Korporativna varnost

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

Letnik 2026, marec • št. 40



Slovensko združenje za korporativno varnost
vključujoča platforma sodelovanja

Tradicionalna 17. mednarodna konferenca
Dnevi korporativne varnosti
Brdo pri Kranju, 18-19. maj 2026


ELES
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.
www.eles.si



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:
marec 2026

Izvod revije je brezplačen

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

ISSN 2232-6170

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

Sodobno varnostno okolje zaznamujejo vse večja kompleksnost, medsebojna prepletenost tveganj in visoka stopnja nepredvidljivosti. Organizacije danes delujejo v prostoru, kjer se kibernetske grožnje prepletajo z geopolitičnimi napetostmi, vplivi podnebnih sprememb, motnjami v dobavnih verigah in pospešenim tehnološkim razvojem. Takšno okolje presega tradicionalne varnostne okvire in zahteva širše, sistemsko razumevanje tveganj, ki lahko hkrati prizadenejo več sektorjev ter ravni delovanja.

V ospredje zato vse bolj stopa vprašanje odpornosti kritične infrastrukture, ki predstavlja temelj stabilnosti države, gospodarstva in družbe. Zagotavljanje njene zanesljivosti ni več zgolj tehnično vprašanje, temveč strateška naloga, ki zahteva usklajeno delovanje javnega in zasebnega sektorja ter povezovanje strateškega odločanja z učinkovito operativno izvedbo. K temu bo pomembno prispevalo tudi iskanje in oblikovanje premišljenih strateških pristopov na področju zagotavljanja odpornosti, ki jih v tej številki podrobneje predstavljamo v osrednji kolumni.

Rdeča nit tokratne številke je prav sistemska odpornost Republike Slovenije. Skozi strateške intervjuje z ministrico za infrastrukturo, generalnim direktorjem Policije, državnim sekretarjem na Ministrstvu za obrambo ter informacijsko pooblaščenko odpiramo razpravo o tem, kako različni sektorji prispevajo k skupni odpornosti države. Njihovi pogledi osvetljujejo pomen medsebojnega usklajevanja, jasnega upravljanja odgovornosti in vlaganj v varne, zanesljive ter prilagodljive sisteme, ki zagotavljajo neprekinjeno delovanje ključnih storitev. Vsebino dopolnjujejo tudi ostale z varnostjo močno povezane vsebine, kot je pogovor s predstavnikoma Nogometne zveze Slovenije ob nedavno končanem UEFA Futsal EURO 2026 in ostala visoko strokovna vsebina.

Zlasti velja izpostaviti, da so pred nami Dnevi korporativne varnosti 2026, ki predstavljajo najpomembnejši strokovni dogodek s področja korporativne varnosti v širši regiji. Dogodek bo ponovno združil ključne odločevalce, strokovnjake in predstavnike kritičnih sektorjev ter ponudil platformo za razpravo o prihodnosti odpornosti, kibernetske varnosti in zaščite kritične infrastrukture. Vsebina tokratne številke tako predstavlja tudi strokovni uvod v razprave, ki jih bomo v kratkem nadaljevali na tem osrednjem regijskem dogodku.

Z izborom intervjujev in strokovnih prispevkov želimo bralkam in bralcem ponuditi poglobljen vpogled v strateške usmeritve ter hkrati praktične izkušnje tistih, ki varnostne procese izvajajo na operativni ravni. Prepričani smo, da prav povezovanje strateškega razmišljanja, zakonodajnih okvirov in konkretnih rešitev predstavlja temelj za dolgoročno krepitev odpornosti kritične infrastrukture ter celotne družbe.

V uredništvu revije *Korporativna varnost* verjamemo, da boste tudi v 40. številki našli strokovne vsebine, ki vam bodo v podporo pri vašem zahtevnem delu in vas spodbudile k nadaljnjemu razmisleku o pomenu sistemske odpornosti v sodobnem varnostnem okolju.

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
mag. Alenka Bratušek,
ministrica za infrastrukturo

ODPORNOSTI DRUŽBE SI BREZ TRANSPORTNEGA SEKTORJA NE MOREMO ZAMIŠLJATI 5



INTERVJU
Damjan Petrič, mag.
generalni direktor Policije

POLICIJA S SVOJIM POSLANSTVOM ZAGOTAVLJA POGOJE ZA VAREN RAZVOJ DRUŽBE 10



INTERVJU
Boštjan Pavlin, mag.
državni sekretar Ministrstva za obrambo RS

SLOVENIJA MED KRIZAMI IN PRILOŽNOSTMI: POT DO SISTEMSKE ODPORNOSTI 20



INTERVJU
dr. Jelena Virant Burnik,
informacijska pooblaščenka Republike Slovenije in
podpredsednica Evropskega odbora za varstvo podatkov

STALNE SPREMEMBE SO POSTALE STALNICA TUDI PRI DELU INFORMACIJSKEGA POOBLAŠČENCA 25



INTERVJU
mag. Martin Koželj, generalni sekretar NZS
mag. Marko Brelih, vodja varnosti in področja integritete

STRATEŠKI IN IZVEDBENI OKVIR ORGANIZACIJE UEFA FUTSAL EURO 2026 31

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

INTERVJU
mag. Alenka Bratušek, ministrica za infrastrukturo

ODPORNOSTI DRUŽBE SI BREZ TRANSPORTNEGA SEKTORJA NE MOREMO ZAMIŠLJATI

Odpornost transportne infrastrukture v Sloveniji je ključna za zagotavljanje neprekinjene mobilnosti ljudi in blaga ter za ohranjanje gospodarske stabilnosti države, zlasti zaradi njenega tranzitnega položaja na pomembnih evropskih prometnih koridorjih. Krepitev odpornosti zahteva sistematično upravljanje tveganj, vlaganja v robustnost in prilagodljivost infrastrukture ter tesno sodelovanje med državnimi organi, upravljavci infrastrukture in zasebnim sektorjem pri preprečevanju, odzivanju ter okrevanju po motnjah. V ekskluzivnem intervjuju z mag. Alenko Bratušek, ministrico za infrastrukturo, smo se pogovarjali, kako država s strateškimi investicijami, rešitvami in udejanjanjem ključnih infrastrukturnih projektov gradi infrastrukturno prihodnost, ki je pogoj za ustrezno raven odpornosti.

Spoštovana ministrica, najprej nam dovolite, da vam in vašim sodelavcem čestitamo za trud, ki ga vlagate v izpeljavo za Slovenijo pomembnih strateških infrastrukturnih projektov. Kateri so tisti projekti, ki bi jih želeli posebej izpostaviti in bistveno vplivajo na dvig odpornosti v Republiki Sloveniji?

To so praktično vsi projekti nadgradnje in izgradnje prometne infrastrukture, ki jih izvajamo na našem ministrstvu. S ponosom lahko povem, da so investicije v gradnjo in vzdrževanje državnih cest in železnic v času sedanje vlade rekordne, znašajo kar 7 milijard evrov. Slovenija še nikoli ni toliko vlagala v svojo prometno infrastrukturo. Obsežen investicijski cikel je viden praktično na vsakem koraku, na številnih gradbiščih po vsej državi.

Ko govorimo o velikih investicijah, sta trenutno tik pred odprtjem dve največji investiciji - drugi tir Divača – Koper, ki na 27 kilometrih poteka v sedmih predorih in na treh viaduktih. S to pridobitvijo, ki je zelo zahteven gradbeni projekt, bomo odpravili ozko grlo na tem železniškem odseku. Z izgrajeno drugo cevjo predora Karavanke, ki jo prav tako odpiramo marca, bomo povečali mednarodno povezljivost. Zaključen je tudi sklop A v projektu nadgradnje železniške postaje Ljubljana, sklopa B in C pa bosta zaključena letošnjo jesen. Tudi železniško vozlišče Jesenice se nadgrajuje, napredek je že dobro viden.

Tudi tretja razvojna os, ki bo potekala od severne proti jugovzhodni Sloveniji, od meje z Avstrijo do meje s Hrvaško, je izjemno pomemben projekt. Na odseku Velenje-Slovenj Gradec je zaključena gradnja štirih sklopov, v gradnji so trije

*avtor je član Slovenskega združenja korporativne varnosti



Ključna prednost projektov je krepitev zavedanja o teh tveganjih in potreba po tesnejšem sodelovanju tako z evropskimi partnerji kot tudi z domačimi upravljavci kritične infrastrukture. Ti lahko neposredno uporabljajo tudi številna orodja, razvita v okviru projektov, kot so digitalni dvojček za vizualizacijo infrastrukturnih sredstev, sistem skupnih opozoril in medorganizacijsko komunikacijo v primeru nesreč, kibernetskih napadov ipd. ali pa recimo orodje za vizualni pregled železniške ter druge infrastrukture z droni.

sklopi, kmalu se bo pričela gradnja zadnjega sklopa A-Velenje. Pripravlja se širitev vseh vpadnic v Ljubljano ter širitev ljubljanskega avtocestnega obroča. Izgradili smo tudi avtocestni priključek Dragomer na odseku primorske avtoceste med Brezovico in Vrhniko, s katerim razbremenjujemo priključek Brezovica, kjer zastoji mnogokrat segajo na območje razcepa Kozarje, ter na zahodno in južno ljubljansko obvoznico.

Spomnim naj še na zgodovinsko najhujšo ujmo poleti 2023, zaradi katere je bilo evidentiranih 92 popolnih zapor in 98 zapor s polovično prevoznostjo. Intervencijsko je bilo pregledanih 1800 km državnih cest, kar je skoraj tretjina državnega cestnega omrežja. V nadaljevanju so bila izvedena še zahtevnejša dela za zagotovitev varne prevoznosti vseh udeležencev v prometu, ne glede na vremenske razmere. Ta dela so bila izvedena na 584 km državnih cest.

Ministrstvo za infrastrukturo je tudi sektorski koordinator za zagotavljanje zaščite kritične infrastrukture v transportnem sektorju. Bi želeli posebej izpostaviti katere od pomembnih koordinacijskih korakov, ki zagotavljajo učinkovito delovanje vseh deležnikov v tem zahtevnem sektorju?

V kontekstu kritične infrastrukture je temeljni cilj Ministrstva za infrastrukturo zagotavljanje varnega, zanesljivega in nemotenega delovanja prometnega sistema Republike Slovenije ter zaščite, odpornosti in neprekinjenega delovanja ključnih infrastrukturnih objektov ter sistemov.

Ministrstvo za infrastrukturo kot sektorski koordinator navedeno dosega predvsem z usklajevanjem dejavnosti in ukrepov med upravljavci kritične infrastrukture ter pristojnimi državnimi organi. Pomembna je tudi priprava, izvajanje in spremljanje ukrepov za zaščito kritične infrastrukture pa tudi sodelovanje pri identifikaciji, ocenjevanju in obvladovanju tveganj, ki lahko vplivajo na delovanje kritične infrastrukture. Ob tem je nujna izmenjava informacij, potrebnih za izvajanje nalog zaščite in odpornosti ter sodelovanje pri načrtovanju in izvajanju ukrepov za zagotavljanje neprekinjenega delovanja kritične infrastrukture v izrednih ter kriznih razmerah.

Kako ocenjujete trenutno pripravljenost slovenske transportne infrastrukture na zahtevne grožnje, kot so kibernetski napadi, poplave in drugi ekstremni dogodki, ki vplivajo na delovanje infrastrukture?

Trenutna pripravljenost slovenske transportne infrastrukture na zahtevne grožnje, kot so kibernetski napadi, poplave in drugi ekstremni dogodki, je dobra. Infrastrukturni sistemi se redno posodabljajo, so vzdrževani in podvrženi rednim analizam tveganj. To omogoča hitre odzive v primeru kriz, kar je bilo mogoče videti v primeru ujme 2023. Kakor ostali resorji se tudi mi soočamo s številnimi izzivi, saj je hitrost razvoja tehnik in tehnologij ter nepredvidljivost ekstremnih dogodkov vedno zahtevna preizkušnja.

Ravno zaradi tega je pomembno poudariti, da se na ministrstvu in pri upravljavcih infrastrukture aktivno dela vnaprej. Sprejemamo preventivne ukrepe, izvajamo simulacije in nadgradnje sistemov, s čimer zagotavljamo, da so potencialne ranljivosti odkrivane in odpravljene še preden pride do realnih situacij. Takšen proaktiven pristop omogoča, da Slovenija ostaja odporna in pripravljena na vse sodobne grožnje na področju infrastrukture.

Katere tri ključne korake bi po vašem mnenju morala Slovenija sprejeti v prihodnjih letih, da okrepi svojo odpornost kritične infrastrukture?

Kritična infrastruktura transportnega sektorja predstavlja temelj za delovanje države in družbe ter varnost ljudi. Če pride do izpada ali napada (npr. kibernetski napad, naravne nesreče ali druge izredne situacije), lahko posledice hitro prizadenejo veliko število ljudi, gospodarstvo in javne storitve. Da se to ne bi zgodilo, mora Slovenija še naprej krepiti odpornost kritične infrastrukture, predvsem z nadaljevanjem modernizacije in digitalizacije infrastrukture – to vključuje posodobitev sistemov, uvedbo pametnih tehnologij ter stalno nadgradnjo IT-varnosti, krepitev preventivnih ukrepov in krepitev.



Javno-zasebno sodelovanje, kot je omogočeno v okviru članstva ministrstva v Slovenskem združenju za korporativno varnost, prinaša številne prednosti. Povečuje izmenjavo znanja in najboljših praks, omogoča celovit pristop k zaščiti kritične infrastrukture ter hitrejše prepoznavanje in odzivanje na varnostna tveganja.

Kompleksnost delovanja moderne družbe se zrcali tudi v močni soodvisnosti delovanja enega sektorja infrastrukture z drugimi. Posebno centralno točko poleg energetike in telekomunikacije predstavlja tudi sektor transporta. Kako ocenjujete ustreznost medsektorskih strateških ukrepov zagotavljanja učinkovite koordinacije odpornosti Republike Slovenije kot celote?

Ustreznost medsektorskih strateških ukrepov za zagotavljanje učinkovite koordinacije odpornosti Republike Slovenije je na visoki ravni. Ključno vlogo pri koordinaciji vseh aktivnosti po posameznih sektorjih, kot npr. energetika, telekomunikacije, transport, zdravstvo oskrbovalne verige, ipd. prevzema Ministrstvo za obrambo, ki zagotavlja strateško povezovanje, usklajevanje ukrepov in skupno odzivanje v kriznih situacijah.

Sektor infrastrukture pri tem predstavlja osrednji element, saj zagotavlja premik ljudi, blaga in nujnih sredstev, njegova učinkovitost pa neposredno vpliva na delovanje drugih sektorjev – motnje v prometu se hitro odražajo v oskrbi z energijo, distribuciji blaga, zdravstvenih storitvah telekomunikacijah.

Dobro in usklajeno medsektorsko sodelovanje se je pokazalo na zadnji nacionalni vaji kriznega upravljanja in odzivanja »ODPORNOST24«, kjer se je preizkušalo odzivnost, koordinacijo in skupno obvladovanje incidentov. Tovrstne vaje omogočajo izboljšanje odpornosti Republike Slovenije kot celote.

Kako pomembno je mednarodno sodelovanje, predvsem z državami EU in regije Zahodnega Balkana – pri varovanju prometnih koridorjev in logističnih poti?

Mednarodno sodelovanje, zlasti z državami EU in regije Zahodnega Balkana je izjemno pomembno pri varovanju prometnih koridorjev in logističnih poti. V okviru tega sodelovanja se med drugim iščejo tudi ustrezne rešitve, vezane na različno zakonodajo po posameznih državah, harmonizacijo standardov, hitro izmenjavo informacij in podatkov, zagotavljanje nadzorov ter kriznega upravljanja na celotni transportni poti. Razhajanja v zakonodaji lahko vodijo do prometnih zastojev in višjih stroškov, kar lahko vpliva na konkurenčnost regije.

Ministrstvo za infrastrukturo je bil pomemben deležnik dveh velikih EU projektov s področja zaščite kritične infrastrukture SUNRISE in ATLANTIS, ki sta bila usmerjena v iskanje rešitev za zagotavljanje odpornosti kritične infrastrukture. Kakšne konkretne koristi taki projekti prinašajo za Ministrstvo za infrastrukturo in posledično tudi za Republiko Slovenijo?

Ministrstvo za infrastrukturo je s sodelovanjem v evropskih projektih SUNRISE in ATLANTIS skupaj s slovenskimi upravljavci kritične infrastrukture pridobilo pomemben vpogled v tveganja moderne dobe, kot so naravne nesreče, kibernetske grožnje, morebitne prihodnje pandemije ter vedno bolj pogosti ekstremni vremenski pojavi. Ključna prednost projektov je krepitev zavedanja o teh tveganjih in potreba po tesnejšem sodelovanju tako z evropskimi partnerji kot tudi z domačimi upravljavci kritične infrastrukture. Ti lahko neposredno uporabljajo tudi številna orodja, razvita v okviru projektov, kot so digitalni dvojček za vizualizacijo infrastrukturnih sredstev, sistem skupnih opozoril in medorganizacijsko komunikacijo v primeru nesreč, kibernetskih napadov ipd. ali pa recimo orodje za vizualni pregled železniške ter druge infrastrukture z droni.

Ministrstvo za infrastrukturo je dolgoletni član Slovenskega združenja za korporativno varnost, kot najmočnejše slovenske varnostne platforme s področja obvladovanja varnostnih tveganj za kritično infrastrukturo. Kompleksnost varnostnega okolja nam danes ne dopušča več silosnega delovanja. Kje vidite tiste posebne vrednosti takega javno zasebnega sodelovanja?

Javno-zasebno sodelovanje, kot je omogočeno v okviru članstva ministrstva v Slovenskem združenju za korporativno varnost, prinaša številne prednosti. Povečuje izmenjavo znanja in najboljših praks, omogoča celovit pristop k zaščiti kritične infrastrukture ter hitrejše prepoznavanje in odzivanje na varnostna tveganja. Ministrstvo za infrastrukturo se redno udeležuje srečanj Slovenskega združenja za korporativno varnost, kjer si izmenjujemo informacije, se seznanjamo s tekočo problematiko in prispevamo k skupnemu iskanju rešitev. Takšna sinergija med javnim in zasebnim sektorjem je danes nujna, saj kompleksnost okolja v katerem živimo, ne dopušča izoliranega delovanja.

Naša kritična infrastruktura je povezana, grožnje pa se lahko pojavljajo in širijo zelo hitro. Le s sodelovanjem javnega in zasebnega sektorja je mogoče učinkovito obvladovanje tveganj. ■

Foto: arhiv Ministrstva za infrastrukturo RS

UČINKOVITO OBVLADOVANJE TVEGANJ ZA ZAŠČITO KRITIČNE INFRASTRUKTURE IN INFORMACIJSKIH SISTEMOV



Motnje v delovanju kritične infrastrukture in kibernetski napadi so danes ena največjih groženj za podjetja in organizacije ter družbo nasploh.

Upravljanje teh tveganj zahteva sistematičen pristop, skladnost s predpisi in podporo naprednih rešitev.

Ekipa Silver Bullet Risk (SBR) vam nudi:

- svetovanje pri identifikaciji, oceni in obvladovanju tveganj,
- podporo pri doseganju skladnosti (NIS2/ZInfV-1, CER/ZKI-1, ISO/IEC 27001, ISO 22301),
- programsko rešitev za digitalizacijo procesov upravljanja tveganj,
- orodja za spremljanje, poročanje (upravi, nadzornim organom, regulatorjem) in odločanje.

Kritična infrastruktura potrebuje sistematično obvladovanje tveganj. Pišite nam in pokazali vam bomo, kako.

info@silverbulletrisk.com - www.silverbulletrisk.com

Avtor: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
Damjan Petrič, mag., generalni direktor Policije

POLICIJA S SVOJIM POSLANSTVOM ZAGOTAVLJA POGOJE ZA VAREN RAZVOJ DRUŽBE

Slovenska policija deluje v času izrazitih gospodarskih, varnostnih in družbenih sprememb, ki od nje zahtevajo visoko stopnjo prilagodljivosti in strokovne usposobljenosti. Naraščajoča kompleksnost varnostnih tveganj, tehnološki razvoj in spremenjena pričakovanja javnosti postavljajo pred policijo nove organizacijske ter strateške izzive. O nadaljnjem razvoju policije in o ključnih usmeritvah v zahtevnih razmerah smo se pogovarjali z generalnim direktorjem Policije.

Kaj so bila vaša vodila pri odločitvi za prevzem funkcije generalnega direktorja Policije?

Odločitev za prevzem te funkcije je bila predvsem izraz odgovornosti do institucije, ki ima v demokratični družbi izjemno pomembno vlogo. Policija ni zgolj organizacija, temveč sistem, ki mora zagotavljati varnost ljudi, varovati njihove pravice in svoboščine ter ohranjati zaupanje javnosti. Vodila me je ocena, da lahko s svojimi izkušnjami in poznavanjem delovanja policije prispevam k stabilnemu, strokovnemu in predvidljivemu razvoju policije. Eno mojih temeljnih vodil je zagotoviti več kontinuitete v vodenju, več spoštovanja do stroke in več predvidljivosti pri upravljanju sistema. Le v stabilnem okolju lahko uresničujemo dolgoročne cilje, krepimo integriteto in profesionalne standarde ter skrbimo za zaposlene, ki so jedro vsake učinkovite policije. Del te spremembe mora biti tudi sodobnejša kultura vodenja, z več jasne odgovornosti, več zaupanja v stroko in več podpore tistim, ki nosijo operativno odgovornost.

ZNUZJV je policiji dal dodatna orodja za učinkovitejše ukrepanje v določenih varnostnih okoliščinah in povečal operativno prožnost sistema. Prvi učinki kažejo večjo odzivnost in boljšo zmožnost hitrega ukrepanja tam, kjer so varnostna tveganja izrazitejša. Ob tem želim posebej poudariti, da cilj zakona ni zgolj represija, temveč součinkovanje ukrepov v prid javnemu redu, varnosti in pravičnosti za vse.

Pri tem me vodi tudi prepričanje, da je policija skupnost ljudi, ki služijo javnosti. Policijsko delo razumem kot poslanstvo, utemeljeno na močnih organizacijskih vrednotah in visokih etičnih standardih.

*avtorica je članica Slovenskega združenja korporativne varnosti

Kako vidite nadaljnji razvoj policije v zahtevnih gospodarskih in družbenih razmerah?

Razvoj policije mora temeljiti na večji prilagodljivosti, odpornosti in jasnem strateškem načrtovanju, kot to predvidevajo tudi usmeritve iz resolucij in razvojnih dokumentov za obdobje 2026–2035. Gospodarske in družbene razmere neposredno vplivajo na varnostno sliko, zato se mora policija hkrati odzivati na klasične varnostne izzive in sistematično razvijati nove zmogljivosti. V ospredju so področja, kot so kibernetska varnost, finančna in gospodarska kriminaliteta, organizirani kriminal ter čezmejne varnostne grožnje. To zahteva močnejšo analitiko, boljše upravljanje informacij in tesnejše sodelovanje z domačimi ter mednarodnimi partnerji. Slovenija je del širšega evropskega varnostnega prostora, zato mora policija ostati močno vpeta v mednarodne mehanizme sodelovanja. V kratkoročnem obdobju se bomo osredotočili na razbremenitev administracije, izboljšanje podpore operativnemu delu in pospešitev izmenjave informacij, saj so to področja, kjer lahko najhitreje dosežemo vidne učinke.

Jedro razvoja pa ostajajo ljudje. Poseben poudarek dajem vlaganju v znanje, kompetence in vodenje. Hkrati vidim velik potencial v digitalni preobrazbi in modernizaciji delovnih procesov, ki morajo razbremeniti policiste administrativnih nalog in jim omogočiti več časa za delo na terenu. Razvoj mora biti voden, merljiv in usmerjen v konkretne učinke za varnost ljudi.

Kako ocenjujete vplive in učinke ZNUZJV na realno delo policije?

ZNUZJV je policiji dal dodatna orodja za učinkovitejše ukrepanje v določenih varnostnih okoliščinah in povečal operativno prožnost sistema. Prvi učinki kažejo večjo odzivnost in boljšo zmožnost hitrega ukrepanja tam, kjer so varnostna tveganja izrazitejša. Ob tem želim posebej poudariti, da cilj zakona ni zgolj represija, temveč sočinkovanje ukrepov v prid javnemu redu, varnosti in pravičnosti za vse. Učinkovito izvajanje ZNUZJV ne more in ne sme temeljiti samo na policiji. Nujen je izrazit medresorski pristop in tesno sodelovanje več resorjev – zlasti šolstva, sociale, financ, FURS-a in drugih pristojnih institucij. Le s takšnim usklajenim delovanjem lahko naslovimo vzroke določenih varnostnih problemov, ne zgolj njihovih posledic.

Hkrati pa je izjemno pomembno, da se zakon uporablja premišljeno, sorazmerno in zakonito. Krepitev pooblastil mora vedno iti z roko v roki s krepitvijo nadzornih mehanizmov, profesionalnih standardov in integritete. Le tako lahko ohranimo legitimnost policije in zaupanje javnosti, kar je dolgoročno eden ključnih strateških ciljev.



Kaj lahko policija stori ob zahtevni kadrovski sliki za večjo prisotnost na terenu in delo z lokalnimi skupnostmi?

Ob omejenih kadrovskih virih moramo najprej izboljšati organizacijo dela in bolj učinkovito uporabljati obstoječe zmogljivosti. To pomeni razbremenjevanje policistov administrativnih opravil, večjo uporabo sodobnih orodij ter bolj ciljno razporejanje kadrov glede na varnostna tveganja. Cilj je, da policist več časa preživi na terenu in manj za mizo. To pomeni poenostavitev poročil, več avtomatskega prenosa podatkov iz evidenc v zapisnike ter odpravo podvajanj vnosov, kjer danes isti podatek pogosto vnašamo v več sistemov. Tam, kjer policist po intervenciji še dolgo pripravlja poročila, moramo s pametnimi obrazci in glasovnim narekom omogočiti, da se administracija skrajša

Pomemben del rešitve je tudi strateško upravljanje kadrov in razvoj vodenja. Upravljanje človeških virov ne sme biti zgolj administrativna funkcija, temveč ena ključnih razvojnih nalog vodstva. Ob tem ostaja ključna krepitev policijskega dela v skupnosti, saj prav prisotnost na terenu in sodelovanje z lokalnim okoljem dolgoročno povečujeta varnost ter zaupanje ljudi.

na nujni minimum. Vsaka ura, ki jo policist prihrani pri administraciji, je ura več za delo z ljudmi in preventivo.

Pomemben del rešitve je tudi strateško upravljanje kadrov in razvoj vodenja. Upravljanje človeških virov ne sme biti zgolj administrativna funkcija, temveč ena ključnih razvojnih nalog vodstva. Ob tem ostaja ključna krepitev policijskega dela v skupnosti, saj prav prisotnost na terenu in sodelovanje z lokalnim okoljem dolgoročno povečujeta varnost ter zaupanje ljudi.

Kaj lahko naredimo na področju opremljanja policije in s tem dviga učinkovitosti?

Opremljanje policije mora biti strateško načrtovano in povezano z razvojnimi cilji. Ne gre le za nabavo nove opreme, temveč za sistematično posodabljanje ključnih sistemov – od komunikacijske in informacijske podpore do zaščitnih in specializiranih sredstev. Oprema ne pomeni zgolj novih vozil ali zaščitnih sredstev, temveč tudi zanesljive komunikacijske in informacijske sisteme, ki delujejo takrat, ko jih najbolj potrebujemo. Zato mora biti poudarek na zanesljivosti, vzdrževanju in načrtnem posodabljanju. Ustrezna oprema neposredno vpliva na varnost policistov in kakovost njihovega dela – to ni strošek, temveč naložba v varnost ljudi.

Kako med mladimi zagotoviti več zanimanja za poklic policista?

Poklic policista moramo predstaviti kot sodoben, strokoven in družbeno pomemben poklic z jasnimi kariernimi možnostmi. Ključno je, da znamo nagovoriti mlade, ki so odgovorni, imajo občutek za pravičnost in iskreno željo pomagati ljudem ter varovati njihove pravice, svoboščine, premoženje in življenje kot najvišje vrednote. Ob tem pa moramo mladim ponuditi tudi ustrezne pogoje za delo in življenje. Dolge razdalje, prometni zastoji in pomanjkanje prostega časa zmanjšujejo motivacijo in kakovost življenja, kar pa za današnje mlade predstavlja velik zadržek pri odločanju za poklic policista. Zato je treba resno razmisliti o uvedbi stanovanjske politike za zaposlene v varnostnem sektorju ter, skupaj z drugimi nastanitvenimi in organizacijskimi rešitvami, mladim omogočiti boljše ravnotežje med delom ter zasebnim življenjem. To ni le socialni ukrep, temveč strateška naložba v privlačnost poklica, zadržanje kadra in dolgoročno stabilnost policije.

Hkrati moramo okrepiti prisotnost policije v izobraževalnem prostoru in javnosti ter pokazati, da je policija pomemben steber varnosti in stabilnosti družbe. V konkurenci za kadre moramo nastopati kot resen, sodoben in zaupanja vreden delodajalec. Vzporedno pa moramo izvajati tudi ukrepe za zadržanje kadrov, ki so že v našem sistemu.

Kakšni so vaši načrti na področju izobraževanja in usposabljanja?

Izobraževanje vidim kot ključni temelj dolgoročnega razvoja policije. Poleg osnovnega usposabljanja bo treba okre-



piti stalno strokovno izpopolnjevanje, specializacije ter razvoj vodstvenih in analitičnih kompetenc. Poseben poudarek bo na novih varnostnih izzivih, kibernetski varnosti, kompleksnih preiskavah in kriznem upravljanju. To je tudi del širšega cilja krepitve odpornosti policije kot sistema in njene pripravljenosti na nepredvidljive razmere.

Kako ocenjujete sodelovanje med Policijo in strokovnjaki za korporativno varnost pri zaščiti kritične infrastrukture?

Sodelovanje je nujno in v osnovi dobro, vendar ga je treba še nadgraditi in bolj sistematično urediti. Zaščita kritične infrastrukture danes presega okvire posameznega sistema in zahteva usklajeno delovanje državnih organov, lokalnih skupnosti in zasebnega sektorja, redno izmenjavo informacij ter skupno načrtovanje in vaje. Korporativna varnost danes ni več ločena od nacionalne varnosti – gre za isti ekosistem tveganj in odgovornosti. Zagotavljanje varnosti je skupna dolžnost vseh ravni, v sodobnem varnostnem prostoru pa se tveganja prelivajo med temi ravnmi, zato tudi odgovori nanje ne morejo biti ločeni ali izolirani.

Kako gledate na prehode kadrov iz policije v korporativno varnost?

Te procese vidim kot del širšega varnostnega sistema. Nekdanji policisti v korporativno varnost prinašajo dragocene izkušnje in razumevanje delovanja javnega varnostnega sistema, kar lahko prispeva k višji ravni varnosti tudi v zasebnem sektorju. Hkrati takšni prehodi krepijo medsebojno razumevanje in olajšujejo sodelovanje med obema sistemoma, kar je v sodobnem varnostnem okolju vse pomembnejše.

Kako vidite potrebo po sistematičnem prenosu znanj s Slovenskim združenjem za korporativno varnost?

Varnostni izzivi danes ne poznajo več jasnih meja med javnim in zasebnim sektorjem, med lokalnim ter državnim okoljem ali med nacionalno in mednarodno ravnijo. Korporativna varnost danes ni več ločena od nacionalne varnosti – gre za isti ekosistem tveganj in odgovornosti. Zato je izmenjava znanj, izkušenj in dobrih praks med policijo in strokovno javnostjo na področju korporativne varnosti ne le koristna, temveč nujna. Največji potencial za tak prenos znanj vidim na področjih kriznega upravljanja, zaščite

Korporativna varnost danes ni več ločena od nacionalne varnosti – gre za isti ekosistem tveganj in odgovornosti. Zato je izmenjava znanj, izkušenj in dobrih praks med policijo in strokovno javnostjo na področju korporativne varnosti ne le koristna, temveč nujna.



kritične infrastrukture, kibernetske varnosti, upravljanja tveganj ter odzivanja na izredne dogodke. Prav na teh področjih se odgovornosti države, gospodarstva in drugih deležnikov najbolj prepletajo in zahtevajo usklajene pristope.

Želite še kaj posebnega sporočiti za konec pogovora?

Za konec želim poudariti, da je moje vodenje usmerjeno v stabilnost, razvoj in krepitev zaupanja v policijo. Besede imajo vrednost le, če jim sledijo jasna dejanja in merljivi cilji. Prioritete morajo biti jasne, dosledne in usmerjene v dolgoročno krepitev policije kot profesionalne, neodvisne in zaupanja vredne institucije.

Moje ključne prioritete so na naslednjih področjih:

Pridobivanje in zadržanje kadra: Policija je kadrovsko podhranjena, kar pogosto pomeni reaktivno delovanje namesto razvoja in preventive. Brez znanja, izkušenj in motivacije zaposlenih ni mogoče graditi močne policije.

Sodobna orodja in tehnologija: Tehnologija ni cilj sama po sebi, temveč orodje, ki policistu pomaga hitreje in bolj učinkovito delati. Digitalna preobrazba mora ljudi razbremeniti rutinskih opravil in jim omogočiti več časa za strokovno in odgovorno odločanje na terenu.

Partnerstvo, ugled in zaupanje v delo policije: Krepitev sodelovanja z drugimi državnimi organi, lokalnimi skupnostmi, mednarodnimi partnerji, sindikati, nadzornimi mehanizmi in mediji je ključna. Transparentnost in odprt dialog sta pogoja za zaupanje javnosti in stalno izboljševanje policijskega dela.

Policija kot servis za ljudi: Le neodvisna, strokovna in zakonita policija lahko dolgoročno ohranja zaupanje javnosti ter učinkovito zagotavlja varnost. Temelj za to so vodje z visoko strokovno in organizacijsko avtoriteto, ki zagotavljajo stabilno, predvidljivo in pošteno karierno okolje za vse zaposlene. ■

Foto: arhiv Policije

Slovensko združenje korporativne varnosti

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

»Ab uno disce omnes (po enem spoznaj vse)«
»Ustvarjamo vezi, ki bogatijo ter tako gradimo pot do uspeha!«

Namen združenja je uresničevanje interesov članstva, ki so:

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

Združenje ima redne, korporacijske in častne člane.

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

GEN SKUPINA	Telekom Slovenije	triglav	PETROL Energija za življenje	CAA	Slovenske železnice
SMART COM	TEB	URSIV	MINISTRSTVO ZA INFRASTRUKTURO	JAVNI MEDOBČINSKI STANOVANJSKI SKLAD MARIBOR	Mestna občina Ljubljana
INFORMATIKA	SIEMENS	AJPES	Pošta Slovenije	Mercator	telemach
Melamin	SPICA	sbr	tenzor	GASILSKA ZVEZA LJUBLJANA	ONKOLOŠKI INŠTITUT INSTITUTE OF ONCOLOGY LJUBLJANA
Elita i.b. d.o.o.	otpbanka	LON	interblock LUXURY GAMING PRODUCTS	NOVARTIS	ZAVOD REPUBLIKE SLOVENIJE ZA BLAGOVNE REZERVE
ZARJA ELEKTRONIKA	UNISTAR PRO	smartis PAMETNI INFORMACIJSKI SISTEMI		ELEKTRONČEK	AKRAPOVIČ
			energetika ljubljana	SIMTECH	CINKARNA

www.ics-institut.si

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



KOLUMNA

PRIPRAVLJEN JE OSNUTEK EVROPSKE STRATEGIJE ZA ODPORNOST KRITIČNE INFRASTRUKTURE

Evropa vstopa v obdobje povečanih sistemskih tveganj, za katerega so značilne prekrivajoče se kibernetske, fizične, okoljske, tehnološke in geopolitične grožnje. Te motnje se vse pogosteje kaskadno širijo med sektorji in čez meje ter vplivajo na kritično infrastrukturo, ključne storitve, javno zaupanje in gospodarsko stabilnost. Evropska strategija odpornosti na motnje se na to spreminjajoče se varnostno okolje odziva z enotnim, strukturiranim in v prihodnost usmerjenim okvirom za krepitev sposobnosti Unije, da preprečuje, vzdrži, se prilagaja ter okreva po večjih motnjah.

Uvod

Uvodoma je treba poudariti, da je pričujoči dokument v obliki osnutka Evropske strategije odpornosti kritične infrastrukture nastal v okviru pomembnega EU projekta ENDURANCE[1], ki je usmerjen v iskanje novih pristopov za zagotavljanje ustrezne odpornosti kritične infrastrukture. Dokument predstavlja rezultat skupnega strokovnega dela projektnih partnerjev, ki so s svojimi znanji in izkušnjami prispevali k oblikovanju celovitega in strateško usmerjenega okvira odpornosti. Pri njegovi pripravi je imel Institut za korporativne varnostne študije ključno koordinativno vlogo, saj je usmerjal vsebinski razvoj, povezoval partnerje in skrbel za metodološko usklajenost dokumenta. Posebna pozornost je bila namenjena integraciji različnih sektorskih pogledov in obstoječih evropskih politik na področju varnosti ter odpornosti.

Osnutek strategije je zasnovan kot strukturiran in v prihodnost usmerjen dokument, ki odgovarja na vse bolj kompleksno tveganjsko okolje v Evropski uniji. Njegov namen je vzpostaviti skupno razumevanje odpornosti kritične infrastrukture in oblikovati operativno izvedljiv okvir za njeno sistematično krepitev. Dokument temelji na analizi obstoječih pravnih, institucionalnih in operativnih mehanizmov ter prepoznanih vrzeli v evropskem prostoru. S tem predstavlja strokovno podlago za nadaljnjo razpravo, usklajevanje in postopno institucionalizacijo enotnega evropskega pristopa k odpornosti kritične infrastrukture. V središču strategije je človek. Njen temeljni cilj je zaščita državljanov, skupnosti, podjetij in javnih institucij z zagotavljanjem neprekinjenega delovanja ključnih storitev ter odpornosti infrastrukture in sistemov, ki podpirajo vsakdanje življenje ter evropsko gospodarstvo. Odpornost tako ni opredeljena kot zgolj tehnična ali sektorsko omejena funkcija, temveč kot skupna odgovornost na lokalni, regionalni, nacionalni ravni in ravni EU, ki vključuje javne organe, upravljavce infrastrukture, zasebni sektor ter civilno družbo.

Strategija temelji na štirih strateških stebrih odpornosti: (1) sistem upravljanja; (2) družbeni in skupnostni sistemi; (3) gospodarski sistemi; (4) infrastrukturni sistemi. Ti skupaj naslavljajo upravljanje, pripravljenost, odzivne zmogljivosti in odporno infrastrukturo ter sisteme.

*avtor je član Slovenskega združenja korporativne varnosti

Za operativno uresničevanje teh stebrov strategija uvaja sklope ukrepov (Action Blocks), ki predstavljajo usklajene skupine političnih, operativnih in razvojnih ukrepov zmogljivosti. Ti sklopi strateške cilje prevajajo v konkretne in izvedljive korake ter zagotavljajo usklajenost med sektorji in državami članicami. Skupaj tvorijo okvir za postopni razvoj evropskega ekosistema odpornosti, ki omogoča usklajene naložbe, razvoj zmogljivosti in stalno izboljševanje.

Ena ključnih značilnosti strategije je pristop »ocenjevanja vseh nevarnosti (All hazard approach)«, ki zajema naravne nesreče, tehnološke okvare, kibernetske incidente, hibridne grožnje, tveganja povezana s človeškim potencialom in obsežne sistemske motnje. Ukrepi odpornosti so zasnovani za delovanje v pogojih negotovosti, pritiska in kaskadnih odpovedi. Strategija zato poudarja interoperabilnost, usklajevanje metodologij ocenjevanja tveganj in uskladitev načrtovalnih ter odzivnih okvirov, saj razdrobljenost ostaja ena ključnih ranljivosti kriznega upravljanja.

Krepitev upravljanja in koordinacije predstavlja osrednji steber strategije. Jasno opredeljene vloge, izboljšano horizontalno in vertikalno sodelovanje ter strukturirani mehanizmi izmenjave informacij so bistveni za učinkovito odpornost. Poseben poudarek je namenjen zaupanja vrednemu upravljanju podatkov, skupni situacijski ozaveščenosti in varni izmenjavi informacij med organi oblasti, upravljavci kritične infrastrukture ter relevantnimi akterji zasebnega sektorja. Te zmogljivosti so temelj za učinkovito odločanje pred, med in po večjih motnjah.

V središču strategije je človek. Njen temeljni cilj je zaščita državljanov, skupnosti, podjetij in javnih institucij z zagotavljanjem neprekinjenega delovanja ključnih storitev ter odpornosti infrastrukture in sistemov, ki podpirajo vsakdanje življenje ter evropsko gospodarstvo. Odpornost tako ni opredeljena kot zgolj tehnična ali sektorsko omejena funkcija, temveč kot skupna odgovornost na lokalni, regionalni, nacionalni ravni in ravni EU, ki vključuje javne organe, upravljavce infrastrukture, zasebni sektor ter civilno družbo.

Strategija prepoznava odpornost kot dinamično zmogljivost. Neprekinjeno usposabljanje, vaje, testiranja in učenje po incidentih so ključni za zagotavljanje, da načrti ter sistemi delujejo tudi pod dejanskim pritiskom. Vključenost vodstva, kompetentnost zaposlenih in organizacijska kultura so opredeljeni kot odločilni dejavniki uspešnosti v kriznih razmerah, kar poudarja potrebo po trajnih naložbah v človeške ter institucionalne zmogljivosti poleg tehnoloških rešitev.



Krepitev upravljanja in koordinacije predstavlja osrednji steber strategije. Jasno opredeljene vloge, izboljšano horizontalno in vertikalno sodelovanje ter strukturirani mehanizmi izmenjave informacij so bistveni za učinkovito odpornost. Poseben poudarek je namenjen zaupanja vrednemu upravljanju podatkov, skupni situacijski ozaveščenosti in varni izmenjavi informacij med organi oblasti, upravljavci kritične infrastrukture ter relevantnimi akterji zasebnega sektorja. Te zmogljivosti so temelj za učinkovito odločanje pred, med in po večjih motnjah.

Strategija je v celoti usklajena z obstoječo zakonodajo in politikami EU, vključno z direktivama NIS2 ter CER in sektorskimi zahtevami glede odpornosti. Evropska strategija odpornosti na motnje tako zagotavlja enoten strateški okvir za preprečevanje, pripravljenost, odzivanje in okrevanje. Z organizacijo odpornosti okoli štirih stebrov in pripadajočih sklopov ukrepov vzpostavlja jasno pot za krepitev evropskega ekosistema odpornosti ter povečuje sposobnost Unije za absorpcijo šokov, zaščito državljanov in ohranjanje družbene ter gospodarske stabilnosti v vse bolj kompleksnem in povezanem varnostnem okolju.

Ob upoštevanju poglavij v omenjenem dokumentu se strategija osredotoča predvsem na naslednje:

- Evropska strategija odpornosti na motnje za kritično infrastrukturo vzpostavlja skupno vizijo, da ključne storitve ostanejo varne, zanesljive in hitro obnovljive v vseh razmerah. Odpornost je opredeljena kot strateška nujnost za zaščito družbene blaginje, gospodarske konkurenčnosti in demokratične stabilnosti v Uniji.
- Strategija določa jasne cilje in ključne ukrepe za krepitev pripravljenosti, izboljšanje medsektorskega in čezmejnega usklajevanja ter pospešitev zmogljivosti za okrevanje. Ti ukrepi strateško vizijo prevajajo v operativne naloge za institucije EU, države članice in upravljavce ključnih storitev.
- Temeljni element strategije je skupna definicija odpornosti, prilagojena potrebam evropske kritične infrastrukture. Odpornost je opredeljena kot sposobnost sistema, da predvidi, vzdrži, se prilagodi in okreva po motnjah, kar predstavlja konceptualno osnovo za usklajene pristope v EU.
- Pregled evropskega okolja odpornosti razkriva kompleksen ekosistem nacionalnih organov, institucij EU in zasebnih upravljavcev z različnimi stopnjami razvitosti ter virov. Kljub številnim koristnim pobudam ostaja razdrobljenost, kar poudarja potrebo po večji usklajenosti in skupnih metodologijah.
- Strategija opredeljuje ključne izzive in vrzeli, med drugim nezadostno interoperabilnost med sektorji, omejeno sprotno situacijsko ozaveščenost, neenakomerno izvajanje obstoječih politik ter pomanjkljive mehanizme za usklajeno ocenjevanje tveganj. Odprava teh vrzeli je bistvena za zmanjšanje sistemskih ranljivosti.

Predlagan je strateški pristop za izgradnjo temeljnih lastnosti odpornega evropskega sistema kritične infrastrukture (predvidevanja, robustnosti, prilagodljivosti in obnovljivosti) z združenimi tehnološkimi, organizacijskimi in političnimi ukrepi. Analiza obstoječega političnega in pravnega okvira priznava napredek z instrumenti, kot sta CER ter NIS2, hkrati pa izpostavlja vrzeli pri operativnih usmeritvah, izvrševanju in medsektorskem usklajevanju.

Za omogočanje bolj usklajenega delovanja strategija uvaja model upravljanja odpornosti na ravni EU, ki jasno določa vloge, poti odločanja in mehanizme izmenjave informacij. Model krepi sodelovanje na vseh ravneh in podpira hitro ter usklajeno odločanje v kriznih razmerah.

Strategija temelji na stebrih odpornosti na motnje, ki zagotavljajo strukturirano podlago za krepitev kritične infrastrukture v Evropi. Ti stebri usmerjajo razvoj operativnega akcijskega načrta z izvedljivimi, razširljivimi in časovno opredeljenimi pobudami za izboljšanje pripravljenosti, sodelovanja ter odzivnih zmogljivosti.

Končno poglavje o nadaljnjih korakih opredeljuje, kako bo strategija institucionalizirana s trajno politično zavezanostjo, ustreznimi naložbami in stalnim vrednotenjem. S pogledom v prihodnost in prilagodljivim okvirom lahko Evropa zgradi integriran ter odporen ekosistem kritične infrastrukture, ki bo sposoben obvladovati prihodnje motnje in zagotavljati neprekinjeno delovanje ključnih storitev za svoje državljane.

Zaključna misel

Sedaj je čas, da izkoristimo to strokovno priložnost in se o omenjenem osnutku strategije pogovorimo v najširšem možnem kontekstu ter v tekst vnesemo še dodatne vidike, ki bodo zagotovili, da bomo imeli pred nami ustrezen strateški dokument. Ta mora nakazovati in nasloviti vse izzive, ki jih bomo z naslednjimi operativnimi koraki na področju zagotavljanja odpornosti začeli ustrezno uveljavljati. V Republiki Sloveniji smo ravno pred sprejemom Strategije odpornosti Republike Slovenije, ki pa že v kratki primerjalni analizi kaže na potrebo po dodatni opredelitvi določenih specifičnih strateških zahtev. V nasprotnem bo nacionalna strategija postala še eden od dokumentov, ki ne bo izkazovala potrebne vrednosti in celovitih strateških usmeritev. Delovanje v smeri silosnih pristopov ne omogoča več ustreznega dinamičnega odzivanja na tveganja, ki jih prinaša zahtevno varnostno okolje. Sploh pa ne če želimo izgraditi učinkovit sistem odpornosti naših evropskih družb, med katerimi ima odpornost kritične infrastrukture in ostalih bistvenih procesov zelo pomembno vlogo.

Zaradi vsega navedenega vas vabimo, da se vključite v razpravo prek varnostne platforme, ki jo predstavlja Slovensko združenje za korporativno varnost in postanete del mednarodne delovne skupine za izmenjavo pogledov na zagotavljanje odpornosti v okviru EU ENDURANCE projekta. Več informacij si lahko ogledate na https://endurance-horizon.eu/project-working-group/. ■

[1] https://endurance-horizon.eu/

SMART COM

Pandorina skrinjica digitalizacije v industriji 2026

Spoznajte, kako se s premišljenimi ukrepi zaščitite pred kibernetskimi napadi in preprečite izpade kritičnih sistemov.

Konkretni primeri **Brezplačno***

23. april 2026 | Fraport, Letališče Ljubljana (LJU)

Več informacij o dogodku in prijava

*Število mest je omejeno

www.smart-com.si

Partnerji dogodka

FORTINET EXCLUSIVE NETWORKS NOZOMI NETWORKS

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije*

INTERVJU
Boštjan Pavlin, mag., državni sekretar Ministrstva za obrambo RS

SLOVENIJA MED KRIZAMI IN PRILOŽNOSTMI: POT DO SISTEMSKE ODPORNOSTI

Slovenija se v zadnjih letih sooča z vrsto prepletenih kriz, od naravnih nesreč in zdravstvenih izzivov do geopolitičnih napetosti ter kibernetskih groženj. Vsaka od teh preizkušenj je razkrila tako ranljivosti kot tudi pomembne zmogljivosti države in njenih institucij. Prav v soočanju s krizami se odpira prostor za premik od odzivnega k sistemskemu pristopu k odpornosti. Pot do celovite odpornosti Slovenije zato pomeni strateško nadgradnjo upravljanja tveganj, okrepitev sodelovanja med sektorji in dolgoročno vlaganje v varne ter prilagodljive sisteme. Več o teh izzivih grajenja sistema odpornosti nam je zaupal Boštjan Pavlin, mag., državni sekretar Ministrstva za obrambo.

Slovenija je v zaključni fazi priprave Nacionalne strategije odpornosti. Kako na ministrstvu razumete pojem odpornosti? Je to zgolj kot sposobnost odziva na krize ali kot širši sistem preprečevanja, pripravljenosti in hitrega okrevanja celotne družbe?

Graditev nacionalne odpornosti razumemo kot proces, ki presega delovanje posameznega resorja. Uresničevanje Strategije odpornosti Republike Slovenije do leta 2030 zato temelji na treh načelih: celovitem medresorskem pristopu, celovitem družbenem pristopu in celovitem pristopu k varnostnim tveganjem ter grožnjam.

Odpornost odraža sposobnost države, družbe in posameznika, da se pripravijo na izredne dogodke oziroma šoke ter motnje, se jim zoperstavijo, se nanje odzovejo in hitro okrevajo po njih. Ministrstvo za obrambo si prizadeva k vzpostavitvi varne in odporne države, ki ima zmožnosti za predvidevanja ter obvladovanja tveganj ne glede na njihovo naravo ali izvor. Prav tako stremi k zagotovitvi ustrezne pripravljenosti in zaščite državljanov ter ohranitvi ključnih funkcij države in družbe tudi v varnostno najbolj zaostrenih pogojih.

V Republiki Sloveniji doslej še ni bil vzpostavljen celovit in osrednji strateški okvir, ki bi sistematično povezoval vse vidike krepitve odpornosti države in družbe. Prav temu je namenjena Strategija odpornosti Republike Slovenije do leta 2030, ki vzpostavlja enoten, usklajen in dolgoročno naravnan vsedružbeni in celovit medresorski pristop k obvladovanju izrednih dogodkov ter krepitvi pripravljenosti in okrevanja. Strategija pri tem upošteva tudi strateške smernice za krepitev odpornosti, oblikovane na ravni Evropske unije in zveze Nato, ter jih smiselno umešča v nacionalni pravni red in normativni okvir Republike Slovenije.

*avtor je član Slovenskega združenja korporativne varnosti



Graditev odpornosti je izrazito medresorski in medsektorski projekt. Kateri so ključni koraki, s katerimi želite povezati državo, lokalne skupnosti, gospodarstvo in civilno družbo v enoten, operativno delujoč sistem?

Graditev nacionalne odpornosti razumemo kot proces, ki presega delovanje posameznega resorja. Uresničevanje Strategije odpornosti Republike Slovenije do leta 2030 zato temelji na treh načelih: celovitem medresorskem pristopu, celovitem družbenem pristopu in celovitem pristopu k varnostnim tveganjem ter grožnjam.

Uresničevanje strategije temelji na tesnem in sistematičnem sodelovanju med državnimi ustanovami, lokalnimi skupnostmi, zasebnim sektorjem, prebivalci ter drugimi relevantnimi deležniki. Pri tem je bistvenega pomena krepitev zaupanja javnosti v ustanove, ki morajo delovati transparentno, odgovorno in učinkovito, hkrati pa spodbujanje proaktivne vloge državljanov pri soustvarjanju celovite odpornosti. Organizirani bodo številni javni dogodki, s katerimi bo promovirana odpornost posameznika, s tem pa tudi lokalne skupnosti, države in družbe. Pomembno dimenzijo predstavlja tudi krepitev partnerstev Republike Slovenije v okviru Evropske unije in sodelovanje z mednarodnimi organizacijami, kot sta Nato ter Združeni narodi. S tem krepimo skupne zmogljivosti za predvidevanje, preprečevanje in obvladovanje izrednih dogodkov ter učinkovitejše omejevanje njihovih posledic.

Strategija bo uspešna le, če bo zaživela v praksi. Kako nameravate zagotoviti, da dokument ne ostane na ravni deklaracij, temveč se prevede v jasne naloge, vire financiranja, odgovornosti in merljive cilje?

Prvi korak implementacije strategije je ponotranjenje oziroma zavedanje o potrebi po krepitvi odpornosti kot eni izmed najpomembnejših vrednot in veščin, ki jih morajo razviti posamezniki, skupnost, družba ter država.

Krepitev odpornosti je kontinuiran in dolgoročen proces, ki se v različnih oblikah izvaja že vrsto let. Zlasti je treba izpostaviti celovito nacionalno vajo kriznega upravljanja in odzivanja Odpornost 24, izvedeno leta 2024, ki je predstavljala pomemben mejnik pri celostnem preverjanju delovanja sistema nacionalne varnosti ter mehanizmov medresorskega in medinstitucionalnega sodelovanja, tako imenovani stresni test države. Na podlagi ugotovljenih pomanjkljivosti in vrzeli so bili pripravljeni konkretni ukrepi, združeni v akcijskem načrtu, katerega namen je izboljšanje pripravljenosti, odzivnosti ter usklajenega delovanja države in družbe v primeru izrednih dogodkov.

V letu 2026 je predvidena izvedba nove celovite nacionalne vaje Odpornost 26, ki bo omogočila nadaljnje preverjanje napredka, učinkovitosti ukrepov in prilagajanje sistema novim varnostnim izzivom.



Tudi sama strategija je ciljno naravnana. Oblikovani so strateški cilji, ki se bodo na ravni ožjih vsebinsko zakroženih delovnih skupin uresničevali z natančno definiranimi ukrepi. Po koncu vaje bo izvedena revizija in prenova obstoječega akcijskega načrta, ki bo poleg opredeljenih ukrepov vključeval tudi merila uspešnosti, odgovorne nosilce, časovnice izvedbe ter vire financiranja. S tem bodo zagotovljeni sprotno posodabljanje akcijskega načrta, njegova vsebinska relevantnost in celovito uresničevanje strategije.

Pred nami so volitve in menjave političnih prioritet. Ali je po vašem mnenju v Sloveniji dovolj zavedanja, da je odpornost nacionalni, dolgoročen projekt, ki mora presegati mandatne cikle, in kako zagotoviti kontinuiteto ključnih programov?

Ne bi se strinjal, da bo marec prinesel menjave prioritet. Za dolgoročno varnost in stabilnost Republike Slovenije je nujno, da odpornost ostane trajen projekt, neodvisen od posameznih mandatov ali političnih prioritet. Strategija z jasno določenim mehanizmom izvajanja zagotavlja, da bodo njeni ključni ukrepi ostali aktivni ne glede na politične spremembe.

Kritična infrastruktura postaja osrednja točka hibridnih groženj, od kibernetskih napadov do motenj oskrbnih verig. Katere sektorje ocenjujete kot najbolj ranljive in kakšno vlogo pričakujete od upravljavcev infrastrukture pri soustvarjanju sistema odpornosti?

Nov Zakon o kritični infrastrukturi opredeljuje 11 sektorjev kritične infrastrukture, ki zajemajo več kot 60 bistvenih storitev, od pitne vode, pridelave, predelave in distribucije živil, energetike, zdravja, pa vse do vesolja. Zagotovo ima vsak od teh sektorjev določene ranljivosti, hkrati pa so tudi med seboj povezani in soodvisni. Tisti upravljavci infrastrukture, ki bodo letos na podlagi Zakona o kritični infrastrukturi določeni za kritične subjekte, bodo vsekakor imeli pomembno vlogo pri krepitvi odpornosti. Vsak od njih bo moral pripraviti oceno tveganj za bistveno storitev, ki jo opravlja, izdelati načrt za odpornost in sprejeti tehnične, varnostne, organizacijske ter druge ukrepe za odpornost. Prav tako bodo morali zagotavljati podatke za potrebe sistema zgodnjega opozarjanja na področju kritične infrastrukture, katerega vzpostavitev Zakon o kritični infrastrukturi prav tako predvideva.

Gospodarstvo, tudi nekateri upravljavci kritične infrastrukture, pogosto opozarjajo na razkorak med regulativnimi zahtevami in realnimi zmožnostmi. Kako boste vzpostavili ravnotežje med nujno stopnjo varnosti in operativno ter finančno vzdržnostjo podjetij?

Upravljavci kritične infrastrukture ne opozarjajo na razkorak med regulativnimi zahtevami in realnimi zmožnostmi. Gre za v veliki večini uspešna javna ali zasebna podjetja, katerim je v interesu neprekinjeno opravljanje njihovih storitev v vseh razmerah. Prav to je tudi namen krepitve odpornosti na področju kritične infrastrukture. Podjetja že sama po sebi skrbi-

jo za kibernetsko varnost, varovanje svojih objektov in infrastrukture, iščejo zanesljive dobavitelje ter vlagajo v usposobljenost svojih kadrov. Sprotno se prilagajajo razmeram in zakonitostim trga. Vedno bolj se zavedajo, da je za njihovo uspešno in gospodarno poslovanje eden od temeljev prav neprekinjeno delovanje ter odpornost sistemov, omrežij infrastrukture itd. Pogosto ugotavljamo, da gre za nerazumevanje zakonskih zahtev in posledično strah, da bo treba izdelati dodatne načrte, sprejeti dodatne ukrepe. Vendar Zakon o kritični infrastrukturi določa, da kritični subjekti lahko uporabijo že pripravljene ocene tveganj, načrte in ukrepe, sprejete na podlagi drugih predpisov, katerih zavezanec so. Če morajo izvesti dodatne ukrepe za odpornost, lahko Vlada Republike Slovenije odloči o dodelitvi sredstev za izvedbo teh ukrepov.

V okviru evropskega projekta ENDURANCE je nastal osnutek Evropske strategije odpornosti kritične infrastrukture. Na kakšen način boste te ugotovitve in predloge vključili v slovenski model ter kako vidite vlogo Slovenije v širšem evropskem varnostnem in odpornostnem prostoru?

Slovenija iz leta v leto potrjuje svojo vlogo vodilne države na področju odpornosti in kritične infrastrukture v Evropi. Besedilo EU Direktive o odpornosti kritičnih subjektov (v nadaljnjem besedilu: CER direktiva) je nastalo v času slovenskega predsedovanja Svetu Evropske unije leta 2021 in se v veliki meri zgleduje po prvem Zakonu o kritični infrastrukturi iz leta 2017. Slovenija je bila tudi ena izmed prvih držav članic Evropske unije, ki so to direktivo z novim Zakonom o kritični infrastrukturi prenesle v svoj pravni sistem. Te izkušnje niso samo zgled za druge države članice Evropske unije, temveč tudi za kandidatke za članstvo in predvsem za Ukrajino, s katero na področju kritične infrastrukture ter odpornosti aktivno sodelujemo. Gre za obojestransko neprecenljivo izmenjavo informacij in izkušenj iz prve roke, kar nikakor ni samoumevno. Odpornost je nacionalna odgovornost vsake države, kar velja tako v Evropski uniji (4. člen Pogodbe o Evropski uniji) kot v Natu (3. člen Severnoatlantske oz. Washingtonske pogodbe). Tudi CER direktiva ne narekuje sprejema Evropske strategije o odpornosti kritičnih subjektov. Na Ministrstvu za obrambo smo zato že pripravili Strategijo za odpornost kritičnih subjektov, ki jo je Vlada Republike Slovenije sprejela 10. februarja 2026.

Projekt ENDURANCE je zgolj eden izmed številnih projektov. Ugotovitev in predlogov kot rezultatov projekta v slovenski okvir za odpornost kritičnih subjektov ni treba vključevati. V Sloveniji bomo sledili zakonodaji Evropske unije na tem področju. Določeni predlogi so že sicer del normativno-pravnega okvira na področju kritične infrastrukture v Sloveniji, kot npr. sistem zgodnjega opozarjanja, izvajanje vaj, stresnih testov itd. Večino predlogov iz osnutka evropske strategije, ki ga omenjate, smo na ministrstvu že predvideli. V osnutku so navedene nekatere inovacije do leta 2032, kot so smernice za odpornost v zasnovi projektov kritične infrastrukture, uvedba digitalnih dvojčkov in sistemov za zgodnje opozarjanje s pomočjo umetne inteligence ter izvedba stresnih testov v več sektorjih. Na obrambnem ministrstvu vse to že več let načrtujemo in v določeni meri tudi že izvajamo. To le še potrjuje dejstvo, da je Slovenija na tem področju pred večino drugih držav.

> Ne bi se strinjal, da bo marec prinesel menjave prioritet. Za dolgoročno varnost in stabilnost Republike Slovenije je nujno, da odpornost ostane trajen projekt, neodvisen od posameznih mandatov ali političnih prioritet. Strategija z jasno določenim mehanizmom izvajanja zagotavlja, da bodo njeni ključni ukrepi ostali aktivni ne glede na politične spremembe.

Če pogledate pet do deset let naprej, kako naj bi bil videti zrel sistem odpornosti Republike Slovenije? Kateri kazalniki bodo pokazali, da smo kot država res sposobni predvidevati krize, jih obvladovati in se po njih hitro pobrati?

V zadnjem desetletju je postalo očitno, da čisto vseh dogodkov ni možno predvideti. Poleg masovnih migracij, epidemij in drugih zdravstvenih kriz, kibernetskih napadov ali celo vojne nas lahko vedno presenetijo tudi naravne nesreče s katastrofalnimi posledicami. Kljub temu lahko s pristopom, ki upošteva vse nevarnosti („all-hazards approach“), nenehno krepimo odpornost države. Tudi kadar ni okoliščin, ki bi lahko vodile v krizo, je treba izvajati vaje in spremljati kazalnike, ki lahko nakazujejo pojav motenj, izrednih dogodkov, krize. Odpornost države je namreč treba krepiti v miru. Sodobne tehnologije nam omogočajo pridobivanje in analiziranje velikih količin podatkov, zato bo ključen ne le celovit medresorski pristop, ampak sodelovanje celotne družbe. To ne pomeni le, da bodo pri izgradnji sistema odpornosti sodelovali tako državni organi, lokalne skupnosti, gospodarstvo in akademska sfera, temveč bodo tudi podjetja, javna ter zasebna, morala dojeti svojo vlogo in pomen deljenja podatkov, informacij ter poročil, s pomočjo katerih bo možno predvidevati krize, jih obvladovati in hitro okrevati.

Prva celovita nacionalna vaja Odpornost 24 je predstavljala pomemben mejnik pri preverjanju odpornosti države in družbe ter sposobnosti usklajenega odzivanja na izredne dogodke. Po našem vedenju smo edina država Evropske unije, ki je izvedla stresni test države. V naslednjih petih do desetih letih bomo z rednimi, dvoletnimi vajami pridobili dodatne praktične izkušnje, na katerih bomo gradili robusten in operativen sistem odpornosti.

Pomembni pokazatelji napredka bodo med drugim povečana samooskrba, krepitev nacionalne zavesti in zavedanja posameznika o njegovi vlogi pri odpornosti skupnosti ter tesnejše sodelovanje države, lokalnih skupnosti, gospodarstva in civilne družbe. Vsi ti elementi bodo prispevali k vzpostavitvi fleksibilnega in trajnostnega sistema, ki se bo sposoben stalno prilagajati novim izzivom časa. ■

Foto: arhiv Ministrstva za obrambo RS

CELOVITE REŠITVE ZA OKOLJA Z NAJVIŠJIMI VARNOSTNIMI ZAHTEVAMI

V okoljih, kjer se upravlja kritična infrastruktura, občutljivi podatki ali procesi, je ključna kombinacija popolne sledljivosti, fizične zaščite in centralnega nadzora.

Digitalno zaklepanje ni več nadgradnja, temveč nujen korak k skladnosti, varnosti in obvladovanju tveganj v sodobnih podatkovnih centrih.

iLOQ S50 digitalni sistem zaklepanja

omogoča upravljanje dostopa do rack omar in tehničnih prostorov prek pametnega telefona.



iLOQ S50 podpira cilje NIS2, saj omogoča:

- jasno identifikacijo vsakega uporabnika,
- sledljivost in revizijsko evidenco dostopov,
- takojšen preklic pravic ob varnostnem incidentu,
- zmanjšanje tveganja zaradi izgubljenih ali kopiranih ključev.

Tubularna varnostna vrata za kontroliran prehod v varovani perimeter

Povsod, kjer je varnost proces, ne zgolj oprema, je nadzor prehoda ključen del zaščite.



- Učinkovito preprečevanje tailgatinga (prehoda dveh oseb).
- Napredno senzorsko zaznavanje nepravilnosti.
- Robustna jeklena konstrukcija in varnostno steklo za industrijsko uporabo.
- Integracija s kontrolo pristopa in evidenco delovnega časa.

ID Shop – povezujemo tradicionalno varnost in pametne tehnologije.

IDealni partner za identifikacijo in varnost

ID Shop d. o. o., Litostrojska 44d, 1000 Ljubljana
T: +386 (0)1500 40 50
E: info@idshop.si **W:** www.idshop.si

Avtor: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
dr. Jelena Virant Burnik, informacijska pooblaščenka Republike Slovenije*
in podpredsednica Evropskega odbora za varstvo podatkov

STALNE SPREMEMBE SO POSTALE STALNICA TUDI PRI DELU INFORMACIJSKEGA POOBLAŠČENCA

Ob 20. obletnici delovanja institucije Informacijskega pooblaščenca se odpira prostor za razmislek o razvoju varstva osebnih podatkov v času izrazitih družbenih in tehnoloških sprememb. Dve desetletji delovanja zaznamujejo stalne prilagoditve novim izzivom, ki jih prinašajo digitalizacija, umetna inteligenca, množični podatki in globalna povezanost. Meje med javnim interesom, varnostjo, gospodarskim razvojem in pravico do zasebnosti so vse bolj kompleksne ter zahtevajo premišljeno in strokovno uravnoteženo presojo. Ob jubileju se zato postavlja vprašanje, kako se bo institucija odzivala na prihodnje izzive in katere vsebinske prioritete bodo zaznamovale njeno delo v naslednjem obdobju. O prihodnjih težiščih delovanja in o viziji razvoja institucije smo se pogovarjali z informacijsko pooblaščenko Republike Slovenije ter podpredsednico Evropskega odbora za varstvo podatkov dr. Jeleno Virant Burnik.

Informacijski pooblaščenec letos obeležuje 20 let delovanja. Kateri dosežki tega obdobja se vam zdijo prelomni za razvoj kulture varstva osebnih podatkov in transparentnosti v Sloveniji ter kje vidite največji premik v zavedanju podjetij in javnega sektorja?

Lahko najprej odgovorim v številkah. V dveh desetletjih smo obravnavali 20.000 kršitev varstva osebnih podatkov. K spodbujanju odgovorne rabe osebnih podatkov prispevamo tudi s svetovanjem, mnenji, pojasnili, smernicami in priročniki. Teh je bilo v tem času več kot 30.000. Več kot 11.000 posameznikov, novinarjev in nevladnih organizacij se je v zadnjih 20 letih obrnilo na nas, ker niso prejeli informacij javnega značaja. Več kot 1300 krat smo v dveh desetletjih opozorili na neustreznost zakonske ureditve. Marsikdaj so naše pripombe upoštevane, večkrat pa ne v celoti. Kar nekajkrat je zato na našo pobudo o neustavnosti odločilo Ustavno sodišče, na primer glede širjenja oblastnih pooblastil represivnih organov, kot so obvezna hramba prometnih podatkov, optična prepoznava registrskih tablic, IMSI lovilci. Zavedanje o varstvu osebnih podatkov in transparentnosti se krepi postopoma, z vsako novo prijavo ali pritožbo, z vsakim odgovorom na zaprosilo za mnenje ter vsakim pogovorom v telefonskem dežurstvu.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



V kontekstu stalnih sprememb je za učinkovito delovanje Informacijskega pooblaščenca ključno grajenje strokovnega znanja in strokovne odličnosti. Tudi na področju poznavanja tehnologije. Graditi moramo mostove med različnimi področji našega delovanja, med pravom, tehnologijo, družbo in etiko ter dosledno varovati neodvisnost institucije.

Na področju varstva osebnih podatkov v dveh desetletjih vsekakor zaznavamo, da so bolj prepoznana tveganja, povezana s prekomerno rabo osebnih podatkov. K temu nas navsezadnje vodi tudi vsako leto večje število pritožb in prijav – največkrat se na nas obrnejo posamezniki, ki želijo obraniti svoje pravice. Kje opažamo največja tveganja? Pri uvajanju novih tehnologij, pri centralizaciji in digitalizaciji velikih podatkovnih zbirk. Prepogosto se z luknjami ukvarjamo šele potem, ko se je že zgodil neželen vdor. Velikokrat opozarjamo tudi na sorazmernost, in da se podatkov ne sme zbirati na zalogo, pač pa le za točno določne namene. Tam, kjer se obdeluje veliko osebnih podatkov, je posledično več možnosti za njihovo zlorabo. Prav tako iz leta v leto narašča število pritožb na področju dostopa do informacij javnega značaja, ne glede na ustaljeno sodno prakso, da ima javnost pravico vedeti, kakšne so plače in dodatki javnih uslužbencev in funkcionarjev, prav tako do podatkov povezanih z okoljem in okoljskimi politikami. Institucije javnega sektorja morajo narediti več, da javnost dobi informacije, do katerih je upravičena in to hitro, ne po več letih zavlačevanja s pravnimi sredstvi.

Vloga vašega organa se je v dveh desetletjih močno razširila, od nadzora nad varstvom osebnih podatkov do dostopa do informacij javnega značaja in digitalnih pravic. Kako se je spreminjal profil tveganj, s katerimi se srečujete, in katere nove kompetence ste morali razviti?

Poleg naraščajočega števila pritožb na vseh področjih našega dela so pri IP edina stalnica - spremembe. Tiste, ki jih prinaša tehnološki razvoj in pa stalne spremembe pravnega okvira našega delovanja. Najprej GDPR, pa z zamudo ZVOP-2, pa obdobje 3.0, ko so se pridružili akti EU digitalne agende, nova procesna uredba in pravila o umetni inteligenci. Kompleksnost pravil in njihovo spreminjanje je lahko veliko breme, tako za organizacije, ki želijo delovati skladno, kot tudi za nadzorni organ. Pravna jasnost je za varovanje temeljnih pravic ključna, njeno pomanjkanje pa pomeni le to, da pravila ostanejo mrtva črka na papirju. Naš trenutni izziv so omnibus uredbe, ki prihajajo iz EU kot odziv na kritiko, da EU preveč regulira in premalo inovira. Če bodo poenostavitve odvzele del birokratskega bremena, jih lahko le podpremo. Vendar pa me skrbi, da nekateri predlogi ustvarjajo dodatne pravne nejasnosti in lahko znižajo standarde, ki smo jih v EU že dosegli.

V kontekstu stalnih sprememb je za učinkovito delovanje Informacijskega pooblaščenca ključno grajenje strokovnega znanja in strokovne odličnosti. Tudi na področju poznavanja tehnologije. Graditi moramo mostove med različnimi področji našega delovanja, med pravom, tehnologijo, družbo in etiko ter dosledno varovati neodvisnost institucije. Močne neodvisne nadzorne institucije, z ustreznimi viri so namreč ključne za odprto in demokratično družbo. V organizacijskem smislu pa to pomeni tudi spodbujanje interdisciplinarnosti, izobraževanja, kreativnosti, tudi prek povezovanja s študenti in različnimi fakultetami.

Varnost podatkov danes ni več zgolj pravno vprašanje, temveč vprašanje upravljanja organizacij in konkurenčnosti. Kako naj vodstva podjetij razumejo vlogo varstva osebnih podatkov, kot omejitev poslovanja ali kot mehanizem za gradnjo zaupanja in odpornosti?

Kot pogosto poudarim, je treba varstvo osebnih podatkov razumeti kot podstat za uresničevanje drugih pravic. Če lahko kdorkoli izkorišča podrobnosti o nas, se ne moremo svobodno gibati in srečevati, deliti svojih misli, verovati. In

tudi ne moremo svobodno oddati svojega glasu na volitvah. Še posebej v kontekstu napredka in uporabe umetne inteligence to ni birokratska ovira razvoju, pač pa njegov garant. Garant, da tehnološki napredek ostaja v službi človeka in ne obratno. Pravila varstva osebnih podatkov ne prepovedujejo, da se podatki zbirajo in shranjujejo, poskrbijo pa za to, da se zbirajo le takrat, kadar je to res treba, in da je njihov obseg čim bolj omejen.

Upoštevanje pravil varstva osebnih podatkov lahko izboljša procese digitalizacije, zmanjša tveganja, da so podatki razkriti, napačno obdelani, da imajo posamezniki negativne posledice. Tu ne gre le za varovanje zasebnosti posameznikov, pač pa za veliko več. Napake pri obdelavah podatkov v zdravstvu npr. lahko pomenijo tveganje za življenje posameznika, nepremišljena obdelava podatkov z umetno inteligenco lahko pomeni, da državljan ne bo prejel neke storitve ali sredstev, čeprav je do njih upravičen, dopuščanje obdelav podatkov za druge namene lahko pomeni, da nas zasledujejo oglasi za dvomljiva zdravila in izkoriščajo naše ranljivosti. Še posebej je to pomembno, ko govorimo o mladostnikih, pa starejših, ki so bolj ranljivi za zlorabe. Zato je varovanje osebnih podatkov vsekakor treba razumeti kot mehanizem za gradnjo zaupanja in odpornosti in ne kot omejitev poslovanju.

Glede na to, da umetna inteligenca poleg prednosti prinaša tudi kar nekaj tveganj, je res pomembno, da se na vseh ravneh zavzemamo za razvoj zaupanja vrednega ekosistema umetne inteligence. Le tako nam bo kot družbi nova tehnologija v resnično korist.

Evropska uredba o umetni inteligenci (AI Act) prinaša povsem nov regulativni okvir. Kakšno vlogo bo imel Informacijski pooblaščenec pri prenosu in izvajanju te zakonodaje v Sloveniji ter kako se pripravljate na nadzor nad sistemi umetne inteligence?

V okvir naše pristojnosti sodijo sistemi UI, ki jih Akt o umetni inteligenci prepoveduje, npr. sistemi za družbeno točkovanje, za napovedovanje izvrševanja kaznivih dejanj in za





sklepanje o čustvih na delovnem mestu ter v izobraževanju. Pravila na tem področju se trenutno že uporabljajo. Nadzorovali bomo tudi visoko tvegane sisteme UI na področju biometrije, izobraževanja, kaznivih dejanj, migracij, azila in nadzora nad mejami ter na področju pravosodja in volitev. Obveznosti glede visoko tveganih sistemov UI naj bi začele veljati avgusta 2026. Poleg nas bodo nadzor izvajali tudi Agencija za komunikacijska omrežja in storitve, Banka Slovenije, Agencija za zavarovalni nadzor ter Tržni inšpektorat. V organizacijskem smislu to pomeni nov oddelek znotraj IP, vse ključne podrobnosti so že na voljo tudi na naši spletni strani in veliko sodelovanja ter povezovanja z drugimi organi v Slovenji in na EU ravni v Odboru za UI.

Kako lahko strateško Informacijski pooblaščenec pripomore pri vzpostavljanju ekosistema zaupanja vredne umetne inteligence v Sloveniji? Kako boste sodelovali z drugimi nadzornimi organi?

Glede na to, da umetna inteligenca poleg prednosti prinaša tudi kar nekaj tveganj, je res pomembno, da se na vseh ravneh zavzemamo za razvoj zaupanja vrednega ekosistema umetne inteligence. Le tako nam bo kot družbi nova tehnologija v resnično korist. Po eni strani so tu različne negativne posledice za pravice posameznikov, ki se lahko zgodijo zaradi pristranosti, napak v podatkih, pa posegi v zasebnost in dostojanstvo. Vse več je govora tudi o davku za okolje. Enormna je poraba energije, elektrike, vode in možnosti hlajenja - npr. za pozive, ki jih vnašamo v storitve ponudnikov generativne UI, katerih edini namen je pravzaprav zabava oz. ustvarjanje *brain rota* kot pravijo najstniki danes.

Informacijski pooblaščenec je v te teme tesno vpet kot nadzorni organ za varstvo osebnih podatkov in organ za nadzor trga za sisteme umetne inteligence, pa tudi preko obravnave pritožb s področja informacij javnega značaja. Pričakujem, da bomo v prihodnje državljani radovedni glede tega, kako javne institucije uporabljajo umetno inteligenco in kaj to pomeni za naše okolje, ter da bomo na IP razkrivali dokumente s tega področja.

Na področju Akta o umetni inteligenci, kjer Informacijski pooblaščenec nadzora ne bo opravljal sam, temveč ga bo izvajalo pet nadzornih organov, je sodelovanje ključnega pomena za zagotavljanje usklajenega delovanja in pravne varnosti. V ta namen je v Sloveniji ustanovljen koordinacijski sosvet organov za nadzor trga. Intenzivno sodelovanje poteka tudi med različnimi področji delovanja IP, saj se zavedamo, da so vsa tri področja tesno prepletena in pogosto nepogrešljiva za razumevanje celotnega regulativnega okvira za UI.

Izredno veliko na IP izvajamo tudi posvetovanj – izdajamo različna mnenja in smernice, ki so upravljavcem v pomoč pri zagotavljanju skladnosti s pravili. Odzivamo se na predloge zakonodaje, s ciljem, da so pravila jasna in ne pomenijo nižanja ravni varstva posameznikov. Po Aktu o UI bodo v Sloveniji vzpostavljeni tudi regulativni peskovniki, v katerih bomo sodelovali različni nadzorni organi in bodo gotovo pripomogli pri grajenju pogojev za ekosistema zaupanja vredne umetne inteligence

V praksi se pogosto pojavlja dilema med inovacijami in skladnostjo. Kaj svetujete vodstvom podjetij, ki želijo uvajati rešitve umetne inteligence, a se bojijo regulatorne negotovosti? Kako naj že v fazi razvoja vgradijo načelo »zasebnost in etika po zasnovi«?

Danes je dihotomija konkurenčnosti in inovacij proti zasebnosti zelo poudarjena. Pogosto slišimo kritiko, da Evropa regulira, svet pa inovira. Trenutno se tako v EU ukvarjamo s predlogi zakonodajnih omnibusov in olajšav za ponudnike umetno inteligenčnih storitev. Upam, da bomo znali ujeti pravo ravnovesje, da bomo zmogli inovativno regulirati. Bistvo je namreč v tehtanju in sorazmernosti. Izredno je pomembno, da se z vprašanji varstva osebnih podatkov oziroma etične uporabe umetne inteligence soočimo že v začetni fazi nekega projekta. Instrument, ki je tu na voljo, je presoja vplivov na varstvo podatkov, ki jo zapoveduje GDPR (t. i. DPIA) in pa presoja vplivov na temeljne pravice, ki jo

zapoveduje Akt o UI (t. i. FRIA). Na naši spletni strani so na voljo podrobnejša navodila, kako presoje izvesti. Ključno je, da DPIA ni pripravljena samo zato, ker to zahteva zakonodaja in na podlagi vnaprej pripravljenih obrazcev, temveč jo organizacija pripravi na podlagi konkretnih podatkov za obdelavo podatkov, ki jo bodo izvajali in ob resnem premisleku o dejanskih tveganjih, ki lahko ob tem nastanejo. Prav tako je pomembno, da se presoje vplivov izvajajo tudi prek cikla obdelav podatkov, ob spremembah. Tako lahko zasnujemo sistem, ki ima vgrajeno varstvo temeljnih pravic.

Uvajanje umetne inteligence bo spremenilo tudi razmerje odgovornosti med ponudniki tehnologij in njihovimi uporabniki. Kdo bo po vašem mnenju nosil ključno odgovornost za zakonito in etično rabo, razvijalci, naročniki ali nadzorni organi ter kakšen model odgovornosti zagovarjate?

Večinoma odgovornosti določa zakonodaja. Glede na Akt o UI imajo različni akterji različne obveznosti: največ zahtev bodo morali izpolnjevati ponudniki sistemov UI, nekatere pa tudi uvajalci, pooblaščeni zastopniki, uvozniki in distributerji. Kadar je UI uporabljena za obdelavo osebnih podatkov, je treba upoštevati delitev vlog in odgovornosti po GDPR – tu poznamo odgovornosti upravljavca podatkov in odgovornosti pogodbenega obdelovalca podatkov. Za neko organizacijo, ki želi uporabljati umetno inteligenco, je tako izredno pomembno, da najprej razume svojo vlogo glede na zahteve zakonodaje. Ali razvija svojo rešitev, morda uporablja del rešitve drugega ponudnika, sama zbira podatke svojih uporabnikov, jih morda posreduje drugemu ponudniku UI rešitve, morda celo v tretji državi, itd. Šele po natančnem mapiranju procesov, uporabljenih tehnologij in zahtev zakonodaje, je mogoče natančneje določiti odgovornosti vseh subjektov v procesu uporabe umetne inteligence. In prav je, da so organizacije previdne in svojo vlogo natančno opredelijo že v začetku, sklepajo ustrezne pogodbene obveze ter ustrezno varujejo pravice svojih strank, zaposlenih. Nadzorni organi bodo v primeru kršitev prav tako natančno preučili odgovornosti različnih členov v verigi uporabe ali razvoja neke UI rešitve.

Če pogledamo naprej, v kakšno institucijo se mora razviti Informacijski pooblaščenec v naslednjih desetih letih? Bo poudarek bolj na klasičnem nadzoru, na strateškem svetovanju državi in gospodarstvu ali na aktivni vlogi varuha digitalnih pravic v dobi umetne inteligence?

Vsaka od teh aktivnosti ima svoj pomen in vlogo. Učinkovito izvajanje nadzora, sankcioniranje kršitev in obravnava pritožb so primarne zakonske pristojnosti Informacijskega pooblaščenca – in zagotavljajo ustrezno izvajanje pravil na vseh treh področjih našega delovanja. Posvetovalne aktivnosti nam nalaga že sama GDPR in na tem področju smo bili vedno zelo aktivni. Opažamo, da velika večina zavezancev želi delovati skladno s pravili, pa morda nima ustreznega znanja, poznavanja problematike in tu konkretne usmeritve zelo pripomorejo. Tudi v prihodnje ostaja to ena naših pomembnih prioritet, tako v smislu posvetovanj za organizacije iz zasebnega sektorja, kot tudi javnega. Ključen je tudi naš angažma v Evropskem odboru za varstvo podatkov. Pred kratkim smo se v Helsinški izjavi nadzorni organi v EU zavezali k temu, da z raznimi orodji in mehanizmi upravljavcem pomagamo na poti k lažjemu doseganju skladnosti s pravili varstva osebnih podatkov. Odbor ima tudi izredno pomembno vlogo pri usklajevanju razumevanja GDPR v različnih EU državah članicah.

> Danes je dihotomija konkurenčnosti in inovacij proti zasebnosti zelo poudarjena. Pogosto slišimo kritiko, da Evropa regulira, svet pa inovira. Trenutno se tako v EU ukvarjamo s predlogi zakonodajnih omnibusov in olajšav za ponudnike umetno inteligenčnih storitev. Upam, da bomo znali ujeti pravo ravnovesje, da bomo zmogli inovativno regulirati. Bistvo je namreč v tehtanju in sorazmernosti.

V smislu vloge varuha digitalnih pravic v dobi umetne inteligence, kot jo imenujete, pa bi omenila zlasti naše aktivnosti za mlade, za generacije, ki bodo živele z odločitvami, ki jih sprejemamo danes. Današnje igrišče je pogosto na spletu, žogi so se pridružile umetno inteligenčne igrače, a pravila bi morala ostajati ista – kako biti spoštljiv, odgovoren, kako varovati zaupnost. Trenutno izvajamo EU projekt Privacy PRO, v katerem smo za mlade pripravili namizno igro, stripe, poučne video posnetke z igralcem Juretom Henigmanom in gradiva za učne ure, ki jih lahko izvajajo učitelji. Zanje pripravljamo tudi več izobraževalnih seminarjev.

Ocenjujete, da bo Informacijski pooblaščenec pomemben del teh izzivov upravljal tudi z nadaljevanjem partnerstva skozi Slovensko združenje za korporativno varnost?

Slovensko združenje za korporativno varnost ima pomembno vlogo pri spodbujanju zavedanja o pomenu korporativne varnosti, kibernetske varnosti in odpornosti. Združuje predstavnike različnih organizacij in organov ter s tem nedvomno prispeva k boljšemu poznavanju zahtev različne zakonodaje s tega področja. Kibernetska varnost in ustrezno upravljanje incidentov sta podstat varnega ter odpornega digitalnega poslovanja. Organizacije nimajo lahke vloge, poslovati morajo skladno z GDPR, s pravili na področju UI in spoštovati tudi obveznosti iz direktive NIS. Da to ni le formalizem, temveč se dejansko zmanjšajo tveganja za kibernetsko varnost, je bistveno, da organizacije zelo dobro poznajo svoje sisteme, tokove podatkov in namene, zaradi katerih določene podatkovne tokove izvajajo. Le tako lahko ustrezno predvidijo tveganja, katerim so podatki, sistemi in procesi izpostavljeni ter predvidijo ustrezne zaščite. Slovensko združenje za korporativno varnost tu ponuja prostor za izmenjavo dobrih praks in veselim se našega sodelovanja v prihodnje. ■

Foto: arhiv IP RS



Vsak IT izziv ima rešitev.
Tudi vaš.

ACTUAL I.T.
A DBA Group Company

ACTUAL PRO
A DBA Group Company



www.actual-it.si

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

INTERVJU
mag. Martin Koželj, generalni sekretar NZS*
mag. Marko Brelih, vodja varnosti in področja integritete

STRATEŠKI IN IZVEDBENI OKVIR ORGANIZACIJE UEFA FUTSAL EURO 2026

UEFA Futsal EURO 2026 je v Ljubljani predstavljal zahteven mednarodni projekt, ki je združeval strateško načrtovanje, organizacijsko usklajenost in visoke varnostne standarde. V pogovoru s predstavnikoma NZS osvetljujemo ključne organizacijske, varnostne in dolgoročne vidike izvedbe prvenstva ter njegove učinke na slovenski športni prostor.

Kako bi z današnje perspektive ocenili organizacijo prvenstva UEFA Futsal Euro 2026 v Ljubljani, ali so bila dosežena pričakovanja in cilji? (mag. Martin Koželj)

Z današnje perspektive lahko organizacijo prvenstva UEFA Futsal Euro 2026 ocenimo kot zelo uspešno. Slovenija je v relativno kratkem času, od junija 2025, prevzela vlogo sogostiteljice ter organizacijsko strukturo hitro uskladila z zahtevami UEFA in s tem »dohitela« Litvo ter Latvijo, ki sta s pripravami začeli že dve leti prej.

Za tako uspešno izvedbo gre posebna zahvala organizacijski ekipi NZS, ki je ob podpori vseh ključnih deležnikov svoje delo opravila strokovno, odgovorno in z veliko predanostjo. V veliko pomoč sta nam bila tako standardiziran organizacijski model UEFA kot tudi bogate izkušnje z izvedbo preteklih velikih tekmovanj, med drugim UEFA Futsal Euro 2018.

Ključno je, da smo uspeli zagotoviti ustrezno infrastrukturo, učinkovito logistiko, zadostno kadrovsko podporo in usklajeno sodelovanje vseh partnerjev. Naš cilj ni bil zgolj doseganje visokih številk obiska, temveč predvsem vrhunska organizacija in celostna, pozitivna izkušnja za reprezentance, gledalce ter mednarodno javnost – in prav v tem pogledu ocenjujemo, da smo zastavljena pričakovanja v celoti izpolnili.

Kateri organizacijski izzivi so se med izvedbo izkazali za največje in kako ste jih uspeli obvladati? (mag. Martin Koželj)

Največji organizacijski izziv je bila uporaba dveh tekmovalnih prizorišč – Arena Stožice in Hala Tivoli – predvsem zaradi zahteve, da se zadnje tekme skupinskega dela odigrajo istočasno. Obe dvorani sta po svojih značilnostih precej različni, zato je bilo treba zagotoviti primerljive pogoje za vse reprezentance, medije in gledalce.

Ob tem je organizacija zahtevala usklajevanje velikega števila ljudi – od približno 50 članov organizacijske ekipe na lokaciji, podizvajalcev, do več kot 200 oseb na dan tekme, ki so skrbeli za varnost, logistiko, gostinske storitve in podporne procese. Pomembno vlogo je imelo tudi preko 100 prostovoljcev,

Ob tej priložnosti velja poudariti tudi zaupanje UEFA in osebno podporo predsednika Aleksandra Čeferina, ki je Sloveniji omogočil soorganizacijo tako pomembnega prvenstva. To zaupanje razumemo kot priznanje naši dosedanji organizacijski kakovosti in kot obvezo, da tudi v prihodnje upravičimo pričakovanja.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



med njimi številni študenti in posamezniki iz tujine. Ključ do uspeha je bil v pravočasnem načrtovanju, izkušnjah in dobrem sodelovanju z UEFA, ki s svojo jasnimi organizacijskimi zahtevami ter postopki bistveno olajša izvedbo.

Kako ocenjujete sodelovanje med NZS, UEFA, državnimi institucijami in Mestno občino Ljubljana v času priprav in same izvedbe? (mag. Martin Koželj)

Sodelovanje je bilo na zelo visoki ravni. UEFA nas je med pripravami večkrat obiskala, skupaj smo pregledali in uskladili vse ključne organizacijske segmente. Prav tako je bilo odlično sodelovanje z državnimi institucijami in Mestno občino Ljubljana, ki je zagotovila podporo pri infrastrukturi ter logistiki. Ob tej priložnosti velja poudariti tudi zaupanje UEFA in osebno podporo predsednika Aleksandra Čeferina, ki je Sloveniji omogočil soorganizacijo tako pomembnega prvenstva. To zaupanje razumemo kot priznanje naši dosedanji organizacijski kakovosti in kot obvezo, da tudi v prihodnje upravičimo pričakovanja.

Prilagodljivost sistema, jasna hierarhija odločanja in stalna operativna koordinacija med deležniki so omogočali optimalno uporabo kadrovskih virov ter visoko raven pripravljenosti skozi celotno prvenstvo. Prav kombinacija pravočasnega načrtovanja in sprotnega prilagajanja razmeram na terenu je bila ključni dejavnik, da je prvenstvo potekalo varno, nemoteno ter v športnem duhu.

Kakšni so po vašem mnenju dolgoročni učinki prvenstva za slovenski futsal in širši športni prostor? (mag. Martin Koželj)

Prepričani smo, da bo prvenstvo imelo pomembne dolgoročne učinke. Že organizacija UEFA Futsal Euro 2018 je futsalu v Sloveniji močno povečala prepoznavnost, tokratno prvenstvo pa predstavlja novo priložnost za nadgradnjo tega razvoja. Verjamemo, da so se ustvarili pogoji za še večje zanimanje mladih za futsal in boljši obisk tekem domačih tekmovanj ter okrepljeno prepoznavnost klubov. Pomemben del zapuščine vidimo tudi v izboljšanju organizacijskih standardov, infrastrukture in podpore lokalnega okolja ter sponzorjev. Hkrati takšni dogodki utrjujejo ugled Nogometne zveze Slovenije kot zanesljive in strokovne organizacije, kar nam odpira vrata tudi za prihodnje mednarodne projekte.

Bi na podlagi izkušenj z organizacijo tega prvenstva danes kaj naredili drugače? (mag. Martin Koželj)

Vsako veliko tekmovanje prinese nova spoznanja in priložnosti za izboljšave. Čeprav ocenjujemo, da je bila izvedba zelo uspešna, bi morda še več pozornosti namenili dodatni pro-

mociji futsala izven klasičnih športnih krogov in še zgodnejši aktivaciji širše skupnosti in gospodarstva.

Sicer pa so nam prav izkušnje z organizacijo preteklih prvenstev – UEFA evropskega prvenstva do 17 let 2012 ter UEFA evropskega prvenstva do 21 let 2021 – dale trdne temelje za učinkovito delo. Ključna dodana vrednost tega prvenstva je prav nadgradnja teh izkušenj in utrditev organizacijskih kompetenc, ki jih bomo lahko še uspešneje uporabili pri prihodnjih projektih.

Kako ocenjujete varnostno situacijo med prvenstvom, ali je dogodek potekal skladno z načrtovanimi varnostnimi scenariji? (mag. Marko Brelih)

Varnostna situacija med prvenstvom je bila stabilna, nadzorovana in v celoti skladna z načrtom varovanja ter pripravljenimi operativnimi scenariji. Varnostni koncept je temeljil na celostni oceni tveganja, izdelani v skladu z nacionalno zakonodajo, usmeritvami UEFA in dobrimi praksami varovanja množičnih prireditev.

Pri načrtovanju so bili upoštevani mednarodni značaj dogodka in prisotnost tujih reprezentanc ter njihovih podpornikov (navijačev), aktualne politične in varnostne razmere v Sloveniji ter Evropi (vključno z udeležbo reprezentance Belorusije), tekme z različno stopnjo tveganja, hkratna izvedba tekem na dveh prizoriščih (Arena Stožice in Hala Tivoli) in povečana medijska ter VIP prisotnost v zaključni fazi prvenstva.

V času prvenstva ni prišlo do hujših varnostnih incidentov. Posamezni prekrški so bili obravnavani hitro, strokovno in sorazmerno, skladno z načeli zakonitosti ter pooblastili varnostnega osebja in ob sodelovanju Policije. Izvajanje ukrepov (prometna ureditev, nadzor zunanjega območja dvorane, območij znotraj dvorane, nadzor vstopov, akreditacijski sistem, varovanje ekip, uradnih oseb in VIP oseb) je ob stalni prisotnosti vseh deležnikov potekalo usklajeno, dosledno in učinkovito, kar potrjuje uspešnost zastavljenega varnostnega koncepta.

Pomemben del uspešnosti je predstavljala tudi premišljena kadrovska struktura. V okviru prvenstva je bilo skupno akreditiranih 410 oseb na področju varovanja (rediteljev in varnostnikov), pri čemer operativno razporejanje ni bilo statično, temveč je temeljilo na dnevnih ocenah tveganja, številu prodanih in dejansko skeniranih vstopnic, strukturi obiskovalcev ter fazi tekmovanja. Na tekmovalne dneve je bilo skupaj razporejenih 1.536 rediteljev in varnostnikov, ki so opravili 15.026 delovnih ur, kar pomeni povprečno 192 varnostnega osebja oziroma približno 1.878 delovnih ur na posamezni tekmovalni dan. Kadrovska dinamika je sledila stopnji tveganja posamezne tekme in pričakovanemu obisku, z dodatnimi poudarki pri tekmah z višjo oceno tveganja ter v zaključni fazi tekmovanja. Prilagodljivost sistema, jasna hierarhija odločanja in stalna operativna koordinacija med deležniki so omogočali optimalno uporabo kadrovskih virov ter visoko raven pripravljenosti skozi celotno prvenstvo. Prav kombinacija pravočasnega načrtovanja in sprotnega prilagajanja razmeram na terenu je bila ključni dejavnik, da je prvenstvo potekalo varno, nemoteno ter v športnem duhu.

Ali ste se med dogodkom soočili z nepredvidenimi varnostnimi izzivi in kako ste jih reševali? (mag. Marko Brelih)

Večjih nepredvidenih varnostnih izzivov ni bilo. Operativni sistem je bil zasnovan dovolj robustno in hkrati prilagodljivo, da je omogočal sprotno odzivanje na manjše spremembe. Med izzivi so bile predvsem:
- dve tekmi na posamezni tekmovalni dan,
- prilagoditve razporeditve varnostnega osebja glede na dejanski obisk ,
- dinamični prihodi gledalcev tik pred pričetkom tekem,
- usklajevanje prometnih tokov ob večjem številu tujih obiskovalcev (predvsem v času obeh tekem Hrvaške reprezentance).

Reševanje je temeljilo na dnevnih operativnih ocenah tveganja, rednih koordinacijskih sestankih med deležniki, jasni hierarhiji odločanja, stalni prisotnosti predstavnikov vseh deležnikov (Policije, organizatorja, varnostne službe, požarne varnosti, zdravstvene varnosti).

Kako ocenjujete sodelovanje med organizatorjem, Policijo in zasebnimi varnostnimi službami v praksi? (mag. Marko Brelih)

Sodelovanje med organizatorjem (NZS v imenu UEFA), Policijo (še posebej Policijsko upravo Ljubljana) in nosilcem varovanja, varnostnim subjektom Valina varovanje d.o.o. skupaj s podizvajalci, je bilo v pripravljalni ter izvedbeni fazi zelo dobro, zgledno, strokovno in učinkovito.

Vzpostavljeni so bili jasni komunikacijski kanali, redni koordinacijski sestanki in usklajeni operativni postopki, kar je dan danes nujen pogoj, da lahko vsi deležniki delujejo enotno, pravočasno izmenjujejo informacije ter usklajeno in strokovno odzivajo na morebitne varnostne situacije. Tak model



Prvenstvo je potrdilo sposobnost slovenskih institucij in organizatorja za izvedbo zahtevnega mednarodnega športnega dogodka v skladu z nacionalnimi in mednarodnimi standardi. Pridobljene izkušnje predstavljajo pomembno strokovno izhodišče za nadaljnji razvoj standardov varovanja množičnih športnih prireditev v Sloveniji in za nadaljnjo profesionalizacijo področja varnosti in varovanja.

sodelovanja je omogočal sprotno prilagajanje ukrepov glede na oceno tveganja in dejanske razmere na prizoriščih in je pomembno prispeval k varnemu ter nemotenemu poteku prvenstva.

Katere varnostne prakse ali tehnološke rešitve so se izkazale za posebej učinkovite? (mag. Marko Brelih)

Učinkovitih praks in rešitev je bilo več, izpostavljamo naslednje ključne elemente:
- celostna in pravočasna izdelava ocene tveganja, ki je predstavljala temelj za načrtovanje vseh nadaljnjih varnostnih ukrepov,
- prilagodljivo razporejanje varnostnega osebja glede na dnevno oceno tveganja, fazo tekmovanja in število obiskovalcev,
- dosleden nadzor vstopov in učinkovito izvajanje akreditacijskega sistema, s čimer je bil zagotovljen nadzor nad dostopom do posameznih območij,
- ločevanje navijaških skupin na tekmah z višjo stopnjo tveganja (npr. Madžarska, Hrvaška), ob tesnem sodelovanju s Policijo,
- jasno označene evakuacijske poti in pripravljeni intervencijskiter evakuacijski načrti, ki so zagotavljali pripravljenost na morebitne izredne dogodke,
- vzpostavljen je bil sistem kriznega komuniciranja, v kolikor bi v primeru potrebe omogočal hitro, usklajeno in transparentno obveščanje vseh deležnikov,
- ustrezno usposabljanje varnostnega osebja, ki je upravičilo svoj namen. Varnostno osebje je bilo deležno dveh oblik usposabljanja, praktičnega na samem prizorišču (Arena Stožice) in dodatnega e-usposabljanja, skladnega s smernicami UEFA.

Med tehnološkimi rešitvami bi izpostavili sistem, ki ga je zagotavljal nosilec varovanja (Valina varovanje d.o.o.). Gre za visokotehnološki sistem videonadzora, ki vključuje uporabo t.i. *body-cam* kamer pri varnostnikih in stacionarne videonadzorne sisteme. S strateško postavitvijo je sistem omogočal nadzor dogajanja v neposredni okolici dvorane (zunanji perimeter) kot tudi znotraj objekta.

Poleg neposrednega nadzora je sistem omogočal stalni širši vpogled v dogajanje na območju prireditve, vključno s spremljanjem tokov gibanja obiskovalcev, njihovega prihoda, zadrževanja in dinamike obremenitve posameznih con oziroma območij. Takšna preglednost je omogočala pravočasno zaznavanje morebitnih odstopanj, identifikacijo kršiteljev, spremljanje njihovega gibanja ter taktično pripravo na ukrepanje (zadržanje osebe/kršitelja in predaja Policiji v nadaljnji postopek). Takšna tehnološka podpora je pomembno prispevala k preventivnemu delovanju, boljšemu situacijskemu zavedanju in hitremu, usklajenemu ter strokovnemu odzivanju ob posameznih incidentih.

Katere ključne lekcije s področja varnosti bi izpostavili kot pomembne za prihodnje velike športne dogodke v Sloveniji? (mag. Marko Brelih)

Kot ključne lekcije za prihodnje velike športne dogodek v Sloveniji izpostavljamo predvsem:
- pomen zgodnje in temeljite priprave, z jasno opredeljenimi odgovornostmi vseh deležnikov,
- celotna ocena tveganja, ki v primeru mednarodnih dogodkov upošteva tudi mednarodni značaj dogodka, strukturo obiskovalcev in aktualne varnostne razmere,
- močno medinstitucionalno sodelovanje, ki temelji na zaupanju, redni komunikaciji in operativni usklajenosti,
- prilagodljivost varnostnega sistema, predvsem pri razporejanju varnostnega osebja in obvladovanju prometne dinamike (promet – vpadnice na območje športnega dogodka ter parkirišča),
- stalno usposabljanje varnostnega osebja in prenos dobrih praks iz mednarodnih športnih okolij,
- poudarek na preventivi, saj je pravočasno načrtovanje in vidna prisotnost varnostnih struktur pomembno prispevala k odvračanju morebitnih incidentov.

Izkušnje s prvenstva FEURO 2026 potrjujejo, da je bil varnostni koncept strokovno utemeljen, sistemsko ustrezno zasnovan in v praksi učinkovito izveden. Na podlagi vseh izvedenih aktivnosti, operativnih ukrepov in dejanskega poteka prvenstva ocenjujemo, da so bili vsi temeljni cilji s področja varnosti in varovanja v celoti doseženi. Ob doslednem spoštovanju slovenske zakonodaje in varnostnih standardov UEFA je bila zagotovljena visoka stopnja varnosti za vse udeležence. Prvenstvo je potekalo varno, nemoteno in v športnem duhu, brez hujših varnostnih incidentov, kar potrjuje ustreznost sprejetih preventivnih ter operativnih ukrepov.

Uspešnost varnostnega koncepta je temeljila na pravočasni in temeljiti pripravi, izdelavi celostne ocene tveganja, jasni razdelitvi odgovornosti ter učinkovitemu sodelovanju med deležniki na področju varnosti in varovanja. Redna komunikacija in operativna usklajenost vseh deležnikov sta omogočali hitro prilagajanje ukrepov glede na fazo tekmovanja, strukturo obiskovalcev ter povečano medijsko in VIP prisotnost.

Pomembno vlogo sta imeli tudi prilagodljivost sistema razporejanja varnostnega osebja in učinkovita uporaba tehnoloških rešitev, zlasti videonadzornih sistemov, ki so omogočali večjo preglednost nad dogajanjem ter pravočasen odziv. Prvenstvo je potrdilo sposobnost slovenskih institucij in organizatorja za izvedbo zahtevnega mednarodnega športnega dogodka v skladu z nacionalnimi in mednarodnimi standardi. Pridobljene izkušnje predstavljajo pomembno strokovno izhodišče za nadaljnji razvoj standardov varovanja množičnih športnih prireditev v Sloveniji in za nadaljnjo profesionalizacijo področja varnosti in varovanja. ■

Foto: arhiv NZS

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: Ita Majnik/Petrol d.d., Ljubljana*



UPRAVLJANJE TVEGANJ KOT TEMELJ SODOBNEGA POSLOVANJA

Upravljanje tveganj ni zaviranje napredka, temveč predvidljiva in varna odskočna deska za tiste, ki v negotovosti prepoznajo prostor za napredek. Gre za sistematičen pristop, ki omogoča sprejemanje premišljenih odločitev tudi v razmerah povečane kompleksnosti in dinamičnih sprememb. Organizacijam pomaga prepoznati ranljivosti, okrepiti odpornost in hkrati ohraniti razvojno usmerjenost. Prav v sposobnosti obvladovanja tveganj se pogosto skriva ključna konkurenčna prednost tistih, ki znajo negotovost preoblikovati v priložnost.

Tveganja skozi čas

Tveganja nas spremljajo skozi celotno človeško delovanje, saj človek nagonsko stremi k prepoznavanju, ocenjevanju in obvladovanju tveganj z namenom preživetja ter nadaljnjega razvoja. V poslovanju so se tveganja pojavila ob prvih oblikah trgovanja, pomorstva in zgodnjih gospodarskih sistemih. Že v antičnih civilizacijah so trgovci razvijali mehanizme delitve izgub, kar je kasneje preraslo v prve oblike zavarovalništva. Sčasoma so se tveganja razširila na finančne trge, industrijo, javne sisteme in digitalno okolje, ki je zahtevalo vedno bolj strukturirane pristope.

Danes je upravljanje tveganj postala organizacijska disciplina, s katero organizacija s sistematičnim, celovitim in metodološko enotnim pristopom tveganja identificira, ocenjuje njihov vpliv in verjetnost (v skupni oceni tveganja izraženi v EUR in ne opisno), odloča o ukrepih za obvladovanje tveganj ter spremlja izvajanje ukrepov in spremembe v samih tveganjih skozi ocenjevalno obdobje.

Zakaj tveganja obstajajo in zakaj jih moramo upravljati?

Tveganja izhajajo iz negotovosti, kompleksnosti in dinamike poslovnega okolja. Vsaka organizacija deluje v kontekstu številnih notranjih in zunanjih dejavnikov, ki lahko vplivajo na doseganje ciljev, zato so tveganja v osnovi opredeljena kot odstopanja od pričakovanega izida, ki so lahko pozitivna ali negativna. V sodobnem okolju tveganja niso več zgolj grožnje, temveč tudi priložnosti.

Upravljamo jih iz več razlogov in večplastno, in sicer iz vzgiba po doseganju finančne stabilnosti, operativne učinkovitosti, zakonske skladnosti, ugleda ter zaupanja in strateške odpornosti.

Zaradi vse obsežnejše regulative in dinamičnih sprememb okolja, obveznost profesionalizacije ter sistematičnega pristopa pri upravljanju tveganj v zadnjih letih vedno bolj ureja zakonodaja, predvsem na področjih financ, bančništva, zavarovalništva, varovanja osebnih podatkov, varnosti in zdravja pri delu, javnih financah, okolijski ter energetski zakonodaji in preprečevanju pranja denarja. Podjetja, ki znajo tveganja pravočasno prepoznati in jih učinkovito upravljati, lahko hitreje inovirajo, sprejemajo boljše odločitve ter se učinkoviteje prilagajajo spremembam, kar je danes v

Podjetja, ki znajo tveganja pravočasno prepoznati in jih učinkovito upravljati, lahko hitreje inovirajo, sprejemajo boljše odločitve ter se učinkoviteje prilagajajo spremembam, kar je danes v tako turbulentnem gospodarskem okolju ključnega pomena.

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

tako turbulentnem gospodarskem okolju ključnega pomena.

Finančno ovrednotenje tveganj

V sodobnem poslovnem svetu, ki temelji na številkah, je finančno ovrednotenje tveganj ključnega pomena. Brez finančne dimenzije tveganj med seboj ni mogoče primerjati, pokritizirati ali navsezadnje utemeljevati nujnosti ukrepov.

Finančno ovrednotenje omogoča:
- izračun potencialnih izgub,
- oceno stroškov ukrepov,
- izračun ROI ukrepov za zmanjševanje tveganj,
- utemeljitev investicij, ki tveganja zmanjšujejo.

Tveganja, ki niso finančno ovrednotena, v sistemu izgubijo težo in so med seboj neprimerljiva, zato je finančna dimenzija nujna za učinkovito odločanje.

Sistem upravljanja tveganj

Učinkovit sistem upravljanja tveganj je integriran, sistematičen in na človeka usmerjen mehanizem kot glavni pripomoček pri vsakodnevnem ter strateškem odločanju. Z jasno opredeljenimi odgovornostmi, ustrezno tehnologijo in kulturo zavedanja tveganj organizaciji omogoča varno, predvidljivo ter strateško usmerjeno delovanje. Vsak učinkovit sistem upravljanja tveganj mora biti skrbno načrtovan, tako z vidika internih in eksternih predpisov kot tudi samih potreb ter načina delovanja organizacije. Seveda obstajajo ključni gradniki sistema, vendar ne smemo mimo dejstva, da mora biti zaradi izredno spremenljivega okolja sistem fleksibilen oziroma pripravljen na spremembe. Celovit sistem upravljanj tveganj vključuje naslednje osnovne procese:
- identifikacijo tveganj,
- ocenjevanje in vrednotenje,
- obvladovanje,
- spremljanje,
- poročanje.

Da bo organizacija ključne procese upravljanja tveganj sploh lahko izvajala, mora pred vzpostavitvijo sistema sprejeti tako politiko kot strategijo upravljanja tveganj, s katerima jasno postavi pristojnosti in odgovornosti, določi vrste tveganj, ki jih bodo upravljali, enotno metodologijo vrednotenja tveganj, vsebino registra tveganj ter registra ukrepov in način poročanja.

Učinkovit sistem upravljanja tveganj je integriran, sistematičen in na človeka usmerjen mehanizem kot glavni pripomoček pri vsakodnevnem ter strateškem odločanju. Z jasno opredeljenimi odgovornostmi, ustrezno tehnologijo in kulturo zavedanja tveganj organizaciji omogoča varno, predvidljivo ter strateško usmerjeno delovanje.

Pasti v procesu vzpostavitve sistema upravljanja tveganj

Kot pri vseh drugih sistemih, ki jih uvajamo v poslovna okolja, ima tudi uvedba sistema upravljanja tveganj svoje skrite pasti.

Strah zaposlenih
Tista prva največja past izhaja iz zaposlenih samih, saj pojem tveganja pogosto nosi negativen prizvok, zaradi česar se zaposleni bojijo, da bo identifikacija tveganj razumljena kot priznanje napak, ali da bodo zaradi identifikacije tveganj kaznovani, spet drugi se bojijo, da bo sistem uporabljen za nadzor, ne za izboljšave, in da bodo zaradi identifikacije tveganj izpostavljeni ter posledično negativno ocenjeni.

Kako lahko zaposlenim enostavno razložimo, da je skrb odveč? Z jasnim sporočilom, da so vsi zaposleni odgovorni za pravočasno naslavljanje tveganj svojim nadrejenim, in da so vse do trenutka, ko tveganj ne naslovijo, sami odgovorni za njihovo upravljanje.

Zaposlenim s tem sporočimo, da je identifikacija in poročanje o tveganjih profesionalna odgovornost, medtem ko je odločanje o njih naloga poslovodstva. Poslovodstvo je prav tako odgovorno za postavitev mej sprejemljivosti posameznih tveganj in določitev načina obvladovanja tveganj.

Nujno administrativno zlo
Naslednja velika past izhaja iz same poplave zakonodajnih obveznosti in razumevanja tveganj v slovenskem prostoru. V Sloveniji upravljanje tveganj pogosto še vedno razumemo kot administrativno obveznost ali formalnost, zato v številnih podjetjih sistem obstaja samo na papirju, v praksi pa ne. Če zaposleni verjamejo, da je sistem uveden zaradi formalnosti ali zunanjega pritiska, ga ne bodo sprejeli. Spremeniti mišljenje zaposlenih je seveda zelo težko, vendar mogoče.





Da bo organizacija ključne procese upravljanja tveganj sploh lahko izvajala, mora pred vzpostavitvijo sistema sprejeti tako politiko kot strategijo upravljanja tveganj, s katerima jasno postavi pristojnosti in odgovornosti, določi vrste tveganj, ki jih bodo upravljali, enotno metodologijo vrednotenja tveganj, vsebino registra tveganj ter registra ukrepov in način poročanja.

*Na dolgi rok lahko tovrstne pasti odpravljamo **s krepitvijo kulture zavedanja o tveganjih** in izjemno visoko stopnjo angažiranosti pri samem upravljanju sistema z vidika nudenja strokovne pomoči, dodatnih razlag ter konec koncev administrativne pomoči.*

*Hitrejša pot do spremembe mišljenja je takojšnja **vzpostavitev povezave med obvladovanjem tveganj in investicijami**. Tveganja so ključni element pri odločanju o investicijah – brez jasne ocene tveganj ni mogoče utemeljiti niti zavrniti investicije.*

Ko investicijske odločitve, ki zmanjšujejo verjetnost dragih incidentov, povečujejo stabilnost poslovanja, izboljšujejo skladnost ali pa krepijo odpornost podjetja, začnemo povezovati s sistemom upravljanja tveganj, zaposleni začutijo priložnost, da svoje ideje lahko upravičijo skozi dejansko vrednotenje tveganj, s čimer neposredno vplivajo na investicijsko odločitev, razporejanje virov, določanje prioritet in dolgoročno strategijo. Zaposlenim tako damo vrednost in tisto potrditev, da so del sistema, ter da lahko sodelujejo pri poslovanju.

Pomanjkanje podpore vodstva

Brez podpore vodstva je postavitev učinkovitega sistema upravljanja tveganj nemogoča, saj je namen sistema, da postane glavno orodje za odločanje poslovodstva tako pri vsakodnevnih kot pri strateških odločitvah. Pred začetkom projekta moramo vodstvo ustrezno nagovoriti, predstaviti prednosti sistema in si s tem zagotoviti ustrezno podporo.

Napačna umestitev funkcije upravljalca sistema upravljanja tveganj v organizacijsko strukturo

Če se zopet navežemo na dojemanje upravljanja tveganj v Sloveniji, kjer upravljanje tveganj velikokrat še vedno razumemo kot nujno administrativno zlo, je v evropskem prostoru dojemanje upravljanja nekoliko boljše, vendar še vedno ne dobro. V Evropi je področje bolj regulatorno usmerjeno, predvsem na finančnem in energetskem sektorju. Vendar tudi tu upravljanje tveganj pogosto ni strateško orodje, temveč del skladnosti.

Povesem drugače je v ZDA, kjer je upravljanje tveganj prepoznano kot strateška funkcija in skrbnik sistema deluje kot ‚desna roka“ poslovodstva.

V največjih svetovnih podjetjih je tako upravljanje tveganj vključeno v:
- investicijske odločitve,
- strateško načrtovanje,
- digitalno transformacijo,
- krizno upravljanje.

Razlika je predvsem v kulturi: v ZDA tveganja niso tabu, temveč temelj odločanja.

Kaj lahko naredimo? Pot je dolga, vendar mogoča. S strokovnim delom, sodelovanjem v projektih in doslednim prikazovanjem dodane vrednosti lahko krepimo razumevanje pomena upravljanja tveganj ter izboljšamo umestitev funkcije v organizacijsko strukturo.

Z ustrezno umestitvijo funkcije upravljalca sistema, upravljalcu povečamo možnost vpliva na pravočasno pridobivanje informacij in odzivnost deležnikov.

Nekompetenten skrbnik sistema upravljanja tveganj

Skrbnik sistema ni le administrator in koordinator, temveč je ključni strateški partner v vodstvu, ki z analitičnim razumevanjem organizacije, presojanjem vplivov ter pravočasnim opozarjanjem na kritična odstopanja soustvarja varno, stabilno in dolgoročno vzdržno poslovanje. Če skrbnik nima ustreznih kompetenc, bomo imeli v procesih znotraj sistema upravljanja tveganj velike težave, ki se bodo na začetku pokazale predvsem kot neustrezna komunikacija.

***Pomembno je, da ima oseba, ki je odgovorna za vzpostavitev sistema in bo kasneje tudi skrbnik sistema, ustrezne kompetence**, in sicer:*

- analitične in tehnične kompetence, predvsem zmožnosti napredne podatkovne analize, razumevanja metod upravljanja tveganj, sposobnosti strukturiranja velike količine informacij ter razumevanja notranjih kontrol,
- komunikacijske kompetence, predvsem pridobivanja podatkov od zaposlenih, prezentacijske spretnosti in diplomatičnosti ter profesionalnosti,
- medosebne in vedenjske kompetence, predvsem visoke stopnje integritete ter zaupnosti, odpornost na pritiske, nevtralnosti in objektivnosti ter sposobnosti gradnje zaupanja,
- organizacijske in strateške kompetence, predvsem razvito strateško razmišljanje ter zmožnost naprednega načrtovanja in organizacije dela ter proaktivnost,
- etične kompetence, predvsem iz naslova spoštovanja etičnih smernic in pravilnega ravnanja z informacijami.

Težave pri implementaciji

Še ena od večjih pasti so težave pri implementaciji sistema. To so težave, ki nastanejo predvsem v fazi identifikacije in vrednotenja tveganj, bodisi zaradi napačno postavljene metodologije vrednotenja, prekompleksnih obrazcev za popis ter vrednotenje, neustrezno izvedenega izobraževanja zaposlenih ali navsezadnje zaradi neustrezne komunikacije z zaposlenimi.

Vsemu se lahko izognemo, s predhodno testno prepoznavo tveganj z raznoliko skupino zaposlenih in ponovnim izobraževanjem, če ugotovimo, da je razumevanje zaposlenih napačno.

Pogosta težava se pojavi pri razvrščanju tveganj. Tveganja v osnovi delimo na finančna in operativna tveganja, kar zaposleni pogosto razumejo na način, da so finančna tveganja tista, ki jih finančno ovrednotimo, vsa ostala pa so operativna. To seveda ne drži, saj določitev ali je tveganje finančno ali operativno, izhaja iz analize vsebinskega izvora, torej izhaja iz finančnih tokov, vrednosti ali obveznosti ali pa iz procesov, ljudi, sistemov in vsakdanjega delovnega okolja.

Napačni razlagi se lahko izognemo *s predhodnim izobraževanjem zaposlenih, v katerem na eni strani jasno predstavimo razvrščanje tveganj na drugi pa pomembnost ocenjevanja in vrednotenja za vsa tveganja, tako finančna kot tudi operativna.*

Sistem upravljanja tveganj je vzpostavljen. Kaj pa sedaj?

Vzpostavitev sistema upravljanja tveganj je zahtevna naloga, ki pa se s samo vzpostavitvijo ne konča, temveč šele začne. Zakaj?

Ko uspemo sistem vzpostaviti, moramo upravičiti njegovo dodano vrednost, zaradi katere nas je navsezadnje poslovodstvo pri projektu tudi podprlo. Če smo uspeli prebroditi vse ‹›porodne težave›› vzpostavitve in imamo sprejete ustrezne notranje predpise, potrjena registra tveganj in ukrepov, določeno mejo sprejemljivosti tveganj ter način poročanja je zdaj pred nami tista največja naloga - sprememba in krepitev korporativne kulture zavedanja ter obvladovanja tveganj, katere glavni nalogi sta:

- da naj je upravljanje tveganj dolgoročno, kontinuirano in uspešno za celotno organizacijo,
- upravljavcem tveganj postopoma prikazati dodano vrednost sistema, odločevalcem na najvišji ravni pa omogočiti, da bo sistem upravljanja tveganj nepogrešljivo orodje in pomoč tako pri strateških kot tudi pri vsakodnevnih poslovnih odločitvah, vse z namenom, da bomo pridobili ustrezne informacije, na podlagi katerih bomo tveganja lahko učinkovito upravljali. Pravil, kako bomo to storili ni, saj so si organizacije med seboj različne, imajo različne profile zaposlenih in živijo svoje kulture. Vsekakor pa sprememba kulture zavedanja in upravljanja tveganj ne sme biti revolucija, temveč evolucija. Zavedati se moramo, da je pred nami dolga pot, z veliko prilagajanja, dodatnih razlag, neplaniranih izobraževanj, spodbujanja k strpnosti in neplaniranih ur dela, ki ga namenimo podpori zaposlenim v času, ko je njim najbolj primeren.

Digitalizacija sistema upravljanja tveganj je nujna

Ko je sistem enkrat vzpostavljen, je digitalizacija sistema ključ do njegove učinkovitosti, saj digitalna orodja omogočajo hitrejše in natančnejše zbiranje podatkov ter bistveno večjo preglednost nad samimi tveganji. Poročila in analize nastajajo avtomatsko, zaradi česar se zmanjšajo administrativne obremenitve. Organizacija tako preide v bolj proaktiven in zrel pristop k upravljanju tveganj, najpomembnejše pa je, da so informacije o tveganjih odločevalcem na razpolago ob vsakem trenutku.

Zaključek

Učinkovito vpeljan sistem upravljanja tveganj je glavno orodje pri vseh odločitvah – tako poslovodstva kot ostalih vodilnih zaposlenih. Ko upravljanje tveganj ni več zgolj formalen proces in postane del organizacijske kulture, lahko rečemo, da postane organizacijska vrednota, s katero organizacija daje poudarek odgovornemu ravnanju, premišljenemu odločanju ter kulturi zavedanja tveganj. Podjetja, ki učinkovito obvladujejo tveganja, obvladujejo svojo prihodnost. ■

ZARJA ELEKTRONIKA

Z NAMI VARNI IN POLNI ZAUPANJA ŽE VEČ KOT 64 LET.

Zarja Elektronika je vodilni ponudnik tehničnega varovanja v Sloveniji in širši balkanski regiji. Pri najzahtevnejših projektih zagotavljamo celovito podporo od prve ideje in implementacije varnostnih rešitev do dolgoročnega vzdrževanja industrijskih, poslovnih ter zasebnih objektov. Poleg lastnih inovacij po najvišjih standardih zastopamo vrhunske svetovne proizvajalce sistemov za javljanje požara, protivlomno varovanje, video nadzor, detekcijo iskre in kontrolo pristopa.



VRHUNSKA KAKOVOST IN INOVACIJE

Lasten razvoj in proizvodnja zagotavljata popoln nadzor nad kakovostjo ter visoko prilagodljivost pri razvoju tehnološko najnaprednejših sistemov.

ENOSTAVNO UPRAVLJANJE

S centralnimi nadzornimi sistemi (CNS) omogočamo pregleden nadzor in varno upravljanje vseh varnostnih parametrov objekta.

24/7 PODPORA IN VZDRŽEVANJE

Regionalna servisna mreža zagotavlja hitro odzivnost, zakonsko skladnost in redno vzdrževanje, kar podaljšuje življenjsko dobo vaše opreme.

CELOVITA PONUDBA NA ENEM MESTU

Združujemo lastne inovacije z zastopstvi vrhunskih svetovnih proizvajalcev za sisteme javljanja požara, gašenja, video nadzora in protivlomnega varovanja.

REŠITVE PO MERI

Specializirani smo za kompleksne industrijske objekte in kritično infrastrukturo, kjer zagotavljamo modularne sisteme, prilagojene vašemu okolju.

ZAUPAJTE VARNOST SVOJEGA OBJEKTA STROKOVNJAKOM Z IZKUŠNJAMI.

www.zarja.com

info@zarja.com

01 831 74 52

Avtor: Tadej Hren / vodja ekipe za odzivanje na incidente na SI-CERT-u*

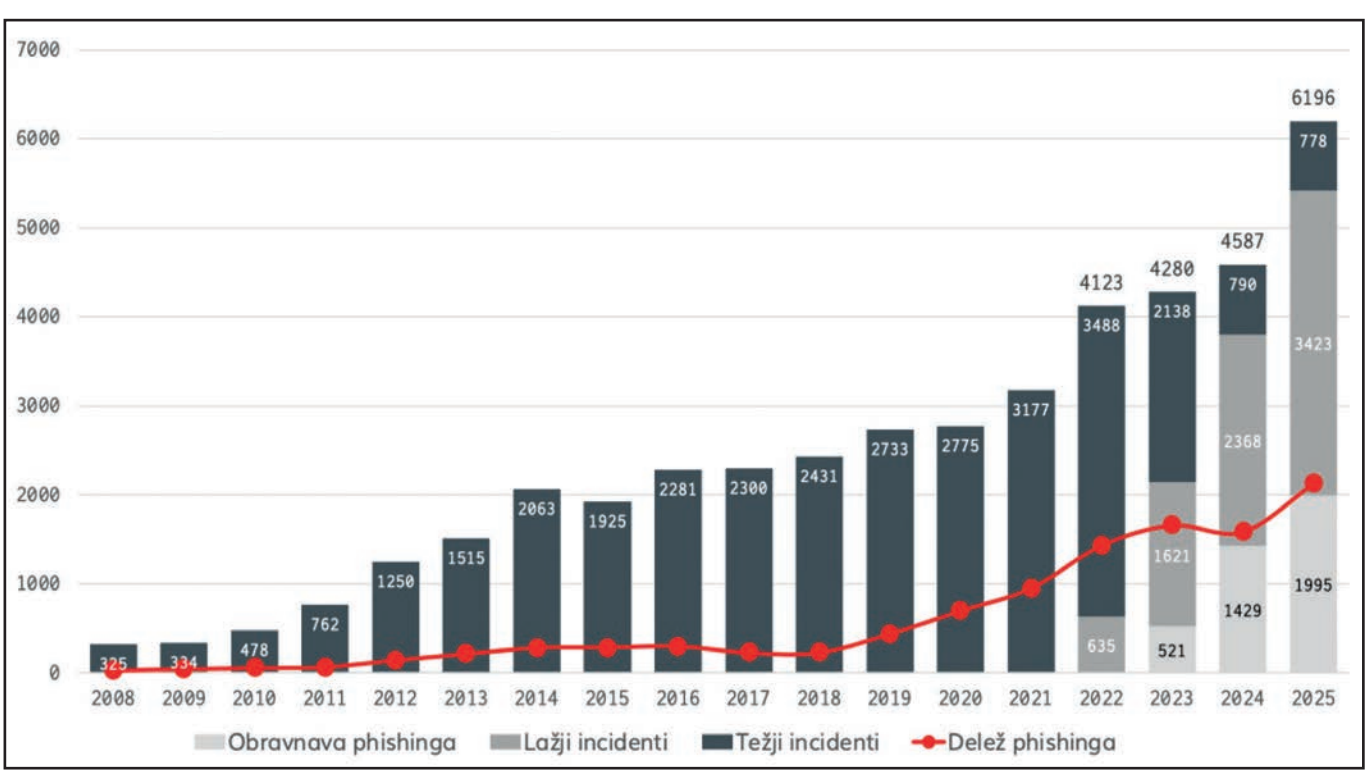


KAJ NAS JE NAUČILO LETO 2025?

Leto 2025 je bilo za Nacionalni odzivni center za kibernetsko varnost SI-CERT eno najbolj intenzivnih let doslej. Pregled statistike preteklega leta kaže na izrazit porast kibernetskih incidentov in večjo prefinjenost napadalcev, kar se posledično odraža tudi v vse višji finančni škodi, ki jo kibernetski napadi povzročijo. Obenem pa na SI-CERT-u zaznavamo tudi okrepljene aktivnosti ozaveščanja in odzivanja na strani podjetij ter organizacij, kar lahko pripišemo tudi vse večjemu zavedanju o pomenu kibernetske odpornosti, ki ga je prinesel nov Zakon o informacijski varnosti.

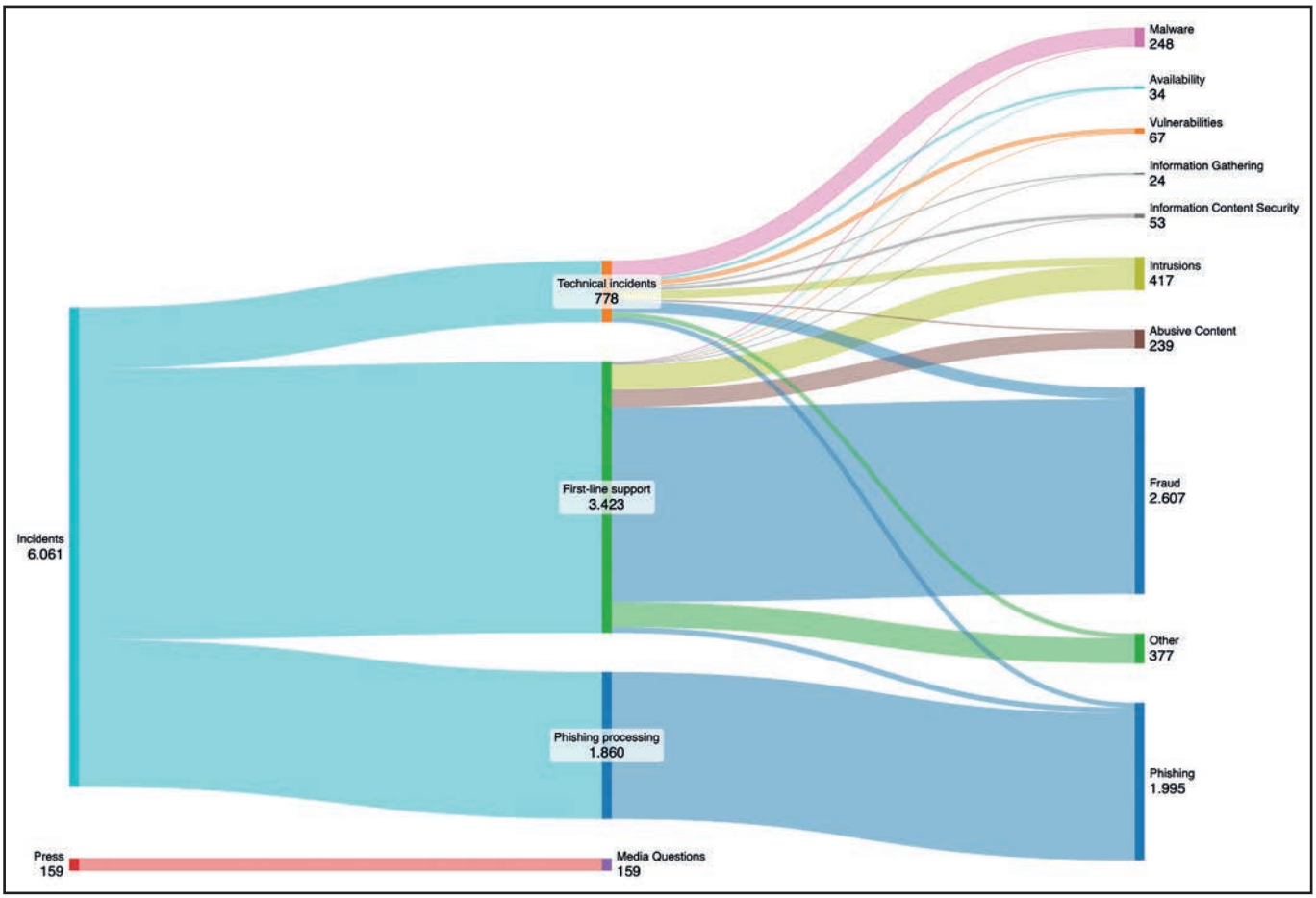
Ključne številke na dlani

V letu 2025 smo na SI-CERT-u obravnavali kar 6.196 incidentov, kar predstavlja 35-odstoten porast v primerjavi letom 2024. Še očitnejši je porast prejetih prijav, ki je bil kar 44-odstoten, kot v primerjavi z letom prej. Podobno rast beležijo tudi mnogi drugi sorodni odzivni centri v Evropi in svetu.



Slika 1: Število obravnavanih incidentov na SI-CERT v letih 2008 - 2025

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



Slika 2: Obravnava incidentov po treh različnih linijah

Najvišji porast incidentov je bil v kategoriji phishing napadov, teh smo obravnavali 1.995, in pa spletnih goljufij, teh je bilo 3.423 oziroma skoraj 45-odstotkov več kot 2024. Podatki, pridobljeni od slovenske policije, razkrivajo, da je skupna prijavljena škoda zaradi spletnih goljufij v letu 2025 znašala 40,4 milijona evrov — kar pomeni 33-odstoten porast glede na leto 2024. Pri tem se moramo zavedati, da mnoge žrtve, tako posamezniki kot podjetja, ne prijavijo incidentov na SI-CERT in oškodovanj na policijo, tako da so realne številke vseh oškodovanj verjetno dejansko precej višje, kot beležijo uradne statistike.

Že sam trend naraščanja številk pove veliko: groženj je čedalje več, a hkrati raste tudi zavedanje o pomenu zaščite.

V letu 2025 smo na SI-CERT-u obravnavali kar 6.196 incidentov, kar predstavlja 35-odstoten porast v primerjavi letom 2024. Še očitnejši je porast prejetih prijav, ki je bil kar 44-odstoten, kot v primerjavi z letom prej. Podobno rast beležijo tudi mnogi drugi sorodni odzivni centri v Evropi in svetu.

Nezadržna rast phishinga

Če je leto 2025 pokazalo en jasen trend, je to neustavljiva rast phishing napadov. Gre za grožnjo, kateri smo že več desetletij izpostavljeni prav vsi uporabniki spletnih storitev (na SI-CERT-u smo o phishing napadih prvič opozarjali leta 2004), pa še vedno predstavlja enega najpogostejših načinov za krajo občutljivih podatkov in pogosto tudi prvi vstopni vektor težjih kibernetskih incidentov. Vidimo, da ne gre za delo posameznikov, temveč organiziranih napadalcev, ki uporabljajo profesionalna orodja in avtomatizirane kampanje, ki so podprta z orodji umetne inteligence. Ta orodja na eni strani močno znižujejo raven tehničnega znanja, ki ga napadalci potrebujejo za izvedbo napada, na drugi strani pa jim omogočajo preprosto izvedbo zelo obsežnih napadov, kakršne smo v preteklosti zaznali le izjemoma. Danes ni več neobičajno, če ena phishing kampanja vključuje tudi več kot 20 različnih lažnih spletnih mest. Prepoznava lažnih sporočil, ki nas vabijo v "potrditev prijavnih podatkov" ali "zagotavljanja dostave pošiljke" je za posameznike vedno težja. V letu 2025 smo na seznam zlonamernih naslovov uvrstili 1995 spletnih naslovov, iz katerih je bilo izluščenih 1100 zlonamernih domen. Te so javnosti prosto dostopne in jih lahko organizacije vključijo v svoje požarne pregrade, SIEM sisteme ali DNS RPZ (Response Policy Zone) sezname za blokado zlonamernih strani.

Ključno sporočilo je, da pravočasna zaznava in prijava phishing napada lahko prepreči širšo škodo.





Slika 3: Lokacije zlorabljenih naprav domačih uporabnikov z določeno vrsto škodljive kode, ki se lahko izrabljajo kot posredniki v napadih

Ko napadalci vstopijo skozi domača vrata

Ena bolj zaskrbljujočih ugotovitev leta 2025 je bila širitev uporabe t. i. posrednikov v gospodinjstvih (residential proxies). V preteklosti je bilo napade mogoče omejevati z geolokacijskim blokiranjem (geofencing). Danes to ni več učinkovita zaščita. Napadalci uporabljajo komercialne VPN storitve, omrežje Tor in vse pogosteje okužene domače naprave slovenskih uporabnikov.

Posebej problematične so poceni naprave za pretočne vsebine (npr. HDMI dongli), ki so lahko že ob nakupu okužene in vključene v posredniška omrežja – pogosto brez vednosti lastnika.

Leto 2025 nas je tako naučilo, da meja med »uporabnikom« in »orodjem napada« postaja vse bolj zabrisana.

Kaj pa lahko pričakujemo v letu 2026: zaenkrat prav nič ne kaže, da bi trendi kazali v smer zmanjševanja števila groženj. Dodatno pričakujemo tudi povečanje prijav incidentov kot posledico začetka uveljavitve novega Zakona o informacijski varnosti, ki bistvenim in pomembnim subjektom nalaga obvezno poročanje o pomembnih incidentih. ■



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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

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

ISO 27001

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

BUREAU VERITAS

DPO

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

Avtor: Jan Setničar/Institut za korporativne varnostne študije*



SMB PODPISOVANJE KOT KLJUČNA RANLJIVOST ACTIVE DIRECTORY OKOLIJ LETA 2026

Področje varnosti Windows omrežij že vrsto let zaznamuje ranljivost, ki izpostavlja eno temeljnih varnostnih nastavitev, ki je kljub svoji dolgoletni razpoložljivosti številne organizacije še vedno ne uporabljajo dosledno – SMB podpisovanje. Gre za varnostni mehanizem, ki bistveno zmanjšuje tveganje napadov tipa »man-in-the-middle« in nepooblaščenega poseganja v omrežni promet, vendar je v praksi pogosto spregledan zaradi napačnih predstav o zmogljivosti ali združljivosti sistemov.

SMB (Server Message Block) je omrežni protokol, ki se v Windows okoljih uporablja za dostop do skupnih virov, kot so datoteke, tiskalniki in druge storitve, ter za izvajanje avtentikacije in sistemske komunikacije med odjemalci ter strežniki v Active Directory okolju. SMB podpisovanje je posledično varnostni mehanizem znotraj protokola SMB, ki zagotavlja kriptografsko preverjanje integritete SMB komunikacije in s tem preprečuje nepooblaščeno spreminjanje ali zlorabo prenesenih podatkov. Čeprav gre za znan varnostni mehanizem, ki obstaja že več generacij Windows sistemov, smo v približno 75 odstotkih penetracijskih testov, ki smo jih izvedli v letu 2025 in začetku 2026, ugotovili, da ta funkcija ni nastavljena kot zahtevana na vsaj večjem delu naprav. Statistično se je prav izraba te miskonfiguracije izkazala za enega izmed najbolj pogostih vektorjev za popolno kompromitiranje celotne domene, v še večjo skrb pa je dejstvo, da je sam napad izjemno enostaven in ne terja poglobljenega znanja ter enumeracije sistema. Z drugimi besedami, najenostavnejša oblika izrabe te miskonfiguracije je ena izmed "vab", ki jih ob začetku penetracijskega testa postavimo in pustimo, če kaj "ugrizne". In večinokrat ta napad deluje ter nam tako v večini primerov priskrbi razširjen dostop, pri nekaterih strankah pa celo priskrbi enega od vektorjev kompromitiranja celotne domene že na prvi dan.

Razlog za to ni vedno pomanjkanje znanja oziroma razumevanja. V mnogih primerih gre za kombinacijo zgodovinskih odločitev, kompromisov zaradi kompatibilnosti s starejšimi sistemi ali preprosto preskakovanje pravilnih nastavitev med implementacijo varnostnih politik. SMB podpisovanje namreč zagotavlja kriptografsko zaščito integritete avtentikacijskih in drugih SMB paketov, kar pomeni, da brez obveznega podpisovanja lahko napadalci prestrezajo in preusmerjajo avtentikacijske podatke, ki se prenašajo med odjemalcem in strežnikom. To daje napadalcem znotraj omrežja priložnost, da sicer legitimno prijavo izkoristijo na druge načine in jo uporabijo proti ciljnemu sistemu, kar je tehnika, ki se v mnogih realnih scenarijih izkaže za učinkovito pot do prevzema nadzora nad sistemom.

Ena od najbolj odmevnih ranljivosti zadnjih let, ki izkorišča takšne pomanjkljivosti, je označena kot CVE202533073. Gre za ranljivost v Windows SMB mehanizmu, kjer lahko sistemi, ki ne zahtevajo obveznega SMB podpisovanja, v določenih scenarijih omogočijo zlorabo legitimne avtentikacije, na primer s posredovanjem ali preusmerjanjem NTLM avtentikacij.

*avtor je član Slovenskega združenja korporativne varnosti



Vektor, ki sem ga že omenil pa absolutno ni edini način izrabe te miskonfiguracije. Bolje je, če jo smatramo kot jedrno točko problema, prek katere se da na vedno več načinov kompromitirati sistem. Govorimo o kombiniranju ene ali več ostalih ranljivosti v sistemu in izdelavi verižnega napada, s katerim iz več ranljvosti različnih stopenj tveganja sestavimo napad, ki kompromitira celotno domeno. Eden iz najbolj svežih primerov v naši praksi je bila izraba napačne konfiguracije v Active Directory Certificate Services (ADCS), PetitPotam ranljivosti na Domenskem Kontrolerju in seveda pomanjkanja vklopljene zahteve po SMB podpisovanju. Tri različne ranljivosti so bile verižene skupaj za izvedbo enotnega napada in pridobitev popolne kontrole nad domeno, ki je bila sicer v drugih pogledih močno zavarovana.

Dodatno pa poleg navedenega prihaja na plano tudi vedno več novih načinov izrabe pomanjkanja te konfiguracije. Ena od najbolj odmevnih ranljivosti zadnjih let, ki izkorišča takšne pomanjkljivosti, je označena kot CVE202533073. Gre za ranljivost v Windows SMB mehanizmu, kjer lahko sistemi, ki ne zahtevajo obveznega SMB podpisovanja, v določenih scenarijih omogočijo zlorabo legitimne avtentikacije, na primer s posredovanjem ali preusmerjanjem NTLM avtentikacij. V takšnem primeru se sicer legitimna avtentikacija znotraj omrežja spremeni v učinkovit napadalni vektor, ki ga je mogoče uporabiti za nadaljnje gibanje po okolju in postopno pridobivanje višjih privilegijev. Gre za ranljivost, ki jo je Microsoft zakrpal v junijskih varnostnih popravkih leta 2025, a je bila zaradi pomanjkljive konfiguracije ali odsotnosti posodabljanja še vedno izkoriščena v številnih okoljih, ki so ostala nepopravljena, ali kjer podpisovanje ni bilo zahtevano. Potem ko je CISA to ranljivost uvrstila na seznam tistih, ki se aktivno izkoriščajo, je postalo jasno, da ni dovolj samo nameščanje popravkov – treba je zagotoviti, da so pravilne varnostne nastavitve dosledno uporabljene.

Poleg tehničnih vidikov je ključen tudi organizacijski premislek o tem, kako pristopamo k varnostnim konfiguracijam in zakaj je pomembno, da niso le priporočene, temveč dosledno zahtevane. V praksi smo večkrat videli okolja, kjer so napredni EDR sistemi, razni dodatni zaščitni mehanizmi, večfaktorska avtentikacija, itd. implementirani po vseh pravilih dobre prakse, vendar pa klasične konfiguracijske nastavitve ostanejo spregledane. Rezultat so scenariji, kjer napadalec zaradi odsotnosti enega samega ukrepa hitro pridobi nadaljnji dostop in premaga številne druge obrambne mehanizme, ki bi sicer potencialno omejili njegov napredek.

Izkušnje iz naših testov kažejo, da je vključevanje SMB podpisovanja kot obveznega elementa varnostne politike ena izmed najstarejših, a bolj učinkovitih obrambnih konfiguracij, ki jo lahko organizacije hitro uveljavijo, saj samo odprava te miskonfiguracije odpravi oziroma onemogoči večje število potencialnih vektorjev, prek katerih bi lahko napadalec poskušal pridobiti nadzor nad sistemom. To je korak, ki bistveno zmanjša možnost prestrezanja in zlorab avtentikacij ter skupaj z rednim nameščanjem popravkov in celovitim pregledom konfiguracij drugih varnostnih mehanizmov predstavlja enega izmed temeljev modernega ter odpornega Active Directory okolja. Delo, ki ga opravljamo skozi penetracijske teste in varnostne preglede, potrjuje, da je prav pozornost do takšnih nastavitev tista, ki loči dobro zaščiteno omrežje od tistega, ki se v primeru napada hitro izkaže za ranljivo.

Hkrati pa je treba razumeti, da popolna uveljavitev SMB podpisovanja v vseh okoljih ni vedno trivialna naloga. V številnih organizacijah, zlasti v javnem sektorju, zdravstvenih in medijskih ustanovah, se še vedno uporabljajo starejši sistemi ali specializirana programska oprema, ki temelji na storitvah, ki SMB podpisovanja ne podpirajo. Takšni sistemi so pogosto vezani na dolgoročne pogodbe, regulativne zahteve ali lastniške rešitve, kjer zamenjava ali nadgradnja ni mogoča brez večjih finančnih in operativnih posledic. Prav v teh primerih je še toliko pomembneje, da se tveganja jasno prepoznajo, ustrezno segmentirajo in kompenzirajo z drugimi varnostnimi ukrepi, saj praksa kaže, da napadalci ravno takšne izjeme najpogosteje izkoristijo kot vstopno točko v sicer dobro zaščiteno okolje. ■

ALCEA
ASSA ABLOY

vaša vstopna točka v revolucijo povezljivosti.

ALCEA GATEWAY

- Oddaljeno odklepanje brez ključa
- Pregled nad situacijo v realnem času
- Visoka kakovost in dolga življenjska doba
- Učinkovitost, udobje in brezskrbnost

alceaglobal.com/gateway





Avtorica: mag. Sabina Muratović / Oddajniki in zveze RTV Slovenija*



ODPORNOST NACIONALNIH MEDIJEV – KLJUČNI IZZIVI

V zadnji številki revije Korporativna varnost smo pri odpornosti nacionalnih medijev na hibridne grožnje obravnavali napade na infrastrukturo, kibernetske vdore, fizične sabotaže in organizirane dezinformacijske operacije. Ti primeri so pokazali, kako ranljiv je medijski sistem, tako tehnično kot psihološko. Tokrat ne gre zgolj za odpornost infrastrukture, temveč odpornost verodostojnosti. Javni mediji v Evropi še vedno uživajo visoko stopnjo zaupanja. Zato je izjemno pomembno graditi odpornost na meji med resničnim in umetno ustvarjenim. Odpornost se danes ne meri le v megavatih in požarnih zidovih, temveč tudi v tem, ali javnost še prepozna, komu verjeti.

Uvod

V zadnjem desetletju so hibridne grožnje in napadi na medije prešli več razvojnih faz, od fizičnih sabotaž oddajniške infrastrukture do kibernetskih vdorov in koordiniranih dezinformacijskih kampanj. Skupna točka vseh teh operacij je praviloma destabilizacija – preizkus ranljivosti in psihološki učinek na javnost. Dodatna dimenzija dandanes je vsebina, ustvarjena z umetno inteligenco. Ta zelo prepričljivo ustvarja navidezno verodostojne, a popolnoma izmišljene podobe, glasove, dogodke. Našo resničnost morda ustvarja algoritem.

Ne izberemo več nujno, kaj bomo gledali – algoritem izbere nas. Iz naših zaslonov brizgajo novice, izjave znanih, mnenja vplivnežev, politikov, pa tudi slehernikov, preplavljajo nas »ekskluzivna« razkritja, teorije zarot vseh pojavnih oblik in dimenzij. Tarča ni več samo infrastruktura, tarča je lahko tudi naše dojemanje resničnosti.

V takšnem okolju se zdi televizija skoraj iz nekih drugih časov. Kdo še sedi pred linearnim programom, če vse vsebine krožijo po platformah? Kako zaščititi resnično informacijo in jo ločiti od umetno ustvarjene? Zdi se, da javni medij kot zanesljiva referenčna točka v takšnem okolju zbledi.

Kdo danes sploh še gleda televizijo?

Spoiler alert - televizija iz repertoarja uporabnikov v resnici ni izginila. Samo spremenila je obliko. Najnovejše EBU poročilo z naslovom Public Service Media 360° Value ugotavlja, da javni mediji tedensko dosežejo 81 % prebivalcev Evrope. Delež je visok tudi med mladimi (69 %). Ob tem javni mediji dosegajo vsaj 92 milijonov mesečnih uporabnikov prek svojih VOD-platform in več kot 50 milijonov aktivnih uporabnikov prek mobilnih aplikacij. Ampak doseg sam po sebi seveda še ne pomeni odpornosti.

Da ne bo dvoma, o kom govorimo: EBU (European Broadcasting Union) je tista evropska zveza javnih medijev, ki med drugim stoji za distribucijo novoletnega koncerta Dunajskih filharmonikov, usklajuje pridobivanje pravic za največje športne dogodke na svetu - od olimpijskih iger, evropskega nogometnega prvenstva UEFA do Dirke po Franciji - in organizira celo tako legendarno razdvajajoče projekte, kot je Evrovizija (Eurosong) z dometom 166 milijonov gledalcev. EBU je skratka organizacija, ki poskrbi, da Evropa vsaj občasno gleda in posluša isto stvar hkrati. In njena raziskava potrjuje, da največ Evropejcev še vedno najbolj spremlja vsebine javnih medijev. Večja verjetnost je torej, da bodo Evropejci namesto o najnovejših geopolitičnih podvigih velikih sil naslednje jutro

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

ob kavi razpravljali o podeljenih točkah žirije. Vendar v okolju, kjer je mogoče generirati verodostojno simulacijo, sama prisotnost ni več zadosten ščit.



Vir: EBU Official – Eurovisionworld.com

> Evropa je še vedno okolje, kjer ljudje verjamejo v javni medij kot zanesljiv sistem preverjanja informacij. V času, ko se javna razprava pogosto osredotoča na domnevni zaton tradicionalnih medijev, podatki kažejo drugačno sliko. Javni mediji še vedno ohranjajo širok doseg. S tem ohranjajo tudi vpliv na oblikovanje skupnega informacijskega prostora. In prav ta skupni prostor, kjer se srečajo preverjene informacije, uredniška odgovornost in javni interes, ostaja eden ključnih temeljev demokratične družbe.

Algoritem namesto urednika

Mednarodna raziskava News Integrity in AI Assistants (EBU in BBC, oktober 2025) je pri odgovarjanju na vprašanja o aktualnih novicah analizirala delovanje štirih vodilnih AI pomočnikov (ChatGPT, Microsoft Copilot, Google Gemini in Perplexity). V študiji je sodelovalo 22 javnih medijev iz 18 držav in 14 jezikovnih okolij. Maja in junija 2025 je bilo na 30 enakih novinarskih vprašanj ocenjenih 2.709 odgovorov.

Rezultat? Skoraj polovica odgovorov (45 %) je imela vsaj eno pomembno napako. AI pomočnikom se je zataknilo pri navajanju virov (31 %) ali pri točnosti navajanja podatkov (20 %). Konkretno: AI pomočniki so navajali zastarele podatke (npr. napačno ime aktualnega papeža), izmišljene ali spremenjene citate, javnim medijem so pripisovali mnenja, ki jih ti niso nikoli izrazili. Navajali so tudi nerelevantne ali neobstoječe povezave. Raziskava dalje ugotavlja, da AI pomočniki redko zavrnejo odgovor, tudi kadar bi bilo to smiselno. Pogosto pa



nastopajo zelo samozavestno, kar pri uporabniku ustvarja vtis uredniške avtoritete in avtonomije, pa čeprav gre v resnici za vsebino brez dejanske uredniške odgovornosti. Uporabnik pa razlike med uredniško potrjeno vsebino in umetno generiranim odgovorom pogosto sploh ne zazna.

Če je mogoče zgenerirati govor politika, ki ga nikoli ni bilo, novinarski prispevek, ki ga v resnici ni ustvaril človek, potem deepfake ne meri več na infrastrukturo, temveč na epistemološko jedro družbe kot celote, na sposobnost ločevanja med resničnostjo in umetno resničnostjo. V takšnem okolju sploh ni več pomembno, kaj kdo verjame. Dovolj je dvom v lastno zaznavo.

Namreč delovanje oddajnika je mogoče sabotirati. Strežnik je mogoče preobremeniti. Spletno stran je mogoče zaviti v temo za nekaj ur ali dni. Takšni napadi so vidni, praviloma pa časovno omejeni. Težje je obnoviti nekaj drugega – zaupanje v to, da je to, kar gledamo in poslušamo. To je bistvena razlika med klasičnimi napadi in manipulacijami z umetno inteligenco. Prvi povzročijo motnjo v delovanju sistemov, drugi izkrivljajo resničnost ali ustvarjajo svojo.

Kako zagotoviti odpornost?

Javni mediji v Evropi neposredno zaposlujejo več kot 42.000 novinarjev. Letno namenijo skoraj 6 milijard evrov za novice in aktualne vsebine, kar je nekaj manj kot tretjina vseh programskih stroškov javnih medijev. S tem je vzpostavljeno razvejeno ustvarjanje programskih vsebin (informacij), ki so pod neposrednim uredniškim nadzorom. Takšno ustvarjanje je zakonsko regulirano in ima urejeno financiranje. Tukaj se začenja odpornost verodostojnosti: da je vsebina rezultat uredniškega procesa, ki ga je mogoče preveriti, in posledično uredniške odgovornosti - ne pa enega od modelov AI.

Poročilo EBU ocenjuje še, da znaša povprečni neto prispevek za javne medije približno 11 centov na prebivalca na dan (63 javnih medijev, 47 trgov). Ta znesek vsebuje delovanje celotnega informacijskega aparata - nacionalne in mednarodne novinarske mreže, krizno obveščanje, regionalna ter lokalna dopisništva in redakcije, digitalne platforme, kulturne ter izobraževalne vsebine, športne prenose. Družba kot celota s tem financira organiziran uredniški proces, ki vključuje preverjanje virov, uredniško odgovornost in jasno določene novinarske standarde. Poenostavljeno, 11 centov je finančni vložek posameznika v kolesje, ki loči preverjeno informacijo od umetno generirane vsebine.

Prav tako je zelo pomemben velikokrat spregledan vpliv javnih medijev na lokalni ravni, kjer algoritmi zaradi uporabniškega poznavanja lokalnega okolja nekoliko izgubijo sapo. Kredibilni mediji imajo praviloma uredniške ekipe stalno na terenu povsod po državi, te ekipe pokrivajo prostor, kjer se sprejemajo konkretne odločitve (občine, lokalne skupnosti). Ko mediji s preverjenim poročanjem redno zapolnjujejo ta prostor preprečujejo učinke lažnih vsebin ali pa vsaj omilijo njihov učinek. Odpornost tako pomeni redno vzdrževanje informacijske infrastrukture na vseh ravneh družbe.

V takšnem okolju in na vseh ravneh družbe je EBU poročilo Public Service Media 360° Value jasno zakoličilo trditev, da javni mediji niso danes ni več zgolj producenti vsebin. EBU jih označuje za »centralne banke informacijske ekonomije«. Kot centralna banka preprečuje razvrednotenje valute in stabilizira finančni sistem, javni medij preprečuje razvrednotenje informacij ter stabilizira informacijski prostor. Kar je centralna banka za denar, je javni medij za informacijo.

Zaključek

Vse bolj se zdi, da iz vseh teh procesov najbolj neopazno izginja prav človeški faktor. Umetna inteligenca ima seveda izjemno vrednost. Je dragocen pomočnik, prihrani ogromno časa in napora, avtomatizira rutinske naloge, pospeši analizo podatkov. Hkrati pa zna ustvarjati vsebine, ki jih povprečen uporabnik težko loči od profesionalno pripravljenih. Meja med resničnim in umetno ustvarjenim izginja.

Zato se pri razpravah o odpornosti morda preveč osredotočamo zgolj na tehnične zaščite. Govorimo o varovanju oddajnikov, strežnikov, podatkovnih centrov, o kibernetski varnosti in redundanci sistemov. Kot da bi verjeli, da je odpornost predvsem tehnično vprašanje. Vloga človeka pa se v teh razpravah pogosto izgubi nekje vmes. Opazimo jo šele, ko začnemo pogrešati tisto človeško, česar tehnologija ne more imeti. Algoritem ne more prevzeti uredniške odgovornosti. Nima notranjega etičnega okvira, nima občutka za okoliščine, občutka za posledice svojih napačnih informacij in vsebin.

Zato je bistveno vprašanje, kako ohraniti referenčno točko verodostojnosti v okolju, kjer je mogoče ustvariti skoraj vsak obraz, gib, glas, dogodek, ki se ni nikoli zgodil. V takšnih življenjih postane vprašanje vira informacij, procesa ustvarjanja informacij in odgovornosti za informacijo bolj pomembno kot kadar koli.

Evropa je še vedno okolje, kjer ljudje verjamejo v javni medij kot zanesljiv sistem preverjanja informacij. V času, ko se javna razprava pogosto osredotoča na domnevni zaton tradicionalnih medijev, podatki kažejo drugačno sliko. Javni mediji še vedno ohranjajo širok doseg. S tem ohranjajo tudi vpliv na oblikovanje skupnega informacijskega prostora. In prav ta skupni prostor, kjer se srečajo preverjene informacije, uredniška odgovornost in javni interes, ostaja eden ključnih temeljev demokratične družbe. ■

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 19. MAJ 2026

17. mednarodna konferenca Dnevi korporativne varnosti

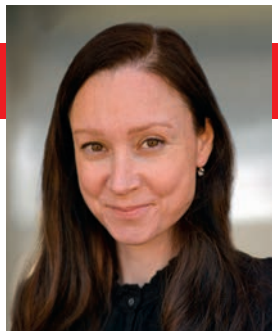


PODELIJO SE IZBRANIM INSTITUCIJAM IN POSAMEZNIKOM ZA NJIHOV INOVATIVNI PRISPEVEK NA PODROČJU RAZVOJA IN UVELJAVLJANJA VARNOSTI. NAGRADO PODELJUJE ICS-LJUBLJANA V SODELOVANJU S SLOVENSKIM ZDRUŽENJEM KORPORATIVNE VARNOSTI. NEODVISNA KOMISIJA OCENJUJE IN IZBIRA KVALITETO TER IZVIRNOST PRIJAVLJENIH UDELEŽENCEV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

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



ODPORNOST KRITIČNE INFRASTRUKTURE: IZKUŠNJE IZ EU PROJEKTA ATLANTIS

Evropska unija se sooča z vse bolj kompleksnim in prepletenim tveganjskim okoljem, v katerem so kritične infrastrukture izpostavljene sočasnim kibernetskim, fizičnim ter hibridnim grožnjam. Odpornost kritične infrastrukture tako ni več zgolj vprašanje tehnične zaščite posameznih sistemov, temveč celostnega upravljanja medsebojno povezanih kibernetsko-fizično-človeških (CPH) ekosistemov. Projekt ATLANTIS – *Enhancing Resilience and Cyber-Physical-Human (CPH) Security of the Key EU Critical Infrastructures* – je k temu prispeval z razvojem metodologij, orodij in modelov za krepitev odpornosti ključnih evropskih kritičnih infrastruktur.

Ranljivosti sodobne družbe

Avgusta 2023 je Slovenijo prizadelo najhujše neurje v zadnjih desetletjih. Močno deževje je povzročilo katastrofalne poplave, ki so zalile cele doline, odnesle mostove in od sveta odrezale številne kraje. Prometne povezave so se ustavile, oskrba z elektriko je bila motena in komunikacija prekinjena. Posledice so bile občutne še dolgo časa po tem, ko je voda odtekla: ohromljene trgovske poti, draga obnova in številne osebne stiske. Le tri leta pred tem je pandemija COVID-19 razgalila drugačno, a nič manj resno ranljivost. Bolnišnice so bile preobremenjene, dobavne verige so razpadle, zaprtje mej pa je ustavilo pretok ljudi in blaga. Kar se je začelo kot zdravstvena kriza, se je hitro prelilo v logistično in gospodarsko krizo.

Ti dogodki nas učijo, da je kritična infrastruktura (KI) hrbtenica našega vsakdana. Ko deluje, življenje teče neopazno. Ko odpove, je lahko paralizirana cela država, celotna družba. Nesreče kažejo tudi, kako so današnja tveganja medsebojno povezana. Ne ozirajo se na organizacijske, sektorske ali državne meje. Železniški promet je odvisen od energetskih sistemov, ti pa od stabilnih telekomunikacijskih povezav. Če nevihta močno in obsežno poškoduje daljnovode, se sčasoma prekine napajanje ter delovanje železnic, s tem pa so hitro lahko prekinjene ključne dobavne verige, ki segajo preko naše regije.

Dolga leta je bil pristop k zaščiti KI jasen. Vsak operater je skrbel za svojo infrastrukturo, za svoj sistem. Takšen silosni pristop je bil smiseln, ko so bile nevarnosti bolj lokalne, predvidljive in obvladljive. Danes pa so sistemi močno prepleteni in zato medsebojno odvisni, nevarnosti pa so zahtevne ter večplastne. To prepoznava tudi novi evropski regulativni okvir: Direktiva CER (Critical Entities Resilience) zahteva, da države članice in operaterji sistematično krepijo odpornost kritičnih entitet proti fizičnim grožnjam, Direktiva NIS2 pa prinaša strožje zahteve na področju kibernetske varnosti. Skupaj oblikujeta celovit okvir, ki presega varovanje posameznih sistemov in zahteva usklajeno obravnavo različnih groženj.

Jasno je, da varovanje enega samega sistema ali sektorja ni več dovolj. Potrebujemo pristope, ki naslavljajo povezanost, modelirajo verižne učinke in omogočajo usklajeno ter učinkovito ukrepanje več organizacij, sektorjev in držav hkrati. Evropa potrebuje sistemsko odpornost.

*avtorica je članica Slovenskega združenja korporativne varnosti



Vir: https://www.gov.si/zbirke/projekti-in-programi/ukrepi-drzave-za-pomoc-po-poplavah-avgusta-2023/

Celovit pristop k dvigovanju skupne odpornosti

ATLANTIS, evropski projekt iz programa Obzorje Evropa (Horizon Europe) je bil zasnovan prav za to nalogo. Njegov cilj je bil preseči zaščito posameznih virov in vzpostaviti sistemski evropski pristop k obvladovanju tveganj in krepitvi odpornosti. Gre za tri leta trajajoč projekt s skoraj 40 partnerji iz različnih držav Evropske Unije, ki se je zaključil septembra 2025. *Spletna stran projekta je dosegljiva na https://www.atlantis-horizon.eu/.*

Jedro ATLANTIS-a je nova metodologija ocenjevanja tveganj, ki ne analizira le ranljivosti ene organizacije, temveč modelira medsebojne odvisnosti med infrastrukturami, sektorji in državami v kontekstu različnih enoličnih ali hibridnih groženj. Upošteva, da se tveganja širijo, da nastajajo verižni učinki, in da se različne grožnje med seboj seštevajo.

Poleg metodologije je ATLANTIS razvil inovativen sistem za podporo odločanju (Decision Support System), ki v realnem času obdeluje podatke različnih senzorjev različnih sistemov in pomaga operaterjem ne le pri kriznih odločitvah, temveč tudi pri vsakdanjem upravljanju KI. Omembe vreden je zlasti razvoj digitalnega dvojčka, ki je plod razvoja slovenskega tehnooškega podjetja SNEP. Gre za orodje, ki ustvari virtualno kopijo kritičnih virov, vizualizira njihove medodvisnosti in omogoča varno preizkušanje različnih scenarijev.

Da bi preverili uporabnost teh rešitev, smo jih testirali v treh velikih pilotih (Large Scale Pilots oz. LSP) po Evropi. Manjša izmed treh (LSP#2 in LSP#3) sta naslavljala sistemska tveganja v finančnem sektorju v Španiji in Nemčiji ter zdravstvenem sektorju v Grčiji in na Cipru. Največji izmed vseh (LSP#1) pa se je osredotočal na dvig odpornosti KI vzdolž Mediteranskega koridorja, enega najbolj pomembnih evropskih tovornih koridorjev, ki poteka prek meja šest držav članic EU in predstavlja pomembno življenjsko žilo evropske trgovine med srednjo Evropo ter Ukrajino. V ATLANTIS-u so Mediteranski koridor zastopali upravitelji tunela Fréjus, ki povezuje Italijo in Francijo, predstavniki italijanskih železnic ter luke v Rijeki in številni slovenski operaterji KI, ki imajo del svoje infrastrukture na območju Luke Koper.





Deležniki v pilotu LSP#1.

Slovenski pilot kot del evropskega preizkusa

V Sloveniji so bili v pilot vključeni ICS kot koordinator celotnega pilota LSP#1, Institut Jožef Stefan za razvoj metodologije za analizo sistemskih tveganj in podjetje SNEP za razvoj digitalnega dvojčka ter številni predstavniki slovenske KI: Luka Koper, Slovenske Železnice, Telekom Slovenije, Petrol, DARS, Ministrstvo za Infrastrukturo in Urad Republike Slovenije za Informacijsko Varnost.

Celotna slovenska ekipa je preučila najbolj relevantne fizične, kibernetske in hibridne grožnje za sodelujoče deležnike oziroma glede na povezave med njimi. Podrobneje smo preučili dva scenarija: pojav obsežnega požara na delu železniške infrastrukture Slovenskih Železnic in dolgotrajen kibernetski napad na infrastrukturo Telekoma Slovenije. Vsak scenarij je bil modeliran tako, da je pokazal odvisnosti med ključnimi viri posameznih organizacij. Kako bi lahko onesposobljen železniški promet vplival na ohromitev cestnega prometa in transporta blaga iz/v Luko Koper ter kako bi prekinjeme komunikacijske poti prekinile ali otežile delovanje procesov več operaterjev KI na območju Luke Koper.

Identificirali smo ključne vire vseh deležnikov in soodvisnosti med njimi, ne glede na geografske, fizične, logične ali kakšne druge meje med posameznimi organizacijami ter sektorji. Ocenili smo potencialne verižne učinke in njihove hitrosti ter posledice. Evaluirali smo tudi kritičnost takšnih dogodkov glede na vpliv, ki bi jih imeli na poslovne procese organizacij, posameznike in družbo ter okolje. S pomočjo vseh teh informacij smo lahko kvantificirali posamezna tveganja, vse informacije pa na uporabniku prijazen način prikazali v digitalnem dvojčku.

S pomočjo grafov soodvisnosti in prikazov v digitalenm dvojčku smo jasno videli "veliko sliko": kako zelo so sistemi med seboj povezani in kje so ti najbolj ranljivi. Še več, ATLANTIS-ove rešitve so se izkazale za pomembno orodje za olajšanje komunikacije med vsemi deležniki. Operaterji KI in odločevalci, odgovorni za področje kritične infrastrukture, so namreč dobili skupen jezik za lažjo razpravo o sistemskih tveganjih. Pilot je prav tako pokazal, da se odpornost ne meri in krepi le znotraj enega podjetja; prava odpornost zahteva skupno zavest, načrtovanje in upravljanje.

Rezultati tega dela in vso nabrano znanje pa niso ostali le znotraj sodelujoče ekipe. Pilot je namreč pomembno prispeval k temu, da se spoznanja iz prakse prenesejo tudi v slovenske in evropske politike. Organizirali smo več relevantnih razprav s slovenskimi odločevalci, pripravili pa smo tudi priporočila za Evropsko Komisijo v smislu izboljševanja evropskih politik in evropskih programov za raziskave in inovacije.

Odpornost je skupna naloga

Projekt ATLANTIS kot celota in slovenski del pilota LSP#1 sta podala jasno, nedvoumno sporočilo: Današnje grožnje se ne ozirajo več na organizacijske, sektorske in državne meje, zato morajo biti tudi naši ukrepi ter odzivi ustrezno prilagojeni: sistemski in usklajeni.
Prvič, sistemska tveganja zahtevajo sistemske rešitve. Varovanje posameznega kritičnega vira, operaterja, ali sektorja preprosto ni več dovolj. Današnji svet je preveč povezan, da bi lahko razmišljali o izoliranih enotah. ATLANTIS je pokazal, da obstajajo konkretni in praktični pristopi, s katerimi lahko prepoznamo, razumemo ter lažje obvladamo kompleksna tveganja. Da obstajajo orodja, ki podpirajo pravočasno in usklajeno informiranje ter odločanje.



Priporočila za Evropsko Komisijo, pripravljena na podlagi znanj in izkušenj, pridobljenih v ATLANTIS-u.

Drugič, sodelovanje čez meje in sektorje deluje in je nujno. Slovenski pilot je pokazal, da lahko predstavniki različnih sektorjev (pa tudi držav) učinkovito sodelujejo. Sodelovanje pa ne pomeni le koordinacije med krizami, temveč tudi deljenje izkušenj, razumevanje soodvisnosti, sooblikovanje ukrepov in izvajanje skupnih simulacij dogodkov, preden se ti zgodijo. Medsebojno zaupanje in skupne vaje so temelj vsakega uspešnega odziva na krizo in prav to smo v projektu ATLANTIS tudi dosegli.

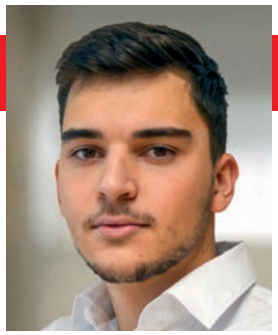
Tretjič, evropski raziskovalni ni razvojni projekti, kot je ATLANTIS, so neprecenljivi poligoni za učenje, testiranje in skupno inoviranje. Omogočajo nam, da nove ideje preizkusimo v kontroliranem okolju, preden jih prenesemo v realne operacije. Dajejo nam prostor, kjer lahko majhne države, kot je Slovenija, aktivno sooblikujemo evropske pristope, delimo svoje znanje in se učimo od drugih. In predvsem omogočajo povezovanje ljudi. To je vrednost, ki daleč presega trajanje enega samega projekta.

Zaključek

ATLANTIS se je zaključil, a izzivi, ki jih je naslavljal, ostajajo. Podnebne spremembe, digitalna ranljivost, geopolitične napetosti in kompleksnost sodobnih sistemov nas opominjajo, da je treba nadaljevati. Ne z izoliranimi ukrepi, temveč z dolgoročno vizijo odpornosti, ki vključuje vse deležnike in vso Evropo. Prav tu imata ključno vlogo direktivi NIS2 in CER, ki ustvarjata evropski okvir za povečanje varnosti ter odpornosti kritičnih entitet. ATLANTIS je s svojimi metodami in orodji prispeval k uresničevanju teh zahtev v praksi in pokazal, kako jih lahko države ter operaterji uporabijo kot priložnost za izboljšanje sodelovanja in skupno krepitev odpornosti. ■



Avtor: Matic Čaleta / Institut za korporativne varnostne študije*



KIBERNETSKE VAJE POMEMBEN MULTIPLIKATOR ODPORNOSTI ORGANIZACIJ

V sodobnem digitalnem okolju postaja kibernetska varnost eno ključnih področij zagotavljanja stabilnega delovanja organizacij, države in kritične infrastrukture. Organizacije so danes izpostavljene vedno bolj kompleksnim in koordiniranim kibernetskim napadom, ki lahko povzročijo motnje v delovanju, izgubo podatkov ali celo širše družbene in gospodarske posledice. Zato se poleg tehničnih varnostnih ukrepov vse več pozornosti namenja tudi preverjanju pripravljenosti organizacij na odzivanje v primeru kibernetskih incidentov. Eden izmed najučinkovitejših načinov za to so kibernetske vaje, ki predstavljajo izjemno pomemben multiplikator informacij o dejanski ravni pripravljenosti organizacij.

Kibernetske vaje omogočajo simulacijo različnih scenarijev kibernetskih incidentov ter preverjanje sposobnosti organizacije za njihovo zaznavanje, odzivanje in obvladovanje posledic. Ključna prednost takšnih vaj je v tem, da združujejo več vidikov delovanja organizacije, od tehničnih ekip, vodstva in kriznega upravljanja do komunikacijskih mehanizmov in sodelovanja z zunanjimi deležniki. Na ta način organizacije ne preverjajo zgolj posameznih tehničnih kontrol, temveč celoten sistem upravljanja kibernetske varnosti.

Spekter možnih oblik kibernetskih vaj je zelo širok. Na eni strani so tako imenovane namizne oziroma »table-top« vaje, ki so zasnovane kot strukturirane razprave med ključnimi deležniki v organizaciji. V takšnih vajah udeleženci obravnavajo hipotetični scenarij kibernetskega incidenta in skozi vodeno razpravo sprejemajo odločitve, ki bi jih morali sprejeti v realni situaciji. Namen teh vaj je predvsem preverjanje razumevanja postopkov, vlog in odgovornosti ter komunikacijskih tokov v primeru incidenta. Namizne vaje so zaradi relativno enostavne organizacije in nizkih stroškov primerne za širok krog organizacij, hkrati pa omogočajo vključevanje vodstva in strateških odločevalcev.

Naslednjo stopnjo predstavljajo funkcionalne oziroma operativne vaje, pri katerih organizacije že simulirajo dejansko izvajanje odzivnih postopkov. V takšnih vajah se preverja delovanje kriznih ekip, koordinacija med različnimi organizacijskimi enotami ter izvajanje ključnih procesov upravljanja incidentov. Udeleženci morajo sprejemati odločitve na podlagi postopno razvijajočega se scenarija, ki lahko vključuje več faz incidenta, eskalacijo dogodkov ter komunikacijo z zunanjimi institucijami.

Najzahtevnejšo obliko predstavljajo tehnične kibernetske vaje, ki vključujejo neposredno testiranje tehničnih zmogljivosti organizacije. Takšne vaje pogosto potekajo v nadzorovanih laboratorijskih okoljih ali posebnih simulacijskih platformah, kjer je mogoče varno izvajati napade in preverjati odziv obrambnih mehanizmov. Pogosto se uporabljajo pristopi, kot so simulirani napadi (t. i. red team / blue team scenariji), penetracijski testi ali simulacije realnih incidentov v informacijskih sistemih. Na ta način organizacije preverjajo dejansko učinkovitost svojih tehničnih zaščitnih mehanizmov, sposobnost zaznavanja anomalij ter hitrost odzivanja varnostnih ekip.

Posebna vrednost tehničnih vaj je v tem, da omogočajo neposredno testiranje posameznih aktivnosti skozi realistične scenarije možnih kibernetskih incidentov. To vključuje na primer simulacijo napada z izsiljevalskim virusom, kompromitacijo uporabniških računov, napade na kritične storitve ali zlorabo ranljivosti v informacijskih sistemih. S tem se organizacije ne učijo zgolj teoretičnih

*avtor je član Slovenskega združenja korporativne varnosti



postopkov, temveč pridobivajo konkretne izkušnje pri obvladovanju kompleksnih situacij.

V trenutnem regulatornem okolju postajajo kibernetske vaje še posebej pomembne. V Sloveniji se številne organizacije soočajo z zahtevami Zakona o informacijski varnosti (ZInfV-1), ki širi krog zavezancev ter uvaja strožje zahteve glede upravljanja kibernetskih tveganj in odzivanja na incidente. Veliko organizacij se prvič srečuje z obveznostjo vzpostavitve celovitega sistema upravljanja informacijske varnosti, kar pomeni, da morajo poleg tehničnih rešitev razviti tudi ustrezne organizacijske in operativne postopke.

V takšnem okolju kibernetske vaje predstavljajo izjemno učinkovit mehanizem za usklajevanje dejanskega stanja organizacij z regulatornimi zahtevami. Skozi izvedbo vaj je mogoče relativno hitro prepoznati vrzeli v postopkih, pomanjkljivosti v organizaciji kriznega odzivanja ali nejasnosti v razdelitvi odgovornosti. Poleg tega vaje omogočajo tudi prenos znanja med različnimi deležniki v organizaciji ter krepitev zavedanja o pomenu kibernetske varnosti na vseh ravneh upravljanja.

Če ta okvir razširimo še na zahteve Zakona o kritični infrastrukturi ter evropske CER direktive (Directive on the Resilience of Critical Entities), postane pomen kibernetskih vaj še bolj izrazit. Omenjena regulativa poudarja potrebo po rednem preverjanju odpornosti organizacij na različne vrste motenj, vključno s kibernetskimi incidenti. Poseben poudarek je namenjen tudi izvajanju vaj stresnega testiranja, s katerimi se preverja sposobnost organizacij za delovanje v pogojih kriznih situacij.

V tem kontekstu kibernetske vaje delujejo kot pomemben multiplikator informacij o dejanski stopnji pripravljenosti organizacij. Rezultati vaj omogočajo vodstvu organizacij, regulatorjem in drugim deležnikom vpogled v realno stanje sistemov kibernetske odpornosti. Hkrati pa predstavljajo tudi izhodišče za načrtovanje nadaljnjih izboljšav, razvoj novih postopkov in nadgradnjo tehničnih zmogljivosti.

Pomemben vidik kibernetskih vaj je tudi preverjanje delovanja kriznega upravljanja. Med vajami se v realističnem okolju preverja sposobnost organizacij za aktivacijo kriznih ekip, koordinacijo med različnimi oddelki ter učinkovito sprejemanje odločitev pod časovnim pritiskom. Prav tako se testirajo komunikacijski mehanizmi, tako notranja komunikacija znotraj organizacije kot tudi komunikacija z regulatorji, partnerji in javnostjo.

Takšne aktivnosti omogočajo celovito preverjanje odzivnih mehanizmov kriznega odzivanja, kar je v realnih incidentih pogosto odločilnega pomena za omejevanje posledic napada. Organizacije lahko skozi vaje prepoznajo šibke točke v svojih procesih, izboljšajo koordinacijo med ekipami ter razvijejo bolj učinkovite strategije odzivanja.

Posebej pomemben element kibernetskih vaj je tudi proces analize in učenja po izvedeni vaji. Organizacije po zaključku vaj praviloma pripravijo podrobno analizo poteka aktivnosti, sprejetih odločitev in odzivnih mehanizmov. Takšna analiza omogoča prepoznavanje dobrih praks ter hkrati razkriva področja, kjer so potrebne izboljšave v procesih, tehnologiji ali organizaciji dela. S tem vaje postanejo ne le orodje za preverjanje pripravljenosti, temveč tudi pomemben mehanizem organizacijskega učenja.

Poleg posameznih organizacij imajo vse večji pomen tudi medorganizacijske oziroma sektorske kibernetske vaje. Te omogočajo preverjanje sodelovanja med različnimi organizacijami, regulatorji in drugimi ključnimi deležniki, ki skupaj tvorijo širši ekosistem kibernetske varnosti. V primeru večjih incidentov namreč pogosto ni prizadeta zgolj ena organizacija, temveč celotne dobavne verige ali posamezni sektorji gospodarstva. Prav zato je usklajeno delovanje med organizacijami in institucijami ključno za učinkovito obvladovanje kriznih situacij.

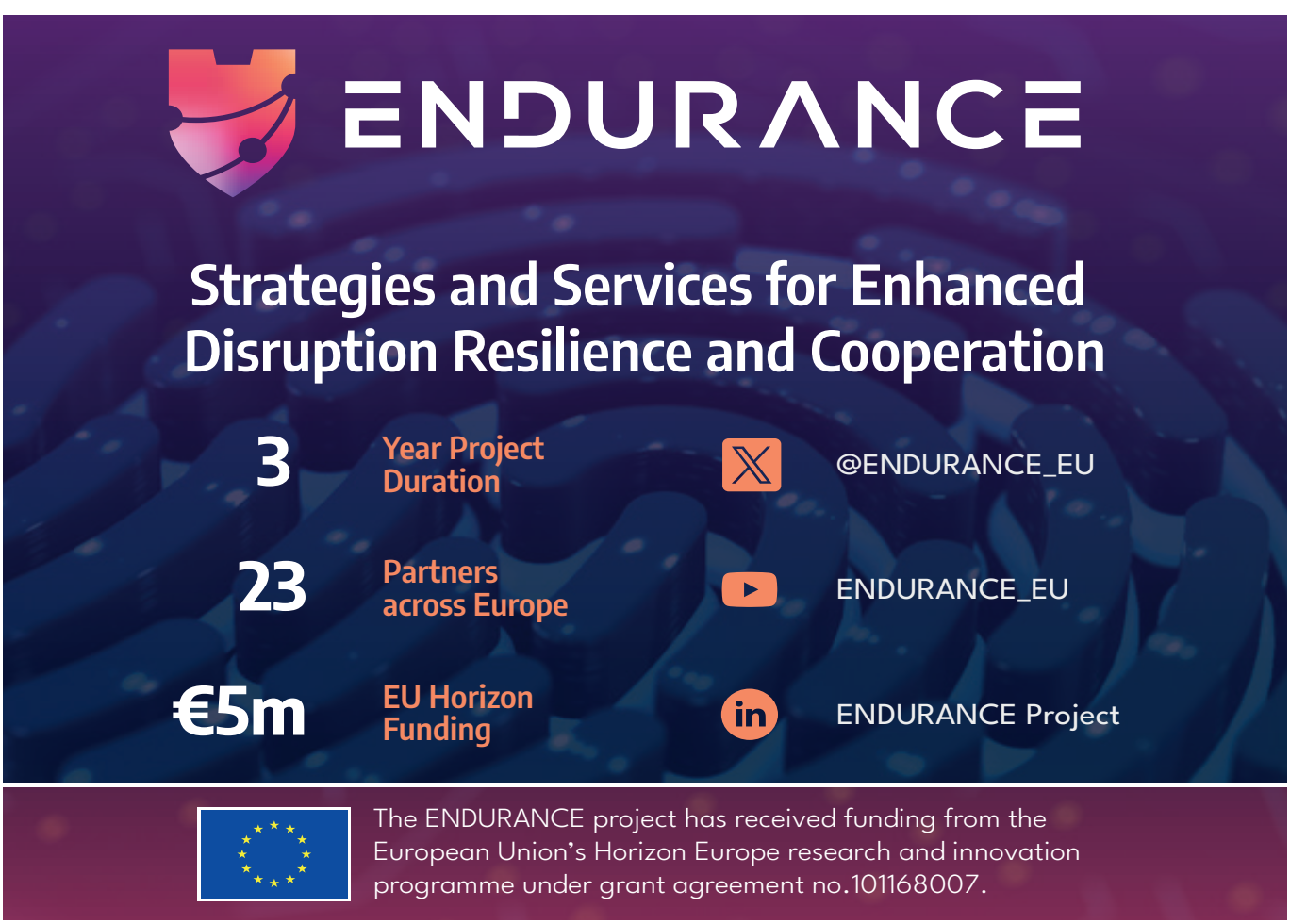
Pomembno je poudariti tudi, da kibernetske vaje pomembno prispevajo k razvoju organizacijske kulture varnosti. V številnih organizacijah se vprašanja kibernetske varnosti še vedno pogosto obravnavajo predvsem kot tehnično vprašanje informacijskih oddelkov. Vendar izkušnje iz vaj jasno kažejo, da učinkovito obvladovanje kibernetskih incidentov zahteva aktivno sodelovanje vodstva, pravnih služb, služb za odnose z javnostmi, kadrovskih oddelkov ter drugih ključnih funkcij. Kibernetske vaje zato omogočajo, da se v organizacijah razvije širše razumevanje tveganj ter odgovornosti posameznih deležnikov pri obvladovanju kriznih situacij.

Ob tem imajo kibernetske vaje tudi pomembno vlogo pri oblikovanju širšega nacionalnega in mednarodnega ekosistema kibernetske odpornosti. Kibernetske grožnje namreč ne poznajo organizacijskih ali državnih meja, zato je za učinkovito obvladovanje incidentov ključna tudi izmenjava izkušenj, dobrih praks in operativnih spoznanj med različnimi organizacijami ter institucijami. Prav skozi skupne vaje se gradijo zaupanje, interoperabilnost in usklajeni postopki delovanja, kar lahko v realnih kriznih situacijah bistveno prispeva k hitrejšemu in učinkovitejšemu odzivanju na kibernetske incidente.

Na podlagi izkušenj številnih organizacij se kaže, da so kibernetske vaje eden izmed najučinkovitejših načinov za krepitev kibernetske odpornosti. Njihova vrednost ni zgolj v preverjanju tehničnih zmogljivosti, temveč predvsem v ustvarjanju skupnega razumevanja tveganj, izboljšanju sodelovanja med različnimi deležniki ter razvoju organizacijske kulture, ki daje ustrezno težo vprašanjem kibernetske varnosti.

V prihodnje bo pomen kibernetskih vaj še naraščal. Digitalizacija družbe, povečana odvisnost od informacijskih sistemov ter vse bolj sofisticirani napadi pomenijo, da morajo organizacije nenehno preverjati in nadgrajevati svojo pripravljenost. Kibernetske vaje tako postajajo ključni element celovitega pristopa k zagotavljanju kibernetske odpornosti ter pomembno orodje za pridobivanje informacij, ki omogočajo strateško načrtovanje nadaljnjega razvoja varnostnih zmogljivosti.

Prav zaradi tega v Institutu za korporativne varnostne študije, ICS-Ljubljana kibernetske vaje razumemo kot enega najpomembnejših multiplikatorjev informacij o dejanski pripravljenosti organizacij. Skozi njih organizacije pridobijo realen vpogled v svoje sposobnosti, identificirajo področja za izboljšave ter oblikujejo konkretne korake za zagotavljanje učinkovite in trajnostne kibernetske odpornosti. Z bogatimi izkušnjami pri organizaciji in izvedbi kibernetskih vaj smo v ICS-Ljubljana pripravljeni tudi v prihodnosti sooblikovati učinkovit ekosistem ustrezno odpornih organizacij. Vsi smo namreč soodgovorni za varno delovanje kibernetskega ekosistema. ■



CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

KIBERNETSKA VARNOST 24/7/356

Podjetja se soočajo z vse pogostejšimi kibernetskimi napadi, zato ni več vprašanje, ali boste napadeni, temveč kdaj.

Sodoben pristop zahteva premik od pasivnega preprečevanja kibernetskih napadov k proaktivnemu odkrivanju in takojšnjemu odzivu. Vse to izvajajo naši visoko certificirani strokovnjaki iz **Centra kibernetske varnosti in odpornosti**, ki **vse dni v letu**, spremljajo in analizirajo varnostne dogodke ter se hitro in učinkovito odzivajo na kibernetske grožnje, odkrivanju in takojšnjemu odzivu.



TelekomSlovenije
Vedno na boljše.

Telekom Slovenije, d.d., Ljubljana

17. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 18. - 19. MAJ 2026



DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI