudi na nacionalno varnost. Korporativna varnost ima v tem kontekstu pomembno vlogo, saj gre za upravljanje varnostnih tveganj znotraj podjetij, vključno s fizičnim in tehničnim varovanjem, varovanjem pomembnih informacij in podatkov ter preprečevanjem morebitnih groženj. Sodelovanje in usklajeno delovanje med zakonskimi obveznostmi na področju zasebnega varovanja in delovanjem korporativne varnosti omogoča podjetjem, da učinkovito obvladujejo varnostna tveganja.

Sodobnim in novim oblikam groženj se je namreč treba nenehno prilagajati na različne načine ter odpornost Republike Slovenije, njene družbe in njenih državnih institucij še povečati, da bi se lahko spopadli s prihodnjimi krizami in katastrofami.

Pri zagotavljanju varnosti kritične infrastrukture je zlasti pomembno, da dosledno uresničujemo cilje, opredeljene v vseh stebrih, pomembnih za učinkovito omejevanje terorizma. Pri tem je ključno, da posameznikom preprečimo dostop do sredstev, ki bi jih lahko uporabili za izvedbo napada, zagotovimo zaščito pred neposrednim ogrožanjem življenja in premoženja ljudi ter kritične infrastrukture.

Sodelovanje s predstavniki korporativne varnosti je torej ključnega pomena. Na še višjo raven ga lahko dvignemo z izvedbami in sodelovanjem pri vajah po različnih scenarijih, kjer se preizkusijo in ugotovijo pomanjkljivosti sistemov in se na tak način poskrbi za dodatne varnostne mehanizme.

Kibernetska tveganja so postala ena od zelo izpostavljenih v modernem varnostnem okolju. Menite, da lahko določeno znanje, ki je razvito v segmentih korporativne varnosti, dodatno pomaga Policiji pri raziskovanju določenih kaznivih dejanj s tega področja?

V zadnjih letih je zaznan izrazit porast kriminalitete, povezane s kibernetskim okoljem. Vse bolj pogosto so napadeni sistemi kritične infrastrukture, državnih ustanov in večjih gospodarskih družb. Za obravnavo tovrstnih kaznivih dejanj ima Policija že vrsto let primerno usposobljene in tehnično opremljene kadre. Zaradi specifičnosti, raznolikosti in mednarodnega elementa kibernetske kriminalitete Policija intenzivno sodeluje z ostalimi pristojnimi institucijami doma in v tujini.

V fazi zbiranja obvestil je dobrodošlo določeno specifično znanje, ki je razvito v segmentih korporativne varnosti, in v predkazenskem postopku dodatno pomaga Policiji izslediti storilca kaznivega dejanja. Specifična znanja, ki jih posedujejo posamezni strokovnjaki v segmentih korporativne varnosti na področju prepoznave in zaznave kibernetskih tveganj, lahko v tem oziru doprinesejo in pomagajo Policiji izbrati ustrezne ukrepe in dejanja, ki imajo lahko bolj daljnosežen vpliv na izvedbo nadaljnjega kazenskega postopka.

Seveda pa tudi varnostni sistemi, ki so razviti in vpeljani v posameznih organizacijskih okoljih, lahko bistveno pripomorejo pri omejevanju kibernetskih tveganj, zlasti ko govorimo o ozaveščanju o nevarnostih spletnega okolja. Po drugi strani pa tudi tehnološke rešitve, ki omejujejo kibernetska tveganja, lahko bistveno pripomorejo pri raziskovanju kaznivih dejanj,

Sodelovanje s predstavniki korporativne varnosti je torej ključnega pomena. Na še višjo raven ga lahko dvignemo z izvedbami in sodelovanjem pri vajah po različnih scenarijih, kjer se preizkusijo in ugotovijo pomanjkljivosti sistemov in se na tak način poskrbi za dodatne varnostne mehanizme.

še zlasti pri ustreznem beleženju in zavarovanju digitalnih dokazov.

Problem ustrezno kompetenčnih kadrov je izpostavljen tudi na področju notranje varnosti. Kakšni so vaši načrti za zagotavljanje dovolj velikega obsega potrebnih kadrovskih potencialov za normalno delovanje področja notranje varnosti?

Kadrovska podhranjenost je prisotna na ravni celotnega nacionalno varnostnega sistema, ne samo na področju notranje varnosti.

Na Ministrstvu za notranje zadeve se stalno trudimo pridobiti in usposobiti nov kader. Naše delo že kaže pozitivne rezultate, saj imamo trenutno prijavljenih veliko kandidatov za šolanje za poklic policista. Prav tako povečujemo zmogljivosti v okviru povečanja števila pomožnih policistov. Policija je nedavno z Zavodom Republike Slovenije za zaposlovanje podpisala dogovor o sodelovanju na področju aktivne politike zaposlovanja v Policiji in promocije poklica policist.

Vsekakor pa je treba korake naprej delati tudi pri infrastrukturi. Tu imam v mislih predvsem nadaljnjo posodobitev obstoječih zmogljivosti Policijske akademije – kjer na primer že poteka obnova strelišča – in tudi drugih vadbenih centrov za usposabljanje vseh deležnikov nacionalno varnostnega sistema.

Lahko tukaj iščemo kakšne sinergije ali skupne nastope med področjema notranje varnosti in korporativno varnostjo?

Učinkoviti bomo le ob sodelovanju Policije in organizacij za zagotavljanje varnosti ter gospodarskih družb. Cilj vseh deležnikov mora biti zagotavljanje varnosti v družbi kot celoti. Izmenjava izkušenj in informacij, predvsem specifičnih znanj o varnostnih tveganjih v poslovnih okoljih, zagotovo prispeva k boljšemu razumevanju in obvladovanju teh tveganj.

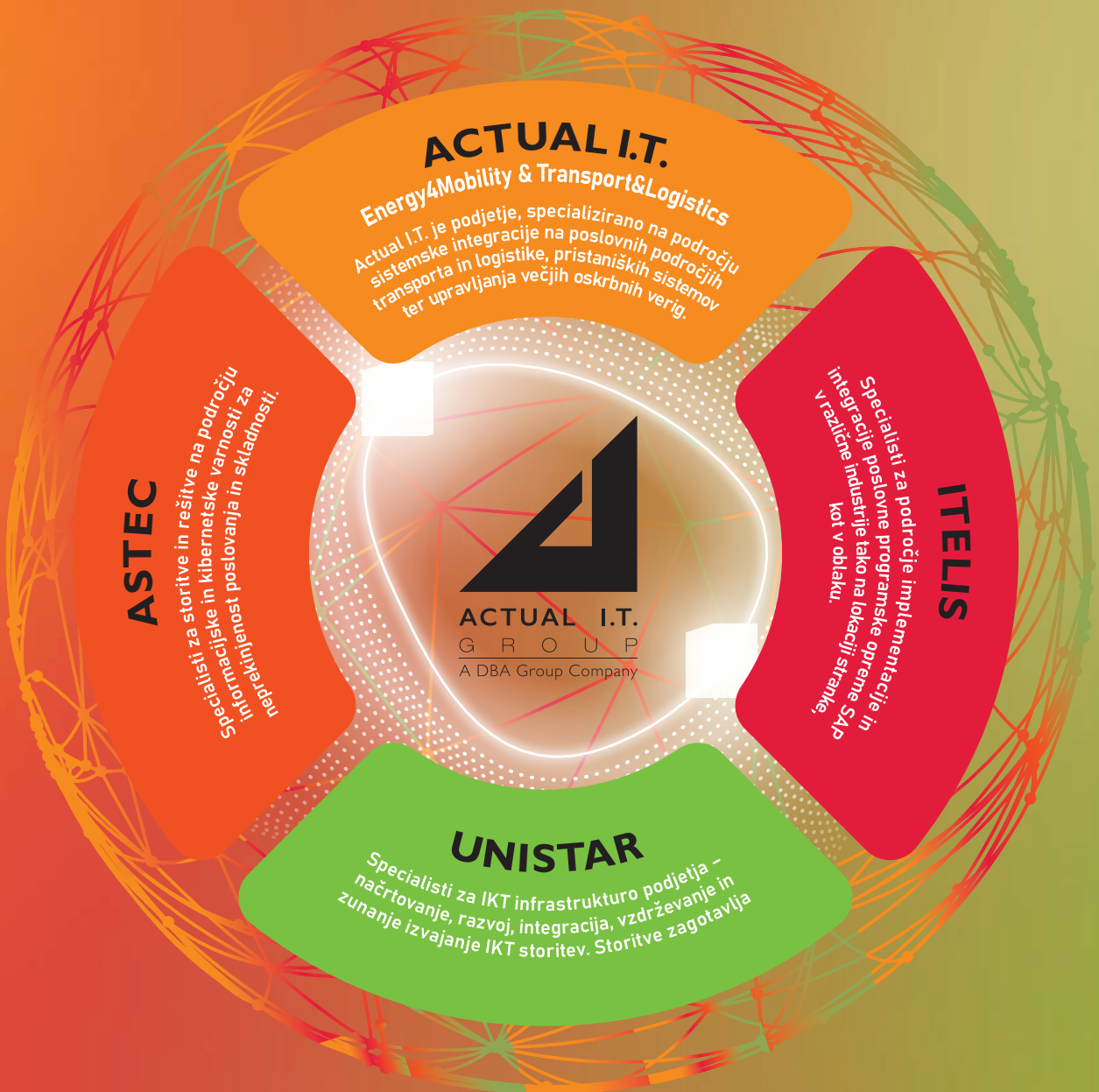
Zagotavljanje varnosti kritične infrastrukture torej temelji predvsem na tesnem javno-zasebnem sodelovanju. Za to je treba zagotoviti ustrezno mero zaupanja, izmenjavo izkušenj, dobrih praks ter strateško in operativno pomembnih podatkov za zagotavljanje učinkovite preventive. Pri tako tehničnem oziroma kompleksnem področju, ki zahteva visoko usposobljene strokovnjake, lahko sodelovanje vsekakor doprinese sinergije in posledično višjo stopnjo odpornosti in zaščite pred različnimi grožnjami.

Slovensko združenje je najpomembnejša nacionalna varnostna platforma za sodelovanje in izmenjavo dobrih praks v katerega so poleg organizacij gospodarskega sektorja vključenih tudi veliki število ključnih državnih organov. Menite, da je že dozorel čas, da se nam uradno pridruži tudi MNZ?

Poleg zavedanja, da smo za varnost odgovorni vsi, je nujno tudi spoznanje, da je nihče ne more obravnavati ločeno. Na Ministrstvu za notranje zadeve pozdravljamo takšno sodelovanje pri vprašanju varnosti, ki se ga je treba lotevati celovito z združevanjem strokovnjakov z različnih področij. Policija je prisotna v teh znanstvenih in strokovnih pobudah. Prepričani smo, da bodo tudi takšne pobude pripomogle k ohranjanju varnega življenjskega okolja, tako prebivalcev Republike Slovenije kot širše regije.

Celovito zagotavljanje varnega življenjskega okolja, v katerem lahko svobodno živimo, ustvarjamo in rastemo kot civilizacija, moramo v času globalizacije razumeti kot vrednoto, katere ohranjanje je odvisno od vseh nas. Odgovornost zanjo se začne na ravni posameznika in njegovega moralnega imperativa, ki ga vodi pri dejanjih. Nadaljuje se pri odgovornem in strokovnem korporativnem upravljanju podjetij in organizacij, ki skupaj s pristojnimi službami, tudi Policijo, iščejo napredne varnostne rešitve za svoje nemoteno delovanje. Nenazadnje pa odgovornost za zagotavljanje varnosti zadeva tudi najvišje odločevalce, ki na ravni držav, nadnacionalnih institucij in mednarodne skupnosti sprejemajo odločitve, pomembne za vse nas in prihodnje generacije. ■

Foto: arhiv Ministrstva za notranje zadeve RS



ACTUAL I.T. UNISTAR PRO astec ITELIS

www.actual-it.si

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

INTERVJU
mag. Matej Tonin, evropski poslanec

ZAGOTAVLJANJE ODPORNOSTI EVROPSKE DRUŽBE

V luči vseh geostrateških varnostnih izzivov, s katerimi se sooča EU, zagotavljanje odpornosti postaja ena izmed najbolj izpostavljenih tematik in izzivov. V luči, da je mag. Tonin postal predsedujoči v pomembni parlamentarni medskupini, ki med drugim v osnovi naslavlja tudi izzive na področju zagotavljanja varnosti in odpornosti, smo izkoristili to priložnost za podrobnejši pogovor s slovenskim evropskim poslancem.

Najprej nam dovolite, da vam še enkrat čestitamo za prevzem pomembne vodilne funkcije v parlamentarni medskupine za varnejšo in odpornejšo Evropo. Nam lahko zaupate kaj bo glavno poslanstvo omenjene skupine?

Hvala za čestitke. Medskupina za varnejšo in odpornejšo Evropo bo imela osrednjo vlogo pri oblikovanju bolj avtonomne, usklajene in učinkovite evropske strategije za obvladovanje kriz. Naraščajoče naravne nesreče in geopolitične grožnje jasno kažejo, da Evropa potrebuje močnejšo odpornost na vseh ravneh – od lokalnih skupnosti do evropskih institucij. Naš cilj je okrepiti krizno upravljanje, vlagati v podnebno odporno infrastrukturo ter zagotoviti ustrezno podporo tistim, ki ob nesrečah prvi posredujejo, zlasti prostovoljnim gasilcem.

Medskupina bo združevala evropske poslance, strokovnjake in ključne deležnike, da skupaj oblikujemo rešitve, ki bodo povečale varnost Evropejcev. Pri tem ne gre le za odzivanje na krize, temveč za proaktivno pripravo in krepitev evropske solidarnosti. Naš cilj je jasen: Evropa mora biti pripravljena, odporna in sposobna zaščititi svoje ljudi v času preizkušenj.

Naraščajoče naravne nesreče in geopolitične grožnje jasno kažejo, da Evropa potrebuje močnejšo odpornost na vseh ravneh – od lokalnih skupnosti do evropskih institucij. Naš cilj je okrepiti krizno upravljanje, vlagati v podnebno odporno infrastrukturo ter zagotoviti ustrezno podporo tistim, ki ob nesrečah prvi posredujejo, zlasti prostovoljnim gasilcem.

Vaš izbor za vodenje tega pomembnega telesa predstavlja priznanje vam in Sloveniji je pa verjetno tudi svojevrsten izziv in obveznost?

Gre za pomemben izziv, saj so odpornost, krizno upravljanje in civilna zaščita ključni stebri varne in stabilne Evrope. Slovenija na tem področju že igra aktivno vlogo, zdaj pa imamo priložnost, da svoj prispevek še okrepimo in soustvarjamo evropske rešitve. Medskupina bo pomemben glas pri zagotavljanju, da ta vprašanja ostanejo na vrhu politične agende, in da Evropa postane bolje pripravljena na prihodnje preizkušnje. To odgovornost sprejemam z največjo resnostjo in trdno zavezanostjo k varnejši, odpornejši ter bolj povezani Evropi.

*avtor je član Slovenskega združenja korporativne varnosti

Katere bodo tiste prioritetne teme, ki jih boste dali v ospredje prvih korakov dela?

V medskupini smo opredelili štiri ključna področja, s katerimi želimo okrepiti evropsko odpornost in pripravljenost na krize. Prvič, povečati moramo vključenost posameznikov v krizno odzivanje, pri čemer bomo posebno pozornost namenili vlogi prostovoljnih gasilcev in drugih prvih posredovalcev v primeru nesreč. Njihovo delo je nepogrešljivo, a pogosto premalo cenjeno, zato si bomo prizadevali za boljšo podporo, zaščito in ustrezno priznanje njihovega prispevka. Prav tako želimo vključiti več državljanov – še posebej mladih – v sisteme civilne zaščite. Drugič, Evropa potrebuje bolj usklajeno strategijo kriznega upravljanja. To pomeni vlaganje v odpornejšo infrastrukturo, boljšo pripravljenost lokalnih skupnosti in učinkovitejše ukrepanje ob naravnih nesrečah ter drugih kriznih situacijah. Tretjič, ključna prioriteta bo krepitev zmogljivosti evropske civilne zaščite. Zmanjšati moramo odvisnost od zunanjih virov, hkrati pa podpreti evropsko industrijo pri proizvodnji ključnih sredstev za krizno odzivanje. Okrepiti želimo tudi koordinacijo med državami, da bodo mehanizmi odzivanja hitrejši in učinkovitejši. Četrtič, osredotočili se bomo na preprečevanje katastrof in izboljšanje mednarodnega sodelovanja. Ključno je nadgraditi sisteme zgodnjega opozarjanja in omogočiti boljše izmenjevanje znanja ter dobrih praks med državami članicami. Le s proaktivnim pristopom lahko zagotovimo, da bo Evropa pripravljena na prihodnje izzive.

Glede na to, da na odpornost širše družbene skupnosti ne vplivajo samo naravne nesreče, nam prosim zaupajte, ali boste določen del tematike posvečali tudi odpornosti delovanja kritične infrastrukture in posebej izpostavljenim kibernetskimi tveganjem?

Seveda! Glavni cilj naše medskupine je okrepiti evropsko odpornost in pripravljenost na krize, pri čemer ima zaščita kritične infrastrukture, še posebej pred kibernetskimi grožnjami, ključno vlogo. Kibernetski napad, ki je poleti 2022 ohromil delovanje nujnih služb slovenske Uprave za zaščito in reševanje, je jasen opomin na tveganja, s katerimi se soočamo. Danes je naša družba močno odvisna od digitalne infrastrukture – od zdravstvenega sistema in energetike do nujnih služb. Vsaka motnja, bodisi zaradi kibernetskega napada ali kaskadnih okvar, lahko povzroči resne posledice za varnost in delovanje osnovnih storitev. Naraščajoče število napadov na ključne sektorje kaže na nujnost preventivnih ukrepov in vzpostavitve zmogljivosti za hitro odzivanje.

Gre za pomemben izziv, saj so odpornost, krizno upravljanje in civilna zaščita ključni stebri varne in stabilne Evrope. Slovenija na tem področju že igra aktivno vlogo, zdaj pa imamo priložnost, da svoj prispevek še okrepimo in soustvarjamo evropske rešitve.

Danes odpornost ne pomeni zgolj hitrega odzivanja na naravne nesreče, temveč tudi zagotavljanje, da se tako fizični kot digitalni sistemi lahko učinkovito obnovijo po vsakršni krizi. Evropa mora biti pripravljena na vse oblike groženj, saj je stabilnost naših digitalnih omrežij enako pomembna kot varnost naše fizične infrastrukture.

V tem okviru se bomo osredotočili na tri ključne cilje: prvič, spodbujanje razprave o kibernetski varnosti v kontekstu kriznega upravljanja; drugič, krepitev naložb v varnostno infrastrukturo, ki bo sposobna prenesti sodobne grožnje; in tretjič, izboljšanje čezmejnega sodelovanja med državami EU pri obvladovanju kibernetskih tveganj. Prav tako vidimo velik potencial v prihajajočih tehnologijah, kot sta umetna inteligenca in real-time nadzor, ki lahko močno prispevata k izboljšanju kibernetske odpornosti ter nemotenemu delovanju ključnih sistemov med krizami.

Danes odpornost ne pomeni zgolj hitrega odzivanja na naravne nesreče, temveč tudi zagotavljanje, da se tako fizični kot digitalni sistemi lahko učinkovito obnovijo po vsakršni krizi. Evropa mora biti pripravljena na vse oblike groženj, saj je stabilnost naših digitalnih omrežij enako pomembna kot varnost naše fizične infrastrukture.

V zadnjem obdobju je bilo na ravni EU sprejetih cel niz pomembnih direktiv na področjih odpornosti kritične infrastrukture, kibernetske varnosti, umetne inteligence in drugih povezanih področij. Iz držav pa so začeli prihajati signali, da je obseg normativnega področja preobsežen za tako kratko obdobje, in da bi države v prihodnosti potrebovale določeno obdobje za ustrezno integracijo teh korakov brez sprejemanja novih aktov na ravni EU. Kakšni so vaši pogledi in izkušnje glede teh procesov implementacije?

To je popolnoma razumljivo. Nedavne direktive EU o kibernetski varnosti, odpornosti kritične infrastrukture in umetni inteligenci so pomembni koraki h krepitvi naše kolektivne varnosti. Kljub temu je naravno, da so nekatere države članice zaskrbljene glede hitrosti teh sprememb in izzivov, ki bodo nastali pri njihovi implementaciji. Oblikovanje kibernetske odpornosti ne zahteva zgolj močne politične volje, temveč tudi zmožnost učinkovitega prilagajanja. EU državam članicam pri upravljanju tega prehoda zagotavlja podporo in pomoč npr. v obliki ENISA vodenja, certificiranja kibernetske varnosti in finančnih programov, kot so Digitalna Evropa in Obzorje Evropa. Kljub temu je jasno, da uspešna implementacija teh reform zahteva čas.

Menite, da lahko pri delu medskupine pomaga tudi strokovna javnost iz Slovenije? Na določenih področjih

imamo kar nekaj mednarodno uveljavljenih slovenskih raziskovalnih organizacij.

Seveda! Slovenija se ponaša z izjemnimi strokovnjaki na področju odpornosti na nesreče, civilne zaščite in krizne pripravljenosti. Znanje in izkušnje slovenskih strokovnjakov so ključnega pomena pri razvoju inovativnih rešitev, ki jih lahko uspešno prenesemo tudi na evropsko raven. Medskupina si prizadeva za tesno sodelovanje s strokovnjaki iz vse Evrope, pri čemer lahko slovensko znanje pomembno prispeva h krepitvi skupne evropske odpornosti ter pripravljenosti na morebitne prihodnje izzive.

Slovenija kot del EU se nahaja v zahtevnem varnostnem okolju in je soočena s celim nizom varnostnih izzivov. To zahteva skupno in usklajeno delovanje vseh ključnih deležnikov. Menite, da je na tej tematiki možno poenotiti strateška stališča vseh političnih deležnikov v Sloveniji in tudi v Bruslju nastopati enotno v korist Slovenije?

Močno verjamem, da si glede varnosti in odpornosti vsi delimo odgovornost, ne glede na politične razlike. Načrt ReArm Europe je temeljna pobuda, ki bi morala biti uresničena že pred tremi leti. Je nujno potrebna za krepitev evropskih obrambnih zmogljivosti, kar je ključno, tako za našo nacionalno varnost, kot za širšo evropsko odpornost. Za podporo slovenskemu položaju moramo v Bruslju delovati združeno, s tem povečati naš vpliv in bolj učinkovito braniti naše nacionalne interese.

V Sloveniji je ključno okrepiti zavedanje, da brez učinkovite evropske obrambe Evropa ne more uveljavljati svojih gospodarskih interesov in zavarovati diplomatskih odločitev. Nestabilno varnostno okolje pomeni slabše možnosti za razvoj podjetništva, nižjo gospodarsko rast, manj investicij in posledično manj blaginje. V skrajnem primeru pa morebitni oboroženi konflikt pomeni ogromne stroške in gospodarsko škodo, tudi če Slovenije neposredno ne ogrozi. Vojna v Ukrajini je na primer za Slovenijo prinesla okrog 3 milijarde evrov posrednih in neposrednih stroškov – pomoč Ukrajini, nižja gospodarska rast, višje cene energentov. Edini učinkovit način za preprečevanje vojaških spopadov in ustavljanje širjenja konfliktov predstavlja odvračanje. Zato mora Evropa in z njo Slovenija nujno okrepiti lastne obrambne zmogljivosti.

Za podporo slovenskemu položaju moramo v Bruslju delovati združeno, s tem povečati naš vpliv in bolj učinkovito braniti naše nacionalne interese.

Menim, da bomo v Sloveniji težko dosegli širši družbeni konsenz glede nujnih vlaganj v obrambo, varnost in odpornost. Bistveno povečanje obrambnih izdatkov je dejstvo. Menim, da bi zato v tej fazi morali več pozornosti in energije vlagati v to, kako ta sredstva dobro in učinkovito porabiti.

Slovensko združenje za korporativno varnost je primer dobre prakse tesnega sodelovanja državnih institucij in organizacij iz realnega sektorja, še posebej na tematiki krepitve odpornosti kritične infrastrukture in izvajalcev bistvenih storitev. Menite, da lahko ta del dobrih praks iz Slovenije uporabite tudi pri delu te parlamentarne medskupine?

Nedvomno. Kot sem že omenil, je ključna prioriteta medskupine krepitev odpornosti kritične infrastrukture. Vključitev tako javnih kot zasebnih deležnikov zagotavlja, da so odzivi na krize ne le bolje usklajeni, temveč tudi bolj učinkoviti in trajnostni. Medskupina predstavlja odlično platformo za izmenjavo najboljših praks, in prepričan sem, da lahko slovenske izkušnje pomembno prispevajo k oblikovanju evropske politike na področju odpornosti, upravljanja nesreč in civilne zaščite.

Iz Slovenije pa vsekakor na raven EU lahko prenesemo naše bogate izkušnje s področja organiziranja prostovoljne gasilske službe. Gasilci so pomemben del odzivanja na naravne nesreče na terenu, prizadeval si bom, da dobijo izdatnejšo podporo in tudi močnejšo institucionalno vlogo na ravni EU. Podpiram ustanovitev Evropske gasilske zveze, s čimer bi izboljšali izmenjavo dobrih praks in operativne koordinacije v primeru čezmejnih naravnih nesreč ali nesreč večjega obsega. Evropska gasilka zveza bi bila tudi močan sogovornik in zastopnik interesov gasilcev na ravni EU. Poleg tega mislim, da bi morali v okviru povečanja izdatkov za obrambno in varnost del evropskih spodbud nameniti tudi gasilcem za nabavo gasilske opreme in tehnike, saj je učinkovit odziv na naravne in podnebno pogojene nesreče prav gotovo del širšega koncepta odpornosti. ■

Foto: Denis Lomme, © European Union 2024 - Source : EP

Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

NOVARTIS

sbr

Mestna občina Ljubljana

GASILSKA ZVEZA LJUBLJANA

Občina Slovenska Bistrica

Melamin

Mercator

telemach

SIEMENS

GEN SKUPINA

SMART COM

URSIV

Onkološki inštitut Institute of Oncology Ljubljana

ELEKTRONČEK

MINISTRSTVO ZA INFRASTRUKTURO

TEB

JAVNI MEDOBČINSKI STANOVANJSKI SKLAD MARIBOR

Telekom Slovenije

Pošta Slovenije

CAA

PETROL

Energija za življenje

AKRAPOVIČ

4AJPES

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O. INFORMATIKA

interblock LUXURY GAMING PRODUCTS

triglav

otpbanka

Elita i.b. d.o.o.

SPICA

tenzor

ZARJA ELEKTRONIKA

UNISTAR PRO

smartis PAMETNI INFORMACIJSKI SISTEMI

LON

CINKARNA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

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

KOLUMNA

ODPORNOST KOT OSREDNJI IMPERATIV EVROPSKE DRUŽBE: VLOGA KORPORATIVNE VARNOSTI V NOVEM VARNOSTNEM OKOLJU

Sodobno evropsko varnostno okolje zaznamujejo hitro spreminjajoči se varnostni in geopolitični izzivi, vse večja digitalizacija, naraščajoča medsebojna povezanost ter izjemna odvisnost od kritične infrastrukture in globalnih dobavnih verig. V takšnem kontekstu postaja odpornost – zmožnost sistemov in organizacij, da prepoznajo, absorbirajo, se prilagodijo in okrevajo po motnjah – osrednja strateška prioriteta. Prispevek osvetljuje pomen celovitega pristopa k upravljanju odpornosti in vlogo korporativne varnosti kot ključnega akterja v tem procesu.

Evropa se nahaja v obdobju temeljitih sprememb, kjer so tradicionalni modeli varnosti in stabilnosti postavljeni pod vprašaj. Geopolitična trenja, ruska agresija v Ukrajini, energetska kriza, globalne zdravstvene grožnje, migracijski pritiski ter porast kibernetskih napadov razkrivajo kompleksnost in medsebojno prepletenost sodobnih tveganj. Odpornost je postala osrednji imperativ evropske družbe.

Čeprav se je globalno varnostno okolje opazno slabšalo smo zanemarjali signale, ki bi jasno kazali na potrebo hitrejših korakov zagotavljanja ustreznih procesnih, infrastrukturnih in kadrovskih ukrepov za zagotavljanje primerne odpornosti naših organizacij. Kljub številnim opozorilnim znakom v preteklosti smo kot družba pogosto prepočasi reagirali. Zanemarili smo strateško načrtovanje razvoja odpornosti, predvsem pa

Kljub številnim opozorilnim znakom v preteklosti smo kot družba pogosto prepočasi reagirali. Zanemarili smo strateško načrtovanje razvoja odpornosti, predvsem pa zanemarili procese sistemske modernizacije, ki vključujejo tehnološko, kadrovsko in institucionalno prilagajanje novim razmeram.

*avtor je član Slovenskega združenja korporativne varnosti

zanemarili procese sistemske modernizacije, ki vključujejo tehnološko, kadrovsko in institucionalno prilagajanje novim razmeram.

Kritična infrastruktura je postala hrbtenica sodobne družbe. V sodobni informacijski družbi si težko predstavljamo delovanje brez zanesljive oskrbe z elektriko, vodo, dostopa do zdravstva, komunikacijskih in bančnih storitev. Kritična infrastruktura ni več zgolj tehnična kategorija – postaja simbol stabilnosti celotne družbene strukture. Zato je zagotavljanje neprekinjenega delovanja teh sistemov neposredno povezano z nacionalno varnostjo, gospodarsko konkurenčnostjo in zaupanjem državljanov. Vsaka motnja, naj bo to kibernetski napad, fizična škoda ali logistični zastoj, ima lahko daljnosežne posledice. Težko si danes v času moderne informacijsko podprte družbe predstavljamo nedelovanje ključnih infrastrukturnih storitev. Neprekinjenost delovanja kritične infrastrukture ima v tem pogledu zagotavljanja odpornosti celotne družbe enega izmed ključnih momentov.

Seveda pa pri zagotavljanju odpornosti družbe nikakor ne smemo zanemariti pomena ustrezno delujoče dobavne verige na vseh nivojih, saj smo v času globalizacije skoraj v celoti zanemarili lokalni ali nacionalni vidik samozadostnosti na nekaterih ključnih področjih. Prav odpornost dobavnih verig mora postati del nacionalne strategije, v kateri bodo tako javni kot zasebni akterji razvijali skupne modele zanesljivosti in robustnosti.

Reševanje vseh teh izzivov in grajenje celovitega dobro delujočega sistema niza deležnikov, ki bodo vsak na svojem nivoju odgovornosti zagotavljali celovito odpornost širše družbene skupnosti, si je nemogoče predstavljati brez aktivne vloge korporativne varnosti. Korporativna varnost v sodobnih razmerah presega okvire fizičnega varovanja ali upravljanja z varnostnimi incidenti. Postaja strateška funkcija, ki mora aktivno sodelovati pri oblikovanju celostnega varnostnega sistema, tako znotraj organizacij, kot tudi na ravni sodelovanja z državo.

Vedno več pomembnih organizacij spoznava, da je mogoče kompleksne izzive učinkovito reševati le z enovitimi in vključujočimi pristopi v dobro delujočem in koordiniranem varnostnem sistemu. Korporativna varnost mora postati in v določenem delu že je integrativni del tega sistema.

Vedno več pomembnih organizacij spoznava, da je mogoče kompleksne izzive učinkovito reševati le z enovitimi in vključujočimi pristopi v dobro delujočem in koordiniranem varnostnem sistemu. Korporativna varnost mora postati in v določenem delu že je integrativni del tega sistema.

Primer dobre prakse na skupno odzivanje na varnostne izzive, ki so pred nami, je Slovensko združenje za korporativno varnost, ki predstavlja vključujočo varnostno platformo sodelovanja in izmenjave dobrih praks ter najnovejših varnostnih spoznanj. Partnerski odnos ključnih državnih institucij in organizacij, ki v večini upravljajo s kritično infrastrukturo in bistvenimi storitvami je odličen pokazatelj poti, ki jo je treba nadaljevati, da bomo lahko zagotovili neprekinjenost delovanja ključnih infrastrukturnih zmogljivosti ter s tem ustrezne odpornosti širše družbene skupnosti.

Če kdaj je sedaj potreba po učinkovitem javno zasebnem partnerstvu med državo in njenimi ključnimi institucijami na eni strani in korporacijami oziroma zasebnimi organizacijami na drugi strani. Javno-zasebno partnerstvo mora postati ne samo deklarativno, temveč v realni praksi temelj trajnostne odpornosti. Če želimo učinkovito upravljati z varnostnimi izzivi sodobne družbe, brez sodelovanja med javnim in zasebnim sektorjem ne bo šlo. Kritično infrastrukturo v veliki meri upravljajo zasebne organizacije, a za celovit sistem zaščite in odziva je potrebna sinergija z državnimi institucijami. Partnerstvo mora temeljiti na medsebojnem zaupanju, skupnih protokolih in vajah ter transparentnosti in skupni strategiji razvoja odpornosti.

Kljub številnim pozitivnim premikom se še vedno srečujemo z deležniki, ki varnost dojemajo kot zgolj interni izziv in se zapirajo v lastne sisteme. Takšni pristopi so nevarni in kontraproduktivni. Seveda je na obeh straneh tega spektra javnih in zasebnih deležnikov nekaj takih, ki ne razumejo varnostne dinamike in realnih potreb skupnega nastopa pri upravljanju varnostnih tveganj ter se zatekajo v izolacionistični pristop. Razlogi so različni in bi jih predvsem lahko iskali v nerazumevanju resnosti varnostne situacije in neznanju spoprijemanja s prihajajočimi izzivi. Na srečo je varnostno zavedanje tudi pri vodstvenih strukturah v porastu, saj se vse bolj zavedajo, da brez učinkovitega upravljanja varnostnih tveganj in zagotavljanja neprekinjenega delovanja ni več mogoče uspešno poslovati na globalnem tržišču, prav tako pa države pa ne morejo več v celoti zagotavljati nacionalne varnosti. Varnost in odpornost družbe nista več sama po sebi umevna pojma in bo treba za nujno uveljavitev zagotoviti ustrezne sistemske pristope.

Kot sem že večkrat javno izrazil, korporativna varnost kot dejavnost ne sme zamuditi »tega zvezdniškega trenutka«, da se v vsem svojem obsegu delovanja pokaže kot eden izmed ključnih dejavnikov za zagotavljanje družbe. Korporativna varnost ima priložnost in odgovornost, da postane osrednji steber varnosti sodobne družbe. S svojim celostnim razumevanjem delovanja organizacij, sposobnostjo hitrega odziva in strateškega povezovanja lahko postane ključni igralec pri gradnji odporne, varne in stabilne prihodnosti.

Zdaj je čas, da ta sistem stopi v ospredje, ne kot podporna funkcija, temveč kot partner pri oblikovanju nacionalnih in evropskih politik varnosti in odpornosti. ■

Zagotovite varno in skladno poslovanje v digitalni dobi

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

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

bit.ly/3X8BvnV

Skupaj do skladnosti

SMART COM

UDEJANJAMO VAŠE VIZIJE

www.smart-com.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
mag. Vesna Prodnik, članica uprave, Telekom Slovenije d.d.*

ZAGOTAVLJANJE ODPORNOSTI ORGANIZACIJE OSTAJA KLJUČNO STRATEŠKO VODILO TELEKOMA SLOVENIJE

Telekom Slovenije s celovitostjo tehnoloških in procesnih pristopov zagotavlja visoko raven odpornosti organizacije, kar ima pomemben vpliv tudi na odpornost širše družbene skupnosti. Ob tej priložnosti smo se o izzivih razvoja in smelih korakih na področju zagotavljanja odpornosti pogovarjali z mag. Vesno Prodnik, članico uprave odgovorno za tehnologijo v Telekomu Slovenije.

Delovanje ključnih infrastrukturnih organizacij v zadnjem obdobju zelo zaposluje iskanje ustreznih korakov za dvig odpornosti delovanja. Kako v Telekomu Slovenije pristopate k tem zahtevnim procesom?

Omrežje Telekoma Slovenije je digitalna hrbtenica komunikacijskih storitev v Sloveniji, zato je zagotavljanje odpornega sistema in njegovo neprekinjeno delovanje naše osnovno poslanstvo. Vedno višjo stopnjo odpornosti sistema v spreminjajočih razmerah dosegamo s sistematičnim in celovitim pristopom. To potrjuje naš certificiran sistem upravljanja neprekinjenega poslovanja po standardu ISO 22301. Veliko pozornost namenjamo fizični, informacijski in kibernetski varnosti – vlagamo v nove tehnologije, znanje zaposlenih in optimizacijo procesov. Delujemo v izjemno dinamični panogi, kjer so spremembe stalnica. To od nas zahteva prilagodljivost, predvsem pa skrbno načrtovanje, diagnostiko v realnem času ter poglobljeno znanje na vseh ravneh organizacije. Le tako lahko ustrezno presojamo tveganja in sprejemamo hitre ter učinkovite ukrepe. V zadnjih letih dajemo vse večji poudarek na zagotavljanju celovite odpornosti. To pomeni, da izvajamo aktivnosti preventive na vseh ključnih sistemih, s katerimi v največji meri preprečujemo dogodke, ki bi lahko imeli negativen vpliv na zagotavljanje neprekinjenega poslovanja. Tudi IT storitve se vse bolj premikajo k upravljanim modelom z zahtevo po visoki razpoložljivosti, podobno kot telekomunikacijske, zato smo organizacijsko zasnovani tako, da združujemo potrebno strukturo z agilnostjo. Naš sistematični pristop vključuje stalno identifikacijo tveganj, implementacijo zaščitnih ukrepov, napredno detekcijo, hiter odziv in učinkovito okrevanje. Zavedamo se, da smo zaradi svoje vloge izpostavljena tarča kibernetskih napadov, kar nas sili v stalno pripravljenost. Letno uspešno preprečimo na tisoče poskusov napadov, tako na lastno infrastrukturo kot na sisteme naših uporabnikov. Visoko odpornost gradimo s kombinacijo sodobnih tehnologij ter znanja in nenehnega urjenja naših ekip. Ključno je tudi zavedanje, da pri odpornosti v smislu kibernetske varnosti ni vprašanje ali bomo napadeni, temveč kako dobro smo pripravljeni prenesti udarce in si po njih hitro opomoči. Ker sto odstotne varnosti ni, je naš cilj doseganje najvišje možne stopnje odpornosti. Seveda pa odpornost sistema pomeni tudi odpornost na ostale vrste nepredvidenih dogodkov, zato tudi omrežje načrtujemo skrbno na način, da zagotavlja čim večjo stopnjo odpornosti v primeru, da se izredni dogodki zgodijo.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Sedaj lahko na pretekle poplave pogledamo z ustrezne distance. Kateri so tisti ključni ukrepi, ki ste jih na TS izvedli v smeri krepitve odpornosti delovanja vaše Infrastrukture v primeru katastrofalnih naravnih vplivov?

Infrastruktura Telekoma Slovenije je že od nekdaj izpostavljena različnim naravnim ujmam, zato je odpornost proti takim dogodkom vpeta v samo zasnovo našega omrežja. Naš cilj je, da je delovanje omrežja v primeru katastrofalnih naravnih vplivov prizadeto v čim manjši možni meri. Struktura omrežja temelji na centraliziranem, a geografsko redundantnem jedrnem delu, regionalno zasnovanem in prav tako redundantnem agregacijskem delu ter močno razpršenem dostopovnem delu. Prav ta razpršenost dostopovnega dela, ki je sicer najbolj izpostavljen, pomeni tudi razpršitev tveganja. Morebiten izpad namreč prizadene ožje geografsko območje. Ključno je, da so v vse segmente omrežja vgrajene ustrezne redundance, ki temeljijo na oceni tveganja uresničitve posamezne grožnje. Osnova za zanesljivo delovanje pa so tudi redundantni sistemi za električno napajanje. Poleg vseh tehnoloških vidikov pa je bistvenega pomena človeški faktor. Imamo pripravljene, usposobljene in ustrezno opremljene terenske ekipe. Zagotovljene imamo zadostne količine rezervnih delov ter dogovore z dobavitelji za hitro odzivanje in dobavo v primeru izrednih razmer. Izjemno pomembno vlogo ima naš Nadzorno operativni center, ki deluje 24/7 in skrbi za nadzor nad celotnim omrežjem. Opremljenost z natančnimi informacijami o stanju na terenu in v omrežju nam omogoča hitro in učinkovito sprejemanje odločitev ter usmerjanje ekip. Pri tem so neprecenljive izkušnje in uigranost naših ekip, ki se nenehno usposabljajo ter dobro poznajo tako zmožnosti kot omejitve omrežnih tehnologij.

Za učinkovitost delovanja ste v zadnjem obdobju izvedli pomembne strukturne in organizacijske pristope znotraj Telekoma Slovenije. Nam lahko zaupate tiste, ki zagotavljajo višjo strokovno sinergijo že tako omejenih virov?

V Telekomu Slovenije stalno izboljšujemo učinkovitost delovanja, še posebej na področju upravljanja naše obsežne infrastrukture in omrežja. V zadnjem obdobju smo izvedli pomembne organizacijske prilagoditve, s katerimi smo dosegli večjo sinergijo in učinkovitejšo rabo naših strokovnih virov. Celotno področje, ki skrbi za omrežje in infrastrukturo, smo organizacijsko še tesneje povezali. Ključna sprememba je bila poenotenje funkcij prve linije operative za vse tržne segmente in vse vrste storitev. To pomeni, da imamo enotno vstopno točko za upravljanje in odpravljanje napak, kar omogoča hitrejši odziv in boljšo izkoriščenost znanj. Takšno poenotenje je bilo mogoče predvsem zaradi naših predhodnih vlaganj v napredno informacijsko podporo, ki omogoča učinkovito upravljanje kompleksnih procesov. Naše ekipe so sedaj organizirane okoli jasno definiranih in logično zaokroženih tehnoloških celot. To pomeni, da so v posamezni ekipi združeni strokovnjaki s sorodnimi veščinami, kar spodbuja izmenjavo znanj in specializacijo. Vsaka ekipa ima jasno opredeljene naloge, cilje in odgovornosti, kar prispeva k večji osredotočenosti in učinkovitosti. Kljub specializaciji pa ekipe še vedno tesno sodelujejo in imajo močno podporo osrednjih operativnih ekip, ki skrbijo za temeljno infrastrukturo. Združevanje strokovnih ekip za dvig kompetenc smo izvedli tudi na področju IT ter v podpori končnim uporabnikom. V vedno kompleksnejšem tehnološkem okolju ob pomanjkanju strokovnega kadra nenehno vlagamo v izobraževanje naših strokovnjakov, prav tako pa aktivno zaposlujemo talente in podeljujemo štipendije za deficitarne poklice.

Zagotavljanje kibernetske varnosti ostaja vaša pomembna strokovna zaveza. Vaš Center kibernetske varnosti in odpornosti ima vedno pomembnejšo vlogo tudi pri zagotavljanju kibernetske varnosti v ključnih sistemih kritične Infrastrukture? Kakšne so dosedanje izkušnje?

Naš Center kibernetske varnosti in odpornosti (CKVO) je resnično postal ključni steber, ne le zaščite Telekoma Slovenije, temveč vse bolj tudi za podporo upravljavcem kritične infrastrukture v Sloveniji. Naše dosedanje izkušnje pri sodelovanju z drugimi sektorji infrastrukture, kjer informacijsko-komunikacijska tehnologija (IKT) ni primarna dejavnost, kažejo, da ti sektorji k uvajanju naprednih kibernetsko-varnostnih rešitev pristopajo z večjo mero previdnosti. Procesi implementacije so zato pogosto počasnejši in bolj premišljeni, kar je razumljivo glede na naravo njihove dejavnosti. Za nas, ki smo vajeni izjemne dinamike v telekomunikacijah in IKT, se ti procesi včasih zdijo počasni, a razumemo potrebo po temeljitosti. Vsak izmed sektorjev kritične infrastrukture ima svoje specifike in domensko znanje, ki ga imajo njegovi upravljalci, kar pa je pri odločitvah glede uvajanja kibernetske varnosti ključno. Dejstvo je, da je Telekom Slovenije zaradi svoje izpostavljenosti in vloge v digitalnem ekosistemu izrazito privlačna tarča za kibernetske napade. Naš CKVO letno zazna in uspešno obravnava več deset tisoč varnostnih incidentov, med katerimi je tudi več tisoč neposrednih poskusov napadov na našo infrastrukturo ali infrastrukturo naših uporabnikov. Menimo, da smo kot podjetje ravno prav veliki – dovolj veliki, da imamo vire, znanje in tehnologijo za izvedbo najzahtevnejših projektov na področju kibernetske varnosti

(„big enough to deliver“), a hkrati dovolj agilni in osredotočeni, da se lahko vsaki stranki, vključno z upravljavci kritične infrastrukture, ustrezno posvetimo („small enough to care“).

Zelo aktivni ste tudi na celem nizu EU projektov. Katere so tiste ključne izkušnje, ki jih prinašate iz projektov s področja KI in kibernetske varnosti?

Sodelovanje v evropskih raziskovalno razvojnih projektih je za nas strateško ključno. Tako krepimo kompetence, mednarodno mrežo in aktivno soustvarjamo prihodnje tehnološke standarde. Kot napreden operater in del ključne infrastrukture imamo s tem neposreden dostop do najnovejših dognanj, zlasti na področju kibernetske odpornosti. Projekti, kot so ATLANTIS, PRECINCT in ENDURANCE, nam dajejo dragocen vpogled v trende in regulativo na področju varnosti omrežij, kar nam omogoča proaktivno in pravočasno načrtovanje. V projektih aktivno sodelujemo pri strategijah, koordinaciji, postavljamo pilote za testiranje rešitev v praksi ter skrbimo za njihovo integracijo. Dober primer tega je pilotni projekt MESO, kjer se osredotočamo na odpornost medsebojno povezanih digitalnega in energetskega sektorja. Ta sodelovanja krepijo naša partnerstva za izmenjavo dobrih praks, krepijo naša domenska znanja in potrjujejo vlogo Telekoma Slovenije kot ključnega tehnološkega igralca v regiji. Verjamemo, da smo iskan partner prav zaradi naše kombinacije tehnološke naprednosti in agilnosti, s katero učinkovito premoščamo vrzel med raziskavami in dejansko implementacijo. Seveda pa si prizadevamo to dragoceno znanje čim bolje prenesti v našo vsakodnevno prakso pri uvajanju najnaprednejših rešitev zase, kakor tudi za naše stranke.

Koraki ki jih energetika izvaja na področju vzpostavitve sektorskega energetskega SOC so vedno hitrejši. Glede na to, da gre za ključno nacionalno infrastrukturo, si je težko zamisliti vzpostavitev tega kibernetskega sistema brez podpore Telekoma Slovenije? Kakšna so vaša pričakovanja glede tega nacionalnega energetskega koraka?

Energetika in IKT sta resnično neločljivo povezani hrbtenici sodobne družbe. Brez električne energije ni IKT, obenem pa so napredne in varne IKT rešitve nujne za odporno delovanje energetskih sistemov. S podrobnimi načrti glede vzpostavitve sektorskega energetskega SOC nismo seznanjeni. Vsekakor pa pozdravljamo vse aktivnosti, ki prispevajo k dvigu kibernetske odpornosti energetskega sektorja ter posledično celotnega ekosistema. Glede na našo vodilno vlogo v IKT, bogate izkušnje z lastnim naprednim Centrom kibernetske varnosti in odpornosti ter dobrim razumevanjem varnostnih izzivov v takšnih konvergenčnih okoljih, smo prepričani, da lahko temu nacionalnemu projektu ponudimo pomembno podporo. Seveda ima energetika svoje sektorsko specifične operativne tehnologije in procese, a prav tu vidimo priložnost za sinergijo, mi lahko prispevamo vrhunsko znanje s področja IKT varnosti, od naprednega nadzora do odzivanja na incidente, prilagojeno potrebam energetskega okolja. Naš cilj in pričakovanje je, da ta nacionalni projekt uspešno združi najboljše iz obeh svetov: poglobljeno znanje energetike in napredno IKT varnost. Vsi se zavedamo, da so vrhunski kibernetski strokovnjaki izjemno iskan in omejen vir, zato je medsektorsko sodelovanje in združevanje moči, ne le smiselno, temveč nujno. Verjamemo, da lahko s tesnim partnerskim pristopom bistveno prispevamo k uspešni vzpostavitvi in delovanju energetskega SOC ter tako skupaj okrepimo odpornost ključne nacionalne infrastrukture, kar je v interesu vseh nas.

Danes se je v tem zahtevnem kibernetskem okolju v celoti nemogoče izogniti kibernetskim napadom in s tem povezanim incidentom. Kako pomembno ja za vas deljenje izkušenj, ki omogočajo, da celotna skupnost postaja bolj odporna na kibernetske napade?

Popolnoma drži, iluzorno bi bilo pričakovati, da se lahko v današnjem digitalnem okolju povsem izognemo kibernetskim incidentom. Grožnje so stalnica našega poslovanja, so vse bolj sofisticirane in se nenehno razvijajo. Tudi sami smo nenehno na prvi bojni črti, naš Center kibernetske varnosti in odpornosti pa se vsakodnevno sooča z varnostnimi izzivi. Prav zato je odprta in pravočasna izmenjava izkušenj, znanj in podatkov o grožnjah med ključnimi deležniki, ne le pomembna, temveč nujna. Kibernetska odpornost je kolektivna odgovornost, saj smo v digitalnem ekosistemu vsi medsebojno povezani. Izmenjava informacij o novih taktikah napadalcev, indikatorjih kompromitacije in učinkovitih obrambnih strategijah nam vsem omogoča, da se hitreje odzovemo, okrepi-

mo svoje obrambne mehanizme in smo bolje pripravljeni na prihodnost. Zato v Telekomu Slovenije aktivno sodelujemo v nacionalnem in mednarodnem varnostnem ekosistemu – tesno sodelujemo s SI-CERT-om in URSIV-om, uporabljamo napredna orodja za izmenjavo podatkov o grožnjah ter sledimo aktivnostim na evropski ravni prek EUROPOL-a in ENISE. Verjamemo, da je prav sodelovanje med zaupanja vrednimi partnerji v Sloveniji, tako iz javnega kot zasebnega sektorja, ključno, ne le za dvig skupne odpornosti, temveč predstavlja tudi temelj za krepitev naše nacionalne digitalne suverenosti.

V EU smo v fazi celovitega vala uvajanja niza pomembnih regulatornih korakov. Tem procesom smo izpostavljeni tudi v organizacijskih okoljih v Sloveniji. Kako ste v Telekomu Slovenije uspešni pri implementaciji minimalnih varnostnih okvirov na področju kibernetske varnosti, ki jih prinaša direktive NIS 2.

Uvajanje nove regulative, kot je direktiva NIS 2, predstavlja pomemben korak k harmonizaciji in dvigu ravni kibernetske varnosti in odpornosti v vsej Evropski uniji. V Telekomu Slovenije te regulatorne korake pozdravljamo, saj postavljajo jasnejša pričakovanja in spodbujajo proaktivno upravljanje kibernetskih tveganj. Za nas implementacija zahtev iz direktive NIS 2 ne pomeni začetka poti na področju kibernetske varnosti, temveč nadgradnjo in dopolnjevanje naših že obstoječih, trdnih varnostnih praks in okvirov. Že dosedanja nacionalna zakonodaja na področju elektronskih komunikacij je vključevala zelo podobne zahteve za zagotavljanje neprekinjenega poslovanja ter informacijske varnosti, ki se sedaj prenašajo in širijo v sklopu zakona o informacijski varnosti. Že vrsto let imamo implementirane mednarodne standarde, kot je ISO 27001 za upravljanje informacijske varnosti in ISO 22301 za upravljanje neprekinjenega poslovanja ter nenehno vlagamo v varnostne tehnologije, procese ter znanje zaposlenih. Zato lahko rečem, da smo na prihod NIS 2 dobro pripravljeni, in da skladnost z direktivo v veliki meri že dosegamo, oziroma jo sistematično nadgrajujemo. Pomembno pa je poudariti, da NIS 2 prinaša nove oziroma razširjene obveznosti, ne le za nas kot operaterja elektronskih komunikacij, temveč tudi za širši krog subjektov, vključno z mnogimi našimi poslovnimi uporabniki in dobavitelji. To bo nedvomno prispevalo k večji odpornosti celotnega digitalnega ekosistema. Seveda pa doseganje in vzdrževanje skladnosti z NIS 2, tako kot vsaka resna zaveza h kibernetski varnosti, zahteva nenehna vlaganja – v tehnologijo, v usposabljanje ljudi in v prilagajanje procesov. To ni enkraten projekt, temveč trajna zaveza, ki terja ustrezne vire. Skladnost z NIS 2 vidimo kot nujno investicijo v zaupanje naših strank in dolgoročno stabilnost našega poslovanja.

Certifikacijske sheme in ustrezni akreditacijski organi predstavlja pomemben korak, ki bo zagotovil učinkovito skladnost in kvaliteto vseh novih tehnoloških rešitev na skupnem trgu EU. Menite, da bomo na trgu kibernetskih storitev in tehnoloških rešitev uspeli ujeti pravo razmerje med kvaliteto certifikacijskih procesov in potrebno dinamiko prihoda novih tehnoloških rešitev v operativno uporabo?

Vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost je pomemben korak k dvigu zaupanja v digitalne proizvode in storitve na enotnem trgu. Standardizirani in transparentni certifikacijski procesi lahko uporabnikom olajšajo izbiro varnih rešitev in spodbudijo proizvajalce k vgrajevanju varnosti že v fazi načrtovanja. Vendar pa se pri tem soočamo z izzivom, ki ste ga omenili, kako najti pravo ravnovesje med zagotavljanjem visoke kakovosti in rigoroznosti certifikacijskih postopkov ter potrebo po hitrem uvajanju inovativnih tehnoloških rešitev, ki jih zahteva dinamika trga. Zgodovinsko gledano so regulatorni in standardizacijski procesi v Evropi pogosto počasnejši od hitrosti tehnološkega razvoja, še posebej na področju IKT in kibernetske varnosti. Obstaja tveganje, da predolgi ali preveč birokratski certifikacijski postopki zavrejo inovacije ali pa postanejo nerelevantni, ker tehnologija medtem že napreduje. Nenazadnje se postavlja vprašanje kje se bodo certifikacije izvajale in podredno ali ima Slovenija ustrezen certifikacijski organ, ki bo zagotavljal certifikacijo na nacionalni ravni. V Telekomu Slovenije smo zagovorniki visokih standardov varnosti in kakovosti, kar dokazujemo z našo skladnostjo z mednarodnimi standardi, kot so ISO 27001 (upravljanje informacijske varnosti), ISO 27018 (varstvo osebnih podatkov v oblaku) in ISO 22301 (upravljanje neprekinjenega poslovanja). Smo tudi edino podjetje v Sloveniji s statusom »Trusted Introducer«, kar potrjuje zrelost naših varnostnih operacij. Ključ do uspeha bo po našem mnenju v agilnosti pri oblikovanju in izvajanju certifikacijskih shem in pri sposobnosti podjetij, da te standarde hitro in učinkovito integrirajo v svoje razvojne cikle. Potrebujemo certifikacijske postopke, ki so prožni, da lahko sledijo tehnološkim spremembam, hkrati pa dovolj robustni, da zagotavljajo dejansko varnost. To bo zahtevalo tesno sodelovanje med regulatorji, akreditacijskimi organi, industrijo in raziskovalno sfero.

Slovensko združenje za korporativno varnost z vsakim letom postaja bolj reprezentativna vključujoča varnostna platforma za združevanje različnih organizacijskih sredin. Kaj bi sporočili organizacijam, ki se še niso uspele priključiti tej varnostni iniciativi?

Slovensko združenje za korporativno varnost (ICS) ima pomembno vlogo pri povezovanju strokovnjakov in organizacij ter pri dvigovanju zavedanja o pomenu celovite varnosti in odpornosti v slovenskem prostoru.

Organizacijam, ki morda še razmišljajo o vključitvi v tovrstne varnostna združenja, je namenjen naslednji premislek: V današnjem kompleksnem in medsebojno povezanem svetu, kjer obstajajo raznolika tveganja, od kibernetskih groženj do fizičnih varnostnih izzivov in potrebe po zagotavljanju neprekinjenega poslovanja, je težko doseči celovito varnost in odpornost brez sodelovanja. Delovanje v izolaciji ni več vzdržna strategija, temveč lahko samo po sebi predstavlja tveganje. Uspešno obvladovanje tveganj in gradnja odpornosti temeljita na sodelovanju, izmenjavi znanj, dobrih praks ter povezovanju z relevantnimi deležniki. Platforme, kot je Slovensko združenje za korporativno varnost, nudijo prostor za učenje, mreženje in skupno iskanje rešitev za izzive, s katerimi se organizacije soočajo.

Prav tako je treba poudariti, da odgovornost za korporativno varnost in odpornost ni zgolj naloga varnostnih strokovnjakov, temveč mora biti del delovanja na ravni poslovodstva. Vodstva organizacij imajo pomembno vlogo pri opredelitvi varnosti kot strateške prioritete in pri spodbujanju varnostne kulture znotraj organizacije. Članstvo in aktivno sodelovanje v združenju, kot je ICS, lahko podpreta ta prizadevanja in omogočita dostop do koristnih virov ter izkušenj. ■

Foto: arhiv Telekom Slovenije d.d.

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

ODPORNOST DRUŽBE SI BREZ RAZUMEVANJA VPLIVA NARAVNIH NESREČ NI MOGOČE ZAMISLITI

Tudi Republika Slovenija ni imuna na pojav naravnih nesreč z vsemi posledicami, ki jih te prinašajo. V zadnjem obdobju postajajo naravni pojavi vedno vplivnejši dejavnik, ki ga bo treba razumeti in upoštevati pri prihodnjem načrtovanju izgradnje ključne infrastrukture. Zaradi navedenega je za zagotavljanje ustrezne odpornosti družbe treba izvesti korenite sistemske korake. O njih smo se pogovarjali z g. Boštjanom Šeficem.

Približujemo se končanju drugega leta aktivnosti obnove po eni največjih naravnih nesreč, ki so prizadele Slovenijo. Kako bi lahko ocenili uspešnost dosedanjih aktivnosti odpravljanja posledic te ujme?

Ko primerjamo razmere, s katerimi smo se soočili po 4. avgustu 2023, ko je velik del naše države utrpel hude posledice velikih poplav in zemeljskih plazov z današnjim stanjem, lahko z gotovostjo in čisto vestjo zatrdimo, da je bilo opravljeno resnično zelo veliko delo. To velja tako za odpravo posledic na občinski in državni infrastrukturi, vodotokih, objektih v lasti fizičnih oseb, gospodarstvu, kot tudi za zagotavljanje varnosti ter večje odpornosti na podobne dogodke v prihodnosti. Posebej velja izpostaviti polno angažiranost praktično vseh državnih organov in lokalnih skupnosti. Ob rednih obiskih na terenu nas pogosto preseneča, da na marsikaterem območju ni več opaznih sledi katastrofe, ki se je zgodila pred manj kot dvema letoma. To seveda ne pomeni, da so vse posledice odpravljene, ali pa da je delo v celoti zaključeno - obojega je še veliko. A v primerjavi z nekaterimi bližnjimi ali malo bolj oddaljenimi okolji lahko rečem, da dobro opravljamo delo.

Pomembno je poudariti, da smo s pomočjo različnih ukrepov vsem prizadetim zagotovili varen začasen dom. Nihče ni prebival v bivalnikih ali celo ostal brez „strehe nad glavo“.

Dejstvo je tudi, da smo praktično končali z identifikacijo najbolj ogroženih objektov, ki predstavljajo tveganje za življenje in zdravje ljudi. To je bil zanesljivo eden najbolj zahtevnih postopkov. Trenutno strokovnjaki vodarske in geološke stroke obravnavajo samo še nekatere posamezne, najbolj zahtevne primere. Za te primere pričakujemo, da bodo strokovna mnenja v kratkem dokončana in

Pravočasno in učinkovito obveščanje ima ključno vlogo pri zmanjševanju posledic naravnih nesreč – ne le z vidika preprečevanja potencialnih žrtev in poškodb, temveč tudi z vidika zmanjšanja materialne škode.

*intervjuvanec je član Slovenskega združenja korporativne varnosti

po izvedenem postopku sprejeti sklepi Vlade. Do sedaj je Vlada Republike Slovenije sprejela sklepe za 328 objektov, opravljene so cenitve praktično za vse ogrožene objekte (za nekatere prihajajo cenitve prav v teh dneh), dokončno pripravljenih je že preko 226 pogodb, 171 jih je bilo izplačanih ali pa so v izplačilu, izplačali pa smo nekaj manj kot 50 milijonov evrov. Z zadovoljstvom ugotavljamo, da so številni lastniki, ki so v ujmi izgubili svoje domove, ali pa se morajo zaradi ogroženosti preseliti, že v zaključni fazi gradnje novih objektov, kar pomeni, da bodo v slabih dveh letih po tej katastrofi v svojih novih domovih. V tem času je bilo treba ugotoviti in utemeljiti ogroženost, pripraviti dokumentacijo, izvesti postopke, pridobiti varna zemljišča in zagotoviti njihovo umestitev v prostorske akte ter pridobiti vsa potrebna dovoljenja zato, da so bodo v naslednjih mesecih imeli nov dom za naslednja desetletja.

Po izvedenih nujnih in izrednih ukrepih na vodotokih prihajajo večji projekti sanacije, ki so zahtevni in morajo biti dobro načrtovani. Področji urejanja vodotokov in sanacija plazov sta izjemnega pomena, saj sta med prebivalci na prizadetih območjih največja skrb in pričakovanje namenjena prav njihovem urejanju. Zato dajemo tem projektom prioriteto, da se katastrofalne poplave preprečijo oziroma bistveno zmanjšajo tveganja. Enako velja za plazove, ki so prav poseben izziv zaradi zahtevnosti sanacije in zagotavljanja velikih finančnih sredstev.

V teh dvajsetih mesecih smo v odpravo posledic naravne nesreče investirali preko 1,1 milijarde evrov. V letošnjem letu se načrtujejo investicije v višini med 400 in 500 milijoni evrov. Dobro je, da smo okoli 110 milijonov evrov že v nekaj mesecih po naravni nesreči namenili gospodinjstvom, in da se sedaj pripravljajo odločbe v okviru pristojnega ministrstva, s katerim bodo v skladu z Zakonom o odpravi posledic naravnih nesreč izplačan še preostanek pomoči fizičnim osebam za sanacijo stanovanj.

Če strnem, s sanacijo ne moremo biti nezadovoljni. Hkrati prav te dni zaključujemo drugo poročilo, v katerem izpostavljamo nekatere ključne izzive in predlagamo ukrepe za dodatno povečanje učinkovitosti izvajanja vseh ukrepov in projektov.

Že v preteklosti ste imeli pred seboj pomembne izzive in zadolžitve. Kako sami ocenjujete zahtevnost in obsežnost tokratnega koordinacijskega izziva? Ste imeli ustrezno podporo različnih državnih in lokalnih struktur pri prizadevanjih za uveljavitev sistemskih rešitev?

Vsaka - na nek način krizna situacija ima svoje značilnosti in posebnosti, kar zahteva specifičen pristop. Na primer, reševanje precej nevarnih razmer v nekdanjem podjetju KIK Kamnik, ki so ogrožale kar precejšen del naseljenega dela Kamnika, je imelo povsem drugačne izzive, kot na primer migracije. Vsakič smo se znašli pred potrebo po iskanju sistemskih rešitev, ki bi morale biti pripravljene že vnaprej. Prav to pa dokazuje, da z znanjem, odločnostjo lahko na videz nerešljive »probleme« rešujemo hitro in uspešno.

Sedanja naloga je brez dvoma posebna in jo težko primerjam z ostalimi. Nedvomno pa je najbolj kompleksna. Prvič zato, ker je vključenih veliko ministrstev in državnih organov, veliko število občin, veliko strokovnjakov različnih strok, ki pa morajo delovati usklajeno. Po drugi strani gre za različna področja, od urejanja vodotokov in vodne infrastrukture, cest, mostov, plazov, cest, železnice, objektov, srečujemo se s problematiko gospodarskih subjektov in še bi lahko našteval. Vendar tisto, kar je najbolj zahtevno so izzivi povezani z odpravljanjem posledic na domovih in zagotavljanje novih domov. To terja uskladitev dela različnih strok in veliko razumevanja za osebne zgodbe ter konkretne življenjske situacije slehernega posameznika. Ocenjujem, da smo zaenkrat delo opravili uspešno, čeprav problemov in izzivov ne zmanjka.

Dejstvo pa je, da imamo s sodelavci ves čas absolutno podporo predsednika vlade, ministrov in vseh ostalih, s katerimi moramo urejati posamezna vprašanja in razreševati konkretne situacije. Posebej sem zadovoljen, da smo vzpostavili dober in konstruktiven odnos z župani, saj je to ključno za izvedbo marsikaterega ukrepa. V veliko zadovoljstvo je celotni ekipi, da imamo kljub zahtevnim okoliščinam zelo pozitivne relacije z upravičenci in prebivalci na vseh prizadetih območjih. To je tudi bistvo našega dela, saj vse kar počnemo, počnemo zanje in zaradi njih.

V zadnjem obdobju je zagotavljanje odpornosti družbe ena od ključnih razprav, ki se odvija na evropskem in nacionalnem nivoju. Ta odpornost je povezana tudi z odpornostjo na izzive, ki jih prinašajo tveganja naravnih nesreč. Lahko ocenite izvedene ukrepe na področju protipoplavne zaščite tudi kot del tega procesa? Smo v Sloveniji po teh po poplavnih ukrepih bolj odporni na pojav takih izzivov naravnega okolja?

Vse kar delamo - od urejanja vodotokov, sanacije infrastrukture in preselitve domov na varna območja - je, poleg zagotavljanja varnosti za prebivalce, tudi v smeri povečevanja odpornosti na prihodnje naravne nesreče. Že z doslej opravljenim delom se je odpornost povečala. Desetletja ni bilo toliko narejenega na vodotokih ali pa na sanaciji

cest in gozdnih cest. S pripravo državnih prostorskih načrtov se bodo umeščali v prostor in izvedli projekti, s katerimi se bodo gradili suhi zadrževalniki voda, vzpostavila se bodo večja razlivna območja, objekti se bodo umaknili iz poplavnih in plazovitih območij, s čimer bomo dosegli višjo stopnjo varnosti za ljudi. V posameznih primerih se daje vodi več prostora, s čimer se bodo zmanjšala tveganja poplav, z ukrepi se bodo ustrezno zaščitile države ceste, zgrajeni bodo primernejši mostovi. Seveda, govorim o odpravi posledic. Nato pa je treba izvesti še vrsto investicij, s katerimi bomo še dodatno povečali odpornost, hkrati bo treba spremeniti in prilagoditi načine gradnje, ustrezneje umeščati objekte v prostor in predvsem ne podcenjevati narave. Da, bolj smo odporni, vendar nas - glede na pričakovane spremembe - čaka še ogromno dela. Odpornost mora postati del slehernega projekta danes in v prihodnje.

Če se osredotočimo na zagotavljanje odpornosti infrastrukture pomembne za nemoteno delovanje širše družbene skupnosti, menite, da so infrastrukturni upravljalci iz tega primera prenesli ustrezne izkušnje v zagotavljanje dodatnih ukrepov in procesov, ki bodo omogočali bolj odporno delovanje infrastrukture ob bodočih negativnih vplivih naravnega okolja?

Glede na pogovore, ki jih imam z različnimi predstavniki inštitucij, projektanti, urbanisti in stroko, ocenjujem, da je ta zavest močneje prisotna kot pred nesrečo. Vprašanje je, ali zadosti. Žal še vedno zasledim mnenja, da se pretirava, in da so podnebne spremembe vedno bile. Seveda, vendar so te spremembe sedaj hitrejše in z večjimi posledicami, kot so bile pred leti. Zato pred njimi ne smemo bežati oziroma si zatiskati oči, ampak se moramo z njimi premišljeno in racionalno soočiti in se prilagoditi. Posebej pomembno je, da ob tem hkrati zmanjšujemo tudi vpliv dejavnikov, ki te spremembe še potencirajo.

Kako vam je uspelo obvladati enega od pomembnih koordinacijskih izzivov, in sicer uskladitve državnih in lokalnih interesov, ne samo pri sanaciji, temveč tudi pri dojemanju potrebe po resnejšem načrtovanju bodočih prostorskih načrtov za širjenje strjenih naselij in umeščanja infrastrukture v prostor?

Tu je moja vloga majhna, ali je pa skorajda ni. Če pa že, je moj prispevek v tem, da smo pridobili v sami službi odlično sodelavko Sašo Piano, ki je velika strokovnjakinja in ima odličen pristop pri sodelovanju z načrtovalci. Drugi pomembni dejavnik je, da je v ta del vključen kolega državni sekretar Jure Leben, ki je v Kabinetu predsednika vlade zadolžen tudi za okolje in prostor. S tem smo bistveno okrepili širšo ekipo, še prav posebej na tem področju. In tretji pomemben dejavnik je dejstvo, da odlično sodelujemo s kolegom Miranom Gajškom na Ministrstvu za naravne vire in prostor ter njegovo ekipo. Vse to zagotavlja, da se na tem področju izvajajo pozitivni premiki. Nedvomno pa to ni enkratna aktivnost, temveč mora to postati del dobro premišljenega in sistematičnega procesa danes in v prihodnosti. Sistem je treba postaviti tako, da se bodo parcialni interesi obvladali. Predvsem pa veliko osveščanja in izobraževanja, ne le načrtovalcev in odločevalcev, temveč nas vseh. To ne bo lahko, je pa hkrati nujno.

Treba se je dotakniti vzpostavitve sistema za zgodnje alarmiranje in obveščanje, s katerim v Sloveniji zamujamo. Ravno pravočasno alarmiranje in obveščanje v takih razmerah ključno prispeva k zmanjšanju števila človeških žrtev in posledično tudi materialne škode. Se je v času aktivnosti po poplavne obnove kaj premaknilo tudi na tem področju? Ste bili ob postopkih, ki ste jih izvajali vključeni tudi v ta pomemben segment?

Strinjam se - alarmiranje in obveščanje je izjemno pomembno. To se je pokazalo v tem primeru in mnogih drugih. Že sedaj imamo učinkovit sistem, z novim nadgrajenim sistemom pa bo obveščanje še bistveno boljše in hitrejše.

S tem področjem se aktivno ukvarjata Uprava RS za zaščito in reševanje in Ministrstvo za digitalno preobrazbo. Prvi zato, ker je to del zaščite prebivalstva in so nosilci vseh priprav in aktivnosti, drugi zato, ker so nosilci vrste projektov s področja digitalizacije in vodijo potrebne postopke. Projekt je v razvojno testni fazi in pričakujemo, da bo v kratkem operativen. Služba za obnovo po poplavah in plazovih v to sicer ni bila neposredno vključena, ker je naša prednostna naloga sanacija. Kljub temu pa aktivnosti spremljamo in jih v celoti močno podpiramo. Pravočasno in učinkovito obveščanje ima ključno vlogo pri zmanjševanju posledic naravnih nesreč – ne le z vidika preprečevanja potencialnih žrtev in poškodb, temveč tudi z vidika zmanjšanja materialne škode. ■

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

ohranite neprekinjeno delovanje kritične infrastrukture

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

ALCEA

ASSA ABLOY

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Marjan Eberlinc, univ. dipl. inž. str., glavni direktor Plinovodi d.o.o.*

CELOVITI PRISTOPI ZAGOTAVLJANJA VARNOSTI SO POSTALI NUJNA DIMENZIJA ENERGETSKEGA SEKTORJA

Ustrezno upravljanje tveganj in zagotavljanje neprekinjenega poslovanja je na področju oskrbe s plinom ena od ključnih operativnih funkcij organizacije. Zagotavljanje visoke odpornosti ključne infrastrukture je pomemben dejavnik, ki ga vodstvo organizacije zasleduje pri razvoju energetskih sistemov in procesov. O sistematičnih pristopih zagotavljanja upravljanja tveganj imamo tokrat priložnost spregovoriti z glavnim direktorjem g. Marjanom Eberlincem.

Najprej nam še enkrat dovolite, da vam čestitamo za prejem letošnje nagrade Slovenian Grand Security Award v kategoriji »najbolj varno podjetje«. Kaj vam v vaši organizaciji pomeni ta nagrada?

Nagrada Slovenian Grand Security Award v kategoriji »najbolj varno podjetje« je za našo družbo velikega pomena, saj potrjuje dolgoročno zastavljene in dosledno uresničevane varnostne strategije ter prizadevanja naših zaposlenih. Nagrada pomeni priznanje našemu dolgoletnemu trudu, profesionalnosti in strateškemu pristopu k obvladovanju različnih tveganj in zagotavljanju varnosti. Nagrada predstavlja tudi validacijo dosedanjega dela, sistematičnih pristopov k upravljanju in obvladovanju tveganj, zavzetosti celotnega kolektiva za ustvarjanje in ohranjanje najvišjih varnostnih standardov in naložb v varnostno infrastrukturo, hkrati pa je tudi izziv ter dodatna motivacija za nadaljnje razvijanje in izboljševanje ter potrjuje našo zavezo k nenehnemu razvoju varnostne kulture. Prepričani smo, da bo nagrada našim zaposlenim dala dodatno motivacijo, saj dokazuje, da so njihova prizadevanja opažena in cenjena tudi s strani strokovne javnosti. Zahvaljujemo se našim strokovnim sodelavcem na varnostno najbolj izpostavljenih področjih in vsem zaposlenim za njihovo skrb in predanost pri zagotavljanju najvišje ravni varnosti.

Geostrateške napetosti in varnostni izzivi so v zadnjih letih posebej vplivali tudi na zagotavljanje plina, kot ključnega energenta za delovanje industrije. Kako se poskušate v Plinovodih odzivati na te globalne izzive, na katere Slovenija zaradi svoje majhnosti nima pomembnega vpliva?

V družbi se zavedamo geostrateških izzivov, predvsem v luči trenutnih aktualnih dogodkov, ki vplivajo na celotni energetski sektor, še posebej na dobavo plina kot enega od ključnih energentov. V družbi se osredotočamo predvsem na krepitev naše odpornosti in zmanjšanje občutljivosti na zunanje vplive. Kot operater prenosnega sistema plina zagotavljamo infrastrukturno možnost diverzifikacije dobavnih poti, ki smo jo dodatno povečali z novo zgrajeno enoto kompresorske postaje v Ajdovščini in gradnjo nove mejne merilno-regulacijske postaje na meji z Italijo, ki bo še dodatno pripomogla k povečanju zmogljivosti iz zahodne dobavne smeri. Redno spremljamo globalne energetske trge in analiziramo možne scenarije tveganj,

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

kar nam omogoča hitrejše in učinkovitejše ukrepanje ob morebitnih motnjah. Sodelujemo tudi v več domačih in mednarodnih institucijah ter na ta način poskušamo zagotavljati kar najvišjo možno raven pripravljenosti v primeru geostrateških tveganj.

Sektor zagotavljanja plina je že sam po sebi zelo zahteven za upravljanje, zato je zagotavljanje ustrezne neprekinjenosti delovanja celotnega sistema eden od ključnih ciljev vašega podjetja. Kako poskušate zagotavljati to neprekinjenost delovanja ključnih tehnoloških in podpornih procesov v organizaciji?

Neprekinjeno delovanje ključnih procesov predstavlja osnovo za zagotavljanje stabilnega in neprekinjenega prenosa plina do končnih porabnikov. Neprekinjenost delovanja našega sistema je eno od vodil že ob sami izgradnji in izbiri tehnično tehnoloških rešitev, saj na ta način določena tveganja omejujemo še z nekaterimi preventivnimi ukrepi. Velik poudarek namenjamo rednemu vzdrževanju obstoječe infrastrukture, investicijam v nove tehnologije in v tehnološko napredne ter robustne rešitve ter uvajanju najboljših praks na področju zagotavljanja kibernetske in fizične varnosti. Redno izvajamo ocene tveganj, identifikacijo potencialnih ranljivosti ter implementiramo tehnične in organizacijske ukrepe za njihovo odpravo ali omejevanje.

Nagrada Slovenian Grand Security Award v kategoriji »najbolj varno podjetje« je za našo družbo velikega pomena, saj potrjuje dolgoročno zastavljene in dosledno uresničevane varnostne strategije ter prizadevanja naših zaposlenih.

Pozorni pa smo, da opremo redno testiramo na odzivnost našega sistema na različne scenarije kriznih dogodkov, kar vključuje tudi testiranje delovanja vseh ključnih podpornih, redundantnih sistemov, primernosti delovanja sistemov na sekundarni lokaciji in primernost vseh povezanih postopkov. Poleg tehničnih in infrastrukturnih ukrepov dajemo velik poudarek tudi izobraževanju zaposlenih, saj je njihova usposobljenost ključnega pomena pri hitrem in učinkovitem odzivu v različnih situacijah, kar pomembno prispeva k celoviti pripravljenosti naše družbe.

V zadnjem času se vedno bolj krepi spoznanje, da celoten energetski sektor potrebuje pomembne korake v smeri združevanja zmogljivosti na področju obvladovanja kibernetskih tveganj. So dogodki, kot je bil kibernetski napad na HSE spodbujevalni faktor, da je treba na tem področju hitreje izvesti določene korake, ali je to samo eden od dogodkov v nizu izzivov, s katerimi se sooča energetski sektor kot celota?

Tovrstnim dogodkom ne bi pripisali posebnega pomena na način, da je bila to prelomna ali spodbujevalna točka za našo družbo z vidika upravljanja s kibernetsko varnostjo, so pa takšni kibernetski napadi vsekakor podali jasen signal celotnemu energetskemu sektorju in vemo, da je področje kibernetske varnosti nujno obravnavati še bolj resno in sistematično. Vsi deležniki se moramo zavedati, da je področje kibernetske varnosti izjemno pomembno za zagotavljanje neprekinjenosti delovanja organizacij. S širjenjem digitalizacije procesov in upravljanja, izmenjave digitalnih podat-

kov ter razvojem novih tehnologij pa to področje še dodatno pridobiva na pomenu. V družbi smo že pred tem dogodkom izvajali vrsto aktivnosti na področju kibernetske varnosti, ki jih izvajamo še naprej.

Glede na omejenost kadrovskih in finančnih resursov je verjetno logična posledica, da se v celotnem energetskem sektorju poišče ustrezne sinergije v združevanju posameznih varnostnih zmogljivosti. Menite, da je lahko skupni Varnostno operativni center energetskega sektorja za kibernetsko varnost eden od teh korakov iskanja potrebnih sinergij?

Vzpostavitev skupnega varnostno operativnega centra lahko seveda prinese sinergijske učinke, predvsem z vidika boljših izmenjav informacij in izmenjav dobrih praks med deležniki energetskega sektorja. Prepričani smo, da bi vzpostavitev tovrstnega, zelo specifičnega in ciljno ozko usmerjenega centra lahko predstavljala tudi vrsto tveganj oziroma izzivov. Treba se je zavedati, da so znotraj posameznih sektorjev družbe, ki imajo različne potrebe in zrelost z vidika kibernetske varnosti, kar bi vsekakor predstavljajo zahtevno prilagajanje takega centra specifičnim tehnološkim in varnostnim potrebam posamezne družbe. Tudi pri samem reševanju incidentov in prioritizaciji incidentov vključenih organizacij bi lahko prišlo do določenih ovir, saj menimo, da skupni center ne more ustrezno prioritizirati vseh zahtev, še posebno v primeru, če bi se dogajali sočasni kibernetski napadi na družbe znotraj posameznega sektorja. Tak varnostno operativni center bi lahko predstavljal sorazmerno veliko izpostavljenost kibernetskim napadom, saj bi napad na skupni center energetskega sektorja pomenil veliko škodo in dodatno tveganje za celoten sektor, ki je za delovanje države izrednega pomena.

Namesto samo enega skupnega sektorskega varnostno operativnega centra je potreben razmislek o pristopu k vzpostavitvi tesnejšega znotraj sektorskega sodelovanja, kot je boljše deljenje podatkov o grožnjah in informacijah o incidentih, hkrati pa ohranitev samostojnega upravljanja varnosti posameznih družb in vključevanje v različne varnostno operativne centre. Menimo, da to zagotavlja boljšo fleksibilnost, diverzifikacijo in specializiran pristop, hkrati pa zmanjšuje tveganja centralizacije.

Kadrovski potencial je v tem trenutku največji izziv vseh organizacijskih okolij. Kako se v vaši organizaciji lotevate teh izzivov predvsem na področju specialistov za posamezna področja?

V družbi Plinovodi se zavedamo, da je kakovosten kader ključ do uspeha, zato aktivno izvajamo politike razvoja in ohranjanja kadrov. V družbi redno vlagamo v razvoj kompetenc zaposlenih z različnimi izobraževalnimi programi, delavnicami ter posluhom za individualne želje po strokovnem razvoju in osebnostni rasti. Naš cilj je, da smo družba, kjer ljudje radi delajo, saj verjamemo, da se z zadovoljstvom zaposlenih neposredno povečuje tudi kakovost njihovega dela in s tem uspešnost organizacije kot celote.

Zagotavljanje varnosti delovanja sistemov, zaposlenih in tudi vplivi na okolje so vedno bolj izraženi in zahtevajo določene finančne in druge vložke. Lahko ocenite, da lastniki ustrezno razumejo to potrebo in vas podpirajo pri teh korakih?

Z zadovoljstvom lahko rečemo, da naši lastniki razumejo pomembnost vlaganj v varnost delovanja sistemov in nas pri teh aktivnostih podpirajo. Zavedajo se, da so investicije v varno delovanje bistvene, ne le za zmanjševanje tveganj, temveč tudi za dolgoročno poslovno uspešnost in trajnostno delovanje organizacije. Zaradi tega imamo zagotovljeno podporo in potrebna sredstva za izvajanje vseh ključnih varnostnih ukrepov in projektov.

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

Združevanje strokovnjakov s področja korporativne varnosti ocenjujemo kot zelo pomembno. Takšna formalna in neformalna združevanja omogočajo izmenjavo izkušenj, najboljših praks in znanja med strokovnjaki iz različnih organizacij in sektorjev, ki lahko bistveno prispevajo k dvigu kvalitete korporativne varnosti v Sloveniji, omogočajo strokovno rast posameznikov in prinašajo številne koristi na področju skupnega soočanja z izzivi, ki jih prinaša vedno bolj kompleksno varnostno okolje. ■

Foto: arhiv Plinovodi d.o.o.

VARNOSTNI PREHODI ZA KONTROLO DOSTOPA V NADZOROVANA OBMOČJA

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

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

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

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

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

ID Shop zagotavlja celovite rešitve za zagotavljanje kontrole pristopa:

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

IDealni partner za identifikacijo in varnost

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

cominfo By GUNNEBO Entrance Control

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

Avtor: Matic Čaleta / Institut za korporativne varnostne študije

INTERVJU
dr. Ciril Kafol, direktor sektorja strateške inovacije, Elektro Gorenjska d.d.*

ENERGETIKA V ISKANJU NOVIH TEHNOLOŠKIH REŠITEV ZA ZAGOTAVLJANJE VIŠJE ODPORNOSTI

Neprekinjenost delovanja ključnih elektroenergetskih organizacij lahko zagotavljamo samo s konstantnim uvajanjem novih tehnoloških rešitev, ki zagotavljajo višjo raven prožnosti in odpornosti zagotavljanja električne energije. O razvojnih izzivih na področju upravljanja s tveganji smo se pogovarjali z direktorjem za strateške inovacije v Elektru Gorenjska.

Elektro Gorenjska je eden izmed manjših distribucijskih podjetij v Sloveniji, vendar izredno agilno v smeri uvajanja novih tehnologij. Kje so po vašem mnenju glavni tehnološki izzivi zagotavljanja učinkovite distribucije električne energije v bližnji prihodnosti?

V Elektru Gorenjska smo se lotili intenzivnega cikla posodabljanja novih tehnologij in uvajanja naprednih sistemov za upravljanje z omrežjem. Ključne izzive vidimo pri integraciji obnovljivih virov saj povečanje deleža energije iz sončnih in vetrnih virov zahteva boljšo integracijo le-teh v električno omrežje.

Naslednji izziv je vključevanje večjih sistemov za skladiščenje energije, kjer je treba razviti načine in vsebine uporabe BHEE ter jih smiselno integrirati v sistem upravljanja. Ukvarjamo se tudi intenzivno uporabo konceptov pametnega omrežja ter načrtovanjem in implementiranjem večje količine le-teh v omrežju. Pri tem je treba integrirati elemente pametnega omrežja in obenem pretehtati smiselnost kombinirane uporabe pametnih in klasičnih prijemov razvoja omrežja.

Zaradi bistvenega povečanja števila OVE je izziv tudi obvladovanje decentralizirane proizvodnje, za kar je treba razviti nove strategije upravljanja in nadzora, da se zagotovi stabilnost in zanesljivost oskrbe. Intenzivna digitalizacija prinaša izzive pri dvigu stopnje kibernetske varnosti; digitalizacija energijskega sektorja zahteva, da se ta zaščiti pred kibernetskimi napadi, ki bi lahko destabilizirali ključne infrastrukturne sisteme.

Zaradi optimalnejšega upravljanja z omrežjem in zniževanjem špičnih obremenitev so izzivi tudi pri spodbujanju sistemov za prihranke in energetsko učinkovitost, kjer skupaj s partnerji razvijamo in spodbujamo uporabo avtomatiziranih sistemov za aktivni odjem oziroma prilagajanje porabe in odjema pri industrijskih in gospodinjskih uporabnikih. Nadalje, širjenje električnih vozil povečuje obremenitev električnega omrežja in zahteva razvoj infrastrukture za polnjenje ter rešitve za podporo večji konici povpraševanja. Zaradi vseh sprememb pa menimo, da se morajo regulacija in modeli poslovanja v energetskem sektorju prilagoditi hitro spreminjajoči se pokrajini, kjer je potrebna tudi uskladitev mednarodnih standardov in politik, zato je izziv tudi ustrezno informiranje in spodbujanje regulatorja k naprednim pristopom regulacije trga.

V zadnjem obdobju ste tudi pomemben del evropskih konzorcijev v projektih na temo različnih vidikov varnosti. Katere so tiste dodane vrednosti, ki jih pridobivate skozi sodelovanje na teh mednarodnih projektih?

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Smo vključeni v več kot 10 evropskih projektov, ki naslavljajo izzive distribucije električne energije v sedanjosti in prihodnosti. V teh projektih se srečujemo tako z dobaviteljskim trgom kot sorodnimi distribucijskimi podjetji, ki so v različnih fazah razvoja, tako produktov kot tudi poslovnih modelov. Dodana vrednost, ki jo iščemo v projektih so bodisi izdelki ali koncepti, ki jih lahko apliciramo na našem omrežju, bodisi rešitve in poslovni modeli, ki jih lahko širše uporabimo pri razvoju in upravljanju omrežja.

Pred organizacijami se nahajajo pomembne zahteve uveljavljanja celega niza zakonskih zahtev, ki imajo podlago v predhodno sprejetih evropskih direktivah, kot na primer direktiva CER in NIS-2. Kako se s temi zahtevami soočate v Elektru Gorenjska, kjer imate kot manjše distribucijsko podjetje verjetno še dodatne izzive?

V Elektru Gorenjska imamo dolg »track record« uvajanja rešitev kibernetske varnosti. Izziv za nas kot manjše podjetje je predvsem v prilagajanju konceptov in rešitev na naše potrebe, in sicer v smeri optimizacije uporabe glede na finančne in kadrovske zmožnosti.

Rešitve iščemo v zunanjem izvajanju in povezovanju z drugimi energetskimi deležniki, tako v RS kot v tujini. Evropske direktive spremljamo in implementiramo v operativno poslovanje.

Kot eno ključnih zadev pa prepoznavamo izvajanje izobraževanja in ozaveščanja, kjer s pogostimi in različnimi aktivnostmi naslavljamo vse zaposlene.

Priča smo vedno obsežnejšem uvajanju informacijske podpore energetskega sistema in digitalizacije procesov, kar na drugi strani povečuje možnost kibernetskih tveganj. Kako se v vaši organizaciji soočate s temi izzivi?

Snovanje rešitev digitalizacije vedno vsebuje tudi komponento kibernetske varnosti. Pri tem se nanašamo na lastne arhitekte in zunanje izvajalce. V tem procesu smo implementirali varnostne politike, uporabili napredne tehnologije za ščitenje IT/OT okolja, izvajamo redne varnostne posodobitve, uporabljamo več faktorsko avtentikacijo in druge ukrepe, na ključnih sistemih smo vpeljali šifriranje podatkov ter izvajamo vrsto preventivnih ukrepov za zaščito pred kibernetskimi napadi. Ravno tako smo vključeni v skupni varnostno operativni center podjetij za distribucijo električne energije, kjer dinamično naslavljamo tveganja s področja kibernetske varnosti.

Vzdrževanje in nadzor nad delovanjem vaše infrastrukture je zahteven predvsem v gorskih predelih, kjer imate razvejano infrastrukturo. Menite, da bi lahko z uporabo brezpilotnih letal učinkoviteje nadzirali stanje in poškodbe na infrastrukturi?

Večina omrežja Elektra Gorenjska je pod zemljo, zato uporabe brezpilotnih letal ne planiramo v večjem obsegu. Smo pa v nekaj projektih analizirali potrebe in bomo na segmentih omrežja, kjer je to smiselno uporabljali skupnostne storitve.

Menite, da bi lahko uporaba umetne inteligence pripomogla k učinkovitejšemu spremljanju parametrov delovanja omrežja in racionalizaciji porabe električne energije?

Da, uporaba umetne inteligence lahko pripomore boljšemu upravljanju z omrežjem. Smo tudi pristopili k nekaj projektom, ki naslavljajo te izzive, nekaj smo jih pa tudi implementirali. Uporabo vidimo predvsem pri boljši podpori uporabnikom in podpori odločanja operaterjem, ki upravljajo z omrežjem.

V zadnjem obdobju so se močno pospešili koraki uvajanja enotnega varnostnega operativnega centra kibernetske varnosti za celoten elektroenergetski sektor. Kako v Elektru Gorenjska dojemate ta projekt in kakšna so vaša pričakovanja?

Podpiramo aktivnosti uvajanja skupnega varnostno operativnega centra kibernetske varnosti za energetski sektor. V tej iniciativi vidimo priložnost za izboljšanje kibernetske varnosti in optimizacijo stroškov in investicij v kibernetsko varnost. Želimo si profesionalen, odziven in kompetenten center, ki bo dvignil raven kibernetske varnosti na tako stopnjo, ki je sami ne bi zmogli doseči. ■

Foto: Dean Dubokovič

Smart Fire / Gas Safety for Energy Transition Sites.

SENSIA

AI Thermal Cameras for Methane/SO_2 Leak Detection – EU Ready

- **Gas Detection**
- **Gas Quantification**
- **Intelligent Thermal & Visual Detection**
- **Flame Detection**

ZARJA ELEKTRONIKA

Kovinarska cesta 4, 1241 Kamnik
T: +386 1 8317 488 • **F:** + 386 1 8317 551 • **Service T:** + 386 1 8317 452
M: +386 30 603 144
E: info@zarja.com • prodaja@zarja.com
www.zarja.com

Avtor: Matic Čaleta / Institut za korporativne varnostne študije

INTERVJU
g. Miha Schnabl, direktor Javne agencije za civilno letalstvo Republike Slovenije*

POMEMBNA VLOGA REGULATORJA NA PODROČJU CIVILNEGA LETALSTVA

Ob dejstvu, da globalno varnostno okolje močno vpliva tudi na letalske operacije, ima v tem pogledu Javna agencija za civilno letalstvo Republike Slovenije pomembno regulativno in svetovalno vlogo pri oblikovanju varnostnih procedur in standardov. Če v ta okvir dodamo še usmerjanje in nadzor nad področjem uporabe brezpilotnih letalnikov je zelo pomembno razumeti vizijo razvoja letalskega področja. O tem in ostalih izzivih smo se pogovarjali z direktorjem g. Miho Schnablom.

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

Strateški varnostni izzivi mednarodnega okolja se v veliki večini pokrivajo s tistimi, s katerimi se sooča letalstvo, s tem pa tudi Agencija. Največje izzive pričakujem na področju kibernetske oziroma informacijske varnosti, saj letališča, kontrola zračnega prometa in letalski organizacije postajajo privlačne tarče za različne vrste napadov.

Tudi terorizem še vedno ostaja eden izmed izzivov, kar potrjujejo nedavni (2024) poskusi sabotaže s pošiljanjem vnetljivih naprav prek paketne dostave DHL v Nemčiji in Združenem kraljestvu. Naprave, ki naj bi bile povezane z rusko vojaško obveščevalno službo, so bile skrite v na videz nenevarnih pošiljkah in so se (na srečo prekmalu) same vžgale v logističnih centrih.

Podnebne spremembe, ki so sicer v ospredju ključnih strateških globalnih izzivov pa seveda vplivajo tudi na letalstvo. Le te namreč povečujejo pogostost in intenzivnost ekstremnih vremenskih pojavov (več neurij, močnih vetrov, toče, turbulenc, tornadov in nenadnih sprememb vremena), kar lahko vse vpliva na varnost letalskih operacij.

Glede preglednosti bi rekel, da je letalski regulativi lastna zapletenost, kar deloma velja tudi za urejanje uporabe brezpilotnih zrakoplovov. Ampak hkrati tudi verjamem, da Agencija uporabnikom zagotavlja dovolj strokovne pomoči, s čimer se relativizira morebitne nejasnosti.

Sedaj je že poteklo dovolj časa, ko smo v pravni red Republike Slovenije prevzeli EU uredbo o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov. Kako ocenjujete uspešnost korakov za uveljavitev te uredbe pri zave-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

zanih posameznikih in organizacijah?

V Sloveniji je trenutno registriranih nekaj manj kot 8000 operatorjev brezpilotnih zrakoplovov in preko 6000 ustrezno usposobljenih pilotov na daljavo. Na splošno ugotavljamo, da je uporabnikov brezpilotnih zrakoplovov, ki ne izpolnjujejo zahtev predpisov EU bistveno več. Po drugi strani pa se iz leta v leto povečuje število operatorjev v posebni kategoriji, kar je pokazatelj, da se brezpilotni zrakoplovi vedno bolj uporabljajo v profesionalne namene, ter da se na tem področju nivo znanja in strokovnosti pri uporabnikih dviguje.

Agencija mora skrbeti za ozaveščanje, zato vsako leto izvaja številne aktivnosti, povezane s promocijo letalske varnosti, med drugim tudi na področju brezpilotnih zrakoplovov (npr. z obiski osnovnih in srednjih šol). Poleg tega Agencija omogoča brezplačno virtualno usposabljanje, v želji biti organ prijazen uporabniku, zato omogočamo tudi spletno registracijo operatorja ter opravo izpita. Na Agenciji imamo še več nerealiziranih idej, prek katerih se želimo približati uporabnikom (npr. z vzpostavitvijo profila, poleg obstoječega na platformi Facebook, še na omrežju TikTok; sodelovanje s televizijskimi hišami), na ta način pa okrepiti doseg naših sporočil.

Je sistemski pristop povezan z licenciranjem brezpilotnih plovil in operatorjev prinesel dovolj preglednosti, da lahko rečemo, da v Sloveniji obvladujemo to zahtevno področje?

Na splošno lahko rečem, da je vzpostavljen sistem učinkovit, in da zagotavlja letalsko varnost, seveda pa so vedno možnosti za izboljšavo. Sam jih vidim predvsem pri uporabnikih, ki brezpilotne zrakoplove še vedno vidijo kot eno izmed igrač. Obvladovanje določenega področja je po eni strani povezano s ciljnim osveščanjem, po drugi strani pa tudi z učinkovitim nadzorom. V Sloveniji imamo nadzor nad uporabo brezpilotnih zrakoplovov razdeljen med več institucij (Agencija, Policija, občinska redarstva, naravovarstveni nadzorniki), kar omogoča učinkovitejši nadzor, saj Agencija zaradi centralizirane organizacije (zgolj v Ljubljani) ne more (hkrati) zagotavljati nadzora nad celotnim ozemljem države. Glede preglednosti bi rekel, da je letalski regulativi lastna zapletenost, kar deloma velja tudi za urejanje uporabe brezpilotnih zrakoplovov. Ampak hkrati tudi verjamem, da Agencija uporabnikom zagotavlja dovolj strokovne pomoči, s čimer se relativizira morebitne nejasnosti.

V zadnjem obdobju je veliko vprašanj in izzivov povezanih z nemotenim delovanjem heliportov na bolnišnični infrastrukturi. Glede na to, da je ta infrastruktura neposredno umeščena na bolnišnične objekte, je varnost operacij še toliko bolj izpostavljena. Katera so tista ključna napotila upravljalcem te infrastrukture, vezana na ustrezen proces licenciranja kadra in infrastrukture?

Agencija skrbi za skladnost bolnišničnih heliportov s priporočili in standardi Mednarodne organizacije za civilno letalstvo (ICAO), prisotna pa je v celotnem življenjskem ciklu heliporta; tako v fazi projektiranja z izdajo ustreznega predhodnega soglasja, (ki je pogoj za pridobitev gradbenega dovoljenja) kot pri izdaji obratovalnega dovoljenja po zaključku gradnje; v času veljavnosti obratovalnega dovoljenja pa Agencija deluje kot nadzorni organ, ki skrbi, da obratovalec heliporta spoštuje standarde in priporočila ICAO, s čimer se zagotavlja varnost zračnega prometa na heliportu in v okolici. Glede ključnih napotil obratovalcem heliportov, o katerih me sprašujete, pa bi našim zavezancem najprej sporočil, da je Agencija sicer res njihov nadzorni organ, ampak da je naše poslanstvo tudi spodbujanje varnosti zračnega prometa, zato so pri nas vedno dobrodošli, z vsemi dvomi in izzivi, s katerimi se soočajo pri obratovanju heliportov. Agencija se trudi biti zavezancem prijazen organ, ki mu zavezanci zaupajo, saj skupno naslavljanje izzivov krepi zagotavljanje varnosti zračnega prometa. Če sem pa konkretnejši, obratovalcem heliportov svetujem predvsem, da namenjajo dovolj finančnih sredstev, tako za usposabljanje kadra, kot za vzdrževanje (in posodabljanje) infrastrukture, saj je zagotavljanje letalske varnosti vedno povezano z zadostnimi sredstvi, namenjenimi kadrom in infrastrukturi.

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

Na formalni ravni je kibernetska varnost kot sestavni del informacijske varnosti v Agenciji urejena s Pravilnikom o informacijski varnosti. Na konkretni ravni pa to pomeni, da smo povezani v državno komunikacijsko omrežje HKOM, ki je v pristojnosti Ministrstva za digitalno preobrazbo. HKOM ima svoje požarne pregrade in interne varnostne politike. Za dostop do našega okolja uporabljamo VPN povezavo, ki je dodatno zaščitena z več faktorsko avtentikacijo (MFA). V našem lastnem omrežju pa uporabljamo t. i. „next-gen“ požarno pregrado. Poleg tega je dostop iz našega okolja do interneta možen izključno prek nadzorovanega PROXY strežnika. Skrbimo tudi za segmentacijo našega omrežja – ločujemo uporabnike, infrastrukturo in virtualne strežnike v različna omrežja, kar bistveno zmanjšuje možnost širjenja morebitnih incidentov. Še dodatna avtentikacija skrbi, da se lahko v naše omrežje povežejo le preverjene naprave. Na vseh delovnih postajah je nameščena stalno posodobljena antivirusna programska oprema, prav tako vsakodnevno izvajamo antivirusne preglede. Agencija ima vzpostavljen sistem varnostnega arhiviranja po načelu 3-2-1 (tri kopije podatkov, na dveh različnih medijih, ena kopija izven lokacije), tako da se podatki shranjujejo na način, ki čim bolj zmanjša tveganje za izgubo podatkov v primeru napake, nesreče, kibernetskega napada ali kateregakoli drugega incidenta. To so naši notranji procesi.

Agencija je sicer upravni, inšpekcijski, prekrškovni in regulatorni organ s področja letalskih predpisov v zvezi z varnostjo in varovanjem v civilnem letalstvu, vendar do sedaj ni imela pristojnosti na področju informacijske varnosti. Z začetkom uporabe določb evropske regulative (t. im. Del-IS) oktobra 2025 pa Agencija pridobiva novo nadzorno pristojnost (procesi navzven), saj bodo morale letalske organizacije vzpostaviti sistem za prepoznavanje in upravljanje tveganj informacijske varnosti, ki bi lahko vplivali na informacijsko-komunikacijske sisteme in podatke, uporabljene za namene civilnega letalstva. Ker gre za povsem novo področje delovanja je Agencija za njene uradne osebe, ki bodo nad zavezanci izvajale tudi nadzor, zagotovila tri dnevno usposabljanje, ki bo izvedeno v začetku maja. Primarni namen tega izobraževanja je usposobiti uradne osebe za opravljanje nadzora, ki pa bo hkrati krepil tudi samozavest uradnih oseb Agencije o pomenu informacijske varnosti.

Poleg tega je Agencija z namenom ozaveščanja naših zavezancev o novih obveznostih s področja Del-IS in z željo vzpodbujati zavest o pomenu informacijske varnosti 28. marca 2025 v sodelovanju z Uradom vlade za informacijsko varnost, Slovenskim inštitutom za kakovost in meroslovje ter Kontrolo zračnega prometa Slovenije pripravila okroglo mizo, ki je pokazala, da so po eni strani večje letalske organizacije že relativno dobro pripravljene na nove zahteve, po drugi strani pa se manjše letalske organizacije šele seznanjajo z novimi obveznostmi.

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

Še preden bi se Agencija sploh lahko soočila z ugotavljanjem, ali lahko privabi strokoven kader, se ukvarjamo s tem, da nam omejitve Zbirnega kadrovskega načrta Vlade že več let sploh ne omogočajo zaposlovanja. Če sem izrazito ciničen, sem nevoščljiv tistim direktorjem, ki se ukvarjajo s tem, kje dobiti strokoven kader, ne pa s tem, da bi ga sploh smeli iskati. ■

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Metod Vidmar, direktor za korporativno varnost, Skupina SIJ*

UPRAVLJANJE VARNOSTNIH TVEGANJ V INDUSTRIJSKIH OKOLJIH ŠE POSEBEJ IZPOSTAVLJENO

Učinkovito obvladovanje tveganj je postalo nujen predpogoj za učinkovito in varno delovanje vsake organizacije. Ko pa govorimo o zahtevnih industrijskih okoljih, pa to področje dobi še dodatne izzive, ki jih je treba pravilno razumeti. Temu posebno mesto namenjajo tudi v Slovenski industriji jekla, ki je s svojo mednarodno vpetostjo, izpostavljena celemu nizu različnih varnostnih tveganj. O pristopih in izkušnjah s tega področja smo se pogovarjali z g. Metodom Vidmarjem, letošnjim nagrajencem v kategoriji »korporativno varnostni manager leta«.

Dovolite, da vam še enkrat čestitamo za prejem letošnje nagrade Slovenska velika nagrada varnosti oziroma Slovenian Grand Securiy Award v kategoriji »korporativno varnostni manager leta«. Kako razumete pomen prejete nagrade?

Najlepša hvala za čestitke, iskreno jih cenim. Nagrado v kategoriji korporativni varnostni manager razumem kot priznanje, ne le mojemu delu, temveč tudi širšemu timu in vodstvu, ki nas že deset let podpira pri realizaciji idej za ustvarjanje varnostne kulture v Skupini SIJ – Slovenska industrija jekla. Smo največja jeklarska skupina v Sloveniji sedežem v Ljubljani, proizvodnimi družbami na dveh lokacijah v Sloveniji in razvejano distribucijsko mrežo podjetij na naših ključnih trgih. S približno 3.600 zaposlenimi smo steber zaposlovanja na Ravnah in Jesenicah in kot eden največjih slovenskih izvoznikov delujemo v mednarodnem poslovnem okolju.

Zame je ta nagrada potrditev, da je v tako veliki skupini z več kot 30 podjetji in velikim številom zaposlenih in partnerjev celovit, odgovoren in sodelovalen pristop k varnosti prepoznan kot pomembna dodana vrednost. Varnost danes ni več samo tehnična in operativna funkcija, temveč strateški element zagotavljanja nemotenega poslovanja družb. To priznanje mi daje dodatno motivacijo, da bomo to vizijo razvijali in uresničevali še naprej.

Nagrado v kategoriji korporativni varnostni manager razumem kot priznanje, ne le mojemu delu, temveč tudi širšemu timu in vodstvu, ki nas že deset let podpira pri realizaciji idej za ustvarjanje varnostne kulture v Skupini SIJ – Slovenska industrija jekla.

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

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Pomembno je poudariti, da korporativna varnost pri tem ne deluje sama – pri zagotavljanju nemotenega poslovanja v družbah naše skupine sodelujemo s številnimi službami. Takšen integriran varnostni sistem omogoča celovitejše obvladovanje varnostnih tveganj, večjo odpornost in boljšo usklajenost procesov.

Drži, že 40 let se tako ali drugače ukvarjam z obvladovanjem varnostnih tveganj. Svojo poklicno pot sem po končani kadetski šoli v Tacnu takrat začel še kot miličnik. Kmalu sem začel tudi s študijem, ki sem ga vedno opravljal ob delu, ker nisem hotel ničesar zamuditi. Vedno me je zanimalo operativno delo in imel sem možnost, da sem se lahko učil od najboljših, in tudi hitro napredoval na vodilna delovna mesta. Po spletu okoliščin sem za osem let odšel na Veleposlaništvo Republike Slovenije v Skopju, kjer sem se srečal z novimi varnostnimi izzivi in tveganji pri varovanju najvišjih predstavnikov države in sodeloval pri obvladovanju migracijskih tokov v Zahodno Evropo. Po vrnitvi v Slovenijo sem se ponovno pridružil policiji, kjer sem se specializiral za področje gospodarske kriminalitete, kasneje pa delal tudi na področju mejnih zadev in tujcev ter kariero v policiji zaključil kot komandir. Z vsemi izkušnjami in znanjem sem bil pred desetletjem povabljen v Skupino SIJ, da takrat kot prvi sodelavec za korporativno varnost vzpostavim sistem in to mi je, kasneje tudi skupaj z ekipo, uspelo.

V zadnjem obdobju ste torej zelo močno vpeti v upravljanje varnostnih tveganj v industrijskem okolju, saj ima Skupina SIJ več proizvodnih lokacij v Sloveniji. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost Skupine SIJ?

V današnjem hitro spreminjajočem se svetu, kjer se varnostna tveganja razvijajo skupaj s tehnološkim napredkom, geopolitičnimi premiki in družbenimi spremembami, je ključnega pomena, da organizacije znajo prepoznati in proaktivno nasloviti tudi nove oblike groženj. Nenehno prilagajanje varnostnim razmeram ter iskanje novih rešitev in izboljšav pomaga zagotavljati nemoteno poslovanje, kar je za podjetja, ki delajo 24 ur in 7 dni v tednu lahko pomembna prednost.

Zmožnost analiziranja, predvidevanja in prilagajanja tem spremembam nam omogoča ne samo zaščititi naše ključne vire in zagotavljati nemoteno poslovanje, temveč tudi graditi zaupanje z našimi partnerji in strankami. Organizacije, ki varnost dojemajo kot strateško prednost in jo vključujejo v svoje poslovne procese, lažje ohranjajo stabilnost, ugled in dolgoročno uspešnost.

Pomembno je poudariti, da korporativna varnost pri tem ne deluje sama – pri zagotavljanju nemotenega poslovanja v družbah naše skupine sodelujemo s številnimi službami. Takšen integriran varnostni sistem omogoča celovitejše obvladovanje varnostnih tveganj, večjo odpornost in boljšo usklajenost procesov. Prav takšna sinergija različnih strokovnih področij nam omogoča, da kot skupina dosegamo visoke standarde kakovosti, kot je na primer ResponsibleSteel, certifikat za trajnostno proizvodnjo jekla, ki ga ima trenutno le 15 jeklarskih skupin na svetu, ki izpolnjujejo najzahtevnejše standarde na področju okolja, družbene odgovornosti in upravljanja. To prispeva k naši konkurenčnosti na globalnem trgu in svoj košček v mozaik družbene odgovornosti, npr. do zaposlenih, poslovnih partnerjev in drugih deležnikov ter trajnostnega upravljanja dodaja tudi korporativna varnost.

Informacijska tehnologija je vedno bolj prisotna tudi v podpori glavnih proizvodnih procesov v industriji. Kako kompleksni so v tem okviru koraki za obvladovanje informacijskih tveganj, ki jim je podvrženo delovanje vašega podjetja?

Informacijska tehnologija je danes neločljivo vpeta v glavne proizvodne procese, kar sicer prinaša večjo učinkovitost in nadzor procesa, hkrati pa tudi dodatna informacijska tveganja. Obdelava velike količine podatkov pomeni tudi številne varnostne izzive, ki izhajajo iz prepleta IT in operativnih tehnologij.

Koraki za obvladovanje tveganj so kompleksni in vključujejo tako tehnične kot organizacijske ukrepe. Gre za stalno ocenjevanje tveganj, uvajanje naprednih varnostnih rešitev, izobraževanje in ozaveščanje zaposlenih. Izvajamo tudi stresne teste, redne varnostne preglede ter tesno sodelujemo z oddelkom IT in drugimi ključnimi službami.

Posebna pozornost je namenjena zaščiti industrijskih kontrolnih sistemov, varnosti podatkov, kibernetski odpornosti in zagotavljanju zanesljivosti celotne infrastrukture. Vse to zahteva usklajeno delovanje in visoko stopnjo zavedanja o pomenu visoke varnostne kulture vseh zaposlenih v skupini. To področje imamo urejeno tudi z ustreznimi internimi pravili, v sklopu katerih v Odboru za informacijsko varnost obravnavamo

Brez dvoma, tovrstne oblike povezovanja so izjemno pomembne. Slovensko združenje za korporativno varnost povezuje strokovnjake z različnih področij in omogoča izmenjavo znanj, izkušenj ter dobrih praks, kar pomembno prispeva h kakovosti dela na področju varnosti v celotni Sloveniji.

vse dejanske izredne varnostne dogodke in ocenjujemo potencialna nova tveganja ter sprejemamo potrebne ukrepe.

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

Popolnoma se strinjam, da je celovit pristop ključen za učinkovito zagotavljanje korporativne varnosti. V zadnjih letih res opažam močan poudarek na področju informacijske varnosti, kar je razumljivo glede na porast kibernetskih groženj, načine izvrševanja kaznivih ravnanj in škode, ki ob tem nastaja.

Preprosto povedano, varnostni sistemi so povezani in eno brez drugega ne gre. Naša naloga je postavljanje ovir, ki storilce odvračajo in jim preprečujejo nedovoljena ravnanja oziroma podaljšujejo čas za izvedbo načrta in povečujejo možnost, da bodo pri svojem ravnanju naredili napako, pustili sledi ali bili pri tem neposredno zaloteni.

Človeški faktor ostaja ključni izziv – ne glede na to, kako dober je sistem, lahko napaka ali malomarnost posameznika povzroči resne posledice.

Vse, kar človek naredi, lahko vedno naredi še boljše, kar žal ne drži samo v pozitivnem smislu. V to zgodbo se je zdaj »vmešala« še umetna inteligenca. Ljudje v njej vidijo predvsem veliko dobrega, le malo pa se jih ukvarja z vprašanjem, kako jo omejiti, obvladovati. Verjetno se bo večina strinjala, da njenega razvoja ni možno več nadzorovati, in da se temu napredku lahko le še prilagodimo, tudi na področju obvladovanja varnostnih tveganj.

Sprašujem se, ali se bo umetna inteligenca na koncu spraševala, ali še potrebuje človeka?

Kako prepričate vodstvo, da za delovanje procesov korporativne varnosti nameni ustrezne organizacijske in finančne vire?

Ni težko prepričevati nekoga, ki se zaveda tveganj in možnih posledic ter prepozna prednosti celovitega sistema korporativne varnosti. Vodstvo Skupine SIJ je prepoznalo pomen ukrepov za zavarovanje svojega premoženja in zagotavljanje nemotenega poslovanja. Lahko rečem, da si je naša služba s svojim trdim in uspešnim delom prislužila zaupanje vodstva. Od tu naprej je vse lažje.

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

Vlaganje v izobraževanje in razvoj kadrov je ključno, tudi ko gre za področje obvladovanja tveganj, saj se okolje in s tem tveganja nenehno spreminjajo. Kot veliko odgovorno podjetje se tega zavedamo in zato temu področju posvečamo veliko pozornosti. V korporativno varnost smo privabili že izobražene in izkušene strokovnjake, kar nam delo zelo olajša. Vsekakor tudi pri nas redno usposabljamo ključne kadre, tako z internimi kot eksternimi izobraževanji. Poleg tega veliko vlagamo v ozaveščanje zaposlenih, tako preko internih medijev kot izobraževanj, na vseh ravneh, saj verjamemo, da varnost ni le odgovornost korporativne varnosti, ampak celotne organizacije. Le z visoko varnostno kulturo smo lahko korak spredaj.

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

Brez dvoma, tovrstne oblike povezovanja so izjemno pomembne. Slovensko združenje za korporativno varnost povezuje strokovnjake z različnih področij in omogoča izmenjavo znanj, izkušenj ter dobrih praks, kar pomembno prispeva h kakovosti dela na področju varnosti v celotni Sloveniji.

Kot korporativni člani takšno sodelovanje vidimo kot priložnost za nadgrajevanje lastnega znanja, hkrati pa se zavedamo tudi svoje vloge pri soustvarjanju standardov in usmeritev, ki lahko koristijo tudi drugim. Povezovanje, strokovne razprave in skupno iskanje rešitev so ključni za razvoj celovite in sodobne varnostne kulture v Sloveniji.

Prepričan sem, da takšno sodelovanje prinaša dodano vrednost, ne le posameznim podjetjem, temveč tudi varnostni stroki kot celoti.

Ne morem mimo tega, da izrazim svojo željo, da bi naše združenje za korporativno varnost v prihodnosti naredilo še korak naprej in razmislilo o ustanovitvi Zbornice za korporativno varnost – podobno, kot to že obstaja pri drugih deležnikih varnostnega sistema Republike Slovenije, kot so varnostne službe in detektivi.
Takšna zbornica bi predstavljala pomemben institucionalni okvir, ki bi nam omogočal tudi izmenjavo relevantnih podatkov ter vpogledov v podatke, s katerimi upravljajo državni organi. Verjamem, da bi s tem okrepili tako strokovnost kot legitimnost delovanja na področju korporativne varnosti in dodatno prispevali k večji varnosti ter odpornosti družbe kot celote.

Cilj vseh je namreč isti, skrb za varnost ljudi in premoženja. ■

Foto: arhiv Skupina SIJ

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

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

Kako zagotovimo skladnost?

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

Kaj morate urediti?

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

Kako vam lahko pomagamo?

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

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

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
g. Andrej Dočinski, direktor Službe za korporativno varnost, UKC Ljubljana*

ZAGOTAVLJANJE VARNOSTI V ZDRAVSTVENEM SEKTORJU VEDNO POMEMBNEJŠI IMPERATIV

Univerzitetni klinični center v Ljubljani predstavlja 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. Andrejem Dočinskim.

Sedaj vodite Službo za korporativno varnost v naši najkompleksnejši zdravstveni organizaciji UKC Ljubljana že določeno obdobje. Nam lahko zaupate, kateri so tisti varnostni izzivi, katerim ste v tem obdobju namenili največ pozornosti?

Vodenje Službe za korporativno varnost (SKV) UKC Ljubljana sem prevzel februarja 2023 in iskreno si tudi predstavljati nisem mogel s kakšni izzivi vse se bom soočil na varnostnem področju. Zavedati se moramo, da kompleksnost ustanove v prvi vrsti izhaja iz dejstva, da gre za največjo zdravstveno ustanovo, ne samo v Sloveniji, temveč tudi širše v regiji. Po številu zaposlenih in razpoložljivih bolniških posteljah smo še najbolj primerljivi z bolnišnico AKH Dunaj. Če pa primerjamo UKC LJ s slovenskimi bolnišnicami, pa vedno rad izpostavim, da imamo v UKC Ljubljana toliko medicinskih sester, kot ima UKC Maribor vseh zaposlenih, toliko podpornega osebja, kot je zaposlenih v Bolnišnici Celje, toliko strežnic in gospodinj, kot je zaposlenih v Bolnišnici Jesenice in toliko zdravnikov, kot imata bolnišnica Izola in Jesenice skupaj vseh zaposlenih. Poleg vseh zaposlenih moramo nato dodati še dnevno fluktuacijo cca 3.000 pacientov in obiskovalcev, zunanjih specializantov, praktikantov, študentov, v času izvajanja obnove tudi delavcev gradbincev. Na prvem mestu zato največ pozornosti namenjamo področju fizične varnosti in nadzora, smo pa v tem času veliko truda vložili tudi v druga področja, še posebej smo okrepili področje kibernetske varnosti in integritete. Naš primarni cilj tako ostaja zagotavljanje varnega okolja za paciente, zaposlene in obiskovalce, pri čemer pa nenehno prilagajamo strategije novim varnostnim izzivom.

Želimo si, da se varnostnih procesov ne bi dojemalo kot uvajanje birokratskih ukrepov, temveč kot nepogrešljiv del zagotavljanja kakovostne in varne oskrbe pacientov. V ta namen pristop prilagajamo medicinskemu okolju, predvsem gre za poudarjanje, da je varnost del medicinske odgovornosti, saj neposredno vpliva na kakovost zdravljenja.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

Organizacijsko ste omenjeno Službo za korporativno varnost postavili na nove organizacijske temelje in jo kadrovsko močno okrepili. Lahko v kratkem predstavite glave spremembe in izboljšave?

Prvi korak je bil ta, da smo se lotili celovite analize obstoječega stanja tako, da smo izpostavili kritične dejavnike tveganj. Eden teh je bila vsekakor kadrovska sestava oziroma bolje rečeno kadrovska podhranjenost službe. Da smo izvedli vse potrebne organizacijske in strukturne spremembe, smo morali pridobiti podporo vodstva zavoda, kar nam je tudi uspelo, in nastala je, kot se je dobro leto nazaj izrazil predstavnik akreditacijske skupine iz Velike Britanije, sodobno zasnovana in napredna služba, ki pokriva širok spekter varnostnih tveganj. Če povzamem, temelji, na katerih smo postavili novo SKV, zagotavljajo celovitejši, bolj usklajen in proaktiven pristop k obvladovanju varnostnih tveganj. Pred mojim prevzemom vodenja SKV je bilo v SKV zaposlenih 12 oseb, danes pa služba zaposluje 46 oseb razporejenih v 6 enot: Enota za fizično in tehnično varovanje, kjer dajemo poudarek nadzoru in izboljšanju tehničnih varnostnih sistemov; Enota za izredno delovanje, katere namen je izboljšati pripravljenost na krizne situacije; Enota za integriteto, preko katere smo vzpostavili mehanizme za preprečevanje notranjih tveganj, korupcije in drugih nepravilnosti; Enoto za kibernetsko varnost, katere namen je izboljšati varnost IKT okolja, Enota za upravljanje s kritično IT infrastrukturo, s katero smo dali večji poudarek zagotavljanju neprekinjenega delovanja digitalnih sistemov v kriznih razmerah in Enota za psihološko pomoč zaposlenim, ki nudi psihološko podporo zaposlenim pri soočanju s stresom in izrednimi dogodki. Službo smo okrepili s strokovnjaki z vseh zgoraj omenjenih področij, še posebej pa sem ponosen, da nam je uspelo privabiti strokovnjake s področja kibernetske varnosti, kriznega upravljanja in fizičnega varovanja, kar nam omogoča boljšo pripravljenost na sodobne varnostne grožnje. Dodatno smo vpeljali stalno strokovno usposabljanje sodelavcev, s poudarkom na zagotavljanju informacijske in kibernetske varnosti, področja krizne komunikacije in obvladovanju nasilnih incidentov, nadgradnji sistema varnostnega upravljanja, ki omogoča boljšo analitiko varnostnih dogodkov in hitrejše odzivanje na incidente ter izdelavi celovitega načrta neprekinjenega poslovanja, ki določa postopke v primeru izrednih dogodkov. Posledično smo okrepili sodelovanje s ključnimi državnimi institucijami kot so policija, državni organi, civilna zaščita in nacionalni center za kibernetsko varnost, vse z namenom boljše usklajenosti pri kriznem upravljanju. Namen reorganizacije SKV je bil bistveno izboljšati odpornost UKC Ljubljana, da lažje in učinkoviteje obvladujemo fizična, digitalna in krizna varnostna tveganja. Naš cilj ostaja jasen – zagotavljati varno in stabilno okolje za bolnike, zaposlene in celotno organizacijo, ne glede na izzive prihodnosti, bistvo reorganizacije pa bila fleksibilnost in nenehno prilagajanje varnostnim izzivom. To lahko dosežemo samo z dobro ekipo sodelavcev in moja je odlična.

Kako se spopadate s potrebo razumevanja uveljavljanja varnostnih procesov v organizaciji, ki je strokovno in mentalno usmerjena v zagotavljanje zdravstvenih storitev?

UKC Ljubljana je organizacija, katere primarna naloga je zagotavljanje zdravstvenih storitev, kar pomeni, da je strokovna in mentalna osredotočenost zaposlenih usmerjena predvsem v skrb za paciente. V takšnem okolju je uveljavljanje varnostnih procesov izziv, saj jih mora osebje dojemati kot podporo svojemu delu in ne kot dodatno obremenitev. Želimo si, da se varnostnih procesov ne bi dojemalo kot uvajanje birokratskih ukrepov, temveč kot nepogrešljiv del zagotavljanja kakovostne in varne oskrbe pacientov. V ta namen pristop prilagajamo medicinskemu okolju, predvsem gre za poudarjanje, da je varnost del medicinske odgovornosti, saj neposredno vpliva na kakovost zdravljenja. Pri tem sta bistvenega pomena sodelovanje in dialog z zaposlenimi tako, da redno vključujemo zdravnike, medicinske sestre in drugo osebje v oblikovanje varnostnih ukrepov, da so le-ti prilagojeni njihovim potrebam. Želimo si zgraditi kulturo varnosti, kjer se bodo zaposleni zavedali, da lahko sami prispevajo k varnejšemu okolju.

Podpora strateškega vodstva organizacije je ključna za uspešno delovanje korporativne varnosti. Menite, da je v UKC Ljubljana zadostni nivo razumevanja in podpore s tega nivoja?

Podpora strateškega vodstva je resnično ključna za učinkovito delovanje SKV. V UKC Ljubljana smo na tem področju

> Menim, da Slovensko združenje za korporativno varnost že vrsto let več kot uspešno opravlja svojo vlogo pri povezovanju strokovnjakov, izmenjavi dobrih praks in razvoju standardov na področju varnosti v Sloveniji.

v zadnjih letih naredili pomembne korake naprej, saj vodstvo vedno bolj prepoznava, da varnost ni zgolj tehnično-operativno vprašanje, ampak strateški dejavnik, ki neposredno vpliva na kakovost zdravstvenih storitev in stabilnost celotne organizacije. Menim, da se vodstvo zavoda vse bolj zaveda pomena celostnega varnostnega pristopa, ki vključuje fizično, kibernetsko, informacijsko in psihološko varnost ter krizno upravljanje. Zaupanje se izkazuje tudi s tem, da se SKV kot sredstvo nadzora čedalje bolj vključuje v nabavne procese, načrtovanje investicij, IT-posodobitve, izdelavo kriznih načrtov in v organizacijske spremembe. Če povzamem, lahko rečem, da se v UKC Ljubljana nivo razumevanja in podpore strateškega vodstva za varnostne izzive izboljšuje, vendar je v to še vedno treba vlagati veliko napora, predvsem pa je potrebna stalna komunikacija in argumentacija. Naša naloga je, da skozi konkretne analize tveganj, različna poročila in preventivne ukrepe pokažemo, da je varnost ključni dejavnik stabilnosti, kakovosti in odpornosti zdravstvenega sistema.

Človeški potencial še vedno predstavlja pomemben izziv s stališča zagotavljanja varnosti. Kakšni so vaši pristopi, ki jih izvajate v UKC Ljubljana v smeri zagotavljanja višje varnostne kulture?

Res je, človeški dejavnik je eden ključnih elementov pri zagotavljanju varnosti, saj se lahko tudi najbolj napredni tehnični ukrepi izkažejo za neučinkovite, če zaposleni niso ozaveščeni in ustrezno usposobljeni. S tem namenom izvajamo ciljno usmerjena usposabljanja o fizični varnosti, kibernetski varnosti, ravnanju v kriznih situacijah in preprečevanju nasilja na delovnem mestu ter organiziramo simulacije varnostnih incidentov, kjer zaposleni pridobijo praktične izkušnje in se naučijo pravilnega odziva v realnih situacijah. Želimo poudariti pomen posameznika pri zagotavljanju varnosti, zato smo tudi s tem namenom vzpostavili dva mehanizma – institut »žvižgača« in »anonimno«, s katerima smo uvedli varne in anonimne kanale, prek katerih lahko zaposleni prijavijo varnostne incidente, grožnje ali kršitve brez strahu pred povračilnimi ukrepi. Idealno bi bilo vzpostaviti okolje, kjer so vsi zaposleni del rešitve pri zagotavljanju varnega delovnega okolja, a se zavedamo, da je do tja, ravno zaradi kompleksnosti sistema, še dolga pot.

Kakor v ostalih organizacijah, se tudi v UKC-Ljubljana, ob zares velikem številu zaposlenih, soočate z določenimi deviantnimi dejanji. Kako ste organizirali procese notranjih varnostnih ukrepov za odkrivanje teh nepravilnosti in kasnejšega sodelovanja s pristojnimi organi?

Bistveno sporočilo SKV, ki ga želimo posredovati zaposlenim je, da mi nismo nekakšna interna policija, ki preiskuje vse in vsakogar, kakor se nam zahoče. V bistvu je bila to ena mojih prvih usmeritev sodelavcem v SKV, saj za to nimamo ne pooblastil ne pristojnosti. Dejstvo je, da se tako kot v vsaki veliki organizaciji tudi v UKC Ljubljana soočamo z izzivi povezanimi z, kot ste izpostavili, deviantnimi dejanji, ki lahko vključujejo kraje, goljufije, nepooblaščene dostope do občutljivih podatkov in druge varnostne nepravilnosti. Kot sem že omenil, je teba za učinkovito obvladovanje teh tveganj vzpostaviti celovit sistem notranjih varnostnih ukrepov, od preventive, do odkrivanja dejanj in ukrepanja. V SKV to področje pokriva Enota za integriteto, ki vključuje strokovnjake za analizo in preiskavo prijavljenih nepravilnosti, pri čemer sodeluje tudi z drugimi oddelki in službami. Ob zaznanem

incidentu izvedemo temeljito preliminarno oceno in ugotovimo obseg težave. Če se potrdi sum nepravilnosti, zberemo in pripravimo dokazno gradivo ter po potrebi izvedemo razgovore z vpletenimi. V primerih zaznave kaznivih dejanj kot so npr. kraje, zlorabe podatkov, finančne goljufije in potencialna korupcijska tveganja, nemudoma obvestimo pristojne organe, to je policijo in KPK ter jim predamo celotno pridobljeno dokumentacijo povezano s posameznim primerom. Šele nato obvestimo vodstvo. Podobno velja pri kršitvah delovnopravne zakonodaje, le s to razliko, da glede na težo kršitve predlagamo ustrezne disciplinske ukrepe, ki lahko segajo od opozoril do odpovedi delovnega razmerja. Kot večkrat poudari vodstvo zavoda, je eden ključnih ciljev ustvariti delovno okolje, kjer so transparentnost, integriteta in varnost temeljni vrednoti vseh zaposlenih, zato je naše delo ključno pri zagotavljanju le-teh.

Informacijska varnost je tudi v zdravstvenem sektorju vedno bolj izpostavljena, kot potreba za zagotavljanje ustrezne varnosti ključnih podatkov, kakor tudi delovanja informacijskih sistemov, ki vedno močneje podpirajo osnovni zdravstveni proces. Kateri so tisti ključni koraki na področju zagotavljanja informacijske varnosti?

Informacijska varnost v zdravstvenem sektorju postaja ključna prednostna naloga, saj se zdravstveni procesi vedno bolj opirajo na digitalne sisteme, občutljivi podatki pacientov pa so vse bolj zaželena tarča kibernetskih napadov. Glede na to, da sem pred prevzemom vodenja SKV 5 let vodil Službo za IT infrastrukturo Področja za informatiko in sem z IT-jem tako ali drugače povezan že skoraj 20 let, lahko rečem, da temu področju v SKV dajemo izreden poudarek. V UKC Ljubljana smo vzpostavili celovit sistem upravljanja varovanja informacij SUVI, ki temelji na preprečevanju groženj, zgodnjem odkrivanju tveganj in hitrem odzivanju na incidente. Poudarek je na strogo nadzorovanem dostopu do informacijskih sistemov z vpeljevanjem različnih varnostnih sistemov, od večstopenjske avtentikacije, določanja najmanjšega obsega pravic uporabnikov informacijskih sistemov do ločevanja dostopov glede na njihove vloge in vpeljevanjem drugih rešitev, ki predstavljajo temelj kibernetske varnosti. Bistven korak, ki smo ga naredili s pomočjo Enote za kibernetsko varnost so redna varnostna usposabljanja za zaposlene, s poudarkom na prepoznavanju kibernetskih napadov, varnem rokovanju s podatki in zaščiti gesel. Z omenjenimi ukrepi želimo graditi odporno in varno informacijsko okolje, ki ščiti tako pacientove podatke kot stabilno delovanje zdravstvenih procesov. Zavedati se moramo, da informacijska varnost ni enkratni projekt, ampak neprekinjen proces prilagajanja nenehno spreminjajočim se grožnjam, ki še posebej v zadnjem času predstavljajo enega ključnih varnostnih tveganj ne samo pri nas, ampak širše v svetu. Posledično je naše sodelovanje z nacionalnimi varnostnimi organi in zunanjimi strokovnjaki za dodatno zaščito pred naprednimi grožnjami toliko bolj pomembno.

Zavedati se moramo, da informacijska varnost ni enkratni projekt, ampak neprekinjen proces prilagajanja nenehno spreminjajočim se grožnjam, ki še posebej v zadnjem času predstavljajo enega ključnih varnostnih tveganj ne samo pri nas, ampak širše v svetu.

Neprekinjenost delovanja naše najpomembnejše zdravstvene organizacije je vitalnega pomena za celotno državo. Zagotavljanje odpornosti organizacije je verjetno termin, ki ga največkrat slišite v zadnjem obdobju. Kako je vaša služba vključena v ta kompleksen proces zagotavljanja odpornosti?

Neprekinjeno delovanje UKC Ljubljana je kritično za zdravstveni sistem celotne države, saj kot največja zdravstvena ustanova oskrbujemo najzahtevnejše bolnike in zagotavljamo nujne zdravstvene storitve v vsakem trenutku. Odpornost organizacije pomeni sposobnost, da kljub motnjam, kot so na primer kibernetski napadi, naravne nesreče, epidemije ali okvare ključnih sistemov, še naprej zagotavljamo kakovostno in varno zdravstveno oskrbo. SKV je vključena v številne procese, od sodelovanja pri upravljanju načrta neprekinjenega delovanja, ki določa postopke za hiter odziv na krizne situacije, do načrtovanja ključnih rešitev za zagotavljanje delovanja kritičnih storitev in varnostnih protokolov za ključne objekte, sodelovanja pri izvajanju rednih vaj kriznega odzivanja, skrbi za stalni nadzor in zaščito IT infrastrukture ter upravljanju s fizičnim varovanjem in tehničnimi varnostnimi sistemi. Novost v slovenskem okolju pa je zagotovo Enota za psihološko pomoč zaposlenim, ki z izvajanjem programa psihološke podpore, ki vključujejo tudi delavnice in svetovanje za krepitev odpornosti osebja na stres, krizne situacije in zahtevne delovne pogoje, prav tako ključno vpliva na dolgoročno odpornost organizacije. SKV ima torej izjemno pomembno vlogo pri zagotavljanju odpornosti, saj skrbimo, da se organizacija lahko hitro prilagaja in učinkovito odziva na krizne razmere, da bolnišnica ostane stabilna, varna in operativna ne glede na zunanje ali notranje grožnje in s tem posredno varujemo zdravje in življenje pacientov.

UKC Ljubljana je dolga leta eden izmed ključnih članov Slovenskega združenja za korporativno varnost. Kako skozi vaše oči vidite dosedanji razvoj omenjenega združenja in vaših bodočih pričakovanj ob nadaljevanju odličnega sodelovanja tudi v prihodnosti?

Menim, da Slovensko združenje za korporativno varnost že vrsto let več kot uspešno opravlja svojo vlogo pri povezovanju strokovnjakov, izmenjavi dobrih praks in razvoju standardov na področju varnosti v Sloveniji. S članstvom v Združenju ima UKC Ljubljana, ki je eno najkompleksnejših in najpomembnejših zdravstvenih organizacij v državi, dostop do najnovejših trendov, znanja in strateškega mreženja na področju varnosti. Združenje predstavlja ključnega partnerja pri strateškem razvoju varnosti v UKC Ljubljana, pa tudi širše v slovenskem zdravstvenem sistemu. Z veseljem bomo nadaljevali in nadgrajevali sodelovanje, saj verjamemo, da lahko skupaj še bolj prispevamo k večji varnosti, odpornosti in stabilnosti naše družbe. ■

Foto: arhiv UKC Ljubljana

YOUR ORGANIZATION COULD BE NEXT.

Welcome to CPP, where your security is our priority.

www.cpp.mk

- Security Operation Center - 24/7 Continuous monitoring security events
- Incident Response 24/7 – Immediate action when threats strike.
- Log Management & SIEM – Real-time monitoring to detect and prevent breaches.
- Penetration Testing – Simulating attacks to expose vulnerabilities before hackers do.
- Vulnerability Management – Identifying risks and securing your digital assets.
- Dedicated Red and Blue Team – Offense meets defense for maximum security.
- Security Awareness Training – Empowering your workforce to be the first line of defense.
- Cyber Security Consultancy & Compliance – Ensuring regulatory compliance and industry standards.

CPP SERVICES

CYBER PROTECTION & PRIVACY SERVICES

Avtor: mag. Venčeslav Perko / Eles in sodelavci na projektu*

UMETNA INTELIGENCA ZA VOC SLOVENSKE ELEKTRO-ENERGETIKE – PRIMER EU PROJEKT ALIENS-SOC

Energetski sektor izredno hitro spreminja analogno okolje v digitalno. Novi načini proizvodnje električne energije so razpršeni, način upravljanja prenosa in distribucije energije do končnih odjemalcev zahteva popolnoma drugačen pristop, ki ne bi bil mogoč brez digitalizacije. Z razvojem digitalizacije v energetiki in povečevanjem odvisnosti digitalnih storitev se povečuje tudi kibernetska ogroženost. Klasičnim tveganjem, ki so bila več ali manj tveganja kritične infrastrukture, je sedaj dodan še širok spekter tveganj iz kibernetskega okolja.

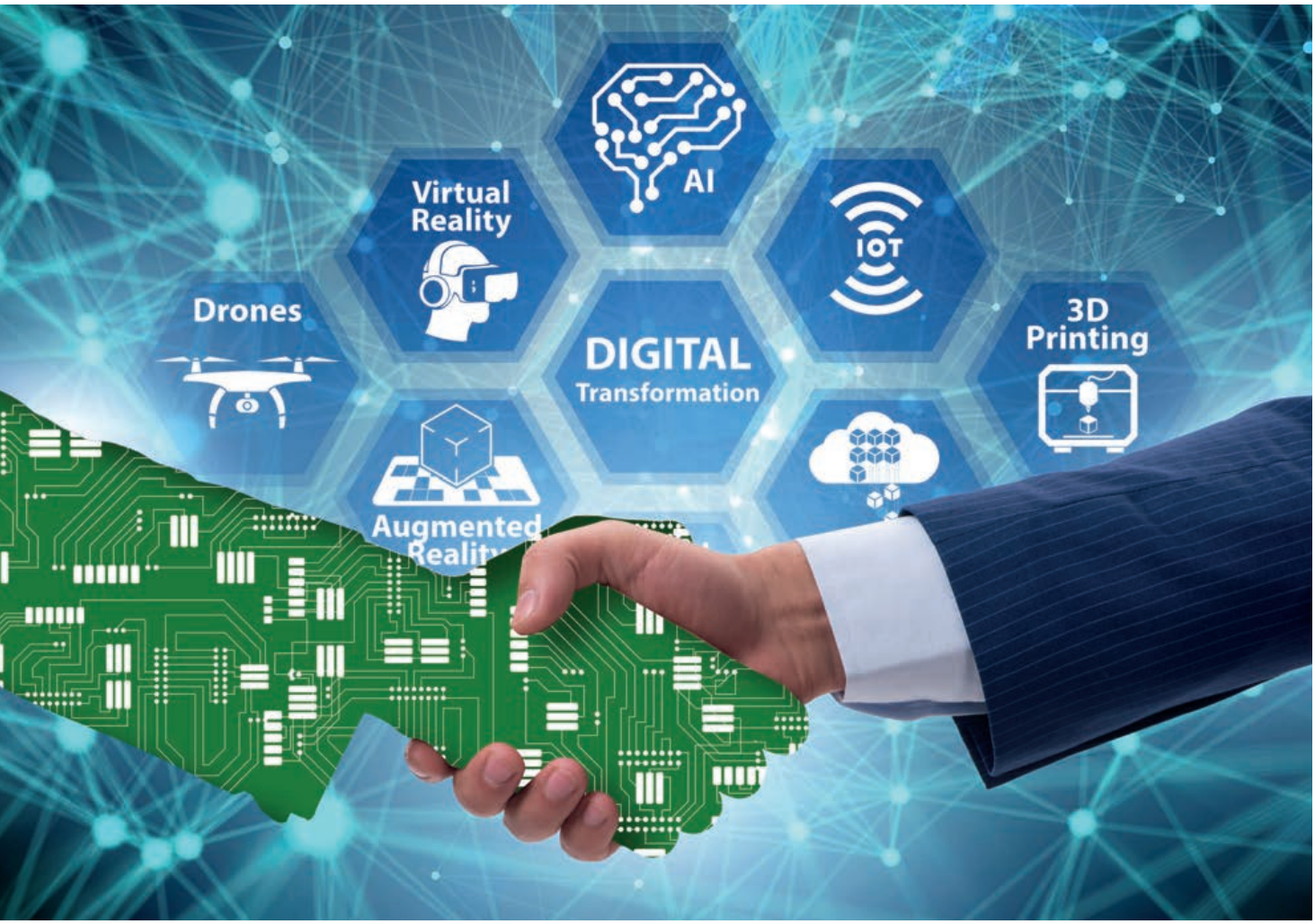
Sistemi za proizvodnjo, prenos in distribucijo električne energije so danes prepleteni z informacijsko infrastrukturo, kar jih dela ranljive za kibernetske napade, ki lahko vodijo do velikih gospodarskih izgub, prekinitev dobave energije in celo ogrožanja varnosti ljudi.

Nepogrešljivost neprekinjene oskrbe z električno energijo uvršča elektroenergetski sektor med najbolj kritične sektorje, kjer izpadi niso zgolj nezaželeni, temveč povsem nesprejemljivi. Glede na obstoječo zakonodajo je ta sektor izvajalec najbolj bistvenih storitev, na katerih temelji delovanje družbe in vseh njenih funkcij in procesov. Ta ključna odvisnost poudarja nujnost robustnih kibernetskih varnostnih ukrepov, ki lahko grožnje predvidijo, zaznajo in ublažijo v realnem času ter tako zagotavljajo neprekinjeno delovanje. Doseganje tako visoke ravni kibernetske varnosti pa je povezano s številnimi operativnimi in tehničnimi izzivi, kot so obvladovanje kibernetskega okolja in tveganj, zagotavljanje tveganjem primerne zaščite, nadzor kibernetskega prostora in reagiranje na anomalije v njem ter krepitev odpornosti in sposobnosti hitre povrnitve delovanja v primeru incidentov v delovanju digitalnih storitev ter zagotavljanju podatkov in informacij.

Slovenski energetski sektor sestavljajo prenosno in distribucijsko omrežje ter podjetja, ki so zadolžena za upravljanje elektroenergetskega prenosnega in distribucijskega sistema. Na elektroenergetski sistem je priključeno tudi več proizvajalcev, termoelektrarn, hidroelektrarn, jedrska elektrarna, v zadnjih letih pa tudi vse več malih proizvajalcev, predvsem malih hidro- in sončnih elektrarn. Z večanjem deležnikov in priključitvijo na električna in digitalna omrežja za upravljanje energetskih storitev se povečujejo tveganja, otežen je nadzor in identifikacija ranljivosti.

Individualni pristopi k zagotavljanju vseh aspektov kibernetske varnosti v tako medsebojno odvisnem in digitalno povezanem okolju niso več učinkoviti in zadostni ter kažejo na potrebo po združevanju kibernetsko obrambnih zmogljivosti, ki se je začela uresničevati skozi proces združevanja varnostno operativnih centrov (VOC), ki delujejo v prenosnem in distribucijskem okolju sektorja. Oba VOC-a se organizacijsko in tehnološko združujeta v eno sposobnejšo organizacijo, ki bo pokrila celoten kibernetski prostor slovenskega elektroenergetskega prostora, prenosnega omrežja in distribucijskega omrežja ter v naslednjih fazah morda vključila v sistem tudi kibernetski prostor proizvajalcev in drugih deležnikov elektroener-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



getskega sektorja, predvsem deležnike v elektroenergetskem sistemu Slovenije, ki so tudi nosilci kritične infrastrukture ter izvajalci bistvenih storitev.

Pomemben aspekt take iniciative je tudi posodobitev tehnološke platforme, ki se bo sposobna v okolju primanjkljaja kadrov in kompetenc soočiti z večjim obsegom okolja, naprav, sistemov, storitev in omrežij za različne namene.

V okolju že obstajajo različne zaščitne tehnologije, kot so požarne pregrade, sistemi za nadzor dostopov, kontrola identitet, sistemi za detekcijo in prevencijo, tudi moderne zaščitne in nadzorne tehnologije SIEM (Security Information and Event Management) in SOAR (Security Orchestration, Automation and Response). Vendar se pri obvladovanju informacij iz vseh teh sistemov kaže potreba po vzpostavitvi rešitve, ki bo integrirala podatkovne vire iz slednjih, avtomatsko reagirala, zaznala in se odzvala na dogodke v kibernetskem prostoru celotnega sektorja.

Individualni pristopi k zagotavljanju vseh aspektov kibernetske varnosti v tako medsebojno odvisnem in digitalno povezanem okolju niso več učinkoviti in zadostni ter kažejo na potrebo po združevanju kibernetsko obrambnih zmogljivosti, ki se je začela uresničevati skozi proces združevanja varnostno operativnih centrov (VOC), ki delujejo v prenosnem in distribucijskem okolju sektorja.

S takim namenom se je začel projekt "ALiEnS-SOC" (Artificial inteLligence in Slovenian Electro Energy Sector – Security Operation Center) (za zanimiv akronim se vrstni red lahko tudi rahlo spremeni), ki v delovanje VOC za sektor energetike uvaja rešitev umetne inteligence.

Celovita rešitev, ki bo delovala v VOC slovenske elektroenergetike (E-VOC), bo sestavljena iz več komponent:

- rešitve, ki uporablja umetno inteligenco za zaznavanje in avtomatizirani odziv,
- platforme, ki bo skrbela za povezavo različnih varnostnih komponent (zgoraj omenjene varnostne, zaščitne rešitve, SIEM, SOAR, požarne pregrade, ticketing in drugi sistemi) ter
- omogočanja posredovanja CTI (Cyber Threats Intelligence) informacij zainteresiranim naročnikom in deležnikom znotraj slovenskega in mednarodnega kibernetskega prostora.

Rešitev, ki bo postavljena v okolje naročnika, poganja umetna inteligenca

(angl. AI ‚Artificial Intelligence'), ki se nauči vsake podrobnosti edinstvenega okolja in gradi razvijajoče se razumevanje »sebe«. To pomeni, da opazi subtilna odstopanja, ki kažejo na ranljivost ali grožnjo. Za vsako interakcijo v digitalnem ekosistemu se rešitev vpraša - Je to normalno? - temelji na neobdelanih podatkovnih točkah in funkcijah podatkov, izboljšanih z umetno inteligenco. Razumevanje okolja je ključ do osvetlitve in prekinitve celotnega nabora kibernetskih groženj, od novih napadov do notranjih groženj.

Samoučeča se UI stoji za vsako komponento in omogoča prilagojene, celovite, vedno vklopljene ter nenehno razvijajoče se varnostne rešitve, ki temeljijo na matematičnih modelih, edinstvenih za vsako posamezno organizacijo, ne glede na velikost ali kompleksnost. Nobena organizacija ni enaka in tudi njihove varnostne rešitve ne bi smele biti.

V realnem času se izvaja detekcija znanih in še neidentificiranih kibernetskih groženj, tako od zunaj kot od znotraj. Sistem se uči in samodejno spoznava normalno stanje IT/IoT/OT in e-mail okolja, ki jih sproti analizira, si zapisuje realna dejstva ter balansira odstopanja od normalnih dogajanj v okolju. S tem samodejno zaznava virusne okužbe, zlorabe, anomalije, vdore, zlonamerna opravila, skeniranje omrežja ter poplave prometa in to ne glede na statična dejstva (pravila, podpisi, konstante).

V rešitvi bosta dve poglavitni komponenti:
- zaznavanje in
- avtomatizirani odziv.

Zaznavanje poganja prilagojeno, nenehno razvijajoče se razumevanje okolja, zagotavlja takojšnjo vidnost groženj – tudi tistih, ki uporabljajo nove vrste zlonamerne programske opreme ali nove tehnike. Samoučeča se umetna inteligenca analizira podatkovne točke za vsak prenosni računalnik, namizni računalnik, strežnik, uporabnika, telefon in tablični računalnik, stikalo, usmerjevalnik ali drugo napravo priključeno na IP omrežje ter se ves čas sprašuje, če je tako obnašanje normalno.

Rešitev bo delovala na način, da povezuje dogajanje oziroma pokaže korelacije med posameznimi dogodki, in sicer tako, da ustvari sliko širšega varnostnega incidenta, preden to predstavi človeškim ekipam. Posledično se čas tria-

že močno skrajša, kar varnostni (VOC) ekipi takoj pomaga razumeti, kaj se je zgodilo in zakaj.

Zazna novo in še nepoznano - stara orodja so slepa za nove grožnje. Rešitve ne morejo predvideti naslednjega napada, če gledajo samo včerajšnje grožnje. Z učenjem vsake podrobnosti v organizaciji bo rešitev ukrepala v nekaj sekundah in nevtralizirala grožnje, ne glede na to, ali so že bile videne, hkrati pa črpa znanje in vzorce nevarnosti kode tudi iz knjižnic, ki so ji licenčno dosegljive.

Avtomatizirani odziv ustavi napade v teku v celotnem digitalnem okolju, vključno s hitrimi napadi izsiljevalske programske opreme.

Vse to podpira UI, ki zagotavlja popoln vpogled v sisteme in podatke v realnem času. Rešitev deluje samostojno in razoroži napade, kadarkoli se zgodijo. Odzove se na grožnje v nekaj sekundah in deluje 24/7, s tem pa opravlja delo za katerega zaposlenih ni zadosti.

Z uporabo globokega učenja tehnologija kontekstualizira varnostne dogodke, se prilagaja novim tehnikam in svoje ugotovitve prevede v berljivo varnostno pripoved. Rešitev avtomatizira odziv na način, ki posnema človeške miselne procese za poglabljanje v napade in njihovo raziskovanje, združuje strokovno znanje ter intuicijo človeških analitikov s hitrostjo in obsegom umetne inteligence, kar močno skrajša čas za triažiranje, klasificiranje in prioritizacijo groženj.

V projekt ALiEnS-SOC je vključeno več slovenskih podjetij in državnih inštitucij. Prijavo smo spisali lansko pomlad, v drugi polovici lanskega leta smo izvedeli, da je projekt odobren, ob koncu leta smo že začeli z izvajanjem aktivnosti. Projekt se financira s strani EU v razmerju 50:50, kar nam bo omogočilo analizo stanja in tveganj, razvoj predloga rešitve, nakup in postavitev tehnološke platforme ter integracije z drugimi sistemi, kot tudi razvoj UI modelov, ki bodo bdeli nad celotnim kibernetskim prostorom družb deležnikov. Projekt bo zaključen s koncem leta 2027, storitev bo delovala v organizaciji E-VOC, varnostno operativnem centru slovenskega elektro-energetskega sektorja. ■

ALiEnS-SOC

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

BIOMETRIJA

Rešitev v skladu z ZVOP-2 (GDPR) zahtevami

- Pomoč pri pridobitvi **IP soglasja** in pri izdelavi **ocene učinka**
- Certifikat Grade4 za **najvišji nivo varnosti** po SIST EN 60839-11-1
- **Brezkontakten in sočasen zajem** slik obeh šarenic (za boljšo uporabniško izkušnjo)
- Možnost izvedbe verifikacije 1-1 ali identifikacije 1-N

HSI IRIS ID

www.hsi.si info@hsi.si 07 600 19 60

SIMTECH
www.simtech.si

Vaš partner za napredne rešitve kontrole pristopa in videonadzora

V podjetju Simtech d.o.o. ponosno zastopamo priznano blagovno znamko Salto Systems, vodilnega proizvajalca pametnih rešitev za kontrolo pristopa. Poleg tega smo uradni distributer vrhunskega Avigilon videonadzornega sistema, ki zagotavlja visoko kakovostno zaščito in napredno analitiko.

Naše storitve segajo dlje od zgolj dobave opreme – za vas poskrbimo tudi za popolno integracijo sistemov v vaše obstoječe informacijsko okolje. Z dolgoletnimi izkušnjami in strokovnim znanjem ustvarjamo varne, učinkovite in prilagodljive rešitve, ki jih prilagodimo specifičnim potrebam vašega podjetja.

Ne glede na to, ali gre za hotelske, poslovne, industrijske ali javne objekte – z rešitvami Simtech d.o.o. boste vedno korak pred izzivi sodobne varnosti.

Zaupajte strokovnjakom.

MOTOROLA SOLUTIONS

salto INSPIRED ACCESS

AVIGILON

SIMTECH d.o.o. • Industrijska cesta 9 • 1290 Grosuplje • Slovenija

Avtor: doc. dr. Brane Bertoncelj / Slovensko združenje za korporativno varnost

»KAKO SOCIALNI INŽENIRING IZKORIŠČA ŠIBKOSTI ZAPOSLENIH?«

Članek obravnava pomen psihologije v svetu informacijske varnosti. Od t. i. victim bias (pristranskost žrtve, prepričanja »meni se to ne more zgoditi«) do ključne vloge čustev pri informacijskih prevarah. Pri tem je pomemben tudi pomen nevrodiverzitete: kako kognitivne sposobnosti zaposlenega vplivajo na reakcije ob različnih incidentih na področju informacijske varnosti. Znanje o informacijskem vedenju spada na interdisciplinarno področje, ki vključuje psihologijo, sociologijo, informatiko in nevroznanost. Proučuje, kako zaposleni posluje, komunicira in se obnaša v digitalnih okoljih. Informacijska varnost je potovanje. Sprejetje pristopa ničelnega zaupanja pa je ena od najboljših obramb pred napadalci.

Napadalci bolj kot tehnične naprave napadajo zaposlene, ker je to učinkoviteje in ceneje. Vpliv zaposlenega na informacijski sistem je eden najmanj zanesljivih in predvidljivih dejavnikov, zato pomeni stalno nevarnost za navedeni sistem in ga ne smemo podcenjevati. Zaposleni (z vsemi svojimi potrebami, motivi, stališči in notranjimi osebnostnimi faktorji) pomeni ključni in kritični člen informacijskega sistema. Vstopa v interakcije s sistemom, zaznava in nadzira ogrožanja, dela napake in jih popravlja. Zlonamerna napaka je odločitev zaposlenega in je iz informacijskega sistema ne moremo izločiti, lahko pa s preventivnimi ukrepi in postopki zmanjšamo njen škodljivi učinek. Vloga zaposlenega je negativna v povzročanju naključnih ali zlonamernih napak in pozitivna v odpravljanju napak. S katerimi mnenji, stališči, prepričanji in vrednotami se zaposleni identificira? Zaposleni pod vplivom stališč do informacijske varnosti, subjektivnih norm in zaznanega vedenjskega nadzora oblikuje vedenjske namere do zaščite podatkov in informacij organizacije. Pri tem je treba upoštevati, da je stališče zaposlenega do določenega vedenja odvisno od njegovega prepričanja o verjetnosti in možnih posledicah incidenta.

Rezultati raziskav psiholoških eksperimentov kažejo, da zaposleni ni ravno najboljši ocenjevalec verjetnosti incidenta, in da v posameznih primerih sistematično krši načela razumnega odločanja pri soočanju z negotovostjo.

Obstajajo številne tehnike socialnega inženiringa, ki jih kriminalci uporabljajo tako v fizičnem kot v informacijskem svetu varnosti. Zaradi pojava umetne inteligence bo odvračanje in preprečevanje tovrstnih napadov še težje. Generativna umetna inteligenca se bo še naprej učila. Uporabljali jo bodo pametni kriminalci, ki želijo od zaposlenega pridobiti občutljive podatke ali sredstva. Proces doseganja učinkovite informacijske varnosti med zaposlenimi se začne z zavedanjem in konča s spremembami v vedenju, ta proces pa vključuje pomemben posredniški dejavnik presojanja in odločanja o informacijski varnosti.

Psihologija presoje je eno najbolj produktivnih področij vedenjskih znanosti. Nobelov nagrajenec Daniel Kahneman je razvil vplivno teorijo o intuitivni in racionalni presoji. Na podlagi njegove teorije posamezniki uporabljajo dve vrsti

Za trajno spremembo vedenja je ključno, da zaposleni razume pomen informacijske varnosti, ima jasno definirane smernice in se počuti vključenega v varnostno kulturo organizacije. Bolj kot je varnost preprosta in dostopna, večja je verjetnost, da jo bo zaposleni resnično upošteval.

mišljenja, intuitivno mišljenje, z različnimi kognitivnimi pristranskostmi, in racionalno mišljenje z natančnejšo presojo. Natančneje, intuitivno mišljenje je asociativno, vključuje malo očitnega truda in zavestnega razmišljanja ter je večinoma povezano s čustvi in preteklimi izkušnjami. Po drugi strani pa je racionalno mišljenje počasno, naporno, temelji na pravilih, namerno nadzorovano in vključuje logične, hierarhične ter vzročne mehanske procese.

Informacijska varnost je odgovornost vsakega zaposlenega in je dobra le toliko, kolikor je dober njen najšibkejši člen, ki je hkrati pogosto spregledan del varnostnega sistema.

Pomembno je, da zaposleni prevzema odgovornost, namesto da jo prelaga na druge. Ključni izzivi so pomanjkanje ozaveščenosti in angažmaja ter potreba po poenostavitvi sporočil, saj zaposleni išče konkretne informacije. Informacijska varnost zadeva tako osebno kot profesionalno življenje zaposlenega, zato je ključno, da se z njo ukvarjamo na obeh ravneh. Lahko imamo najsodobnejše tehnološke rešitve za informacijsko varnost, a če zaposleni ne razume varnostnih tveganj, ali ne ravna odgovorno, je celoten sistem ranljiv. Pomembno je, da zaposlenemu z ozaveščanjem ne povzročamo frustracij. Namesto tega ga moramo opolnomočiti, da prevzame odgovornost za svojo varnost in varnost organizacije, brez nepotrebnega strašenja pred posledicami incidenta.

Šibkosti zaposlenega

Šibkosti zaposlenega so pri socialnem inženiringu ključni dejavnik, zaradi katerega ta oblika manipulacije učinkovito deluje. Napadalci izkoriščajo psihološke in vedenjske šibkosti zaposlenega, da pridobijo občutljive informacije ali dostop do sistemov. Šibkosti se zlasti nanašajo na napake, kršitve, malomarnost, pomoto, nezgodni spodrsljaj, nepremišljeno vedenje, resnično nevednost, slabo presojo, zlorabo informacij, zavrnitev informacij, zloraba ciljev poslovanja, kršitev ciljev, slab odnos do tveganj, slabo komunikacijo in neusklajevanje aktivnosti. Nekatere najpogostejše šibkosti so:

- pomanjkanje ozaveščenosti (pogosto niso dovolj seznanjeni s taktikami socialnega inženiringa in ne vedo, kako prepoznati sumljive zahteve ali nenavadne prošnje),
- pretirano zaupanje (ljudje so po naravi zaupljivi in želijo pomagati, zlasti, če jih nekdo prepričljivo nagovori),
- strah pred avtoriteto (če se nekdo predstavi kot varnostni inženir ali drug pomemben uslužbenec, zaposleni pogosto ne preveri njegove identitete, boji se negativnih posledic, če zavrne zahtevo),
- rutina (zaposleni posluje po navadah in pogosto ne preveri dvomljivih zahtev, če se te zdijo kot del vsakodnevnega delovnega procesa, izkorišča se utrujenost za vdor v sistem),
- čustvena manipulacija (napadalci pogosto igrajo na čustva, kot so občutek nujnosti, strahu ali sočutje),
- slabe prakse pri izbiri gesel (uporaba šibkih ali enakih gesel za več sistemov, deljenje gesel s sodelavci),
- nezadostno preverjanje identitete (pomanjkanje preverjanja pristnosti klicatelja, e-poštnih sporočil ali obiskovalcev organizaciji, klikanje na sumljive povezave ali odpiranje neznanih priponk brez preverjanja).

Najbolj ranljivi zaposleni

Najbolj kritičen del informacijske varnosti so vsi zaposleni, saj lahko vsak

zaposleni predstavlja vstopno točko za informacijske napade. Vendar pa so nekateri profili zaposlenih še posebej ranljivi ali ključni za informacijsko varnost organizacije. Najbolj kritične skupine zaposlenih so:

- vodstvo in uprava (cilj napadalcev zaradi dostopa do zaupnih podatkov in finančnih sredstev, so pogosta tarča napadov, imajo manj tehničnega znanja o varnosti),
- zaposleni v financah in računovodstvo (tarča »spear phishing« napadov, ki poskušajo pridobiti lažna nakazila),
- IT in sistemski administratorji (imajo največji dostop do omrežij, podatkov, strežnikov in gesel, napadalci lahko pridobijo skrbniške pravice nad celotnim sistemom in privilegiranimi računi, upoštevati princip najmanjših privilegijev),
- kadrovska služba (napadalci pošiljajo lažne prošnje za delo s pripetimi okuženimi datotekami),
- vsi zaposleni, ki komunicirajo z zunanjimi osebami - podpora, prodaja, marketing (pogosto prejmejo e-pošto od neznanih virov in lahko nenamerno odprejo sumljive priponke ali povezave, napadalci se izdajajo za stranke ali poslovne partnerje, tveganje za razkritje zaupnih informacij po javnih kanalih oziroma omrežjih).

Sprememba vedenja zaposlenih

Sprememba vedenja zaposlenih je ključna za izboljšanje informacijske varnosti v organizaciji. Tehnične in organizacijske varnostne rešitve so pomembne, vendar zaposleni ostaja ena od največjih ranljivosti.

Kako spremeniti vedenje zaposlenih glede informacijske varnosti?

- Ozaveščanje in izobraževanje (redna ozaveščanja, namesto enkratnih delavnic je bolj učinkovito skozi krajše, praktične module, realni primeri in simulacije, zaposleni se bolje uči skozi resnične primere, prilagoditev različnim učnim slogom — vizualna gradiva, interaktivni kvizi in kratki videoposnetki),
- spodbujanje varnostne kulture (vodstvo kot zgled, pozitivna okrepitev — namesto kaznovanja napak je bolje spodbujati pravilne varnostne prakse s pohvalami in nagradami, organizacija lahko uvede sistem nagrajevanja za varnostno odgovorno vedenje, varnost naj bo integrirana v vsakodnevno delo, ne le kot dodatna obremenitev),
- poenostavitev varnostnih praks (uporaba enostavnih in razumljivih smernic, avtomatizacija varnostnih procesov — uporaba upraviteljev gesel, enotne prijave in večfaktorske avtentikacije zmanjšajo potrebo po zapomnitvi zapletenih pravil, pogoste posodobitve),
- načelo najmanjših privilegijev (zaposleni naj imajo dostop samo do podatkov in sistemov, ki jih nujno potrebujejo za delo),
- merjenje in izboljšava vedenja (spremljanje napredka — anketiranje zaposlenih in analiza odzivov na simulacije napadov, neposredne povratne informacije pri napačnih ali tveganih dejanjih izboljša dolgoročno vedenje),
- varnostna kultura (informacijska varnost ni le odgovornost IT-oddelka, ampak celotne organizacije, merjenje uspešnosti varnostnih programov s ključnimi kazalniki uspeha),
- pomembni so tudi drugi vidiki (tehnologija, procesi, pravila, organizacija dela), vendar brez varnostno ozaveščenih zaposlenih nobena zaščita ne bo učinkovita.

Kako doseči spremembo vedenja?

Sprememba vedenja zaposlenih na področju informacijske varnosti zahteva kombinacijo izobraževanja, jasnih pravil, tehnološke podpore in spodbujanja pozitivne informacijske kulture. Organizacije, ki vlagajo v te elemente, zmanjšujejo tveganje informacijskih napadov in zagotavljajo bolj varno delovno okolje.

Sprememba vedenja zaposlenih na področju informacijske varnosti je zahtevna naloga, saj so zaposleni že oblikovane osebnosti, pogosto se upirajo spremembam, podcenjujejo tveganja ali pa jih pomanjkanje izkušenj vodi do nepazljivosti. Glavni izzivi vključujejo:

- nizko ozaveščenost o tveganjih (zaposleni pogosto ne razume posledic varnostnih incidentov),
- pomanjkanje ustreznih znanj (brez rednega ozaveščanja ostanejo varnostne grožnje premalo poznane),
- odpor do dodatnih ukrepov (zaposleni lahko dojema varnostne ukrepe kot nepotrebno obremenitev, poseg v njegovo polje udobja),
- pomanjkanje spodbud (če organizacija ne nagrajuje varnega vedenja, ga zaposleni ne bodo dosledno izvajali).

Zaključek

Socialni inženiring, v katerem se od zaposlenega z manipulacijo pridobi in zlorabi njegove zasebne informacije in premoženje, predstavlja resno grožnjo v informacijskem okolju. Zaposleni predstavlja lažjo »tarčo« kot napad na strojno opremo, socialni inženirji pa postajajo vse bolj profesionalni. Še pred napadom izvedejo obsežno raziskavo svoje žrtve, sposobni so psihološke manipulacije, komuniciranja, prepoznavanja čustev in vedenja, zato si pridobijo zaupanje zaposlenega. Kršitve varnosti so v organizacijah pogoste in številne kršitve pripisujejo napakam zaposlenih.

Socialni inženiring vpliva na šibkosti zaposlenih tako, da izkorišča človeške lastnosti, kot so zaupanje, radovednost, strah, želja po pomoči ali pritisk avtoritete. Gre za manipulativne taktike, s katerimi napadalci prepričajo zaposlene, da razkrijejo občutljive informacije, omogočijo nepooblaščen dostop ali izvedejo dejanja, ki bi lahko ogrozila finančno poslovanje in varnost organizacije.

Ocenjevanje tveganja informacijske varnosti dodatno otežuje pretirana prepričanost o pravilnosti lastne sodbe. Zaposleni prevečkrat pretirano zaupa lastni, tudi napačni sodbi. Psihološka osnova za to je verjetno neobčutljivost za pomanjkljivost domnev, na katerih sloni njihova sodba. Najbrž noben dejavnik presojanja ni bolj odločujoč kot pretirana samozavest. Splošno znanje povzroča razmeroma visoko stopnjo pretirane samozavesti, velja pa tudi obratna trditev. Informacijske varnosti ne smemo utemeljevati z verjetnostjo, da se bo nekaj zgodilo, ampak z možnimi posledicami. Gre za preprosto vprašanje: Ali si lahko organizacija na eni strani privošči »razkošje informacijske nevednosti«, na drugi strani pa izgubo informacijskega premoženja?

Poudarjanje človeškega dejavnika zahteva kulturno in psihološko preobrazbo, ki se nanaša na spremembo vedenja. Kateri dejavniki so najpomembnejši za razumevanje in napovedovanje vedenja? Na žalost enoznačnega in univerzalnoga odgovora na to vprašanje še ni. Številne statistične analize so potrdile hipotezo o večji povezanosti vedenja in stališč, ki so oblikovana na podlagi direktne izkušnje kot obratno. To pomeni, da ne obstajajo neka absolutna „notranja pravila“ oziroma pogoji, ki morajo biti izpolnjeni, da se bo zaposleni vedno vedel konsistentno z njimi.

Ključnega pomena pri tem je ustvariti okolje, ki nagrajuje pravilno vedenje in ne kaznuje napak. Usmerjeni moramo biti v preseganje tehničnih rešitev in gradnjo požarnega zidu zaposlenih, ki naj bodo prva obrambna linija organizacije. S tem, ko smo na spletu, smo vsi ranljivi za izkoriščanje podatkov, enake tehnike prepričevanja, kot jih uporabljajo informacijski kriminalci, pa uporabljajo tudi zakonita podjetja za zbiranje naših podatkov. Se spomnite škandala Cambridge Analytica?

Menim, da je stopnja informacijske varnosti v največji meri odvisna od stopnje motiviranosti in pripadnosti zaposlenih organizaciji, ker to pomeni samovarovalno ravnanje v korist organizacije in pravočasno izločanje subjektivnih motilnih elementov v delovnih procesih. Tega ne moremo nadomestiti z nobeno varnostno organizacijo in tehniko ter še tako izurjenim nadzornim in varnostnim osebjem.

Za trajno spremembo vedenja je ključno, da zaposleni razume pomen informacijske varnosti, ima jasno definirane smernice in se počuti vključenega v varnostno kulturo organizacije. Bolj kot je varnost preprosta in dostopna, večja je verjetnost, da jo bo zaposleni resnično upošteval. Ne moremo „zavreti oceana“, da bi zmanjšali vsa tveganja. Počutiti pa se moramo umirjeno ob zavedanju, da smo osredotočeni na upravljanje najbolj kritičnih in visokih tveganj, ob razumevanju nagnjenosti k tveganju organizacije. ■

Avtor: Gašper Pintarič / direktor operacij, Špica International d.o.o.*

PROJEKTIRANJE VARNE KONTROLE PRISTOPA: SINERGIJA FIZIČNE IN IT-VARNOSTI

V sodobnem poslovnem okolju se prepletata fizična in informacijska varnost, zato postaja celovito projektiranje kontrole pristopa ključnega pomena. Učinkovit sistem ne le ščiti fizične prostore podjetja, temveč tudi varuje občutljive podatke pred nepooblaščenim dostopom.

Tradicionalno sta bili skozi zgodovino fizična in informacijska varnost obravnavani ločeno. Nič več, saj sodobni pristopi poudarjajo njuno integracijo. Razlogi so očitni: nepooblaščen fizični dostop lahko vodi tudi do zlorabe IT-sistemov, medtem ko lahko pomanjkljiva informacijska varnost omogoči manipulacijo fizičnih varnostnih sistemov. Zato je nujno, da sistemi kontrole pristopa združujejo oba vidika, saj lahko le tako zagotavljajo celovito zaščito.

Z varnostjo ljudi in podatkov pač ni šale. Pri projektiranju kontrole pristopa ima glavno besedo varnost, katere osnovni cilj je zaščita ljudi, premoženja in podatkov. Kot so nam zaupali v podjetju Špica, kjer veljajo za ene največjih strokovnjakov na tem področju v Sloveniji, je treba pri projektiranju kontrole pristopa združiti več želja naročnika v smiselno celoto. Poleg tega morajo biti vsi sistemi skladni z zakonodajo in standardi. Izzivov torej ne manjka.

Eden takšnih je že večnamembnost prostorov. Sodobni delovni prostori pogosto vključujejo skupno rabo sejnih sob, pisarn in delovnih mest. Torej morajo tudi sistemi kontrole pristopa postati fleksibilni, če naj omogočajo prilagajanje tem dinamičnim potrebam. Zaščita prostorov, urniki, preverjanje identitete uporabnikov, evakuacijske poti ... vse to so spremenljivke, ki sestavljajo tokratno enačbo. Enačbo, za katero lahko veljajo posebna pravila in scenariji (npr. da uporabnik ne more ven, če ni šel v nek prostor ali obratno, da se ena vrata ne odprejo, dokler so odprta druga in je treba najprej prva zapreti ipd.).

Tehnologija je več kot le orodje

Uporaba naprednih tehnologij, kot so mobilne aplikacije za odpiranje vrat, biometrična identifikacija in značke RFID, zagotavlja visoko stopnjo varnosti in udobja za uporabnike. Intuitivni vmesniki in enostavna uporaba pa še povečujejo sprejemanje sistema kontrole pristopa med uporabniki ter zmanjšujejo možnost napak pri uporabi. Tehnološka naprednost rešitve je v praksi močno povezana z (dobro) uporabniško izkušnjo.

A največ je v očeh podjetja vredna kakovostna integracija, saj mora sistem kontrole dostopa delovati kot celota, ne glede na to, katere ključavnice, vrata, krmilniki in senzorji so uporabljeni. Z vidika prilagodljivosti je dobrodošlo tudi to, če vpeljane rešitve omogočajo gostovanje tako v oblaku kot delovanje na lokaciji podjetja, pri čemer sta pomembni tudi enostavnost nadgradnje in prilagodljivost glede na specifične zahteve organizacije. Ko smo že pri integraciji – sistem kontrole pristopa velja za kar največjo poslovno korist povezati tudi s sistemom za evidenco delovnega časa ter vpeljati avtomatsko izmenjavo podatkov. Tudi na tem področju Špicinim strokovnjakom ni para.

S pravilno integracijo tehnologij, upoštevanjem standardov in osredotočenjem na uporabniško izkušnjo lahko podjetja ustvarijo varno in prilagodljivo delovno okolje, pripravljeno na izzive prihodnosti. Sistema kontrole pristopa in evidence delovnega časa lahko podjetjem prineseta olajšanje ali pa povzročita težave – vse je odvisno od načina njune implementacije. Zato je priporočljivo, da uvedbo takšnih sistemov v poslovanje izvedejo strokovnjaki. ■

Promocijski članek

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 20. MAJ 2025

16. mednarodna konferenca Dnevi korporativne varnosti

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

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

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

Analogno. Digitalno. Dva svetova. Ena rešitev.

REISSWOLF

Uničevanje dokumentacije:

Varen in sledljiv proces uničevanja.

Varnostni zabojniki z elektronskim sistemom zaklepanja (e.l.sy)-beleženje vseh dogodkov (revizijska sled).

Uničevanje skladno z evropskimi standardi in Uredbo GDPR.

Uničevanje vseh vrst podatkovnih nosilcev (papir, trdi diski, CD-ji, RTG slike, itd.).

Elektronski zajem in hramba podatkov:

Certificiran, varen in zanesljiv e-proces, skladen z Uredbo GDPR.

Skeniramo vse formate od A0, vključno s projektno in tehnično dokumentacijo.

Stroškovno učinkovita rešitev.

Neomejen 24/7 dostop do dokumentov.

Povečanje produktivnosti.

Fizična hramba:

Najvišji nivo varnosti in sledljivosti ter skladnosti z Uredbo GDPR.

Učinkovit in uporabniku prijazen spletni dostop do arhiva 24/7.

Najsodobnejša tehnologija upravljanja z dokumenti.

Stroškovno učinkovita rešitev fizičnega arhiviranja.

Reisswolf – varno, nadzorovano in sledljivo upravljanje z dokumentacijo:

Rešitve po meri uporabnika z mednarodnimi izkušnjami.

Optimizacija digitalnih in analognih potreb.

Primerno za majhna, srednja in velika podjetja.

Okolju in uporabniku prijazne storitve.

Upoštevanje varnostnih standardov.

Ob oddaji povpraševanja do 31.05.2025 prejmite enkratno ekskluzivno ugodnost pri vseh storitvah REISSWOLF!

Pokličite nas na: **01 541 22 66**

Ali nam pišite na: **info@reisswolf.si**

TÜV AUSTRIA CERTIFIED

Družini prijazno podjetje

simply. done.

Organize your Security.

With our Software Solutions
AIM and **WinGuard**

AIM
Identity Management Platform

- Integrated Access Control
- Unified Credential Management
- Centralized Authorization Models
- Seamless Migration Possibilities
- Automated Compliance

winguard
Open Integration Platform

- Vendor-neutral Integration
- Central Event Visualization
- Dynamic Workflows
- Dashboards & Reporting
- Modular and scalable

Get more info about our Solutions.

advancis.net

advancis

GRADIMO ENERGETIKO PRIHODNOSTI

Elektroenergetika je na pragu tektonskih podnebnih in družbenih sprememb. Naša skupna odgovornost je, da se nanje prilagodimo in si hkrati prizadevamo za ogljično nevtralnost. Pred nami je novo, drugačno obdobje prenosa in distribucije električne energije.

ELES je in bo ostal hrbtenica zelenega prehoda v Sloveniji. Z zanesljivo, varno in trajnostno oskrbo z električno energijo skrbi za to, da bo elektroenergetska infrastruktura bolj prilagojena potrebam jutrišnjega dne. Predvsem pa bo še naprej oral ledino pri postavljanju novih standardov družbenega napredka. ELES bo Slovenijo popeljal v boljšo, zeleno prihodnost.

ELES

PRENAŠAMO ENERGIJO. OHRANJAMO RAVNOVESJE.