Korporativna varnost

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

Letnik 2022, december • št. 30



Tradicionalna 14. mednarodna konferenca »Dnevi korporativne varnosti 2023«

Brdo pri Kranju, 23-24. maj 2023

Slovensko združenje korporativne varnosti vključujoča varnostna platforma prihodnosti



VAŠA 360° VARNOST 365 DNI V LETU

MODRO JE IZBRATI OPERATIVNI CENTER KIBERNETSKE VARNOSTI

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

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

telekom.si/poslovni

TelekomSlovenije

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



Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

Glavni in odgovorni urednik:
izr. prof. dr. Denis Čaleta

Trženje:
ICS-Ljubljana
info@ics-institut.si

Oblikovanje in DTP:
Robert Mostar

Tisk:
tiskano v Sloveniji

Datum izida:
december 2022

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.

Pred nami se nahaja jubilejna 30. številka revije Korporativna varnost, ki kaže na dejstvo, da je revija vsebinsko uspela in v vseh teh letih izhajanja strokovni javnosti ponudila kvalitetne vsebine, ki so ji v pomoč pri obvladovanju vedno bolj zahtevnega varnostnega okolja. Približujemo se prazničnemu času ob koncu leta, kar je vedno priložnost za analizo narejenega v tekočem letu, ki se poslavlja, in seveda priprava na zahtevne okoliščine in pričakovanja prihajajočega leta. Leto, ki se izteka nam bo strokovno ostalo v spominu kot leto, ki nam je prineslo obilo zahtevnih okoliščin, katere so od nas zahtevale maksimalno osredotočenost na tiste ključne dejavnosti potrebne za zagotavljanje neprekinjenosti delovanja naših ključnih procesov v organizacijah. Ob krizah, iz katerih smo iskali uspešno izhodno strategijo, med katerimi velja posebej izpostaviti svetovno pandemijo COVID-19, nas je že doletela nova kriza, in sicer vojna v Ukrajini, ki je čez noč potisnila pandemijo iz našega fokusa in pred nas postavila cel niz novih izzivov od političnih, varnostnih, kibernetskih, energetskih pa vse do človeških. Evropa, katere del je tudi Slovenija, se še sedaj ne more popolnoma izviti iz krča negativnih geopolitičnih in gospodarskih vplivov situacije, v katero je bila potisnjena s strani drugih velikih geopolitičnih igralcev globalnega varnostnega okolja. Ravno zaradi tega želimo v reviji vedno večjo pozornost namenjati tudi vsebinam, ki našim bralcem pomagajo razumeti širšo mednarodno okolje in v ta okvir postaviti tudi določene parcialne izzive, ki so vezani na uvajanje novih pristopov na področju korporativne varnosti. Le ti so v zadnjem obdobju vedno bolj povezani s procesi na področju kibernetske varnosti in s tem povezane pospešene digitalizacije naše družbe, izzivov, ki jih prinašajo zaposleni in seveda uvajanja novih tehnologij na vseh področjih delovanja naših organizacij. V zadnjem obdobju smo tudi s pomočjo razprav in stališč objavljenih v tej strokovni reviji prispevali k dvigu zavedanja o pomembnosti delovanja kritične infrastrukture in zagotavljanju potrebe po njenem neprekinjenem delovanju. Poleg strokovne javnosti imajo tukaj ključno mesto ravno strateški odločevalci v nacionalnem in gospodarskem okolju. Temu področju je bilo v zadnjem obdobju namenjeno zelo veliko pozornosti, kar se odraža tudi v pričujoči številki, ki prinaša intervjuje s pomembnimi strateškimi odločevalci in njihove poglede na pomen zagotavljanja nacionalne in korporativne varnosti sistemov in organizacij, katere tudi s svojim vodenjem pomembno oblikujejo to področje.

Ravno zaradi tega smo v tokratni številki revije želeli vsebinsko osvetliti dovolj širok spekter strokovnih prispevkov. V uredništvu revije upamo, da bo tudi pričujoča jubilejna številka revije v skladu z vašimi visokimi pričakovanji. Za vas se bomo skupaj trudili tudi v bodoče. Za konec nam dovolite, da vam vsi v uredništvu revije Korporativna varnost zaželimo uspešno in srečno v prihajajočem novem letu. Naj bo okolje v katerem delujemo čim bolj prizanesljivo do vseh nas.

izr. prof. dr. Denis Čaleta
Glavni urednik



INTERVJU
mag. Tatjana Bobnar, ministrica za notranje zadeve Republike Slovenije

ZA UČINKOVITOST OBVLADOVANJA VARNOSTNIH TVEGANJ JE POTREBNO DOBRO RAZUMETI DINAMIKO VARNOSTNEGA OKOLJA

5



INTERVJU
dr. Aida Kamišalić Latifić, državna sekretarka v Službi Vlade Republike Slovenije za digitalno preobrazbo

DIGITALNA PREOBRAZBA JE KLJUČEN PROCES ZA HITREJŠI DRUŽBENI RAZVOJ

10



INTERVJU
mag. Mojca Kunšek, direktorica Agencije Republike Slovenije za javnopravne evidence in storitve (AJPES)

INFORMACIJSKA VARNOST JE KLJUČNEGA POMENA ZA PREDVIDLJIVOST IN TOČNOST PODATKOV

20



INTERVJU
dr. Matjaž Eberlinc, izvršni direktor sektorja proizvodnje, Holding Slovenske elektrarne

NEPREKINJENO DELOVANJE ELEKTRO-ENERGETSKEGA SEKTORJA ŠE NIKOLI TAKO POMEMBNO

25



PRILOŽNOSTI VESOLJA ZA INDUSTRIJO IN DRUŽBO

V moderni družbi varnostnih tveganj in groženj, pa tudi priložnosti, so vsebine vezane na področje vesolja, v okviru Republike Slovenije, Evropske unije, Evropskih agencij in drugih mednarodnih aktivnosti, vedno bolj aktualne za industrijo in družbo.

36

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

INTERVJU
mag. Tatjana Bobnar, ministrica za notranje zadeve Republike Slovenije

ZA UČINKOVITOST OBVLADOVANJA VARNOSTNIH TVEGANJ JE POTREBNO DOBRO RAZUMETI DINAMIKO VARNOSTNEGA OKOLJA

Ministrstvo za notranje zadeve je tisti del nacionalno-varnostnega sistema, ki je v največjem obsegu soočen z zahtevnimi vplivi stalno se spreminjajočega varnostnega okolja. Za učinkovito obvladovanje spreminjajoče se situacije je potrebno zagotoviti ustrezno prožnost organizacije in njenih zaposlenih. O viziji razvoja in ključnih vsebinskih temah, ki stojijo pred ministrstvom za notranje zadeve smo se pogovarjali z mag. Tatjano Bobnar.

Najprej nam dovolite, da vam čestitamo ob nastopu te pomembne funkcije. Bodite tako prijazni in nam v kratkem zaupajte težiščna področja katerim boste pri vodenju ministrstva za notranje zadeve posvečali posebno pozornost?

Hvala za čestitke. S svojo najožjo ekipo smo se takoj na(po) začetku mandata lotili, v javnosti zelo izpostavljenega področja, migracij. Pripravljamo sodobno, v prihodnost usmerjeno strategijo, ki je osredotočena na varnost, integracijo, človekove pravice in zakonitost. Zavzemam se za celovito upravljanje migracij, ki z vidika policijskega dela izhaja iz načel zakonitosti, humanosti in skrbi za varnost skupnosti.

> Človek kljub tehnološko visoko razvitim informacijskim sistemom še vedno ostaja tisti element, ki v procesu obvladovanja različnih varnostnih tveganj igra ključno vlogo. S svojim delovanjem lahko bistveno vpliva na učinkovitost sistemov obvladovanja tveganj.

Ena naših prednostnih nalog je tudi učinkovita obravnava nasilja v družini, tudi v luči morebitne spremembe zakonodaje. To je področje, na katerem moramo biti kot država in družba izredno aktivni, saj se v domovih, ki bi morali biti prostor varnost, še vedno dogajajo utišane zgodbe nasilja. Če namreč okolica tolerira ravnanje nasilneža, ta svojo agresijo le še

*avtor je član Slovenskega združenja korporativne varnosti



stopnjuje. Zato je tu moje ključno sporočilo, da le prijava ustavi nasilneža. Prav tako želim učinkoviteje nasloviti vprašanje femicida, torej intimno partnerskega nasilja. Konec novembra pripravljamo strokovni posvet na to temo.

Lotili smo se nekaterih sistemskih (zakonskih) ukrepov za še bolj učinkovito delo resorja. Pred kratkim je bil v Državnem zboru sprejet Zakon o spremembah in dopolnitvah Zakona o organiziranosti in delu v policiji. Ta prinaša večjo samostojnost policijskih uprav na področju postopkov investicijskega vzdrževanja, kar bo vplivalo na večjo učinkovitost. Delovna mesta, za katera se zahteva poklic policista, bodo lahko zasedali ne le policisti z višjo strokovno izobrazbo, temveč tudi policisti z najmanj srednješolsko izobrazbo in pridobljenim certifikatom NPK policist. Vzporedno pa že pripravljamo nove spremembe - predvsem glede imenovanja generalnega direktorja policije in direktorja Nacionalnega preiskovalnega urada (NPU) ter večje avtonomije NPU. Glavni cilj je večja imunost pred političnim vplivom. Pripravljamo obsežne normativne spremembe Zakona o nalogah in pooblastilih policije. Tako nameravamo med drugim zagotoviti učinkovitejše delovanje policije pri opravljanju nalog, ki izhajajo iz njenih temeljnih zakonskih dolžnosti, in natančneje urediti posamezne mehanizme nadzora nad njenim delom, predvsem pa preprečiti tudi vpliv politike v povezavi z uporabo prisilnih sredstev.

Omeniti moram še predlog sprememb Zakona o detektivski dejavnosti. Od uveljavitve veljavnega Zakona o detektivski dejavnosti v letu 2011 v praksi se je namreč izkazalo, da nekatera pomembna vprašanja niso bila dokončno zakonsko urejena in da zakon vsebuje določene pomanjkljive rešitve. To seveda odseva pri uporabi zakona, pa tudi pri učinkovitosti delovanja detektivov, ki delujejo kot pomembno dopolnilo k zagotavljanju zasebne varnosti. V pripravi pa je sploh prvi Zakon o Inšpektoratu za notranje zadeve. Ta bo urejal načela delovanja, organizacijo, naloge in pooblastila inšpektorata, pravice ter posebnosti delovno-pravnih razmerij javnih uslužbencev inšpektorata in druga vprašanja, povezana z njegovim delovanjem. In še bi lahko naštevala.

Novi varnostni izzivi s katerimi se sooča Republika Slovenija tudi za ministrstvo za notranje zadeve predstavljajo vedno nove zahteve? Kako vi ocenjujete trenutno stanje učinkovitosti sistema, ki ga vodite?

Naše ministrstvo ima v državi ključno vlogo pri zagotavljanju notranje varnosti. Živimo v časih, ko se tveganja spreminjajo v zelo kratkem času in lahko vzniknejo praktično čez noč. Pri tem mislim *še zlasti* na tveganja, ki vplivajo na zdravje, tu je tudi bližina vojne, vojaških konfliktov ipd. Zaradi tega je svojevrstna naloga, da ves čas zagotavljamo učinkovitost sistema, ki ga vodim. To terja, da poleg ustaljenih metod dela, uvajamo tudi nove, predvsem v smeri digitalizacije. A treba je jasno povedati, Policija zagotavlja visoko stopnjo varnosti in Slovenija je ena izmed najbolj varnih držav na svetu. Zavedamo se groženj, kot so organiziran kriminal, terorizem, radikalizacija, kibernetske grožnje in podobno, a Policija stalno prilagaja taktike in metode svojega delovanja aktualnim varnostnim izzivom. Ocenjujem, da delo policije poteka učinkovito in da so varnostne razmere ugodne.

Kateri so tisti segmenti sistema notranje varnosti, ki mogoče še kličejo po določenih prenovah ali spremenjenih podlagah o pristojnostih, ki bi stanje dvignili na višji nivo učinkovitosti?

Človek kljub tehnološko visoko razvitim informacijskim sistemom še vedno ostaja tisti element, ki v procesu obvlado-

vanja različnih varnostnih tveganj igra ključno vlogo. S svojim delovanjem lahko bistveno vpliva na učinkovitost sistemov obvladovanja tveganj. Zaposleni tako tudi predstavljajo tisti najmočnejši, pa tudi najšibkejši člen v sistemu zagotavljanja notranje varnosti. Z neprekinjenim izvajanjem procesnega izobraževanja, usposabljanja in posledično dvigovanjem ravni zavedanja varnosti sebe in drugih, pa tudi varnosti organizacije, v kateri je zaposlen, se to tveganje lahko bistveno zmanjša. Poseben poudarek je torej treba dati upravljanju s človeškimi viri, s čimer se bo dvignila tudi varnostna kultura v sistemu notranje varnosti.

Čeprav je vojna v Ukrajini in energetska kriza nekoliko zasenčila migrantsko problematiko, se še vedno soočamo s povečanjem števila nelegalnih prehodov državne meje. Kje so po vaši oceni še tiste rezerve, ki bi povečale uspešnost varovanja, predvsem schengenske meje, za katero je zadolžena Republika Slovenija?

Tu je poleg klasične naloge policije – torej varovanja državne meje – izrednega pomena mednarodno sodelovanje, še zlasti v regiji. Kot veste, letos beležimo visoke številke nezakonitih prehodov meje državljanov iz tretjih držav, ki doslej niso bili del migracijskih tokov (na primer Indije, Burundija in Kube). Hitro in usklajeno delovanje več držav članic EU (sama sem pisala komisarki za notranje zadeve Ylvi Johansson in opozorila na nujnost uskladitve vizumskih režimov držav Zahodnega Balkana z EU) in Komisije je že prineslo konkretne rezultate, in sicer je Srbija nedavno ukinila brez vizumski režim za državljane Burundija in Tunizije. Na mednarodni ravni se seveda posvečamo tudi vprašanju vračanja nezakonito prebivajočih državljanov tretjih držav.

Policiji pomagajo pripadniki Slovenske vojske in pomožni policisti. Poleg tega uporabljajo tehnično opremo, kot so helikopterji, droni, video nadzorne kamere, mobilne, stacionarne in ročne termo vizije, kamere za preglede podvozij ipd. Krepimo aktivnosti pri preiskovanju organiziranih kriminalnih združb, ki delujejo na področju nezakonitih migracij, kar je tudi ena od naših prioritet. Tudi tu je ključno učinkovito mednarodno sodelovanje in hitra izmenjava informacij, pomembnih za uspešne preiskave, odpiranje skupnih preiskovalnih skupnih in vzporednih preiskav s tujimi varnostnimi organi ter učinkovito koriščenje analitičnih kapacitet Europola oziroma Europolovega centra za boj proti nezakonitim migracijam.

Digitalizacija je proces, ki se mu ne bomo mogli izogniti niti na področju zagotavljanja notranje varnosti. Kako gledate na uvajanje novih tehnoloških rešitev v Ministrstvo za notranje zadeve?

V ministrstvu podpiramo digitalizacijo postopkov in procesov v državi, pri čemer je namen dvig *u*činkovitosti, lažja dostopnost do podatkov in storitev tudi za državljane ter seveda skrajšanje upravnih postopkov. Vendar morajo biti nove tehnološke storitve hkrati tudi varne. Na ravni EU se trenutno pripravljata dva predpisa na področju digitalizacije. Akt o kibernetski odpornosti bo namenjen dvigu zaščite proizvodov, Direktiva o omrežjih in informacijski varnosti pa bo namenjena dvigu zaščite omrežij in informacijskih sistemov. Oba akta sta ključna za zagotavljanje varnosti in dostopnosti podatkov in storitev.

Slovenska policija se podobno kot druge policije v EU sooča z izzivi, ki jih predstavljajo hiter razvoj in širjenje informacijskih tehnologij, spletnih aplikacij in storitev. Zaradi vse večje dostopnosti, medsebojne povezanosti in mobilnosti sodobnih informacijskih tehnologij ter prodora novih, pričakujemo veliko povečanje podatkov, ki jih bo treba ustrezno in pravočasno zavarovati, urediti in analizirati. Slednje od policije zahteva prilagoditve ne samo s tehničnega vidika, temveč tudi preskok v samem razumevanju in delovanju policije. Policija si želi iti v korak s časom. To nam v veliki meri tudi uspeva, a je vse pogojeno in povezano s finančnimi sredstvi, kar prestavlja še dodaten izziv, zlasti za majhne države in policije. Določene policijske postopke smo že povsem avtomatizirali (digitalizirali) in tako močno racionalizirali delo. Na ta način smo odpravili del administrativnega bremena, pridobljen čas pa se lahko usmeri v neposredno izvajanje nalog policije. Z okrepljeno digitalizacijo oziroma avtomatizacijo dela smo izboljšali tudi kakovost zbranih podatkov in zmanjšali stroške poslovanja. Vzpostavili smo tudi e-povezavo s tožilstvom. Podatki in dokumenti, ki so se prej pošiljali v fizični obliki, se zdaj lahko pošiljajo elektronsko. To predstavlja tudi dobro podlago za nadaljnje izboljšave. Prav tako smo na področju preiskovanja kaznivih dejanj vzpostavili e-arhiv. Prav tako je pomembna dostopnost podatkov, ki so zdaj v elektronski obliki in jih je tako lažje obdelovati in statistično prikazovati. Zlasti pri slednjem smo zahvaljujoč novim tehnološkim rešitvam naredili velik kvalitativni in kvantitativni preskok.

Kibernetska tveganja so postala del vsakdana. Kaj lahko kot strateška voditeljica naredite za krepitev struktur znotraj ministrstva za notranje zadeve, katere so zadolžene za preiskovanje in pregon kibernetskega kriminala?

Naši zaposleni sodelujejo v različnih medresorskih in mednarodnih skupinah na področju kibernetske varnosti in preprečevanja kibernetskega kriminala. Poseben poudarek dajemo izobraževanju in usposabljanju na tem področju, saj lahko le na tak način sledimo novim tehnologijam in pristopom pri kibernetski kriminaliteti. Hkrati se zavedamo, da je strokovnjake na tem področju težko dobiti in *še težje* zadržati, saj javni sektor v okviru trenutnega plačnega sistema težko konkurira zasebnemu sektorju.

Za uspešno, učinkovito in kakovostno preiskovanje sodobnih oblik kriminalitete, kamor nedvomno spadajo tudi kazniva dejanja kibernetske kriminalitete, slovenska policija redno krepi svoje zmogljivosti, tako kadrovske kot tudi materialno-tehnične.

Problematiko kibernetske kriminalitete ves čas spremljamo in se ustrezno odzivamo z usposobljenimi kadri, učinkovito komunikacijo med deležniki ter obenem predlagamo ustrezne dopolnitve oziroma spremembe zakonodaje, ki bi sledila tem trendom. Temu področju bo tudi v bodoče treba nameniti posebno pozornost, saj se kriminalne dejavnosti vse bolj selijo v kibernetski prostor, povečuje se finančna škoda, informacijske tehnologije pa se širijo skoraj na vsa področja družbe.

Veliko sledi in dokazov, ki jih policija pridobi pri obravnavi primerov kibernetske kriminalitete, vodi v različne dele oziroma države sveta, zato se izdatno poslužuje mednarodnega sodelovanja, predvsem preko Europola in Interpola.

Močan interes države je, da je infrastruktura, ki je pomembna za nemoteno delovanje države, tudi ustrezno varovana.



Torej krepitev struktur za boj proti kibernetski kriminaliteti zahteva:

- nenehno usposabljanje kadra ter posodabljanje in nabavo sodobne računalniške opreme,
- učinkovito mednarodno sodelovanje,
- učinkovito in sodobno mednarodno in državno zakonodajo,
- ustrezno kadrovsko krepitev, vzporedno z naraščanjem problematike.

Čeprav niste nosilni resor za sistemske ukrepe na področju varovanja kritične infrastrukture, je vseeno vaša vloga na različnih segmentih ključnega pomena za zagotavljanje ustreznega varnostnega okolja, kjer deluje ta kritična infrastruktura. Kako po vašem mnenju lahko še okrepimo sistemske ukrepe, da bodo zagotavljali na pro aktivnosti temelječ pristop?

Res je, Zakon o kritični infrastrukturi je v pristojnosti Ministrstva za obrambo, vendar pa predpisi s področja zasebnega varovanja, ki so v pristojnosti Ministrstva za notranje zadeve, posegajo tudi na to področje. Mi v tem delu močno sodelujemo z nosilci sektorjev pri določanju zavezancev, ki morajo organizirati varovanje. Močan interes države je, da je infrastruktura, ki je pomembna za nemoteno delovanje države, tudi ustrezno varovana. Tako je bilo v zadnjem času precej povečano število zavezancev v skladu s predpisi zasebnega varovanja, prav tako so bili tudi organizirani individualni sestanki z določenimi zavezanci, sklenjeni so bili tudi posamezni sporazumi. Tukaj govorim o individualni obravnavi oziroma odnosu med ministrstvom oziroma policijo in zavezanci. Ključen je prenos informacij, ki lahko vplivajo na varnost teh subjektov in ministrstvo ima interes pri nudenju pomoči za zagotavljanje čim višje stopnje varnosti. S tako prakso bomo tudi nadaljevali. Nekatere zakonske pristojnosti na tem področju ima tudi Inšpektorat RS za notranje zadeve, ki opravlja inšpekcijske nadzore pri pravnih subjektih, zavezancih po Uredbi o obveznem organiziranju službe varovanja.

Kje so po vašem mnenju še mogoče izboljšave in rezerve v razmerju sodelovanja organov ministrstva za notranje zadeve in segmentov korporativne varnosti v pomembnih gospodarskih organizacijah za boljše zagotavljanje varnostnih procesov delovanja pomembnih infrastrukturnih zmogljivosti?

Obdobje epidemije nam je na marsikaterem področju pokazalo na določene ranljivosti pri upravljanju državnih sistemov. Tako smo se v tem času lotili sprememb določenih pravnih podlag. Kot sem že povedala, na ravni ministrstva oziroma policije že obstajajo določeni sporazumi, predvsem z gospodarskimi subjekti, ki so pomembni za delovanje države. Nedvomno pa smo tudi na ministrstvu pripomogli k dodatni določitvi dejavnosti, da se raven varnosti dvigne. Med take subjekte spadajo npr. zdravstvene ustanove. Nadgrajevalo se bo sodelovanje na tistih področjih, kjer se bodo tveganja povečala, kot je, denimo, področje energetike.

Svojo vlogo krepi tudi Inšpektorat RS za notranje zadeve predvsem z vključevanjem policijskih strokovnjakov s področja kibernetske varnosti, nevarnih snovi in eksplozivov ter orožja v svoje delo. Sodelovanje ob izvajanju nadzorov nad javnimi prireditvami pa je že stalnica več let.

Ali lahko z nivoja ministrstva za notranje zadeve pričakujemo določene pobude, ki bi še okrepile razprave znotraj nacionalno-varnostnega sistema, predvsem pa izgradile most za diskusijo med ključnimi državnimi institucijami in civilno družbo?

Našo vlogo tu vidim predvsem s spodbujanjem raziskovalnih projektov, ki jih izvajajo razne strokovne institucije. Tako se zaključuje ciljni raziskovalni program o pritožbenih postopkih na področju zasebnega varovanja, detektivov in občinskega redarstva. V njem bodo prikazane rešitve, kako se bo na bolj sprejemljiv način varovalo človekove pravice in temeljne svoboščine. V pripravi pa je že nov raziskovalni projekt na temo priprave strategije področja zasebnega varstva, ki je tudi del sistema nacionalne varnosti.

Slovensko združenje za korporativno varnost je primer dobre prakse sodelovanja državnih, javnih in gospodarskih institucij. Kakšno je vaše mnenje o tem okolju sodelovanja in kje bi lahko našli še dodatne sinergije, ki bi krepile to platformo sodelovanja in izmenjav dobrih praks?

Predvsem bo v prihodnosti treba prilagoditi določene predpise. Kot sem omenila, je v javni obravnavi Zakon o detektivski dejavnosti, pričenja se postopek priprave Strategije zasebnega varovanja. Razvoj tehnologije v varnostnem segmentu v zadnjih letih je skokovit, uporabljen pa mora biti na zakonit način. ■

Foto: arhiv Ministrstva za notranje zadeve RS

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.

INFORMATIKA



Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

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

Vplivi kibernetskih napadov na različna področja v energetiki:

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

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

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

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

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

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

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

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

ČAS JE ZA ODLOČILEN KORAK

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

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

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

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

www.informatika.si

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*

INTERVJU
dr. Aida Kamišalić Latifić, državna sekretarka v Službi Vlade Republike Slovenije za digitalno preobrazbo

DIGITALNA PREOBRAZBA JE KLJUČEN PROCES ZA HITREJŠI DRUŽBENI RAZVOJ

Navkljub pomembnim varnostnim in energetskim izzivom trenutna vlada procesom digitalizacije družbe namenja posebno pozornost. Digitalizacije družbe brez ustreznega zagotavljanja informacijske varnosti ni možno učinkovito izpeljati v njenem polnem obsegu. Nekaj ključnih misli o izzivih, ki stojijo na tej poti, nam je zaupala dr. Aida Kamišalić Latifić.

Digitalizacija ostaja pomembna prioriteta Vlade RS in s tem tudi vašega ministrstva. Kateri so tisti ključni koraki s katerimi boste zagotavljali pospešeno uvedbo procesov digitalizacije?

Naša ekipa intenzivno dela na pripravi strategije Digitalna Slovenija, ki bo predstavila in zaobjemala ključna področja, na katerih bomo gradili digitalno preobrazbo Slovenije, določila glavne usmeritve in cilje s kazalniki. Ta ključna področja so: načrt razvoja gigabitne infrastrukture, digitalna preobrazba gospodarstva, digitalne javne storitve, digitalne kompetence in vključenost, pametna družba 5.0 in kibernetska varnost. Ob tem bo strategija naslovila tudi področje podpornega okolja, ki je izjemnega pomena za pospešeno uvedbo zastavljenih procesov digitalne preobrazbe.

Strategiji bo sledil akcijski načrt, kjer bodo zaobjeti konkretni načrtovani ukrepi po področjih. Na področju digitalne vključenosti je ena od njih npr. novela Zakona o spodbujanju digitalne vključenosti, ki je v javni obravnavi ter medresorskem usklajevanju. Pripravljamo tudi ukrepe za spodbujanje digitalne vključenosti prebivalstva v vseh starostnih skupinah (osnovnošolci, srednješolci, mladi, starejše osebe, invalidi, idr.).

Načrt razvoja gigabitne infrastrukture do leta 2030, sprejet na vladi avgusta letos, predstavlja strateški dokument Republike Slovenije za vzpostavitev – delno pa tudi za spodbujanje uporabe – infrastrukture, ki bo omogočala gigabitno povezljivost vseh slovenskih gospodinjstev ter glavnih spodbujevalcev socialno-ekonomskega razvoja, obenem pa tudi neprekinjeno pokritost z omrežjem 5G vseh naseljenih območij ter glavnih prizemnih prometnih poti. Načrt je v celoti usklajen s temeljnimi digitalnimi cilji Evropske unije na področju povezljivosti. Kot enega izmed ključnih vmesnih ciljev, ki morajo biti izpolnjeni do leta 2025, načrt predvideva zagotovitev dostopa do internetne povezljivosti s hitrostjo najmanj 100 Mb/s za vsa slovenska gospodinjstva, ki se lahko nadgradi v gigabitno hitrost. Načrt vključuje cilje in potrebne ukrepe na področju razvoja gigabitne infrastrukture, da se Slovenija do leta 2030

Pričakujemo, da bo večji poudarek tudi na področju kibernetske varnosti, ki je za digitalno preobrazbo družbe in prebivalstva zelo pomembna (na vseh ravneh od osnovnošolcev do starejših oseb). Varnost v digitalni družbi bo zagotovo determinirala hitrost načrtovanja ter uvajanja digitalizacije v različne segmente vsakdanjega življenja.

*avtorica je članica Slovenskega združenja korporativne varnosti

uvrsti med digitalno najbolj napredne države in da se zagotovi gigabitna povezljivost za vsa gospodinjstva na podeželju in v mestih ter pokritost z omrežjem 5G za vsa naseljena območja.

Zagotavljanje digitalizirane družbe je stalno razvijajoči se proces, ki mu je nemogoče določiti končno stanje. Posebej v tem delu je pomembno zagotoviti spremembo miselnega okvirja, da je digitalizacija ključen proces za nadaljnji razvoj družbe. Kako nameravate zagotoviti hitrejšo transformacijo te zahteve v učne vsebine na vseh ravneh šolanja in izobraževanja?

Učni načrti so v pristojnosti Ministrstva za izobraževanje, znanost in šport (MIZŠ). Z njimi sicer uspešno sodelujemo in se pogovarjamo tudi o tem, kaj bi bilo potrebno spremeniti v učnih načrtih. MIZŠ je torej pristojen za formalne oblike izobraževanja, za neformalno izobraževanje pa bomo na Službi vlade za digitalno preobrazbo (SDP) izvajali različne lastne ukrepe (npr. sofinanciranje delavnic za OŠ, SŠ, sofinanciranje usposabljanj za starejše osebe, sofinanciranje različnih programov, ki jih imamo predvidene, vzpostavitev računalniškega sklada, ipd.), poleg tega pa želimo s spremembo zakonske podlage (ZSDV) aktivneje in celoviteje vključiti nevladne deležnike ter vse ostale, ki že danes prispevajo k digitalni transformaciji.

V vseh sferah družbe se srečujemo s pomanjkanjem strokovnjakov s področja informacijsko komunikacijskih tehnologij. Zato bomo morali začeti z aktivnostmi prekvalifikacij in z dodatnimi izobraževanji zaposlenih v javnem sektorju.

Organizacijsko nameravate v naslednjem obdobju izvesti določne spremembe. V okvir vašega ministrstva naj bi se vključil tudi Urad RS za informacijsko varnost. Katere sinergijske učinke pričakujete s temi organizacijskimi spremembami?

Pričakujemo, da bo večji poudarek tudi na področju kibernetske varnosti, ki je za digitalno preobrazbo družbe in prebivalstva zelo pomembna (na vseh ravneh od osnovnošolcev do starejših oseb). Varnost v digitalni družbi bo zagotovo determinirala hitrost načrtovanja ter uvajanja digitalizacije v različne segmente vsakdanjega življenja. Z organizacijskimi spremembami, ki se obetajo, pričakujemo številne sinergijske, predvsem pa multiplikativne učinke, saj je digitalizacija interdisciplinaren proces, ki posega v vsa področja človekovega delovanja. To pomeni, da je sinergij ogromno. Poleg učinkovitejše komunikacije in hitrejšega prenosa znanj pričakujemo tudi učinkovitejše soočanje z izzivi in nevarnostmi, ki jih proces digitalizacije prinaša. Našli bomo tudi ustrezne rešitve in temu primerno nadgradili tudi vidik informacijske varnosti v javni upravi.



Predvsem je pri kritični infrastrukturi pomembna zanesljivost digitalnih rešitev, zrelost tehnologij in zaupanje v dobavitelje rešitev.

Za hitrejše uvajanje digitalizacije bo potrebno zagotoviti dodatna finančna sredstva. Bo možno v teh kriznih razmerah računati na to, da bomo vseeno zagotovili določen obseg sredstev za pospešitev razvojnih momentov na tem pomembnem področju?

Nekaj sredstev imamo za te namene načrtovanih tudi na evropskem nivoju. Program je bil že potrjen s strani Vlade RS, trenutno pa je v potrjevanju še pri Evropski komisiji. Kar pa zadeva proračunska sredstva, pa se to ureja z Zakonom o izvrševanju proračuna, ki je sprejet za nadaljnji dve leti in potem še z rebalansi, v kolikor do tega pride. Naša Vlada ima vsekakor strateški interes, da zagotovi določen obseg sredstev za digitalno preobrazbo, a zavedati se je treba, da je digitalizacija tek na dolge proge, kar pomeni, da to ni samo strateško-razvojna prioriteta naše Vlade, temveč celotne družbe, ki se bo v prihajajočih desetletjih soočala z rezultati sodelovanja različnih deležnikov v tem desetletju.

Ko govorimo o povečanju obsega digitalizacije družbenih procesov nikakor ne moremo mimo učinkovitega zagotavljanja informacijske varnosti. Kako nameravate zagotavljati, da bo razvoj na področju digitaliziranih rešitev skladen z zahtevami informacijske varnosti?

Kot ste že sami napisali, je primarni fokus na razvoj digitalnih rešitev v skladu z zahtevami informacijske varnosti, ki jo opredeljujejo različne nacionalne in supranacionalne ureditve. Digitalne rešitve morajo že danes ustrezati določenim varnostnim standardom, in to se bo v prihodnje samo še povečevalo in krepilo. Področje informacijske varnosti je sicer v pristojnosti Urada za informacijsko varnost (URSIV), s katerim redno sodelujemo, saj gre za področja, ki so med seboj tesno povezana. Kot že omenjeno, bomo v sodelovanju z URSIV to področje informacijske varnosti zaobjeli tudi v strategiji Digitalna Slovenija 2030.



Ključen bo uspešen in učinkovit prenos evropskih uredb na tem področju v slovenski pravni red, ozaveščanje o varni in trajnostni uporabi interneta ter digitalnih rešitev, vse skupaj pa se seveda začne z ustreznimi digitalnimi kompetencami, s katerimi je mogoče še najbolj vplivati na stanje informacijske varnosti. Najšibkejši člen v t.i. »digitalni varnostni verigi« je namreč človek.

Posebej organizacije, ki upravljajo s kritično infrastrukturo so pri uvajanju na digitalizaciji temelječih rešitev bolj konservativne. V teh primerih bo verjetno potrebno zelo tankočutno ocenjevati kam in do katerega nivoja je še smotrno uvajati take rešitve?

Predvsem je pri kritični infrastrukturi pomembna zanesljivost digitalnih rešitev, zrelost tehnologij in zaupanje v dobavitelje rešitev. Ker so podatki praktično center digitalne ekonomije in avtomatiziranih digitalnih rešitev, bo treba rekonceptualizirati internet kot tak, saj je praktično nemogoče zagotoviti popolno varnost digitalnih sistemov kritične infrastrukture zaradi same narave »eksoskeletona« interneta, ki je bil primarno narejen s ciljem učinkovitosti, torej hitrosti in ne varnosti.

Kje so po vašem mnenju še določene priložnosti pri večji usklajenosti izvajanja ukrepov med javnim in gospodarskim sektorjem?

Priložnosti so predvsem v (še) večjem povezovanju javnega in gospodarskega sektorja, bodisi na področju uvajanja novih tehnologij, kot tudi izvajanja usposabljanj, ki pripomorejo k večji digitalni pismenosti. Priložnosti so tudi pri prenosu dobrih praks med obema sektorjema, ter in nenazadnje pri izkoriščanju potenciala za iskanje inovativnih (digitalnih) rešitev med obema njima. Takšno sodelovanje bomo spodbujali, saj imamo tudi že predvideno financiranje ukrepov za podporno okolje, ki bo omogočilo prenos znanj in tehnologij v gospodarstvo.

Raziskave in razvoj so lahko pomemben razvojni moment za področje digitalizacije. Boste v svoji



strategiji namenili pozornost tudi določenim aktivnostim za podporo slovenskim raziskovalnim institucijam, ki konkurirajo na zahtevnih mednarodnih razpisih?

V preteklosti je Direktorat za informacijsko družbo že podpiral RRI aktivnosti, kjer je povezoval raziskovalni, akademski svet z gospodarstvom. Iz tega naslova je bilo ustvarjenih precej uspešnih konzorcijev, ki so pripeljali do novih rešitev. Naša naloga je vsekakor prenašanje informacij z nivoja Evropske unije na nacionalno raven ter s tem odigrati povezovalno nalogo tako na nacionalnem kot mednarodnem nivoju. Strategija bo naslavljala tudi oblikovanje podpornega okolja, ki bo namenjeno tudi tovrstnim aktivnostim.

Kako lahko po vašem mnenju civilno družbene organizacije pripomorejo k učinkovitejši stopnji zavedanja o pomenu digitalizacije družbe?

Kot država imamo odgovornost in nalogo, da poiščemo sistemske rešitve tudi v sodelovanju z NVO-ji. V SDP uspešno sodelujemo z nevladnim sektorjem. Z njimi izvajamo tako delavnice, kot tudi različne posvete in okrogle mize. V načrtu imamo tudi objave javnih razpisov, ki bodo namenjeni NVO sektorju; pomagamo pa jim že na primer, pri najemu prostorov za njihovo delovanje. Civilno družbene organizacije so ključne pri učinkovitem ozaveščanju ter promociji o vlogi ter pomenu digitalizacije v sodobni družbi, so tisti, ki zagovarjajo t.i. »tretjo pot« - v človeka usmerjeno digitalizacijo. Naš cilj je nuditi civilno družbenim organizacijam vso možno podporo pri spodbujanju digitalne vključenosti prebivalstva.

Slovensko združenje za korporativno varnost predstavlja pomembno asociacijo za dvigovanje varnostnega zavedanja v širši družbeni skupnosti. Lahko v prihodnje pričakujemo tesnejše sodelovanje in določene skupne korake pri iskanju dodatnih možnosti hitrejšega in varnega uvajanja digitalnih rešitev v širše družbeno okolje?

Seveda, na Službi Vlade RS za digitalno preobrazbo smo vedno pripravljeni sodelovati, saj v sodelovanju vidimo pot naprej – v vključujočo, digitalno, trajnostno in konkurenčno družbo. ■

Foto: arhiv Službe Vlade RS za digitalno preobrazbo

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

Članstvo v združenju je prostovoljno. Združenje ima redne, korporacijske in častne člane.

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

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

www.ics-institut.si

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



KOLUMNA

KRIZA JE POSTALA REALNOST NAŠEGA OPERATIVNEGA OKOLJA

Krizne situacije, ki jih pred naše organizacije postavlja moderno varnostno okolje, so postale stalnica, ki od nas zahtevajo pomembne spremembe v konceptih dojemanja prioritet. Zagotavljanje neprekinjenega delovanja organizacij ni več hipotetična predispozicija, temveč resen izziv s katerim se strateška vodstva v organizacijah spoprijemajo na dnevni ravni.

Če smo v bližnji preteklosti krize merili v časovnih amplitudah, v razmerju pet do deset let, so zadnja tri leta prinesla popoln preobrat v dojemanju krize in seveda potrebni hitrosti prilagajanja nenehno se spreminjajočim dejavnikom varnostnega okolja. Pandemija COVID-19, vojna v Ukrajini, strateško preurejanje globalnega varnostnega okolja, nelegalni migracijski tokovi in podnebne spremembe z zahtevnimi vplivi na človeštvo, so samo nekatere trenutno najbolj izpostavljene. Marsikatera organizacija je to krizno pospešitev pričakala nepripravljena. Ni bilo malo primerov, ki so pripeljali tudi do prenehanja njihovega delovanja. Težave s prilagajanjem na dinamiko kriznih sprememb so imele tudi organizacije, katere so imele vzpostavljeno bolj robustno strukturo in so bile bolj odporne na nepričakovane vplive na delovanje in zagotavljanje njihovega osnovnega poslanstva. Tudi v teh organizacijah smo bili priča neverjetno dinamičnemu spreminjanju pomembnih konceptov zagotavljanja strateškega ocenjevanja varnostnega okolja in s tem povezanih analiz tveganj. Če so bili strateški dokumenti včasih postavljeni za okvire nekajletnega razvoja oz. ocenjevanja srednjeročnega razvoja vplivnih dejavnikov mednarodnega varnostnega okolja, smo danes priča hitremu spreminjanju in sprejemanju strategij. Omenjeno stanje od nas zahteva ustrezno dinamičnost in prožnost, ki omogoča, da strateškemu vodstvu zagotavljamo ustrezne podlage za sprejemanje potrebnih odločitev. Pomanjkanje ustreznih kadrovskih virov oz. strokovnih profilov, ki bodo s svojim kompetenčnim okvirom sposobni zagotavljati to dinamiko, je že sedaj močno izpostavljeno, v prihodnosti pa bo še bolj izrazito.

Na tem mestu si velja postaviti vprašanje, kako se tem spremenjenim globalnim varnostnim izzivom prilagaja korporativna varnost kot dejavnost, ki v organizaciji zagotavlja ključne procese za upravljanje varnostnih tveganj. Paradoksalno je vsaka kriza priložnost za racionalizacijo, iskanje boljše učinkovitosti in predvsem izpostavljanje pomembnosti procesa korporativne varnosti v razmerju do ostalih procesov v organizacijah. Generalno lahko ocenimo, da so strokovnjaki korporativne varnosti v organizacijah znali izkoristiti svoj »zvezdniški trenutek« in v kriznih časih uspeli uveljaviti svojo strokovnost in koordinacijsko sposobnost, ki je v veliko organizacijah močno olajšala soočanje s temi zahtevnimi razmerami.

Paradoksalno je vsaka kriza priložnost za racionalizacijo, iskanje boljše učinkovitosti in predvsem izpostavljanje pomembnosti procesa korporativne varnosti v razmerju do ostalih procesov v organizacijah. Generalno lahko ocenimo, da so strokovnjaki korporativne varnosti v organizacijah znali izkoristiti svoj »zvezdniški trenutek« in v kriznih časih uspeli uveljaviti svojo strokovnost in koordinacijsko sposobnost, ki je v veliko organizacijah močno olajšala soočanje s temi zahtevnimi razmerami.

*avtor je član Slovenskega združenja korporativne varnosti

učinkovitosti in predvsem izpostavljanje pomembnosti procesa korporativne varnosti v razmerju do ostalih procesov v organizacijah. Generalno lahko ocenimo, da so strokovnjaki korporativne varnosti v organizacijah znali izkoristiti svoj »zvezdniški trenutek« in v kriznih časih uspeli uveljaviti svojo strokovnost in koordinacijsko sposobnost, ki je v veliko organizacijah močno olajšala soočanje s temi zahtevnimi razmerami. Tukaj še posebej izpostavljamo organizacije, ki upravljajo kritično infrastrukturo ali izvajajo bistvene storitve, kjer so predstavniki korporativne varnosti postali nepogrešljiv člen ožjih koordinacijskih skupin, ki strateškemu vodstvu pomagajo pri izvajanju ključnih aktivnosti upravljanja in soočanja s kriznimi razmerami. V okvir procesov korporativne varnosti so se premaknili segmenti za zagotavljanje informacijske varnosti. Pomembno mesto imajo na področju analize, identifikacije in upravljanja s tveganji, zagotavljanja sistema neprekinjenosti delovanja, da sploh ne omenjamo nalog na širokem področju zagotavljanja preventivnih aktivnosti varnostnega usposabljanja in osveščanja, ob dejstvu, da je človeški potencial, kot varnostno tveganje, še vedno zelo izpostavljen. Torej je poleg tradicionalno pozicioniranih nalog zagotavljanja fizične in tehnične varnosti, korporativna varnost v svoj obseg dobila dodatna zahtevna področja, ki so seveda nujna, če želimo upravljanje s tveganji in zagotavljanje korporativne varnosti gledati s stališča celovitosti in učinkovitosti. Skozi primere, ki smo jim bili priča v času pandemije, kjer je korporativna varnost na sebe prevzela velik del koordinacijskih aktivnosti pri neposrednem zagotavljanju in uveljavljanju pravil delovanja v teh zahtevnih razmerah, lahko vidimo, da je naravna evolucija delovanja v krizi, v ospredje potisnila tiste organizacijske procese, ki jim v preteklosti ni bilo namenjeno dovolj potrebne pozornosti.

V tem kontekstu je potrebno izpostaviti nekaj pomembnih dejavnikov, ki bodo imeli močan vpliv na smer in hitrost razvoja dejavnosti v okviru korporativne varnosti. Prvi in najpomembnejši je seveda kadrovski vidik, ki bo zahteval zagotavljanje ustreznega števila strokovnih kadrov s potrebnim kompetenčnim modelom znanj. To bo zahtevna zgodba, saj ni odvisna samo od dejavnosti same, temveč zahteva izreden koordinacijski napor med izobraževalnim sektorjem pri razumevanju potreb in hitrejši dinamiki prilagajanja izobraževalnih programov ter potrebnih virov za podporo izobraževalnega procesa in realnim sektorjem, kjer bo dovolj hiter prenos uporabniških zahtev in seveda vključevanja v izvedbo tistih delov izobraževalnih programov, ki so povezani z integracijo teoretičnega okvirja znanja s praktičnimi izkušnjami in dobrimi praksami. Na podlagi trenutne analize vseh raziskovalnih programov, katero smo izvedli v Institutu za korporativne varnostne študije, na žalost ugotavljamo, da v Sloveniji nimamo niti enega ustreznega programa, ki bi zagotavljal ustrezen kader na področju informacijske ali ožje kibernetske varnosti. To stanje je zelo podobno tudi na ostalih področjih, ki so integrirani v dejavnosti korporativne varnosti. Torej predpostavke na tem področju kažejo na zelo zahtevno stanje s katerim smo v realnem sektorju organizacij javnega in zasebnega okolja že soočeni. Na žalost samo prehod kadrov iz inštitucij nacionalne varnosti, ki so že same močno podhranjene, v gospodarstvu ne bo rešil težav, ki nastajajo na tem področju. Kader, ki prehaja ima pomemben deficit potrebnih znanj, ki ga je potrebno skozi procese dopolnilnih izobraževanj ustrezno nadgraditi. Zagotovo se bo potrebno problema lotiti čisto na začetku, da mladim predstavimo zanimivosti, potenciale in priložnosti na tem področju. Trenutno se nam zdi nepredstavljivo, da ob velikem pomanjkanju izobraženih strokovnjakov na področju informatike, ostaja ogromno mest, ki so na izobraževalnih institucijah nezasedeni. Vsekakor pa si bo morala tudi država s svojimi institucijami resno nastaviti ogledalo in si odgovoriti, katere programe in smeri študija bo skozi koncesioniran model še naprej podpirala. Na žalost smo v tem trenutku na napačni poti oz. ne vidimo jasne strateške poti, ki je potrebna za zagotovitev tistih profilov, ki jih realni sek-





tor nujno potrebuje. Drug pomemben izziv pa je strokovne narave in je povezan tudi s povečanim vplivom vsakokratne politike tudi na področje ključnih funkcij v okviru korporativne varnosti. Povečevanje pomena korporativne varnosti in seveda njeno ustrezno pozicioniranje na strateškem nivoju v neposredni bližini strateškega nivoja vodenja, je ta proces in ta delovna mesta javno bolj izpostavil. To pomeni, da smo bili v zadnjih treh letih priča pogostemu menjavanju strateških vodstev v podjetjih, tudi tistih, ki upravljajo s kritično infrastrukturo, kar je imelo za posledico tudi menjavanje strateškega vodstva v korporativni varnosti. To je izredno nevaren proces, ki za seboj potegne še dodatno kadrovsko siromašenje te dejavnosti, ki je že tako in tako kadrovsko podhranjena. V tem okviru moramo narediti vse, da se zavedanje o nevarnosti tega početja zasidra v glavah odločevalcev, ki morajo razumeti kako pomemben je učinkovito delujoč sistem korporativne varnosti za organizacije, ki jih vodijo, oziroma na drugi strani, kakšno veliko nevarnost sami na koncu sprejemajo na svoja pleča v primeru postavitve nekompetentnih oseb na ta ključna delovna mesta.

Za konec bi veljalo izpostaviti procese sodelovanja tako znotraj organizacije kakor tudi zunaj nje. Notranje sodelovanje je pomembno ustrezno procesno opredeliti tako, da se preprečuje grajenje nepotrebnih zidov med ključnimi procesnimi funkcijami in nivoji znotraj organizacije. Za vsako ceno je potrebno preprečiti silosni pristop, ki troši dodatne vire, upočasnjuje delovanje in organizacijo dela manj fleksibilno na potrebno hitro odzivanje v času kriznih situacij. Naslednja raven sodelovanja pa je vsekakor med-organizacijska raven, ki jo lahko vidimo kot raven sodelovanja na nivoju posameznih sektorjev ali grozdov organizacij ali pa sodelovanje na relaciji javno-zasebnega sodelovanja. Vsi vidiki tega sodelovanja so ključni za to, da so se sposobni vsi organizacijski deli te družbe pravočasno in dinamično odzivati na zahteve, ki jih pred nas postavljajo kompleksne krize. V analizi, ki smo jo izvedli glede izkušenj strateškega odzivanja na krize, je bilo možno ugotoviti, da je bilo s strani države narejenih kar nekaj pomembnih napak pri strateškem komuniciranju in vodenju kompleksnih kriz, kar je potrebno v prihodnosti odpraviti. Zanimive ugotovitve so bile, da so zaposleni v organizacijah bolj zaupali odločitvam svojih vodstev, kakor sprejemali ukrepe s strani države. Vsekakor pa imamo v tem pogledu tudi pozitivne primere dobre prakse, ki se odražajo predvsem v tesnem sodelovanju med javnimi in zasebnimi organizacijami znotraj Slovenskega združenja korporativne varnosti. O pomembnosti tega sodelovanja priča tudi vedno več javnih organizacij, ki se priključuje omenjeni asociaciji. Ta akumulacija znanj, izkušenj in predvsem grajenja zaupanja, je potrebno, da se v kriznih situacijah časovna dimenzija komuniciranja in raven sodelovanja močno povečata, kar pomembno vpliva na iskanje učinkovitih odzivov na krizo.

Za konec lahko ocenimo, da je dinamika pojavljanja kriznih situacij vedno višja. Korporativna varnost, kot pomembna organizacijska dejavnost za obvladovanje tveganj, pozitivno izkorišča »priložnosti«, ki so jih pred nas postavile krizne situacije. Moramo pa biti vseeno pozorni na določene izzive, na nekatere smo opozorili že v prispevku. Visoko motivirani strokovnjaki s področja korporativne varnosti, ki posedujejo ustrezno kompetenčno raven znanj, so lahko garant za to, da bodo naše organizacije sposobne bolj učinkovito delovati v tem, vedno bolj zahtevnem in hitro spreminjajočem se poslovnem okolju. ■



OKREPITE VARNOST

4-dnevni tečaj

KIBERNETSKA VARNOST ICS/OT/IoT OKOLIJ

Kibernetski napadi na kritično infrastrukturo predstavljajo 5. največje globalno tveganje.

5,6 mio USD je v letu 2021 znašal povprečen strošek kibernetskega napada na kritično infrastrukturo.*

Spoznajte, kako učinkovito vzpostaviti zaščito pred zlorabami in kibernetskimi napadi, da zagotovite neprekinjeno delovanje kritične infrastrukture in industrijskih okolij.

Skenirajte za prenos programa

https://bit.ly/program-OT

info@smart-com.si

01 561 16 06

*Vir: Guidehouse Insights Cyber Insurance for Energy Industry

SMART COM

Zanesljiv, tehnološko napreden partner za kibernetsko varnost, informacijsko-komunikacijska omrežja in podatkovne centre.

UDEJANJAMO VAŠE VIZIJE
www.smart-com.si

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

INTERVJU
mag. Mojca Kunšek, direktorica Agencije Republike Slovenije za javnopravne evidence in storitve (AJPES)*

INFORMACIJSKA VARNOST JE KLJUČNEGA POMENA ZA PREDVIDLJIVOST IN TOČNOST PODATKOV

Moderna informacijska družba zahteva nove pristope tudi na področju upravljanja z javnimi evidencami podatkov, ki morajo biti dostopni različnim ciljnim uporabnikom v Republiki Sloveniji. O izzivih, ki se pojavljajo pri zagotavljanju varnosti in točnosti javnih podatkov, smo se pogovarjali z gospo Mojco Kunšek.

Spoštovana vodite izredno pomembno Agencijo Republike Slovenije za javnopravne evidence in storitve. Prosimo, če nam lahko na kratko opredelite glavna težišča vaših pristojnosti.

AJPES je osrednja nacionalna institucija na področju registracije poslovnih subjektov ter zbiranja, objavljanja in posredovanja podatkov in informacij za zagotavljanje preglednega nacionalnega in evropskega poslovnega okolja. Tako je AJPES tudi aktivno vključen v izvajanje številnih predpisov in sodeluje s številnimi resorno pristojnimi ministrstvi in drugimi državnimi organi. V okviru izvajanja nalog točk SPOT, na dvanajstih lokacijah po Sloveniji, je AJPES osrednja informativna in vstopna točka za registriranje gospodarskih subjektov, saj registrira preko 50 % vseh poslovnih subjektov v državi in je odgovoren za registracijo s.p.. Ena osrednjih nalog je tudi upravljanje Poslovnega registra Slovenije, ki se povezuje v mrežo evropskih poslovnih registrov, tako preko interesne platforme EBR, kot tudi preko platforme e-justice pri Evropski komisiji. Pristojnosti AJPES zajemajo tudi upravljanje informacijskega sistema sodnega registra, zagotavljanje rešitev, preko katerih poslovni subjekti in sodišča objavljajo podatke in dokumente na spletnem portalu AJPES, zbiranje in javna objava letnih poročil družb in podjetnikov, ter vodenje prekrškovnih postopkov ob opustitvi predložitve. AJPES je zadolžen tudi za zbiranje vrste drugih informacij in vodenje drugih registrov, ki povečujejo varnost v pravnem prometu poslovnih subjektov ali na drug način pripomorejo k preglednemu poslovnemu okolju, ter hkrati omogočajo učinkovito poslovanje poslovnih subjektov in institucij javne uprave. Tržne storitve AJPES obsegajo zlasti izdelavo bonitetnih informacij, izvajanje večstranskega pobota medsebojnih obveznosti poslovnih subjektov in zagotavljanje podjetniško usmerjenih orodij in informacij.

V AJPES si prizadevamo narediti največ, kar je trenutno glede na razmere mogoče, da zagotavljamo varnost in neprekinjenost poslovanja za izvajanje poslovnih procesov javne službe.

Ključni del vašega delovanja zajema predvidljivost in točnost podatkov, ki jih zagotavljate za različni se-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



gment končnih uporabnikov. Kako vplivajo vedno močnejši procesi digitalizacije in informatizacije na vašo organizacijo?

AJPES je digitalno dokaj napredna institucija. Krajevno pristojnost izpostav smo namreč odpravili že pred 10 leti, s čemer poslovne primere, ne glede na lokalni izvor, lahko rešuje katerakoli izmed izpostav v 12 regijah. Prav tako omogočamo uporabnikom dostopnost do podatkov preko 10 spletnih servisov ter zagotavljamo pravno varnost s predhodnim preverjanjem potencialnih podjetnikov z interoperabilnostjo spletnih mest v državi (FURS, MNZ, IRSD, MRVL). Prav tako tudi sledimo tehnologijam in trendom digitalizacije in informatizacije ter skušamo zagotoviti ustrezna investicijska sredstva za stabilno informacijsko infrastrukturo in informacijske sisteme ter izvedbe projektov državnega pomena s pogodbenimi partnerji.

Kako močno na to področje vplivajo spremembe, ki se dogajajo na področju evropskih in posledično nacionalnih podlag za varovanje osebnih podatkov?

Pri AJPES se pomena varovanja osebnih podatkov zavedamo še iz časov pred Splošno uredbo o varstvu podatkov (v nadaljevanju GDPR), zato z njenim sprejemom ni bilo posebnih presenečenj. Seveda smo morali imenovati pooblaščeno osebo za varstvo osebnih podatkov, ki je pri nas zunanja, in prilagoditi katerega izmed procesov; kljub temu pa tu do sedaj ni bilo kakih večjih pretresov. Več izzivov smo imeli z nacionalno zakonodajo npr. z zadnjo spremembo Zakona o gospodarskih družbah (ZGD-1), saj smo zaradi zavezujoče objave e-poštnih naslovov pravnih subjektov, med katerimi so tudi naslovi posameznikov, zaznali več nejevolje med našimi podjetji in samostojnimi podjetniki, pa še to predvsem zaradi povečane količine neželene e-pošte. Ob sprejemu GDPR smo na tržnem delu dejavnosti AJPES vpeljali nove rešitve za področje neposrednega trženja storitev, na javnem delu pa uredili ustrezne pravne podlage ter prilagodili procesno dokumentacijo za zagotavljanje zakonite obdelave osebnih podatkov, ki jih ima AJPES v upravljanju. Prilagoditev poslovanja v skladu z zahtevanimi standardi in normativno regulacijo z GDPR je nedvomno pomenila določene spremembe v poslovnih procesih, v katerih se podatki obdelujejo, saj smo jih morali prilagoditi tako iz tehničnega kot tudi iz procesnega vidika.

Z uvajanjem novih tehnologij je tesno povezano tudi spreminjanje organizacijske kulture organizacije. Kako uspete zagotavljati to transformacijo pri zaposlenih v Agenciji?

V AJPES zagovarjamo načelo vseživljenjskega učenja, saj le strokovno dovolj kompetentni zaposleni lahko suvereno izvajajo storitve. Koncept vseživljenjskega učenja širimo ne le na vsebinska področja, temveč tudi v zagotavljanje ustreznega nivoja digitalnih kompetenc ob vsesplošnem zagotavljanju varnosti. Visok nivo digitalnih kompetenc, zavzemanje za neprekinjeno poslovanje in povezanost med zaposlenimi, ne glede na mesto opravljanja dela, pa je bila tudi ena ključnih prednosti pri hitrem prehodu na delo od doma tudi ob pojavu epidemije v marcu 2020, tako da so lahko nadaljevali z enakim tempom in obsegom dela na daljavo z uporabo sodobnih komunikacijskih naprav kot v času pred epidemijo.

Čeprav se AJPES srečuje tudi s kadrovskimi izzivi, kot je težje nadomeščanje odhodov v pokoj kot tudi pridobivanje kadrov, pa skuša novo zaposlene sodelavce z mentorskim pristopom čim prej usposobiti za samostojno opravljanje dela ob poznavanju konteksta delovanja agencije. Ob omejenih mož-

nostih nagrajevanja zaposlenih v javnem sektorju pa skuša vendarle prepoznavati tudi najboljše kadre. Svoje zavzemanje za dobro organizacijsko energijo pa AJPES izkazuje tudi s prejemom certifikata v okviru projekta Nacionalno merjenje organizacijske energije v letih 2021 in 2022.

Novi varnostni izzivi med katerimi so najbolj izpostavljena ravno kibernetska tveganja vplivajo na delovanje vseh organizacij. Verjetno se tem izzivom težko izogibate tudi pri delovanju vaše organizacije. Kako pomembno mesto namenjate razvoju tega področja?

Skladno s strateško usmeritvijo AJPES – nuditi napredne informacijske rešitve z visoko stopnjo razpoložljivosti – je kot strateški cilj AJPES opredeljeno tudi zagotavljanje varnosti, zaupnosti, celovitosti in razpoložljivosti informacijskega sistema ter zagotavljanje neprekinjenega delovanja ključnih poslovnih procesov v primeru izrednih dogodkov. Na področju informacijske varnosti AJPES sledi strateškim usmeritvam države, Nacionalni strategiji kibernetske varnosti in usklajuje svoje delovanje z Zakonom o informacijski varnosti in Uredbo o informacijski varnosti v državni upravi. Prav tako pa AJPES zaradi globalne situacije na področju kibernetske varnosti izvaja tudi priporočila pristojnih institucij za izvedbo ukrepov za zagotovitev visoke stopnje varnosti omrežij in informacijskih sistemov, za kar ima oblikovano tudi posebno delovno skupino za zagotavljanje ustreznih varnostnih politik ter obravnavo morebitnih varnostnih incidentov, v katerih delujejo vsi ključni deležniki, od pravne službe, preko IT, informacijske varnosti in neprekinjenega poslovanja, do pooblaščene osebe za varstvo osebnih podatkov, ki poročajo direktno meni oz. moji namestnici.



Prav tako pa se izvajajo tudi kontinuirana izobraževanja, ki združujejo tako kibernetska tveganja, varovanje informacij, varstvo osebnih podatkov, kot tudi s področja neprekinjenega poslovanja. Zavedamo se namreč, da je kibernetska tveganja mogoče zmanjšati samo s celostnim pristopom.

Dodatno izobraževanje in usposabljanje je verjetno postala stalnica modernega organizacijskega delovanja. Ali vašim zaposlenim namenjate tudi izobraževanja in usposabljanja iz varnostnih vsebin, ki so pomembna za dvigovanje varnostnega zavedanja?

AJPES za zaposlene obdobno organizira tudi izobraževanja in usposabljanja iz varnostnih vsebin, predvsem s ciljem ustreznega informiranja ter pravočasnega zaznavanja in prepoznavanja morebitnih varnostnih groženj. V AJPES se zavedamo, da je pomembne cilje mogoče izvajati le s kompetentnimi in predvsem motivirani kadri v zdravem delovnem okolju. Zato si AJPES prizadeva za stalno in redno strokovno usposabljanje in izpopolnjevanje zaposlenih, pravočasno in učinkovito vključevanje novih nalog v poslovne procese in izboljševanje kakovosti izvajanja storitev. Prav tako AJPES spodbuja tudi redni interni prenos znanja, veščin, vrednot in primerov dobrih praks med zaposlenimi tudi preko internega sistema e-izobraževanj, ki jih pripravljajo zaposleni. Izboljšanje varnostnega zavedanja pa izboljšuje tudi z rednim testiranjem odziva zaposlenih za primere različnih varnostnih incidentov v različnih organizacijskih enotah, ki se izvaja enkrat letno. V kratkem pripravljamo še preverjanje, pri katerem bomo način izvedbe usmerili predvsem v zaznavanje ribarjenja (phishinga). Zavedamo se, da je tako preverjanje za naše zaposlene lahko stres, zato gledamo dolgoročno in se predvsem trudimo poudarjati dobre odzive.

Kje kot strateška voditeljica javne organizacije vidite glavne varnostne izzive za nemoteno delovanje zakonitega, strokovnega, preglednega in družbeno odgovornega poslovanja vaše organizacije?

V AJPES si prizadevamo narediti največ, kar je trenutno glede na razmere mogoče, da zagotavljamo varnost in neprekinjenost poslovanja za izvajanje poslovnih procesov javne službe. V AJPES imamo vzpostavljen register tveganja, da zagotavljamo obvladljivost prepoznavnih dejavnikov tveganja v organi-



zaciji. Kot strateška voditeljica javne organizacije menim, da je za obvladovanje varnostnih izzivov nujno nadaljevanje digitalne transformacije v organizaciji s stalnim izobraževanjem in informiranjem zaposlenih, rednim prenosom znanja, usposabljanjem naslednikov ter predvsem s skrbnim in rednim posodabljanjem informacijske infrastrukture. Pri vzdrževanju varnostnih procesov AJPES aktivno sodeluje z zunanjimi strokovnjaki na področju zagotavljanja kibernetske varnosti in sledi novim praksam na tem področju.

Z dvigovanjem varnostnih standardov včasih trčimo na drugi strani v željo po čim hitrejšem in čim lažjem dostopu do določenih javnih podatkov. Imate kakšne izkušnje z odzivom vaših uporabnikov, ker bi jih določeni dodatni varnostni koraki motili pri dostopanju do teh evidenc?

Ugotavljamo, da se najdejo uporabniki, ki jim je nadležno dostopanje do javnih podatkov za kakršnim koli t.i. „zidom“. Marsikdo bi najraje videl, da je vse javno objavljeno dostopno brez registracije oz. prijave. Menimo, da je najmanj problematičen (ter najmanj nadležen) dostop s predhodno registracijo oz. prijavo uporabnika. Dostopa s KDP (kvalificiranim digitalnim potrdilom, certifikatom) ali z uporabo državne centralne storitve SI-PASS pa za uporabnike predstavljata več nevšečnosti. Dostop s SI-PASS je kar kompliciran za povprečnega uporabnika, vendar je prednost, da tak dostop lahko uporabnik kreira sam. Dostop s KDP pa povzroča nevšečnosti predvsem takrat, ko mora certifikat uporabnik pridobiti na ustrezen način (SIGEN-CA traja vsaj 10 dni, Halcom in drugi pa so tudi plačljivi). Občasno, npr. ob zadnjih zakonskih spremememba z obveznostjo e-naslovov pa smo naleteli tudi na negativni odziv zgolj z vidika realiziranja zakonskih zahtev, ki včasih uporabnikom niso logične in svoje nezadovoljstvo žal usmerijo na tehnične rešitve pri AJPES.

Vaša organizacija ima vzpostavljen in vpeljan standard kakovosti ISO 9001. Ste mogoče razmišljali tudi o kakšnem koraku uvajanja standarda ISO 27001 na področju informacijske varnosti?

AJPES uporablja dobre prakse standardov iz družine ISO/IEC 27001, prav tako pa ima AJPES že vzpostavljen sistem obravnave neprekinjenega poslovanja. Razmišljamo pa tudi o uvedbi ISO 27001, saj smo omejeni s kadrovskimi viri, predvsem na področju zagotavljanja primerno izurjenega osebja.

Slovensko združenje za korporativno varnost je primer dobre prakse sodelovanja državnih, javnih in gospodarskih institucij. Lahko v prihodnosti pričakujemo, da se boste tesneje povezali z delovanjem omenjenega združenja in tako skozi to pomembno mrežo zagotavljali izmenjavo dobrih praks, izkušenj in novih spoznanj na področju varnosti?

AJPES se zavzema za izmenjavo poslovnih praks in opolnomočenje vseh vrst uporabnikov, saj le-to prinaša enostavnejšo in varnejšo uporabo portala in podatkov. Nedvomno lahko rečemo, da smo sodelovanju naklonjeni, glede na naše zmožnosti pa bo potem odvisno v kolikšni meri ga bomo lahko tudi izvedli. ■



Actual I.T.

Energy4Mobility & Transport&Logistics

Actual I.T. je podjetje, specializirano na področju sistemske integracije na poslovnih področjih transporta in logistike, pristaniških sistemov ter upravljanja večjih oskrbnih verig.

PRO.Astec

Specialisti za storitve in rešitve na področju informacijske in kibernetske varnosti za neprekinjenost poslovanja in skladnosti.

Itelis

Specialisti za področje implementacije in integracije poslovne programske opreme SAP v različne industrije tako na lokaciji stranke, kot v oblaku.

Unistar PRO

Specialisti za IKT infrastrukturo podjetja – načrtovanje, razvoj, integracija, vzdrževanje in zunanje izvajanje IKT storitev. Storitve zagotavlja tudi v lastnem PRO.Cloud podatkovnim centrom.

ACTUAL I.T.
SKUPINA

Actual IT, d.d., Ferrarska ulica 14, 6000 Koper

ACTUAL I.T. UNISTAR PRO astec ITELIS

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
dr. Matjaž Eberlinc, izvršni direktor sektorja proizvodnje,
Holding Slovenske elektrarne*

NEPREKINJENO DELOVANJE ELEKTRO-ENERGETSKEGA SEKTORJA ŠE NIKOLI TAKO POMEMBNO

Trenutna varnostna in s tem tudi energetska kriza pred elektro-energetske sisteme postavlja pomembne zahteve za neprekinjenost delovanja. Vsaka, še tako majhna prekinitev delovanja, ima v takih razmerah lahko mnogo večji vpliv, kot bi ga imela v normalnih okoliščinah. Zaradi tega je učinkovito upravljanje teh sistemov nacionalnega pomena. O izzivih, s katerimi se soočajo v HSE, smo se pogovarjali z dr. Matjažem Eberlincem.

V HSE opravljate izredno pomembno vlogo strateške skrbi za operativno delovanje zmogljivosti HSE kot izvršni direktor proizvodnje. Nam lahko podrobneje opišete obseg svojih pristojnosti.

Ključna vloga sektorja proizvodnje HSE je povezovanje in optimizacija procesov obratovanja in vzdrževanja v družbah skupine HSE. V okviru te vloge naš sektor skrbi za ustrezno odzivanje na potrebe in pričakovanja z vidika procesov trženja na eni strani ter zmožnostim in potrebam proizvodne infrastrukture z vidika obratovanja in vzdrževanja s ciljem ohranjanja njene razpoložljivosti in zanesljivosti na drugi strani. Posebna izziva, s katerima se srečujemo pri doseganju visoke obratovalne zanesljivosti, varnosti in razpoložljivosti proizvodne infrastrukture, sta racionalna raba sredstev za potrebe vlaganj v proizvodno infrastrukturo in maksimizacija dobička iz naslova obratovanja proizvodnje. Ustrezna odgovora na postavljeni izziv tržnim razmeram sta primerna strategija obratovanja proizvodnih enot z optimalno hidro-termo koordinacijo ter enotna politika in strategija vzdrževanja proizvodne infrastrukture, ki poleg konsolidacije informacijske podpore vzdrževanju vključuje tudi širitev obsega vzdrževanja glede na stanje naprav.

Nahajamo se v zahtevnem obdobju velikih energetskih izzivov, kjer je neprekinjenost delovanja elektroenergetskega sistema ključnega pomena. HSE predstavlja izredno pomemben del proizvodne hrbtenice v Republiki Sloveniji. Kako zagotoviti, da bo v obdobju, ki je pred nami, celotna proizvodnja elektro energetskega sistema zagotovila pričakovan

Za delovanje vodenja obratovanja niso potrebne samo odlično delujoče naprave, ampak – in predvsem usposobljeni strokovni kadri, ki so jim te naprave in s tem celotno obratovanje sistema zaupane. Zaradi vse večjega števila naprav, njihove različnosti in vse manjšega števila zaposlenih se tudi v tem segmentu povečuje tveganje.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



obseg nujno potrebne količine elektrike.

Ustrezno vodena, vzdrževana, razpoložljiva in zanesljiva proizvodna infrastruktura je eden izmed pogojev za doseganje načrtovanih poslovnih rezultatov skupine HSE oziroma je poleg robnih pogojev, ki jih definirajo tržne razmere in hidrologija ter spreminjajoči se regulatorni okvirji, pomemben del enačbe. To dejstvo nalaga upravljavcem proizvodne infrastrukture posebno skrb pri načrtovanju vzdrževanja in vlaganj v proizvodno infrastrukturo kot tudi pri načinu obratovanja. Posebna skrb je nujna zaradi visoke vrednosti same infrastrukture, ki zahteva relativno visoka vlaganja. Zaradi dolgih življenjskih dob proizvodnih objektov, kar za potrebe minimizacije proizvodnih tveganj praviloma zahteva posebno skrb za ohranjanje znanj in kompetenc ter razvoj zaposlenih v skupini kot tudi skrb za zagotavljanje nasledstvenih procesov in prenosa znanj na mlajše kadre.

Operativni sistemi elektro energetike so vedno pogostejša tarča kibernetskih napadov. Kompleksnost teh sistemov je zelo zahtevna za zagotavljanje učinkovite informacijske in s tem posledično kibernetske varnosti. Kakšne so vaše usmeritve in dobre prakse pri zagotavljanju ustreznih ukrepov za neprekinjenost delovanja ključnih operativnih zmogljivosti vaših sistemov?

Ohranjanje in zagotavljanje visoke kibernetske varnosti bomo dosegali z verifikacijskimi notranjimi pregledi. Potrebno je spremljanje konfiguracijskih sprememb, s katerimi se zazna in odpravi morebitna ranljivost, izvajali pa smo in bomo tudi v prihodnje letne notranje preglede. Po pravilih dobre prakse se zunanji varnostni pregled izvaja vsaj enkrat letno ali ob večjih uvedbah novih storitev. Nadalje smo in bomo ozaveščali zaposlene o varni uporabi interneta. Ozaveščen uporabnik je bistven pri zagotavljanju celovite informacijske varnosti. Kontinuirano bomo ažurirali varnostne politike in protokole. V vsakem trenutku se je potrebno zavedati kdo, od kje in kam dostopa. Potrebno je redno posodabljanje programov v uporabi ter na relevantna mesta namestiti varnostne popravke. Uvajanje novih produktov mora biti sistematično načrtovano, predvsem s stališča informacijske varnosti, in sicer od samega začetka uvajanja novih produktov.

Učinkovita koordinacija celotnega elektro energetskega sistema Republike Slovenije je ključna za njegovo nemoteno delovanje. Glede na to, da ima HSE tukaj eno od ključnih vlog, nas zanima, kako v tej skupni koordinaciji z ostalimi deležniki elektro energetskega sistema Slovenije zagotavljate usklajene odzive na zahtevne varnostne izzive, katerim je izpostavljena ta infrastruktura?

Vlada Republike Slovenije je poleti razglasila prvo stopnjo ogroženosti na področju proizvodnje električne energije. Namen s tem sprejetih ukrepov in smernic je priprava elektro-energetskega sistema ter znotraj tega predvsem sistemskih elektrarn za zanesljivo obratovanje v času kriznih razmer. Enako je tudi s sistemskim operaterjem prenosnega omrežja ELES, kjer se tedensko usklajujemo glede obratovanja proizvodne infrastrukture skupine HSE.

Potreba po strokovnih kadrih je pereča tudi v elektro energetskih organizacijah. Kako se v HSE spopadate z izzivi pomanjkanja ustreznega operativnega kadrovskega potenciala?

Za delovanje vodenja obratovanja niso potrebne samo odlično delujoče naprave, ampak – in predvsem usposobljeni strokovni kadri, ki so jim te naprave in s tem celotno obratovanje sistema zaupane. Zaradi vse večjega števila naprav, njihove različnosti in vse manjšega števila zaposlenih se tudi v tem segmentu povečuje tveganje. Zato skupina HSE veliko pozornost posveča pravočasni usposobitvi dovolj kvalitetnih kadrov. To pomeni, da so nasledstveni procesi zelo pomembni, zahtevnejši in dolgotrajnejši. Tu je potrebno dodati, da proizvodnja poteka neprekinjeno – torej 24 dni na teden, 365 dni v letu, zato je potrebno s kadri zagotavljati kontinuiteto izvajanja aktivnosti in procesov. Usmeritve morajo dati zahteve za minimalno kadrovsko zasedbo upoštevajoč vse robne pogoje in skrajne scenarije ter rezervo za odsotnost in fluktuacijo. Obratovanje z daljinsko vodenimi objekti brez posadke zahteva izurjene ekipe, ki se šolajo več let. Te ekipe morajo biti sposobne varno obratovati tudi v izrednih razmerah. Prav tako lahko hitro ugotovimo, da se bodo zahteve v kombiniranem hidro-termo proizvodnem sistemu v prihodnosti še hitreje spreminjale in bodo morali kadri tem spremembam tudi slediti.

Pandemija COVID-19 je na pred nas postavila nove izzive na katere nismo bili v celoti pripravljeni. Posebej je bil izpostavljen izziv zagotavljanja ključnega kadra na pomembnih koordinacijskih točkah, kot so centri vodenja. S kakšnimi ukrepi ste uspeli uspešno zagotavljati, da je proces koordinacije proizvodnje električne energije nemoteno deloval?

Hkratno obvladovanje epidemije in zagotavljanje neprekinjenega obratovanja ter proizvodnje električne in toplotne energije v družbah skupine HSE je in bo v prihodnje naš izziv in skupni cilj. V skupini HSE smo se že ob začetku epidemije zavedali nevarnosti izbruha in širjenja novega koronavirusa v delovnem okolju. Zato smo nemudoma sprejeli več preventivnih in zaščitnih ukrepov za preprečevanje njegove širitve ter z njimi seznanili zaposlene, vse s ciljem njihove zaščite na eni ter nemotene proizvodnje električne energije na drugi strani. Aktivirali smo tudi ključni kader za nemoteno delovanje proizvodnih objektov in poslovanje celotne skupine. Ukrepe smo vse do danes skladno z usmeritvami države prilagajali in dopolnjevali. Lahko ugotovimo, da so bili sprejeti in izvajani ukrepi uspešni.

Uvajanje novih tehnoloških rešitev lahko pomembno pripomore k zmanjšanju izpostavljenosti kadrovskega potenciala, posebej v situacijah, kot smo jim bili priča v preteklih dveh letih. Ste v HSE naklonjeni uvajanju novih tehnologij v operativne procese vašega podjetja?

Na področju obratovanja, vzdrževanja in investicij v skupini HSE smo postavili cilje za obdobje 2022-2033. S strategijo so postavljene usmeritve za obvladovanje proizvodne infrastrukture, digitalizacije obratovanja in vzdrževanja, obvladovanje celotnega življenjskega cikla z vpeljavo BIM modela, maksimizacija utilizacije centrov vodenja in uvedba optimizacijskega programskega orodja za obratovanje proizvodnih enot ter vpeljava napovednega vzdrževanja. Na-



Verjetnost nekega dogodka ni dovolj, da bi lahko samo na tej osnovi določili tveganja in stopnjo ogroženosti ali celo oceno ogroženosti delovanja posamezne funkcionalnosti. Različna tveganja oziroma nevarnosti, ki lahko vplivajo na obratovanje, imajo namreč različne vplive tako na opremo kakor tudi na stopnjo celotne funkcionalnosti.

men vseh teh projektov je informacijsko celovito podpreti ter izboljšati procese planiranja in vodenja proizvodnje. Poudarek je na izboljšanju ekonomske iztržljivosti in na doseganju najvišje možne učinkovitosti proizvodnje, kar je seveda nujno glede na obstoječe in prihajajoče izzive proizvodnje, kot so razpršena proizvodnja in pogostejše avkcije na sistemskih storitvah. Večji izziv je bil prehod na 15-minutni časovni obračunski interval, kjer smo imeli veliko priprav, obsežnih nadgradenj in prilagoditev aplikacij ter podatkovnih tokov. Obsežna nadgradnja in prilagoditev je, to lahko potrdim, kljub okoliščinam, povezanim z epidemijo, potekala brez težav. Prehod je bil izveden v enem dnevu. Brez prave ekipe in timskega dela, to ne bi bilo izvedljivo!

Kako pomemben je za vas proces ocenjevanja varnostnih tveganj za nemotenost delovanja proizvodnih zmogljivosti v HSE? Koliko v te procese vključujete strokovnjake iz posameznih organizacijskih delov, predvsem proizvodnih enot vašega holdinga?

Zelo pomemben. Z oceno tveganj in občutljivosti želimo tveganja preslikati v nekatere usmeritve, da jih s tem zmanjšamo. Zavedamo se, da je v tako kratkem času in tudi drugače zelo težko z matematičnimi številkami izraziti verjetnost in intenzivnost nekega neželenega dogodka. Zato zmoremo le oceniti tveganja, kar pa temelji na dolgoletni statistiki, oceni nevarnosti in ogroženosti, podane s strani pristojnih inštitucij, oceni trenutnega stanja infrastrukture in korelaciji med tipom ogroženosti in konfiguracijo naprav, ki zagotavljajo redundantnost pri konkretni ogroženosti. Verjetnost nekega dogodka ni dovolj, da bi lahko samo na tej osnovi določili tveganja in stopnjo ogroženosti ali celo oceno ogroženosti delovanja posamezne funkcionalnosti. Različna tveganja oziroma nevarnosti, ki lahko vplivajo na obratovanje, imajo namreč različne vplive tako na opremo kakor tudi na stopnjo celotne funkcionalnosti. Kot primer si lahko ogledamo tri možne nesreče, ki imajo lahko različne vplive na samo obratovanje: prvič – epidemija oteži obratovanje zaradi ogrožanja ljudi, nikakor pa ne ogroža opreme; drugič – puščanje strehe med neurjem lahko ogrozi opremo, ne ogroža pa ljudi; in tretjič – potres ogroža tako ljudi kot opremo. Zato strokovnjaki z različnih področij – informacijske varnosti, korporativne varnosti, tehnične varnosti ter različnih družb v skupini HSE, neprekinjeno preverjajo stanje delovanja naših sistemov. Izsledke iz pregledov redno sporočajo tistim, ki jih za svoje delo potrebujejo.



Za konec nam zaupajte kateri so po vašo strokovni oceni tisti izzivi, ki jim bo potrebno v naslednjem obdobju namenjati največ pozornosti v elektroenergetskem sistemu Slovenije?

Izzivi v naslednjem obdobju bodo usmerjeni v kakovostno, količinsko in časovno ustreznost dobave električne energije ter prilagodljivost potrebam elektroenergetskega sistema, ob upoštevanju okoljskih standardov, ukrepov varovanja okolja in ljudi. Lotili se bomo digitalnega inovacijskega sistema z namenom, da uporabnikom omogočimo v prihodnost usmerjene tehnologije, kot so strojno učenje. Namen je torej zagotoviti skladnost z naprednimi razvojnimi trendi na področju vzdrževanja proizvodne infrastrukture, ki je ključna in kjer so zahteve po zanesljivosti delovanja in razpoložljivosti proizvodnih kapacitet velike, hkrati pa vedno prisotna težnja po učinkoviti in racionalni izrabi razpoložljivih virov za vzdrževanje. Na tej podlagi se torej pričakuje trajno višja predvidljivost in zanesljivost obratovanja proizvodnih kapacitet - agregatov (manj neuspešnih zagonov, manj nepredvidenih izpadov iz obratovanja) in večja dodana vrednost. Zato je strategija obratovanja in vzdrževanja proizvodne infrastrukture v skupini HSE postavljena za naslednjih deset let. ■

VISOKA VARNOST, NAPREDNA TEHNOLOGIJA IN MODEREN DIZAJN

Varnostne omarice za upravljanje s ključi.

Ko imate v obtoku veliko število ključev in želite zagotoviti sledljivost, nadzor in pregled nad kroženjem ključev v organizaciji.

Protivlomna zaščita, vgrajen alarmni sistem, zvočni in svetlobni opozorilni signali in druge funcionalnosti po meri.

Na voljo tudi enote za shranjevanje dokumentov, predmetov, orožja in druge vredne opreme.



Zaupajte našim 20-letnim izkušnjam na področju zagotavljanja rešitev tehničnega varovanja, sistemskega zaklepanja in kontrole pristopa.

Za vas raziskujemo, vam svetujemo in ponujamo inovativne rešitve, digitaliziramo sisteme zaklepanja in s tem zmanjšujemo varnostna tveganja ter stroške v vaši organizaciji.

ID Shop – Vaš IDealni partner na področju identifikacije in varnosti.



Hitri prehodi za kontrolo pristopa

Varnostni prehodi, ki se prilagodijo vsakemu prostoru in odgovarjajo potrebam sodobnih organizacij.

Namenjeni preprečevanju nepooblaščenih prehodov.

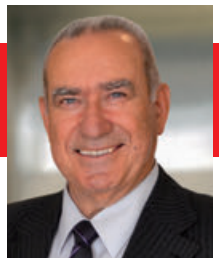
Primerni za zunanje ali notranje namestitve, opremljeni s senzorji, zvočnimi in svetlobnimi signali, na voljo čitalci RFID kartic, terminali za preverjanje vstopnic, biometrični čitalci, ...

IDealni partner za identifikacijo in varnost

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

cominfo Security First SAIK

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





VARNOSTNI IZZIVI V KRITIČNI INFRASTRUKTURI - POGLED V PRIHODNOST

Prišli smo do spoznanja kaj pomeni in kako pomembna je kritična infrastruktura v kriznih stanjih, ko gre za vprašanja normalnega in/ali omejevalnega delovanja posameznih sektorjev. Smo v vrtiljaku vedno hitrejših sprememb, ki jih je težko tekoče obvladovati, še posebej pa jih je težko obvladovati s strateškimi odločitvami. Zaradi navedenega je še pomembnejše zavedanje o pomenu neprekinjenosti delovanja kritične infrastrukture.

1. Izhodišče

Prišli smo do spoznanja kaj pomeni in kako pomembna je kritična infrastruktura v kriznih stanjih, ko gre za vprašanja normalnega in/ali omejevalnega delovanja posameznih sektorjev. Zavedamo se kaj pomenijo omejitve v oskrbi z elektriko, plinom in nafto, kaj pomeni, če nam hekerji, krekerji in vohuni vdirajo v komunikacijske in informacijske sisteme, kaj pomeni, če so prenosna in distribucijska omrežja ter plinovodi ali naftovodi podvrženi poškodbam (eksplozije, požari, sabotaže, vdori) in kaj pomeni, če kritično infrastrukturo pestijo poplave, viharji, suše, žledolomi in druge naravne nesreče. Vse to se že dogaja in vnaša v normalno življenje, delo in poslovanje nemir, negotovost in nove varnostne izzive. Z varnostnega vidika, ki je usodno povezan z življenjskimi, delovnimi, ekonomskimi, poslovnimi, finančnimi in tržnimi vidiki, so še zlasti za kritično infrastrukturo, ključnega pomena naslednji varnostni izzivi:

- redefiniranje varnostnih dokumentov (politik, ocen, analiz, scenarijev, načrtov),
- sistematično in načrtno obvladovanje ranljivosti, ogroženosti in odpornosti sistemov in procesov,
- bolj učinkovito (profesionalno) upravljanje varnostnih in drugih tveganj z uvajanjem varnostnih standardov,
- nenehno spremljanje varnostnih pojavov v lastnem, lokalnem in širšem okolju,
- redno vnašanje varnostnih in drugih izboljšav v varnostne sisteme,
- letno (po potrebi bolj pogosto) preverjanje scenarijev možnih izrednih dogodkov kriminalnega, terorističnega in naravnega izvora,
- natančnejše obvladovanje kakovosti in ekonomičnosti lastnega in/ali pogodbenega fizičnega in tehničnega varovanja,
- ustreznost organiziranosti področja korporativne varnosti, ki upravlja z integralnim varnostnim sistemom, varnostnimi tveganji in varnostnimi izzivi,
- kontinuirano zagotavljanje finančnih virov za upravljanje s sistemom korporativne varnosti,
- sistemsko načrtovanje in celostno upravljanje ključnih kadrov za potrebe neprekinjenega delovanja in upravljanja izrednih dogodkov.

Smo v vrtiljaku vedno hitrejših sprememb, ki jih je težko tekoče obvladovati, še posebej pa jih je težko obvladovati s strateškimi odločitvami. Strategije so namreč postale glavna težava odločevalcev v politiki, gospodarstvu in civilni družbi. S tega zornega kota bi bilo koristno, da se strokovni timi ter strateški in operativni odločevalci v kritični infrastrukturi v prihodnje lotijo učinkovitejšega prepoznavanja in obvladovanja varnostnih izzivov.

*avtorja sta člana Slovenskega združenja korporativne varnosti

Smo v vrtiljaku vedno hitrejših sprememb, ki jih je težko tekoče obvladovati, še posebej pa jih je težko obvladovati s strateškimi odločitvami. Strategije so namreč postale glavna težava odločevalcev v politiki, gospodarstvu in civilni družbi. S tega zornega kota bi bilo koristno, da se strokovni timi ter strateški in operativni odločevalci v kritični infrastrukturi v prihodnje lotijo učinkovitejšega prepoznavanja in obvladovanja varnostnih izzivov. To je pot preprečevanja še večjih šokov, katastrof in ogromnih škod v vedno bolj negotovi prihodnosti.

2. Varnostni izzivi v sektorjih kritične infrastrukture

2.1 Energetika - elektrika, nafta, plin

Bolj ali manj je vsem jasno, da gre za visoko stopnjo ranljivosti energetike, torej ranljivost jedrskih, vodnih in termo elektrarn ter naftovodov in plinovodov. Kajti omejitev dobave, okvara, nesreča ali namerno poškodovanje samo enega elementa v teh sistemih lahko povzroči hude motnje v posameznih sektorjih gospodarstva, v državnih institucijah, lokalnih skupnostih in/ali v civilni družbi. S tega zornega kota je v energetiki še toliko bolj pomembno načrtovanje neprekinjenega poslovanja in kriznega vodenja. Pri tem je pomembno definiranje kritičnih procesov, obvladovanje (zlasti varnostnih) tveganj, obvladovanje izrednih dogodkov z načrti alarmiranja in odzivanja, varovanje osebja, premoženja (zgradb, opreme, omrežij), zaupnih informacij in elektronskih komunikacij v skladu z varnostno politiko in varnostnimi standardi. Iz tega izhaja, da je prepoznavanje varnostnih izzivov v energetiki treba iskati v naslednjih energetskih težavah, ki v bistvu predstavljajo varnostne izzive:

- zmanjševanje negotovosti obvladovanja povečanih tveganj zaradi uvozne odvisnosti in zmanjšanja zanesljivosti oskrbe z energijo – pomembno je izvajanje zakona o ukrepih za obvladovanje kriznih razmer na področju oskrbe z energijo,
- skrajševanje dolgotrajnih postopkov umeščanja alternativnih (obnovljivih) virov energije v prostor in odvisnost teh virov od naravnih sil,
- še vedno - kljub energetskemu soglasju - ni zaključen postopek izgradnje NEK 2,
- pospešitev razvoja sistemov kibernetske varnosti v proizvodnji, prenosu in distribuciji električne energije,
- povečanje naporov za razvoj hranilnikov energije,
- potrebne so bolj poglobljene analize posledic avtomobilske elektrifikacije, ki bo zarezala v porabo električne energije.

Upravljavci, lastniki in menedžment energetike so pravi naslov za reševanje aktualnih energetskih vprašanj in posledično za obvladovanje prihajajočih varnostnih izzivov.

2.2 Informacijsko - komunikacijska omrežja in sistemi

Motnje v informacijsko-komunikacijskih omrežjih in sistemih lahko povzročajo naslednji dogodki: pretrganje optičnih kablov, okvara strojne opreme, vdori v računalniška omrežja in v informacijske sisteme, prestrezanje in prisluškovanje klasični telefoniji in elektronskim komunikacijam, naravne nesreče, iznos zaupnih podatkov, poškodbe RTV oddajnikov, baznih postaj mobilne telefonije, poškodovanje teleko-





munikacijskih central in nadzornih centrov, prenasičenost komunikacijskih poti – izpad mobilne telefonije zaradi preobremenjenosti, ogrožanje prometa zaradi motenj v prometni signalizaciji ipd.

Kritični objekti v informacijsko komunikacijski infrastrukturi, so: mednarodne centrale in optični kabli (optična hrbtenica) mednarodnih telekomunikacij, centrale in bazne postaje mobilne telefonije, centri upravljanja (vodenja) cestnega in železniškega prometa (ogroženost predorov, viaduktov, mostov), RTV oddajniki, informacijsko-komunikacijski sistemi letališč in kontrol zračnega prometa, pomorski informacijski sistemi, informacijski sistemi bank, državnih institucij in korporacij/multinacionalk z mednarodnim poslovanjem.

Razvoj informacijsko telekomunikacijskega sistema države gre v smeri poenotenja (sistem TETRA), ki bo omogočil učinkovitejšo informacijsko in telekomunikacijsko povezanost vseh interventnih institucij kot so: Policija, Slovenska vojska, Civilna zaščita, reševalne službe in gasilstvo.

Iz zapisanega izhajajo ključni varnostni izzivi, ki so:
- izboljšanje učinkovitosti obvladovanja kibernetske kriminalitete – obvladovanje vdorov, lažnih informacij, zlonamerne programske opreme, idr.,
- bolj zavzeto ugotavljanje in odpravljanje varnostnih vrzeli v sistemih varovanja podatkov, informacij, elektronskih komunikacij in zaupnih dokumentov,
- kadrovske krepitve služb za informatiko, skladno z boljšo organiziranostjo in kadrovsko postavitvijo služb za korporativno varnost,
- načrtno preverjanje, vzdrževanje in posodabljanje sistemov avtonomne energijske podpore informacijskim in telekomunikacijskim sistemom,
- uvedba informacijskih standardov in standardov upravljanja s tveganji, ki zagotavlja višjo raven učinkovitosti integralnih sistemov varovanja.

Proučevanje varnostnih izzivov je naloga služb za informatiko in služb za korporativno varnost, vse v cilju izboljšanja omrežne, računalniške in informacijske varnosti ter varnosti kot celote.

2.3 Promet – kopenski, zračni, vodni

Promet je zelo razvejano področje kritične infrastrukture, ki sega daleč čez državno mejo, torej je evropska (globalna) kritična infrastruktura. Pod sektor prometa spadajo: kopenski, letalski (zračni) in pomorski promet, poleg tega pa še žičničarstvo in logistika.

Prometno infrastrukturo ogrožajo prometne nesreče, potresi, poplave, plazovi, zastoji, blokade, motnje v svetlobni signalizaciji, izpadi nadzornih centrov in drugi izredni dogodki. Ključni varnostni izzivi se zrcalijo v naslednjem:

- uresničevanje ukrepov za izboljšanje prometne varnosti, razvoja prometne infrastrukture in mobilnosti, ki so opredeljeni v Strategiji razvoja prometa v Republiki Sloveniji do leta 2030,
- izboljšanje informacijske, komunikacijske in odzivne povezanosti in usklajenosti med deležniki profesionalnih intervencij na izredne dogodke – policisti, gasilci, reševalci, izvajalci vlečnih služb,

- krepitev medsebojnega sodelovanja, izmenjave informacij in iskanja odgovorov na razvojna vprašanja med ključnimi državnimi in civilnimi institucijami – Policija, Ministrstvo za infrastrukturo, Gasilska zveza Slovenije, AMZS, Agencija za varnost prometa idr.

Za upravljanje nakazanih varnostnih izzivov je najširše kompetentno Ministrstvo za infrastrukturo, ki lahko za boljše sodelovanje motivira tudi druge deležnike.

2.4 Prehrana – dobavitelji, oskrbne verige, trgovina, potrošnja

Prehrana ljudi in živali je vsekakor življenjsko pomemben sektor kritične infrastrukture. Velika specifika sektorja prehrane je, da mora delovati, se razvijati in obvladovati mnogotera tveganja v skladu z mednarodnim standardom HACCP, ki definira analizo tveganj in določanje kritičnih točk. To je zahteva evropskega pravnega reda za to področje in zahteve slovenske živilske zakonodaje – Zakona o zdravstveni ustreznosti živil in izdelkov ter snovi, ki prihajajo v stik z živili. HACCP je torej obvezen za gostinska podjetja, za živilsko predelovalno industrijo (mlekarstvo, pivovarstvo, živinorejo, mesno industrijo), za trgovine z živili, idr. Velja tudi za transport in skladiščenje prehranskih izdelkov. Z uvedbo HACCP se podjetje zaveže, da bo vzpostavilo takšen notranji kontrolni sistem, ki bo obvladoval vsa tveganja in vse ugotovljene kritične kontrolne točke v procesih proizvodnje, predelave, transporta, skladiščenja in trgovanja na katerih lahko pride do nevarnih situacij. V dobavnih verigah prehranskih izdelkov prihaja do raznoterih tveganj, ki se še povečajo, če so dobavne verige čezmejne. V takih primerih je potrebno uvesti mednarodni standard ISO 22000 Food Safety Management, ki omogoča zagotavljanje varnosti živil vseh živilskih proizvodov, ki prečkajo meje. V uporabi je tudi standard IFS (International Food Standard), ki omogoča ocenjevanje proizvajalcev živil in ocenjevanje izvajalcev v logističnih (dobavnih) verigah. Torej gre za zelo strog režim prehranske varnosti, ki preprečuje nastanek in razvoj raznih bolezni.



Glavni varnostni izziv prehranske varnosti je potemtakem dosledno upoštevanje evropske regulative, nacionalne zakonodaje in varnostnih standardov. K temu izzivu je treba obvezno dodati izboljšanje nadzornih mehanizmov, to je učinkovitost inšpekcijskega nadzora varnosti in sledljivosti v celotnih prehranskih verigah.

2.5 Preskrba s pitno vodo

Voda je nujno potrebna dobrina za obstoj in preživetje ljudi. Govorimo seveda o pitni vodi, ki ji je treba posvečati posebno pozornost tako z vidika nenehne kontrole kakovosti in redne oskrbe, kot tudi z vidika zdravja ljudi. V Sloveniji se nam ni treba bati pomanjkanja vode, razen v primeru, če bi podnebne spremembe povzročile kakšen katastrofalni dogodek. Sicer je Slovenija glede vodnih virov med najbogatejšimi evropskimi državami. Tudi po kakovosti pitne vode smo na vrhu.

V Sloveniji je 866 oskrbovalnih območij s pitno vodo na katerih so zgrajena vodovodna omrežja, vodohrami, zajetja in druga vodna infrastruktura. V splošnem lahko rečemo, da se v sektorju preskrbe s pitno vodo soočajo s specifičnimi tveganji, ki so: okvare na omrežju, neredno vzdrževanje, neredno posodabljanje, onesnaževanje, problem zdravstvene ustreznosti, prekuhavanje, problemi mikrobiološke skladnosti, možnosti zastrupitve, problem pesticidov, škodljivost nevarnih snovi pri prevozih po vodovarstvenih območjih, plazovi, poplave, potresi, suše, nesreče, idr.

Iz nakazanih tveganj lahko izluščimo nekaj varnostnih izzivov, ki so:
- upravljavci vodnih virov in podjetja za oskrbo s pitno vodo naj dosledno upoštevajo evropsko direktivo o pitni vodi iz leta 2021, ki določa visoke standarde varovanja in zanesljivosti oskrbe s pitno vodo,
- varnost in kakovost pitne vode mora biti zagotovljena v celotni verigi od izvira in preko javnega vodovodnega omrežja do uporabnikov - zato je v preskrbovalni verigi pitne vode potrebno uporabiti standard HACCP,
- za ugotovitev realnega stanja ranljivosti, ogroženosti in novih tveganj je treba prenoviti ocene tveganj, varnostne politike in načrte preventivnih in kurativnih ukrepov,
- s transparentnimi vzorčenji, analizami in poročanji o kakovosti pitne vode povečati zaupanje uporabnikov v delo upravljavcev vodnih virov in podjetij za nemoteno oskrbo s pitno vodo.

Glede na to, da je (in bo) pomanjkanje vode eden od glavnih svetovnih problemov 21. stoletja, je prav gotovo smiselno, da kompetentni razmislijo o varnostnih izzivih v tem sektorju.

2.6 Zdravstvo

Zdravstvo že kar nekaj časa pretresajo razne afere, nedokončani projekti, neučinkovit strateški menedžment, problemi z javnimi naročili, korupcijska tveganja, nerazumno dolge čakalne vrste, pomanjkanje družinskih zdravnikov, neurejeno kadrovsko načrtovanje, težave okoli razmejitve javnega in zasebnega zdravstva in še marsikaj drugega. Torej virov tveganj je ogromno in vse naslednje vodilne strukture čaka zahtevna naloga obvladovanja tveganj. Evidentno je, da vsa tveganja v zdravstvenem sektorju niso dovolj dobro obvladovana. Vprašljivo je obvladovanje poslovnih, kliničnih, kadrovskih, varnostnih in korupcijskih tveganj. Iz tega izhaja, da je obvladovanje tveganj ena od prioritetnih nalog strateškega in operativnega menedžmenta UKC-jev, bolnišnic, zdravstvenih domov in drugih ključnih deležnikov v sektorju.

Razreševanje nakazane problematike v zdravstvu bi lahko potekalo s pomočjo obvladovanja naslednjih varnostnih izzivov:
- prvi korak vodstev in služb za upravljanja korporativne varnosti je izdelava in sprejetje ocene o ranljivosti in ogroženosti, drugi korak pa izdelava in sprejetje varnostne politike,
- za upravljanje kliničnih tveganj je koristno uvesti standarde za zdravstvene organizacije AACI, ISO 15189 in EN 15224,
- delovanje UKC-jev, bolnišnic in zdravstvenih domov ob naravnih in drugih nesrečah urediti v skladu z načrtom odzivanja zdravstva ob naravnih in drugih nesrečah (2022),
- obvladovanje korupcijskih tveganj je pogojeno s preureditvijo javnega naročanja za potrebe zdravstva in povečanjem učinkovitosti nadzornih mehanizmov.

Nakazane varnostne izzive lahko upravlja le močna služba za korporativno varnost ob podpori vodstva na strateški ravni.

2.7 Finance – bančni sistem

Sektor financ, ožje gledano bančni sektor upravlja finance za državo, gospodarstvo, civilno družbo in prebivalstvo. Večji del poslovanja poteka pod lupo bančnih skrivnosti, torej jih omejeno obravnavamo v sklopu obvladovanja tveganj v kritični infrastrukturi. Je pa jasno, da je zagotavljanje varnosti bank ena od glavnih skrbi lastnikov in vodstev finančnih institucij. Potemtakem nas morajo zanimati varnostna tveganja znotraj in zunaj bank. Bančna skrivnost in varnost si tu pa tam podajata roki, vendar se močno zapleta, ko gre za zahteve razkrivanja bančnih skrivnosti v primeru kaznivih ravnanj. Banke se namreč težko sprijaznijo s takimi zahtevami. S tega zornega kota je eden od poglavitnih varnostnih izzivov ta, da se banke pač sprijaznijo z zahtevami tožilcev, preiskovalnih sodnikov in kriminalistov po razkrivanju bančnih skrivnosti, ko gre za preiskovanje konkretnih kaznivih ravnanj znotraj in/ali zunaj bank.

2.8 Varovanje okolja

Varovanje okolja je eno od ključnih globalnih, regionalnih in lokalnih problemov. Gre za varstvo voda, zraka in zemlje, kjer imajo velik vpliv toplogredni plini, razna sevanja, izpusti nevarnih snovi, razni komunalni in drugi odpadki, hrup idr. Tu se lomijo kopja med pravimi privrženci tega področja in med lastniki kapitala, ki jim gre bolj za dobičke, kot za zdravo in varno življenje na našem planetu. Četudi obstaja že kar nekaj mednarodnih sporazumov, obširno zakonsko urejanje tega področja in številne mednarodne standarde, pa v praksi še marsikaj šepa (npr. problemi odpadkov). Velik vpliv na to področje pa imajo tudi podnebne spremembe, ki so – kljub sodobni tehnologiji spremljanja in merjenja teh sprememb - še vedno v veliki meri nepredvidljive. Zeleno Slovenijo, ki je bogata s pitno vodo, z gozdovi in z biotsko raznovrstnostjo je treba čim bolj zaščititi pred naravnimi nesrečami in škodljivostjo človeških virov.

Iz tega izpeljemo ključni varnostni izziv, ki se glasi: Pri oblikovanju varnostnih politik, ki zajemajo tudi varovanje okolja sta vsebinsko prikladni za uporabo resolucija o Nacionalnem programu varstva okolja za obdobje 2020-2030 in Agenda za trajnosti razvoj do leta 2030.

2.9 Ključni kadri v kritični infrastrukturi

Vsi zgoraj omenjeni sektorji kritične infrastrukture se, ne glede na specifike varnostnih izzivov, ki so tipični za posamezni sektor, soočajo z enotnim izzivom, to je prepoznavanjem potreb po ključnih kadrih (vodstva, krizni menedžerji, informatiki, strokovnjaki s ključnimi znanji, inovatorji in razvijalci, varnostni menedžment ipd.) in njihovi dosegljivosti in razpoložljivosti za potrebe neprekinjenega delovanja in upravljanja z izrednimi dogodki. Zadnja pandemija COVID nam je postavila ogledalo na tem področju in nam nakazala, kako pomembni so za upravljavce kritične infrastrukture ključni kadri in kako organizirati njihovo dosegljivost in razpoložljivost ob izrednih dogodkih in razmerah tudi za daljše časovno obdobje.

Na tem področju lahko izpostavimo naslednje izzive:
- prepoznavanje ključnih kadrov, njihovih kompetenc, njihovega razvoja, njihove dosegljivosti in razpoložljivosti ter njihove nadomestljivosti v primeru odhoda,
- vzpostavitev strateškega upravljanja ključnih kadrov, ki bo zagotavljal njihovo stalnost v organizaciji,
- obvladovanj demografskih sprememb in s tem povezanih izzivov – zaradi zmanjševanja prebivalstva v nekaterih evropskih regijah je obvladovanje demografskih sprememb v Evropski uniji ključna politična tema trenutne Evropske komisije,
- beg ali pridobitev možganov zaradi stalnih emigracij,
- starajoče se prebivalstvo - zaradi naraščajoče pričakovane življenjske dobe napovedi kažejo, da bo leta 2070 več kot 30% prebivalstva starega 65 let ali več (v primerjavi z letom 2019 jih je bilo nekaj več kot 20%),
- zmanjševanje kadrov zaradi avtomatizacije in digitalizacije procesov – ostajajočim kadrom se nalagajo vse bolj zahtevne in kompleksne zadolžitve, ki od njih po eni strani zahtevajo hitro prilagodljivost, sposobnost hitrega učenja in vse širši nabor znanj in spretnosti, po drugi strani pa to organizacijam povzroča še večje izzive za zagotavljanje njihove dolgoročne razpoložljivosti, dosegljivosti in nadomestljivosti.

Iz navedenega lahko zaključimo, da postaja upravljanje s ključnimi kadri eno osrednjih (ključnih) tveganj in tudi varnostnih izzivov predvsem pri upravljavcih kritične infrastrukture.

3. V razmislek

Celotna kritična infrastruktura je na preizkušnji. Bo prenesla omejitve, napade, ovire in poškodbe? To je ključno vprašanje razburkane sedanjosti in negotove prihodnosti. Za rešitve ni receptov, ni samoumevnih dogajanj kot tudi ni izdelanih razumnih strategij. Prepoznavanje, proučevanje, razumevanje in upoštevanje varnostnih izzivov je samo eden od pristopov h krepitvi varnostne kulture in graditvi integralnih sistemov varovanja ljudi, premoženja in človeških vrednot. Kajti varnost vse bolj postaja vrednota, ki jo čutimo na vsakem koraku. ■

ZARJA ELEKTRONIKA

Varno v nov dan.



- razvoj
- inženiring
- proizvodnja
- projektiranje

sistemov za tehnično varovanje

60 LET TRADICIJE

www.zarja.com

Avtor: dr. Milan Tarman / Institut za korporativne varnostne študije*



PRILOŽNOSTI VESOLJA ZA INDUSTRIJO IN DRUŽBO

V moderni družbi varnostnih tveganj in groženj, pa tudi priložnosti, so vsebine vezane na področje vesolja, v okviru Republike Slovenije, Evropske unije, Evropskih agencij in drugih mednarodnih aktivnosti, vedno bolj aktualne za industrijo in družbo. Ob številnih projektih, kjer se slovenska podjetja že uspešno dokazujejo, se odpirajo številne možnosti za okrepljeno sodelovanje podjetij in inštitucij z javno upravo ter priložnosti tudi na mednarodnem področju.

Uvod

Uvodoma velja omeniti, da je s sprejemom Zakona o vesoljskih dejavnostih v letošnjem letu Republika Slovenija legislativno in sistematično uredila predmetno področje. Ključno vlogo je s strani javne uprave v nacionalnem okviru ter okviru mednarodnega sodelovanja pri tem prevzela Delovna skupina za vesolje, ki je bila ustanovljena s sklepom Vlade Republike Slovenije v letu 2020 s ciljem usklajenega delovanja na nacionalnem in nadnacionalnem nivoju ter enotnega zastopanja stališč v okviru delovanja Republike Slovenije v mednarodnih inštitucijah (zlasti Evropske vesoljske agencije - ESA) in delovnih telesih Evropske unije (EU). V delovni skupini, ki jo vodi Ministrstvo za gospodarski razvoj in tehnologijo (MGRT), sodelujejo predstavniki: Ministrstva za izobraževanje, znanost in šport (MIZŠ); Ministrstva za okolje in prostor (MOP); Ministrstva za infrastrukturo (MZI); Ministrstva za obrambo (MO); Ministrstva za zunanje zadeve (MZZ); Ministrstva za zdravje (MZ); Ministrstva za finance (MF); Ministrstva za javno upravo (MJU); Ministrstva za kmetijstvo, gozdarstvo in prehrano (MKGP) ter Urada Republike Slovenije za varovanje tajnih podatkov (UVTP). Z navedenim je bil dan dodatni pomen vsebinam, vezanim na področje vesolja, v okviru Slovenije in na mednarodnem področju (npr. možnost uporabe programov Govsatcom, EUROQCI, Galileo/Egnos, Eumetsat, CERN, ITER, Obzorje, ipd.) in so se s tem odprle dodatne možnosti za okrepljeno sodelovanje podjetij in inštitucij z javno upravo ter sodelovanje v okviru različnih mednarodnih pobud, v sodelovanju z mednarodnimi partnerji in v mednarodnih forumih, zlasti v OZN COPUOS.

V primerjavi z drugimi primerljivimi državami članicami EU, ki tudi finančno izdatneje spodbujajo sodelovanje podjetij, raziskovalno razvojnih inštitucij in javne uprave, tako v nacionalnem kot v mednarodnem okviru, obstaja v Republiki Sloveniji še veliko potenciala na področju vesolja ter s tem povezanimi aktivnostmi. Nadalje je potrebno intenzivno razvijati strateški in celovit pristop z znatnejšimi finančnimi spodbudami ter kadrovskimi resursi, saj le to omogoča prosperiteto ter odpiranje dodatnih možnosti na področju vesolja.

V tem kontekstu so aktualno izpostavljena zlasti naslednja področja:

Upravljanje vesoljskega prometa (STM).
Gre za enega ključnih dosjejev na področju vesolja v okviru EU, katerega cilj je uskladiti skupen pristop EU do STM v prvi polovici leta 2023. Evropska unija mora namreč slediti tren-

*avtor je član Slovenskega združenja korporativne varnosti

dom razvoja vesoljskih aplikacij in vesoljskih tehnologij kot novodobnega hitro rastočega trga. Še zlasti je EU pod močnim pritiskom predvsem zaradi trenutno šibke tehnološke neodvisnosti, ki naj bi se izboljšala s konsolidacijo aktivnosti EU na področju STM.

Predlog programa Varna povezljivost

Zakonodajni predlog Uredbe o vzpostavitvi Programa Unije za varno povezljivost za obdobje 2023–2027, katerega namen je izgradnja globalnega varnega komunikacijskega sistema Evropske unije v vesolju, je med ključnimi novimi pobudami Evropske komisije za leto 2022. Cilj programa Varna povezljivost je vzpostavitev večnamenske satelitske konstelacije na več orbitah, s katero bi lahko fleksibilno pokrivali komunikacijske potrebe vladnih uporabnikov v Evropski uniji po zanesljivih, varnih in stroškovno učinkovitih komunikacijah za zaščito kritične infrastrukture, zunanje akcije (external actions), krizno upravljanje, vključno s človekoljubno pomočjo ter za pomorski in zračni nadzor prostora, ki poleg Evrope zajema tudi Afriko in Arktiko. Program predvideva tudi zagotovitev satelitskega širokopasovnega dostopa visokih hitrosti do interneta po vsej EU, kar bo prispevalo k boljšemu delovanju enotnega trga. Poleg Copernicusa in Galilea/EGNOS program Varna povezljivost tvori tretji steber vesoljskega programa Evropske unije. Pomemben je tako za podjetja, javne organe kot širšo javnost, saj je njegov namen poleg zagotavljanja večje odpornosti pred kibernetskimi in hibridnimi grožnjami, tudi izkoriščanje tehnološkega potenciala digitalne in vesoljske industrije v Evropski uniji. Program bo malim in srednjim podjetjem ponudil vrsto novih poslovnih priložnosti, spodbudil bo tehnološki razvoj, z novo razvitimi lastnimi tehnologijami, infrastrukturo in storitvami pa bo prispeval k evropski tehnološki avtonomiji in suverenosti.

Sklepi Sveta EU o Copernicusu do 2035

Razvoj storitev programa Copernicus je pomemben pri doseganju ciljev *Zelenega dogovora*, saj Copernicus zagotavlja znanstveno relevantna orodja in kazalnike za ocenjevanje trenutnega stanja podnebja, vzroke in trende, pa tudi dolgoročne projekcije oz. scenarije podnebnih sprememb, ki so pomembna pri odločitvah, ki jih sprejemajo odločevalci. Pri *digitalnem prehodu* je Copernicus nepogrešljiv pri upoštevanju ustreznih novih trendov pri razvoju novih tehnologij, znanosti in digitalni transformaciji in za razvoj okoljevarstvenih politik.

Na področju odpornosti in varnosti se pričakuje razvoj zmogljivosti službe EU za obvladovanje izrednih razmer ter krepitev varnostnega portfelja, še posebej pri vprašanju migracij prebivalstva zaradi podnebnih razmer.

Ta program je potrebno v naslednjih letih, ne le vzdrževati, temveč tudi nadgraditi. Trije glavni izzivi pri razvoju programa vključujejo zeleni dogovor, digitalni prehod ter odpornost in varnost. Uspeh programa temelji na strokovnem znanju Evropske komisije, držav članic EU, in osrednjih partnerjev, tj. organizacij ESA, EUMETSAT, EUSPA, ECMWF, Mercator Ocean International, EEA, EU SatCen, EMSA in Frontex. Vložek uporabniškega foruma Copernicus je pomemben v celotni vrednostni verigi.



Dostop do storitev, podatkov in informacij programa Copernicus s strani uporabnikov naj bi bil uporabniku prijazen, dostop do teh podatkov pa lahko tudi pripomore k razvoju evropske vrednostne verige z izvajanjem in promocijo evropskih podatkov in Storitve dostopa do informacij (DIAS).

Odbor Združenih narodov za miroljubno uporabo vesolja (COPUOS)
Delovna skupina za vesolje je usklajevala stališče glede predloga ko-sponzoriranja resolucije o »Agendi 2030 za vesolje: vesolje kot gonilo trajnostnega razvoja«, ki je nastala v okviru Odbora OZN za miroljubno uporabo vesolja (COPUOS). Dokument predstavlja možnosti okrepitve vloge vesolja pri uresničevanju trajnostnega razvoja, kot tudi pri boju proti podnebnim spremembam in zmanjšanju tveganja nesreč. Vsebuje štiri cilje, ki se nanašajo na gospodarske in družbene vidike ter na dostop do vesolja in vesoljsko diplomacijo, ter usmeritve za njihovo uresničevanje. DS je predlog za kosponzoriranje resolucije, ki je bila obravnavana na plenarnem zasedanju Generalne skupščine OZN, 25. oktobra 2021, soglasno podprla. Konec l. 2021 je Slovenija postala 100. članica COPUOS.

Mednarodne inštitucije

Vezane na področje vesolja delujejo številne mednarodne inštitucije – v nadaljevanju so izpostavljene nekatere z osnovnimi informacijami, s katerimi že aktivno sodelujejo naša podjetja, raziskovalno razvojne inštitucije in javna uprava.

ESA (European Space Agency) - Evropska vesoljska agencija je svetovno priznana medvladna organizacija, ki je bila ustanovljena v sedemdesetih letih prejšnjega stoletja z namenom povezati znanje in sredstva posameznih evropskih držav za razvoj vesoljskih tehnologij. V današnjem času, ko se z vesoljskimi tehnologijami ukvarja čedalje več držav in tudi zasebnih podjetij, je ena od najpomembnejših vesoljskih agencij na svetu. Leta 2010 je Republika Slovenija sklenila Sporazum evropske sodelujoče države med Republiko Slovenijo in Evropsko vesoljsko agencijo, ki je omogočil sodelovanje Republike Slovenije z Evropsko vesoljsko agencijo, v letu 2016 pa je s podpisom Pridružitvenega sporazuma med Vlado Republike Slovenije in Evropsko vesoljsko agencijo Republika Slovenija postala pridružena članica Evropske vesoljske agencije. Oktobra 2020 je bil podpisan nadgrajen Pridružitveni sporazum med Vlado Republike Slovenije in Evropsko vesoljsko agencijo, ki vključuje nove aktivnosti na področju vesoljske tehnologije. Zaradi vključitve Republike Slovenije v Evropsko vesoljsko agencijo je prišlo do hitrega razvoja vesoljskega sektorja v Sloveniji. Slovenska podjetja in institucije so se začela aktivno ukvarjati tudi z razvojem satelitov in drugih vesoljskih objektov.

EUSPA (European Union Agency for the Space Programme) - Agencija Evropske unije za vesoljski program (EUSPA) zagotavlja varne in zaščitene evropske satelitske navigacijske storitve, spodbuja komercializacijo podatkov in storitev sistemov Galileo, EGNOS in Copernicus ter usklajuje prihodnji program vladnih satelitskih komunikacij Evropske unije GOVSATCOM. Odgovorna je za varnostno akreditacijo vseh komponent vesoljskega programa EU. S spodbujanjem razvoja inovativnega in konkurenčnega vesoljskega sektorja ter sodelovanjem s celotno vesoljsko skupnostjo EU prispeva k evropskemu zelenemu dogovoru ter digitalnemu prehodu, varnosti in zaščiti Unije in njenih državljanov, hkrati pa krepi njeno avtonomnost in odpornost.

EC DEFIS (Defence Industry and Space) - Generalni direktorat za obrambno industrijo in vesolje vodi dejavnosti Evropske komisije v sektorju obrambne industrije in vesolja. Na področju obrambne industrije je DEFIS zadolžen za ohranjanje konkurenčnosti in inovativnosti evropske obrambne industrije z zagotavljanjem razvoja sposobne evropske obrambne tehnološke in industrijske baze. Na področju vesolja je GD DEFIS zadolžen za izvajanje vesoljskega programa EU, ki ga sestavljajo evropski program za opazovanje zemlje (Copernicus), evropski globalni satelitski navigacijski sistem (Galileo) in evropska geostacionarna navigacijska storitev (EGNOS).

OZN COPUOS (Committee on the Peaceful Uses of Outer Space) – Odbor OZN, ki že preko 60 let igra pomembno vlogo pri mednarodnem sodelovanju in miroljubni uporabi vesolja, preučevanju vesoljskih dejavnosti, spodbujanju vesoljskih raziskav in reševanju pravnih izzivov povezanih z raziskovanjem vesolja.

CERN (European Organization for Nuclear Research) – laboratorij, katerega delo pomaga odkriti, iz česa je sestavljeno vesolje in kako deluje. To dosežejo tako, da raziskovalcem zagotovijo edinstveno paleto pospeševalnikov delcev, da bi pomaknili meje človeškega znanja.

EUMETSAT (European operational satellite agency for monitoring weather, climate and the environment from space)
- evropska operativna satelitska agencija za spremljanje vremena, podnebja in okolja. Upravlja sistem meteoroloških satelitov, ki opazujejo atmosfero, oceane in kopno – 24 ur na dan, 365 dni v letu. Ti podatki se posredujejo nacionalnim meteorološkim službam držav članic in sodelujočih držav organizacije v Evropi ter drugim uporabnikom po vsem svetu. Storitev, ki jo zagotavlja EUMETSAT, pomaga izboljšati in varovati vsakdanje življenje evropskih državljanov. Meteorologom pomagajo pri prepoznavanju in spremljanju razvoja potencialno nevarnih vremenskih situacij ter pri izdajanju pravočasnih napovedi in opozoril službam za ukrepanje ob izrednih dogodkih in lokalnim oblastem, pomagajo blažiti posledice hudih vremenskih razmer ter varujejo življenja in premoženje ljudi. Te informacije so ključnega pomena tudi za varnost letalskega, ladijskega in cestnega prometa ter za vsakodnevno poslovanje kmetijstva, gradbeništva in mnogih drugih panog.

Programi in pobude

Izpostaviti velja tudi naslednje programe ter pobude.

GALILEO je strateški program držav članic in skupni projekt Evropske komisije in Evropske vesoljske agencije (ESA – European Space Agency). Gre za civilni projekt, ki zagotavlja avtonomijo na področju satelitske navigacije, hkrati pa zaradi interoperabilnosti z že obstoječimi satelitsko navigacijskimi sistemi (GPS) pripomore k večji natančnosti pozicioniranja po vsem svetu. Poleg interoperabilnosti in globalne dosegljivosti Galileo zagotavlja visoko stopnjo zanesljivosti sistema in informacijsko integriteto. Namen posebnih ciljev programa Galileo je zagotoviti, da se signali, ki jih oddaja sis-



tem, lahko uporabijo za naslednje funkcije: Ponuditi »odprto storitev« (OS – *Open Service*), ki je brezplačna in zagotavlja informacije o določanju položaja in časa ter je namenjena množični uporabi satelitske radionavigacije. Ponuditi »storitev varovanja življenj« (SoL – *Safety of Life Service*), ki je namenjena uporabnikom, za katere je varnost bistvenega pomena, in ki izpolnjuje zlasti zahteve letalskega, pomorskega in železniškega sektorja. Storitev izpolnjuje tudi zahtevo po stalnosti in ima funkcijo celovitosti, ki omogoča, da je uporabnik obveščen o nepravilnem delovanju sistema. Ponuditi »komercialno storitev« (*CS – Commercial Service*), ki z večjo učinkovitostjo in s podatki, ki imajo večjo dodano vrednost od podatkov, dobljenih z »odprto storitvijo«, omogoča razvoj aplikacij za poslovne ali komercialne namene. Ponuditi »javno regulirane storitve« (PRS – *Public Regulated Service*), namenjene izključno uporabnikom, ki jih pooblasti vlada, za občutljive aplikacije, ki zahtevajo visoko raven stalnosti storitve. »Vladna storitev« uporablja močne in šifrirane signale. Sodelovati pri storitvi iskanja in reševanja (SAR – *Search and Rescue Support Service*) sistema COSPAS-SARSAT z odkrivanjem nujnih signalov, ki jih oddajajo radijski oddajniki, in vračanjem sporočil tem oddajnikom.

EGNOS je prva evropska pobuda na področju satelitske navigacije. Osnovni cilj tega sistema je bil zagotavljanje komplementarnih informacij kot dodatek signaloma satelitskih navigacijskih sistemov GPS in GLONASS (Rusija) ter izboljšanje parametrov delovanja navigacijskega sistema. Gre za sistem, ki služi zagotavljanju izboljšanja signalov za satelitsko navigacijo, ki jo nudita ta navigacijska sistema. Te signale EGNOS sprejme, jih korigira in opremi z informacijo o integriteti ter pošlje uporabnikom.

GMES je skupna pobuda Evropske komisije in Evropske vesoljske agencije, njen cilj pa je doseči neodvisno in operativno sposobnost opazovanja Zemlje. Cilj je racionalizirati uporabo več virov podatkov, da bi dobili pravočasne in kakovostne informacije, storitve in znanje, ter zagotoviti avtonomen in neodvisen dostop do informacij v zvezi z okoljem in varnostjo. Glavni uporabniki sistema GMES bodo pripravljavci zakonodaje, saj jim bo GMES omogočil, da pripravijo nacionalni, evropski in mednarodni zakonodajni okvir na področju okolja (tudi podnebnih sprememb) ter ukrepe za spremljanje izvajanja te zakonodaje.

COPERNICUS - je program Evropske unije za opazovanje Zemlje, ki proučuje naš planet in njegovo okolje v korist vseh evropskih državljanov. Ponuja informacijske storitve, ki črpajo iz satelitskega opazovanja Zemlje in podatkov in situ (ne iz vesolja). Program upravlja Evropska komisija. Izvaja se v partnerstvu z državami članicami, Evropsko vesoljsko agencijo (ESA), Evropsko organizacijo za uporabo meteoroloških satelitov (EUMETSAT), Evropskim centrom za srednjeročne vremenske napovedi (ECMWF), agencijami EU in Mercator Océan. Ogromne količine globalnih podatkov iz satelitov ter zemeljskih, zračnih in pomorskih merilnih sistemov nudijo informacije, ki pomagajo ponudnikom storitev, javnim organom in drugim mednarodnim organizacijam izboljšati kakovost življenja evropskih državljanov in širše. Zagotovljene informacijske storitve so brezplačne in uporabnikom javno dostopne.

GOVSATCOM – Program Evropske unije za vladne satelitske komunikacije (GOVSATCOM) je namenjen zagotavljanju varnih in stroškovno učinkovitih komunikacijskih zmogljivosti za varnost in kritične misije in operacije, ki jih upravljajo Evropska unija in njene države članice, vključno z akterji nacionalne varnosti ter agencijami in institucijami EU.

EUROQCI - Pobuda za evropsko kvantno komunikacijsko infrastrukturo. EuroQCI bo zaščitil občutljive podatke in kritične infrastrukture z integracijo kvantno temelječih sistemov v obstoječe komunikacijske infrastrukture, kar bo zagotovilo dodatno varnostno plast, ki temelji na kvantni fiziki. Okrepil bo zaščito evropskih vladnih institucij, njihovih podatkovnih centrov, bolnišnic, energetskih omrežij in drugega ter postal eden glavnih stebrov nove strategije kibernetske varnosti EU za prihodnja desetletja.

Priložnosti za industrijo in raziskovalno razvojne inštitucije

V naši državi se krepi zavedanje ter se v sodelovanju podjetij, raziskovalno razvojnih inštitucij in javne uprave vse aktivneje identificirajo priložnosti in možnosti uporabe sredstev EU programov, mednarodnih institucij (npr. ESA, CERN, EUMETSAT, Copernicus, Egnos/Galileo, Obzorje, GOVSATCOM...). Tovrstne informacije se zlasti s strani MGRT usklajeno posredujejo podjetjem in institucijam s ciljem, da se poveča obseg informiranja o tovrstnih priložnostih.

Javna agencija SPIRIT Slovenija in MGRT sta izdala Katalog slovenske vesoljske industrije in raziskovalnih institucij (dostopen na povezavi: Katalog slovenske vesoljske industrije in raziskovalnih institucij). Promocijsko je bil v te namene pripravljen tudi video (dostopen na povezavi: https://www.youtube.com/watch?v=o7wbRdpmcjo).

Že samo sodelovanje z Evropsko vesoljsko agencijo (ESA) predstavlja priložnost tako za industrijo kot razvojno raziskovalne inštitucije. Programi ESA spodbujajo znanstveno in tehnološko odličnost, podpirajo kritične industrije, ustvarjajo nova podjetja in delovna mesta. Vsak evro vložen v programe ESA pritegne do 2,8 evra dodatnih naložb. Pomembni so tudi učinki prelivanja in s tem ustvarjanja gospodarskih in širših družbenih koristi (npr. uporaba laserske tehnologije razvite na področju vesoljske tehnologije za izvedbo očesnih operacij, uporaba infrardečih kamer prvenstveno razvitih za uporabo na satelitih za pametne naprave, uporaba inovativnih materialov razvitih za vesoljske objekte v letalski in avtomobilski industriji itd.). ESA v zadnjem obdobju močno krepi sodelovanje z EU in ostalimi mednarodnimi inštitucijami. Republika Slovenija sodeluje v štirih opcijskih programih ESA (Splošne tehnologije, Opazovanje Zemlje, Človeške in robotske raziskave ter znanstveni program Prodex). Priložnosti za podjetja in inštitucije so tudi v okviru EU programov in inštitucij: Copernicus (za katerega je bil za obdobje 2021 do 2027 sprejet finančni načrt v višini 5,4 mrd eur) in EGNOS/Galileo; Obzorje; GOVSATCOM; EuroQCI; EUMETSAT, CERN, kjer so tudi številne možnosti projektov in sodelovanja.

Zaključek

Ob številnih projektih, kjer se slovenska podjetja že uspešno dokazujejo, se odpirajo dodatne možnosti za okrepljeno sodelovanje podjetij in raziskovalnih inštitucij z javno upravo ter priložnosti tudi na mednarodnem področju. V primerjavi z drugimi primerljivimi državami članicami EU, ki tudi finančno izdatneje spodbujajo sodelovanje podjetij, raziskovalno razvojnih inštitucij in javne uprave, tako v nacionalnem kot v mednarodnem okviru, obstaja v Republiki Sloveniji še veliko potenciala na področju vesolja ter s tem povezanimi aktivnostmi. Nadalje je potrebno intenzivno razvijati strateški in celovit pristop z znatnejšimi finančnimi spodbudami ter kadrovskimi resursi, saj le to omogoča prosperiteto ter odpiranje dodatnih možnosti na področju vesolja. Pomembna so povezovanja med deležniki, strateška partnerstva in poslovni podporni nacionalni ekosistem s širokim dosegom obveščenosti in omogočanjem dostopa do programov in projektov s čim manj birokratskimi ovirami.

Tudi v ICS je na področju vesolja v ospredju združevanje in razvijanje novega znanja, izkušenj, spoznanj, potreb ter uveljavljanje interesov na področju korporacijske varnosti v nacionalnem in mednarodnem okolju. V okviru Inštituta, kjer deluje Slovensko združenje korporativne varnosti, ki združuje pravne in fizične osebe s področja korporativne varnosti in drugih povezanih področij, kontinuirano spremljamo in skrbimo za organizirano uresničevanje osebnih in poslovnih interesov tudi na tem področju, zato ste vabljeni, da nas za nadaljnje informacije kontaktirate. Namreč le ob naših skupnih prizadevanjih lahko dvig izkoriščenih strateških in poslovnih priložnosti prinaša vsestranske pozitivne učinke za podjetja, raziskovalno razvojne inštitucije in državo ter družbo.

Literatura in viri

1 Zakon o vesoljskih dejavnostih, dostopno na: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7767

2 Ministrstvo za gospodarski razvoj in tehnologijo (MGRT), Aktivnosti in objave, dostopno na: https://www.gov.si/drzavni-organi/ministrstva/ministrstvo-za-gospodarski-razvoj-in-tehnologijo/ EUSPA, dostopno na: https://www.euspa.europa.eu/sites/default/files/euspa_celebrates_its_first_365_days_of_existence_sl.pdf

3 ENISA, dostopno na: https://www.enisa.europa.eu/about-enisa/about/sl

4 EC DEFIS, dostopno na: https://ec.europa.eu/info/departments/defence-industry-and-space_en

5 OZN COPUS, dostopno na: https://www.gov.si/novice/2021-09-03-odbor-zdruzenih-narodov-za-miroljubno-uporabo-vesolja-copuos-potrdil-clanstvo-slovenije/

4 COPERNICUS, dostopno na:

https://www.copernicus.eu/sl/o-programu-copernicus

5 EUSPA, dostopno na: https://www.euspa.europa.eu/european-space/govsatcom

6 EUROQCI, dostopno na: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

7 CERN, dostopno na: https://home.cern/about/who-we-are/our-mission

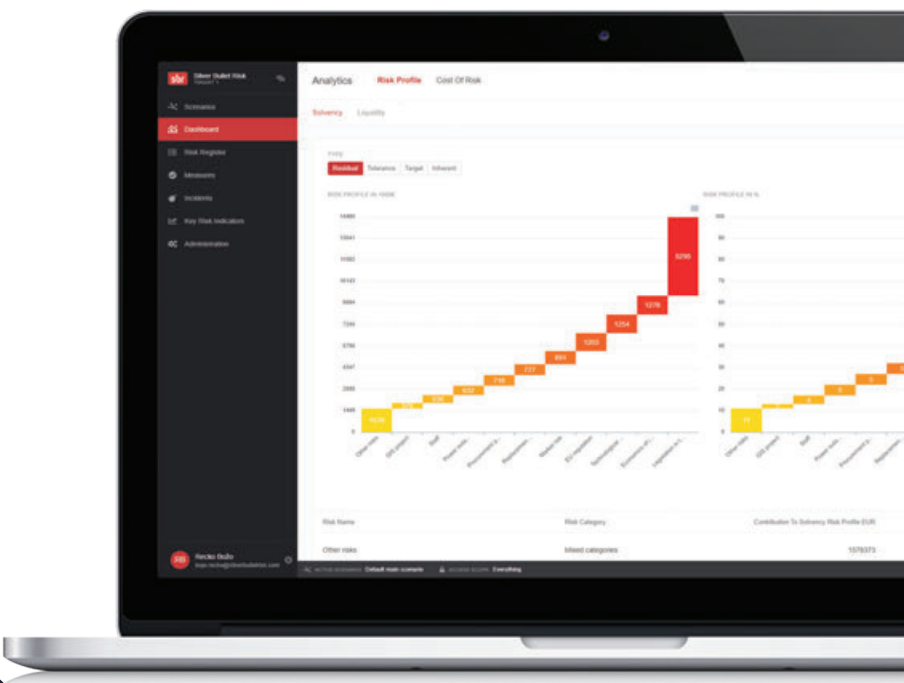
8 EUMETSAT, dostopno na: https://www.eumetsat.int/about-us/what-we-do

9 Javna agencija SPIRIT Slovenija in MGRT, dostopno na: Katalog Vslovenske vesoljske industrije in raziskovalnih institucij in https://www.youtube.com/watch?v=o7wbRdpmcjo ■

WWW.SILVERBULLETRISK.COM

Tveganja povežite s poslovnimi kazalniki uspešnosti

Kulturo upravljanja tveganj pa vpeljite v čisto vse organizacijske procese



SVETOVANJE O UPRAVLJANJU TVEGANJ

CELOVITO **UPRAVLJANJE TVEGANJ**

UPRAVLJANJE **ŠKODNIH DOGODKOV**

Silver Bullet Risk je vodilno podjetje na področju celovitega upravljanja in obvladovanja tveganj v Sloveniji.

Izkoriščamo moč znanja, izkušenj in tehnologije, da lahko podjetjem in organizacijam ponudimo najcelovitejši nabor storitev s področja upravljanja tveganj na enem mestu.

V zadnjih nekaj letih je našo programsko opremo in svetovalne storitve uporabilo več kot 100 največjih podjetij v Sloveniji.

UČINKI IN IZBOLJŠAVE ZA VAŠO ORGANIZACIJO

- 30-50% učinkovitejša izraba časa za upravljanje tveganj
- Nižji stroški realiziranih tveganj
- Spremljanje finančnih in drugih vplivov
- Gradnja lastne baze znanja o tveganjih
- Ustrezno ukrepanje v realnem času
- Zagotovljena skladnost z zahtevami in predpisi

Avtor: mag. Matjaž Beričič / Director of Technology & Solution Development, Iskratel, d.o.o., Kranj*



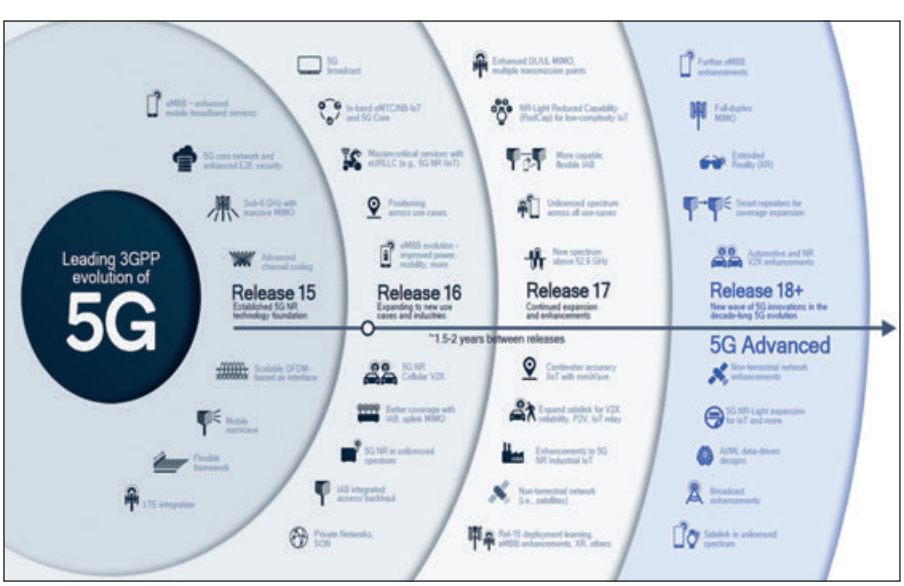
UVAJANJE 5G V SVETU IN V SLOVENIJI

Peta generacija mobilnih komunikacij (5G) v razvitem svetu postaja vse bolj vzpostavljena tehnologija javnih mobilnih omrežij, ki pa še vedno prevladujoče temeljijo na tehnologiji 4G (LTE). Omrežja 3G ob tem postopoma ugašajo – niso več relevantna – 2G omrežja pa še vedno ostajajo kot temeljna plast predvsem za klasične mobilne govorne storitve z zelo pomembno storitvijo klica v sili.

Preteklo desetletje (2010-2020) je bilo v znamenju uveljavitve tehnologije 4G. Na svetu je okoli 800 javnih komercialno delujočih 4G omrežij, ki ponujajo širokopasovne mobilne, več kot polovica teh omrežij pa ponuja tudi fiksne (FWA – Fixed Wireless Access) storitve. Ob tem pa pravzaprav zgolj okoli 300 4G omrežij podpira napredno različico LTE-A, ob tem pa podpirajo tudi VOLTE – govor preko LTE. Slednje pa je predpogoj za vpeljavo javnih 5G omrežij, ki, poleg podatkovnih in video komunikacij, še vedno podpirajo tudi klasične govorne storitve. To desetletje pa poteka v znamenju uvajanja 5G, kateremu okoli leta 2030 sledi nadgradnja na 6G.

5G je globalni standard

5G se razvija skladno z globalnimi 3GPP standardi (Slika 1). Seveda omogoča bistveno večje zmogljivosti kot prejšnja generacija. V osnovi prinaša možnost doseganja gigabitnih hitrosti prenosa podatkov, predvsem pa razvoj novih storitev tako za zasebno kot profesionalno sfero – preko javnih ali preko zasebnih omrežij. 5G omrežja v prvi fazi delujejo v načinu NSA (non-standalone) in temeljijo na 3GPP Rel15 (nadgradnja 4G), počasi postajajo skladna že z Rel16 iz leta 2020, letos pa je bil izdan že Rel17. V pripravi pa je že tudi Rel18 oziroma t.i. 5G-advanced.

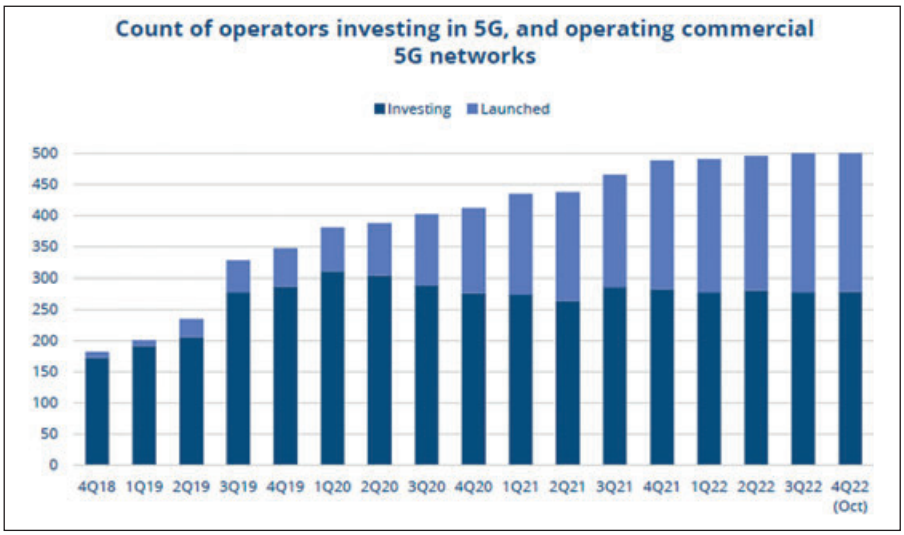


Slika 1: Razvoj standardov 5G (vir: Qualcomm)

V svetu v 155 državah 509 operaterjev tako ali drugače investira v 5G omrežja ali to aktivno načrtuje. V 92 državah pa komercialno deluje že 228 javnih mobilnih omrežij 5G (Slika 2). Telekom Slovenije je v letu 2020 kot prvi v Sloveniji in kot 100. na svetu izvedel nadgradnjo omrežja na 5G. 111 operaterjev se pripravlja na prehod na 5G SA tehnologijo, od teh jih je trenutno 35 to že naredilo.

Napredni operaterji že postopoma uvajajo samostojna (SA - standalone) omrežja 5G z novo, na oblačni tehnologiji temelječo virtualizirano jedrno infrastrukturo, ki temelji na mikrostoritvah oziroma tehnologiji kontejnerizacije. 5G SA omrežja bodo najbolj zmogljiva in to tako za javna kot zasebna omrežja – šele v tem koraku, ko bo v polni meri izpolnjena načrtovana zmogljivost 5G. V svetu je na voljo že preko 1.200 različnih komercialnih končnih naprav 5G – njihovo število se je v letu dni praktično podvojilo in velika večina že podpira tudi 5G SA. Ta ekosistem je izjemno pomemben za razvoj industrijskega 5G omrežja predvsem v sklopu primerov uporabe, ki bodo aktualni v zaprtih zasebnih mobilnih omrežjih 5G. Tu igra ključno vlogo nekaj globalnih proizvajalcev čipov, prav tako pa igrajo pomembno vlogo tudi različna združenja, kot je na primer 5G-ACIA (https://5g-acia.org/). Izjemnega pomena pa so standardi in priporočila glede varnosti omrežij 5G.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



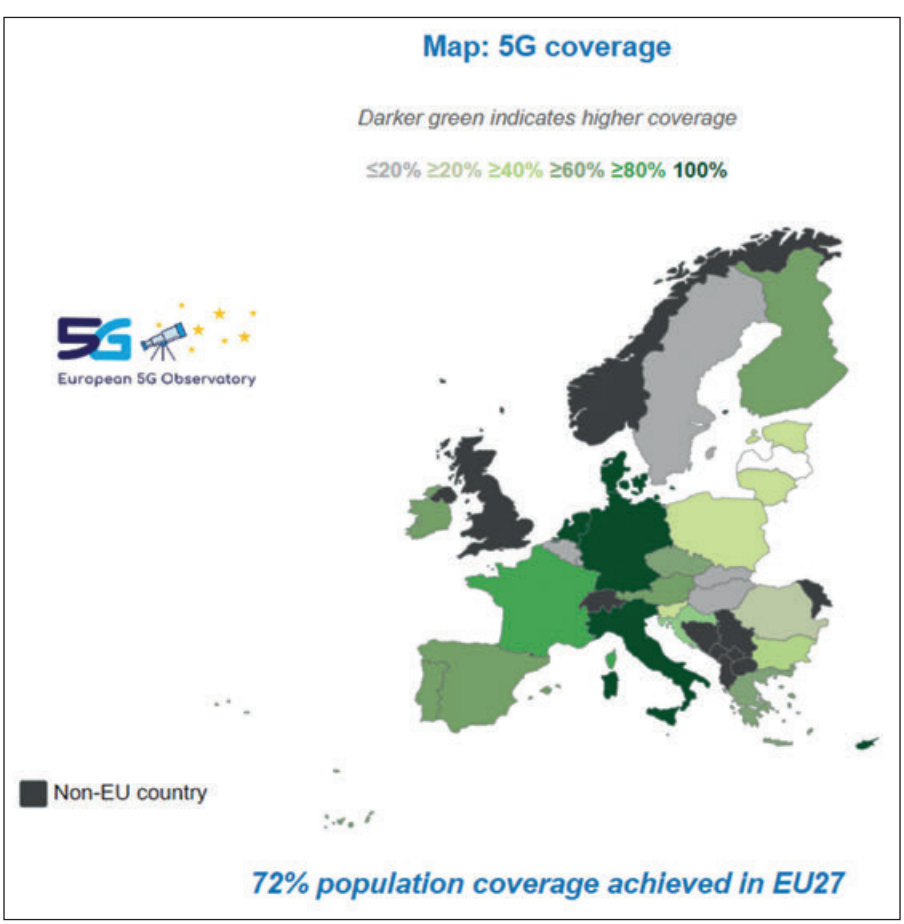
Slika 2: Rast števila 5G omrežij v svetu (vir: gsacom.com)

Slovenija in prehod iz 4G na 5G

V Sloveniji delujejo 4 javna mobilna omrežja, od teh so tri omrežja (Telekom Slovenije, A1 in Telemach) že nadgrajena s tehnologijo 5G. Med njimi poteka živahna konkurenčna tekma in lahko trdimo, da ima Slovenija visoko kakovost javnih mobilnih omrežij 4G, ki pa so tudi podvržena zahtevnim mednarodnim standardom glede varnosti, a tudi strogim predpisom glede elektromagnetnih obremenitev okolja. Tako imamo opraviti z zelo zanimivim konkurenčnim bojem, pri čemer je sicer kratkoročno kakovost 4G omrežja še vedno ključna. Dolgoročno pa bo vse bolj pomemben 5G – tudi glede na vztrajno rast prodane 5G terminalne opreme, števila uporabnikov, podatkovnega prometa, predvsem pa potreb digitalizacije industrije, transporta (cest, železnic, letališča, pristanišča), energetike ipd. Nekateri tudi že ponujajo FWA preko 5G. Primerjalna poročila kakovosti mobilnih omrežij Opensignal kaže, da sta v letih 2021 in 2022 operaterja A1 in Telemach močno izzvala primat prvega 5G omrežja Telekoma Slovenije, ki pa verjetno ne bo ostal križem rok. Kakovost omrežij stare generacije 2G, obstoječe generacije 4G in sedaj tudi nove generacije 5G je pomemben element primerjave ponudnikov na trgu, kar ima pozitivne učinke za razvitost trga.

Slovenija je predvsem v letu 2020 in 2021 naredila opazen preskok na tem področju – z visoko kakovostjo in sodobnostjo 4G omrežij, uvedbo prvega 5G omrežja Telekoma Slovenije že v letu 2020, raziskovalno-razvojnimi projekti (5G Varnost, 5GLOGINNOV) in z večfrekvenčno dražbo, s katero je uspešno podelila vse ključne spektre za razvoj javnih in tudi zasebnih mobilnih omrežij. Zaradi tega je takrat tudi opazno napredovala v DESI indeksu. Operaterji bodo po pridobitvi frekvenc morali zadostiti obveznostim pokrivanja v mestih in souporabi na zahtevnih območjih ter varnosti. Na javni dražbi je AKOS ponudil pasove 700 MHz, 1500 MHz, 2100 MHz, 2300 MHz, 3600 MHz in 26 GHz za obdobje 15 let.

Očitno je, da so nekateri operaterji po dražbi dinamiko razvoja javnega 5G omrežja pospešili (slika 4), toda gledano v celoti, Slovenija pri uvajanju 5G zaostaja za povprečjem EU – tako pri javnih kot tudi zasebnih omrežjih. Kaže, da je Slovenija v zadnjem času spet nekoliko zaostala, tako pri DESI indeksu mobilnih omrežij, kot konkretno pri 5G pokritosti. 4G pokritost prebivalstva v Sloveniji je lani znašala 99,9 % (povprečje EU 27: 99,8 %) in na ruralu 99,8 % (povprečje EU 27: 99,6 %). 5G pokritost prebivalstva je v Sloveniji lani znašala 36,6 % (povprečje EU 27: 65,8 %), na ruralu pa 2,8 % (povprečje EU 27: 34,7 %). Nekateri operaterji v Sloveniji so letos nekoliko obstali v razvoju, drugi so pospešili delo na pokritosti 5G, ki se giblje med 40 in 60% prebivalstva (EU je sicer že preko 70%), spet drugi pa bolj poudarjajo visoke hitrosti prenosa podatkov. V prvi fazi je bolj verjetno ključna dobra pokritost in konsistenca omrežja 4G/5G. Kapacitete za omogočanje vse višjih hitrosti prenosa podatkov se bodo postopno nadgrajevale, saj je 5G sistem zelo skalabilen. Globalni indeks Speedtest (https://www.speedtest.net/global-index) za september 2022 sicer kaže, da je Slovenija na področju zagotavljanja hitrosti prenosa podatkov v mobilnih in



Slika 3: Pokritost 5G v Evropi (vir: 5G Observatory)



Slika 4: Primerjava pokritosti slovenskih omrežij 5G november 2022 – TelekomSLO, A1 in Telemach (vir: www.telekom.si; www.a1.si; www.telemach.si)

fiksnih omrežjih ta trenutek nekje v povprečju, uvršča pa se nekje med 35. in 40. mestom med vsemi državami.

Zasebna mobilna omrežja

Ob tem se v zadnjih letih v svetu intenzivno razvijajo mobilna zasebna omrežja 4G in 5G. V svetu poteka veliko razvojnih projektov, kar pomeni, da bodo mobilna zasebna omrežja v pomembni meri omogočila digitalizacijo gospodarstva in kritične infrastrukture – bodisi preko navideznih zasebnih omrežij znotraj javnega omrežja, preko hibridnih javno-zasebnih ali preko povsem izoliranih zasebnih omrežij – predvsem v odvisnosti od varnostnih zahtev. Mnoga podjetja bodo imela koristi od zasebnih omrežij in tehnologije 5G za avtomatizacijo poslovnih procesov, zmanjšanje varnostnih tveganj ali zaščito zaposlenih pred nevarnimi situacijami. 4G, predvsem pa 5G tehnologije, postajajo zrele in skalabilne ter cenovno dostopne, da bodo nekoč težko izvedljiva mobilna zasebna omrežja postala ekonomsko upravičena za številne primere uporabe v industriji, energetiki, transportu ipd. Na svetu je ta trenutek že preko 1.000 takšnih ali drugačnih postavitev zasebnih mobilnih omrežij, pri čemer prednjačijo ZDA in Nemčija, predvsem na segmentu pametnih tovarn, ki bodo s 5G tehnologijo postale visoko avtomatizirane. Po napovedih bo na svetu v naslednjih 5 letih preko 20.000 zasebnih mobilnih omrežij.

Slovenija se na tem področju šele počasi prebuja. Določeni operaterji izvajajo določene raziskovalno razvojne projekte s partnerji, določeni operaterji pa že promovirajo rešitve. V Sloveniji je pri tem zelo aktivno podjetje S&T Iskratel (https://www.snt-iskratel.si), ki je del mednarodne skupine Kontron, ki v sklopu celovite rešitve razvija tudi lastno 5G mobilno jedro, na osnovi sodobnih oblačnih tehnologij, namenjeno zasebnim operativnim okoljem gospodarstva in kritične infrastrukture s posebnimi zahtevami. Na svetu se bo odstotek povezanih naprav v industriji in kritični infrastrukturi zagotovo zelo povečal, prav tako pa smo priča trendu deglobalizacije, digitalne suverenosti in vzpostavljanju zasebnih IKT oblakov omrežij za poslovni segment, vlade oziroma javne uprave in kritično infrastrukturo. Ob tem se razvijajo partnerski ekosistemi, ki bodo združevali najboljše iz obeh svetov: vodilne ponudnike telekomunikacijskih rešitev in ponudnike rešitev za različne industrije.



Začenja se že dolgoročni razvoj 6G

Postopoma pa se v svetu začenja tudi razvoj 6G, katerega uvajanje lahko pričakujemo koncem tega desetletja, verjetno v sklopu 3GPP Rel21 in naprej. Koncept 6G šele nastaja v raziskovalni sferi. Zagotovo bo temeljil na uporabi vseh sodobnih tehnologij, ki bodo koncem desetletja realne (umetna inteligenca, kvantno računalništvo, avtomatizacija-robotizacija, metaverse itd.), uporabljal pa bo nove frekvenčne spektre in omogočal terabitne hitrosti. Tudi Evropa povečuje naložbe v razvoj 5G in raziskave 6G v sklopu SNS JU (Smart Networks and Services Joint Undertaking), kjer se upravlja prvi portfelj 35 raziskovalnih, inovacijskih in poskusnih projektov, da se omogoči razvoj ekosistemov 5G in spodbuja raziskave 6G v Evropi. S skupnim financiranjem tega novega portfelja v višini približno 250 milijonov EUR je cilj zgraditi prvorazredno evropsko dobavno verigo za napredne sisteme 5G in zgraditi evropske tehnološke zmogljivosti 6G. Vse večji poudarek pa je spodbujanje učinkovite rabe energije in trajnostnega razvoja, hkrati pa tehnološke suverenosti Evrope. Slovenija se mora aktivneje in bolj organizirano vključiti v te razvojne tokove, sicer tvega tehnološki in gospodarski zaostanek. ■

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



VARNOST, BREZ KOMPROMISOV

HUAWEI

Avtor: mag. Matjaž Drev / Center za informatiko v zdravstvu, NIJZ*



PROAKTIVNI PRISTOPI K VAROVANJU PODATKOV

Premislek o splošnem stanju na področju informacijske varnosti v Sloveniji je podoben zlaganju sestavljanke, kjer polovica koščkov manjka. Zaplete se že pri enotnem pojmovanju kaj informacijska varnost je oziroma kako široko jo interpretirati, da bodo s tem zadovoljni vsi ključni deležniki.

Pravzaprav se zaplete že tu. Kdo so ključni deležniki? Nadzorni organi, izvajalci bistvenih storitev, organizacije, ki vzdržujejo kritično infrastrukturo? Tudi, če se opisanih izzivov ne dotaknemo, ostane vprašanje podatkov na katere se opreti. V pomoč so lahko letna poročila SI-CERT in Informacijskega pooblaščenca. Iz njih izhaja, da število obravnavanih incidentov iz leta v leto raste. Zakaj? Je incidentov dejansko več? Ali pa smo postali bolj ozaveščeni in predvsem boljši pri njihovem odkrivanju? Je več incidentov (tudi) posledica kadrovske krepitve nadzornih organov? Verjetno vse navedeno in še kaj - na primer vedno več IT naprav, ki so »pametno« vključene v »internet stvari«, ter s tem povezano eksponentno naraščanje podatkov. Kljub (odprtim) vprašanjem je opazno naslednje: omenjena letna poročila kažejo trend naraščanja incidentov s področja informacijske varnosti in varstva osebnih podatkov, zakonodaja, ki področje ureja, se množi, prav tako dobivamo nove nadzorne organe. In še pomembneje, formalne zahteve, ki izhajajo iz zakonov, so vse bolj usmerjene k proaktivnemu soočanju z varnostnimi izzivi.

Eden teh neprijetnih izzivov je »umetnost« tolmačenja zakonodajnih zahtev. V teoriji navedene zakone tolmači zakonodajalec, v praksi nadzorni organi s svojim operativnim delom. Preširoko ali nekonsistentno tolmačenje lahko hitro privede do zmede in zadržkov pri implementaciji zahtev.

Proaktivni pristopi

Že v devetdesetih letih prejšnjega stoletja je v slovenski prostor začela postopoma vstopati ideja o vzpostavitvi sistemov upravljanja z varovanjem informacij (SUVI). Ta je postala še posebej relevantna z »uvozom« mednarodnega standarda ISO 27001, ki ureja področje informacijske varnosti. Osnovni koncept je: v organizacijah oblikovati sistem, ki bo omogočal celovit in proaktiven pristop k obvladovanju izzivov v zvezi z informacijsko varnostjo. Tak sistem naj bi obsegal imenovanje odgovornih oseb, ki bodo skrbele za načrtovanje, izvedbo in nadzor SUVI, popis vseh relevantnih IT sredstev, izvedbo ocene tveganj in sprejem ukrepov za obvladovanje teh tveganj, pripravo ustreznih varnostnih politik in pravilnikov, izvedbo tehničnih in organizacijskih ukrepov za zagotavljanje zaupnosti, celovitosti ter dostopnosti podatkov in vzpostavitev sistema poročanja varnostnih incidentov.

SUVI je v praksi doživel različno usodo. Delno zato, ker organizacije (skladno s proračunom, vizijo vodstva in zagnanostjo zaposlenih) različno tolmačijo obseg zahtev, ki jih SUVI nalaga, delno zato, ker so različni sektorji bolj ali manj strogo regulirani. V bančništvu se je zaradi strogih zahtev zakonodaje in mednarodnih standardov implementacija SUVI dobro obnesla, v zdravstvu pa se tega izziva lotevamo postopoma in zadržano – v duhu »žlahtne konservativnosti«, ki na račun počasnega prilagajanja zagotavlja družbeno stabilnost.

Kljub temu ni mogoče spregledati, da se je osnovna ideja SUVI vendarle zasidrala tudi v srce zakonodajalca, ki je v drugi polovici leta 2018 sprejel dva za to področje ključna zakona: Zakon o informacijski varnosti (ZInfV) in Zakon o kritični infrastrukturi (ZIK). Za nadzor nad prvim skrbi Urad za informacijsko varnost RS, za drugega inšpektorat

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



MORS. Zakona sta strukturno in vsebinsko precej podobna, s to razliko, da pokrivata različne segmente organizacij.

Ob bežnem branju pade v oči sorodnost z zahtevami SUVI kakor izhajajo iz že omenjenega standarda ISO 27001. Zakona namreč zahtevata, da izvajalci bistvenih storitev oziroma kritične infrastrukture implementirajo prej naštete zahteve. Osnovni namen zakonov zato ni več sankcioniranje kršitev, ampak usmerjanje (resda z grožnjo glob) k celovitemu in proaktivnemu upravljanju z izzivi na področju informacijske varnosti.

Podoben pristop je opazen tudi na področju varstva osebnih podatkov. Splošna uredba o varstvu podatkov (GDPR) je uvedla kar nekaj (zdaj že dobro znanih) novosti, ki spodbujajo upravljavce in obdelovalce k celovitemu in proaktivnemu obvladovanju izzivov v zvezi z varstvom osebnih podatkov. Osnovne zahteve so sicer še zmeraj enake: skrb za pravno podlago, omogočanje posameznikom, da uveljavljajo svoje pravice, skrb za pogodbe o obdelavi podatkov, previdnost pri iznosu podatkov izven ozemlja EU, in seveda uvajanje tehničnih ter organizacijskih ukrepov za zavarovanje osebnih podatkov pred nepooblaščeno obdelavo. Vendar GDPR zahteva še več: upravljavci in obdelovalci morajo (resda le v nekaterih primerih) imenovati pooblaščeno osebo za varstvo podatkov (DPO), proaktivno poročati o hujših kršitvah, izvajati ocene učinkov v zvezi z varstvom podatkov (DPIA), in usmerjati prizadevanja k uresničevanju vgrajenega in privzetega varstva podatkov.

Vgrajeno varstvo podatkov

Osnovna izhodišča »vgrajenega in privzetega varstva podatkov« je že v devetdesetih letih prejšnjega stoletja v eseju »Privacy by design« zapisala takratna kanadska informacijska pooblaščenka Ann Cavoukian. Skušala je spodbuditi upravljavce in obdelovalce, da že na začetku načrtovanja procesov obdelave podatkov premislijo o načinih in ukrepih, ki bi omogočali doseganje legitimnih ciljev, vendar tako, da bi bilo tveganje za posege v zasebnost posameznikov kar najmanjše. Določila je sedem osnovnih načel: (1) proaktivnost namesto reaktivnosti; (2) zasebnost kot privzeta izbira; (3) zasebnost, ki je sestavni del zasnove rešitve; (4) polna funkcionalnost - igra s pozitivno vsoto, (5) zavarovanje podatkov v celotnem ciklu obdelave podatkov; (6) transparentnost; (7) spoštovanje posameznika.

Njena ideja »vgrajene zasebnosti« se je ponovila v GDPR, ki v členu 25 opredeljuje »vgrajeno in privzeto varstvo podatkov«. To obsega predvsem spodbujanje »minimizacije« oziroma najmanjšega obsega obdelave podatkov, pa tudi nekatere tehnike zakrivanja podatkov, npr. psevdonimizacijo in šifriranje. Manj podatkov, manj tveganj. Podobno velja tudi za širše področje informacijske varnosti.

Sicer pa se težnja po »vgrajevanju« zasebnosti smotrno navezuje na še eno novost GDPR, in sicer na izvedbo ocene učinkov v zvezi z varstvom podatkov. Ta zahteva, podobno kot SUVI, spodbuja organizacije, da se z neprijetnimi izzivi soočijo čim prej.



Izziv za vse

Eden teh neprijetnih izzivov je »umetnost« tolmačenja zakonodajnih zahtev. V teoriji navedene zakone tolmači zakonodajalec, v praksi nadzorni organi s svojim operativnim delom. Preširoko ali nekonsistentno tolmačenje lahko hitro privede do zmede in zadržkov pri implementaciji zahtev. Tega si (z morebitno izjemo svetovalnih podjetij) nihče ne želi. Pred večino nas, ki to revijo beremo in (so)ustvarjamo, je postavljen izziv implementacije SUVI (če tega še nismo naredili) in »vgrajenega varstva podatkov« (česar verjetno še nismo naredili). Pred nadzorne organe pa nič manj zahtevna naloga konsistentnega in razumnega tolmačenja zahtev zakonodaje. Žal bo le čas pokazal kako uspešno in »proaktivno« smo se z izzivom soočili.

Viri

- Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes of Regulation 2016/679.
- Cavoukian, A. (2009) Privacy by Design. The 7 Foundational Principles.
- Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. IEEE Consumer Electronics Magazine, (9:2), str. 78-82.
- Informacijski pooblaščenec (2022). Letno poročilo 2021.
- ISO/IEC 27001:2013.
- ISO/IEC 27701:2019.
- SI-CERT (2022). Poročilo o kibernetski varnosti za leto 2021.
- Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
- Zakon o informacijski varnosti (ZinfV). Ur. l. RS. 30/18.
- Zakon o varstvu osebnih podatkov (ZVOP-1). Ur. l. RS. 94/07. ■

Avtor: Vencel Cserháti / Vodja za kibernetsko varnost in varstvo zasebnosti
Huawei Technologies Madžarska in regija Adriatik



KIBERNETSKI PARADOKS – ZAUPANJE SE GRADI NA SPLOŠNI NEZAUPLJIVOSTI

Z naraščajočo odvisnostjo od digitalnih tehnologij se posamezniki, podjetja in vlade po svetu spopadajo z vse večjim številom groženj v spletnem prostoru. V mnogih primerih se postavlja vprašanje: koliko lahko zaupati digitalnemu svetu in družbenim medijem? Ali so informacije, ki jih prejemamo, verodostojne in zanesljive ali pa so namerno spremenjene?

Ničelno zaupanje – zgolj modni trend?

V zadnjih nekaj letih postajata vsesplošna nezaupljivost in nadzor informacij – kot nekakšen obrambni mehanizem – vse bolj sestavni del našega družbenega življenja, kar je med drugim posledica pojavov, kot sta epidemija koronavirusa in eksplozija lažnih novic. Koncept ničelnega zaupanja v informacijsko tehnologijo (IT) temelji na enakih načelih, in sicer, da smemo v pristnost informacij ali zahtevi za dostop zaupati šele po obsežnem preverjanju. Morda boste mislili, da je ničelno zaupanje nov pojem oz. eden od modnih izrazov, ki so v svetu IT pogost pojav, vendar je veliko več kot to.

Prvi, ki je opredelil koncept ničelnega zaupanja, je bil Stephen Paul Marsh, ki je v svoji doktorski disertaciji aprila 1994 zaupanje formaliziral kot računski koncept. Leta 2009 je Google uvedel arhitekturo BeyondCorp, ki temelji na ničelnem zaupanju. Ameriški nacionalni inštitut za standarde in tehnologijo (NIST) je leta 2018 objavil prispevek, v katerem obravnava koncepte in pristop k ničelnem zaupanju. Veliko spodbudo sprejetju modela je dala odredba ameriškega predsednika Joeja Bidna iz lanskega leta, po kateri morajo za zaščito kritične infrastrukture vse ameriške zvezne agencije do leta 2024 sprejeti koncept ničelnega zaupanja.

Učinek je bil ustrezen: po raziskavi podjetja General Dynamics iz maja 2022 so zvezne agencije naredile pomemben korak naprej, vsaj kar se tiče oblikovanja strategije in začetka izvajanja le-te. 63 odstotkov agencij vključenih v študijo je prepričanih, da bodo zahteve izpolnile do roka leta 2024. Raziskava je tudi pokazala, da agencije čakajo še številni izzivi, kot sta potreba po zamenjavi zastarele infrastrukture in negotovost glede tega, kateri tehnološki sklop, paket ali niz tehnologij izbrati za izvajanje strategije.

S sprejetjem koncepta ničelnega zaupanja se bodo organizacije lahko v veliki meri prilagodile nenehno spreminjajočemu se okolju groženj, saj ničelni koncept upošteva namere in cilje neznanih notranjih in zunanjih zlonamernih akterjev, ki bi lahko v najslabšem primeru vplivali na celotno državo ter onemogočili dostop do kritičnih storitev. Zaradi tega ničelno zaupanje ni le modni izraz, ampak paradigma, ki je pripravljena na prihodnost in ki bi jo morala podjetja uporabiti pri svojih načrtovanih ali sedanjih digitalnih rešitvah in projektih.

Ničelno zaupanje za učinkovitejšo zaščito

Toda kaj natančno je koncept ničelnega zaupanja? Je to nova tehnologija ali nov proizvod? Nič od tega. Ničelno zaupanje je koncept, okvir za dosego idealnega stanja, pri katerem organizacije v samem bistvu ne zaupajo ničemur in nikomur. Niti uporabniku niti napravi ali svojemu internemu omrežju – ki običajno velja za najbolj varno – niti zunanjemu omrežju, zato preverjajo vse, preden izvedejo kakršnokoli operacijo, transakcijo ali zahtevo za dostop. To je varnostni model, osredotočen na podatke in informacije, ki med drugim uporablja načela, kot so dostop z najnižjimi pravicami in podrobno sledenje dogodkom, ki se uporabljajo za vsako operacijo (npr. zahteva za dostop).

Tradicionalni pristop h kibernetski varnosti temelji na perimetrični zaščiti, ki jo večinoma predstavljajo požarni zidovi, in predvideva varno območje znotraj omrežja. S prihodom storitev v oblaku je postala tako imenovana napadna površina veliko večja, izpostavljenost notranjim varnostnim incidentom in napadom z bočnim premikanjem od znotraj pa je še posebej velika. Tu nastopi načelo ničelnega zaupanja, ki enotno nadzoruje vse, ne glede na to, kako in iz katere naprave ali lokacije je bila poslana zahteva za dostop.

ABC ničelnega zaupanja: primer podjetja

Načelo ničelnega zaupanja uporablja tudi družba Huawei Technologies, ki je eno od vodilnih svetovnih podjetij na področju informacijsko-komunikacijske tehnologije. Celotne operacije družbe že leta delujejo po t. i. »načelu ABC«, ki temelji na treh stebrih: *Ničesar ne jemlji za samoumevno! Ne verjemi nikomur!* in *Preverjaj vse!* Pomemben del tega pristopa je načelo sledljivosti, tj. ugotavljanje in preverjanje, kdo je npr. izdelal posamezni proizvod, kdo je naredil zadnjo spremembo v posameznem programu ali od kod izvira strojna oprema. Pristop ničelnega zaupanja zajema celotno organizacijo in delovanje družbe, od oblikovanja, proizvodnje, nabave, logistike, skladnosti z zakonodajo, človeških virov do raziskav in razvoja. Uporablja se celo za podizvajalce, partnerje in tretje osebe, ki dobavljajo blago ali opravljajo storitve.

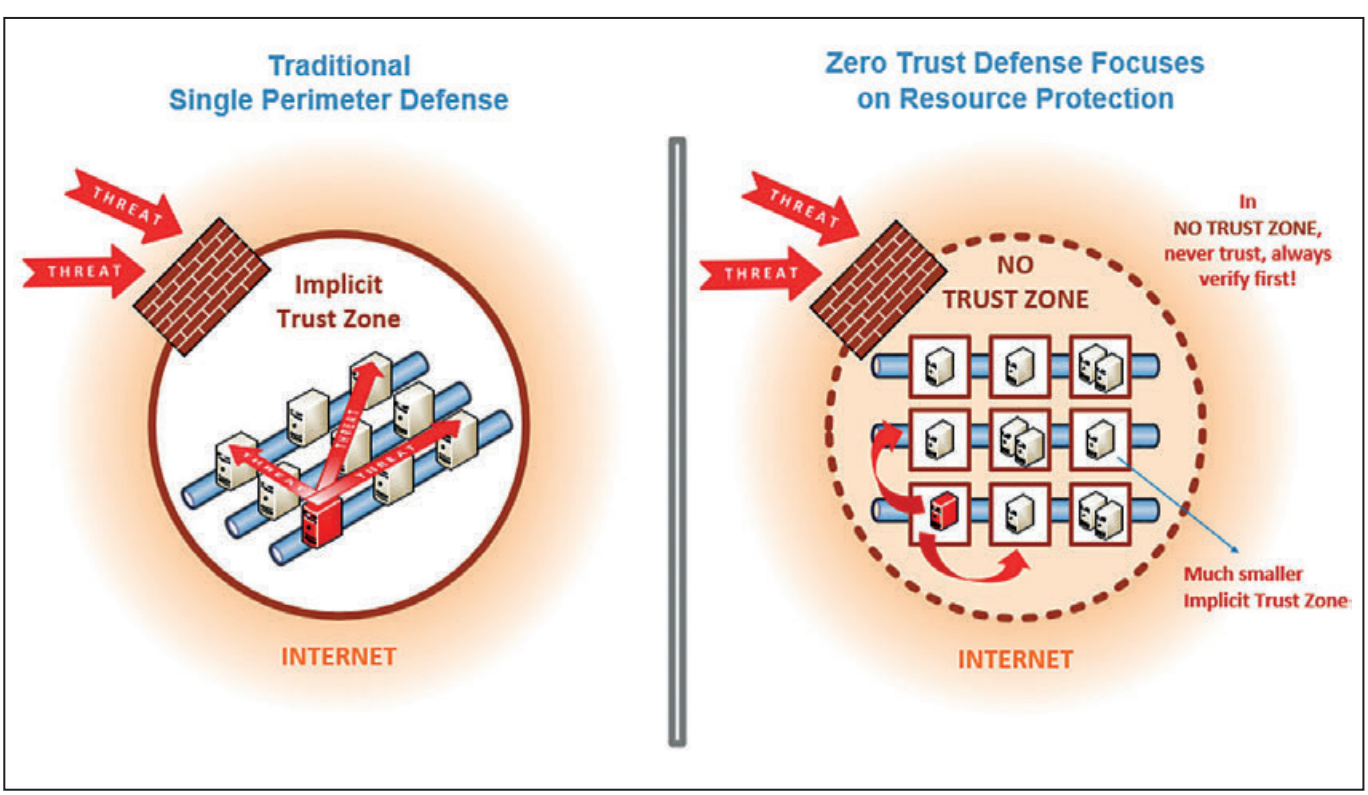
Huawei je doslej z več kot 3800 dobavitelji podpisal sporazume o zahtevah glede kibernetske varnosti, ki jih morajo ti izpolnjevati. Dober primer ničelnega zaupanja je proces oblikovanja arhitektur 5G, kjer pristop zajema štiri glavna področja, ki so: uporabnik, omrežje, skrbnik, ki upravlja omrežje, in omrežne naprave. Načela načrtovanja kibernetske varnosti za omrežja 5G temeljijo tudi na letih prakse na področju telekomunikacij. Huawei je razvil tri slojni varnostni model, ki vključuje neprekinjeno ocenjevanje in dinamično avtorizacijo, zaščito pred vdori in napadi z bočnim premikanjem ter dinamično neprekinjeno optimizacijo, ki temelji na tako imenovanem ogrodju kibernetske varnosti IPDRR.

Pomembno je razumeti, da ko govorimo o kibernetski varnosti, govorimo o objektivnem področju, ki mu je mogoče slediti in primerjati s tehnološkimi in industrijskimi standardi. Eden od pomembnih stebrov varnosti je skladnost tehnologije in uporabljenih omrežnih naprav s standardi kibernetske varnosti.

Glede na vse omenjeno Huawei v največji možni meri spodbuja skladnost s standardi testira svoje omrežne naprave v skladu s splošno sprejetim standardom NESAS/SCAS za omrežne naprave ter na tej osnovi organizira lasten proces razvoja izdelkov.

Več kot zgolj »moden izraz«

Z uvedbo modela ničelnega zaupanja domnevamo, da je do varnostnega incidenta že prišlo ali da bo do njega zagotovo prišlo, zato uporabljamo metode



SLIKA 1: NIČELNO ZAUPANJE – Shema razlike med tradicionalnim omrežjem, zaščitenim s požarnim zidom, ki privzeto velja za zaupanja vrednega, in mikrosegmentiranim omrežjem, temelječim na ničelnem zaupanju. Avtor: A. Kerman, NIST.
Vir: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

obvladovanja tveganj, ki se nenehno natančno prilagajajo in katerih cilj je zmanjšati verjetnost pojava incidenta na skoraj nič.

Celovito varnostno spremljanje, nadzor dostopa, ki temelji na najnižjih pravicah, in avtomatizirano preverjanje izvora ter celovitosti povezav, naprav ali uporabnikov so zelo zaželene prednosti, vendar so cena za to nekatera načela »varnosti v zasnovi, ki za razvoj in implementacijo zahtevajo čas.

S sprejetjem koncepta ničelnega zaupanja se bodo organizacije lahko v veliki meri prilagodile nenehno spreminjajočemu se okolju groženj, saj ničelni koncept upošteva namere in cilje neznanih notranjih in zunanjih zlonamernih akterjev, ki bi lahko v najslabšem primeru vplivali na celotno državo ter onemogočili dostop do kritičnih storitev. Zaradi tega ničelno zaupanje ni le modni izraz, ampak paradigma, ki je pripravljena na prihodnost in ki bi jo morala podjetja uporabiti pri svojih načrtovanih ali sedanjih digitalnih rešitvah in projektih.

Zaključek

Preglednost je na prvem mestu. Poleg uporabe standardov je preglednost enako pomemben del kibernetske varnosti organizacije. V Huawei Centru za transparentnost in kibernetsko varnost v Bruslju, ki je bil odprt leta 2019 in je dostopen za javnost, lahko strokovnjaki za kibernetsko varnost izvajajo tako imenovane preizkuse s »črno skrinjico«. Center strankam omogoča tudi vpogled v svojo izvorno kodo – kot edini med svojimi konkurenti – kjer predstavlja sisteme in prakse kibernetske varnosti v celotni organizaciji družbe Huawei, ter omogoča komunikacijo in izmenjavo informacij med družbo Huawei in ključnimi akterji v industriji. ■





SLIKA 2: HUAWEI Center za transparentnost in kibernetsko varnost, Bruselj. Vir: Huawei





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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

EC-Council CHFI CERTIFIED
EC-Council CPENT CERTIFIED
EC-Council CEH CERTIFIED
EC-Council ECIH CERTIFIED
OFFENSIVE SECURITY OSCP

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

BUREAU VERITAS 1828

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

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije*



ZAČETEK DVEH POMEMBNIH EU PROJEKTOV S PODROČJA ZAŠČITE KRITIČNE INFRASTRUKTURE

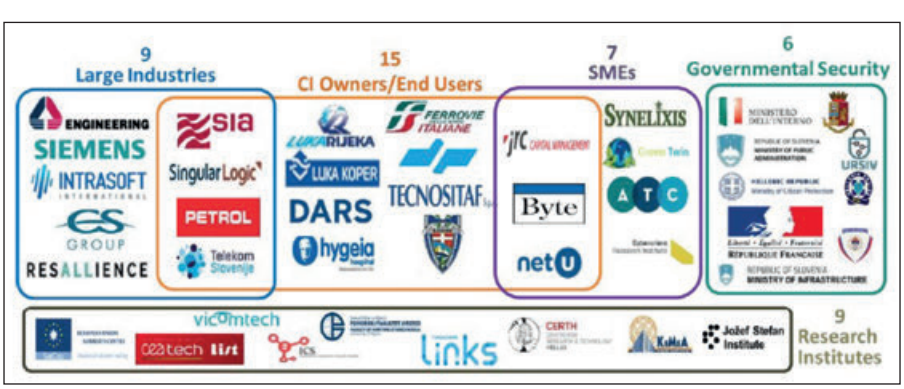
Zaščita in zagotavljanje odpornosti delovanja kritične infrastrukture za EU ostaja ključna naloga. To dokazuje tudi skozi trud in sredstva, ki jih vlaga v razvoj in raziskave povezane s področjem dvigovanja odpornosti kritične infrastrukture.

V letošnjem letu je EU skozi raziskovalno-razvojni mehanizem HORIZON Europe izbrala in financirala dva ključna projekta. Prvi je bil, v okviru razpisane teme »INFRA-01-01: European infrastructures and their autonomy safeguarded against systemic risks«, izbran projekt ATLANTIS - Improved resilience of Critical Infrastructures against large scale transnational and systemic risks. Drugi pa je bil v okviru klica »INFRA-01-02: Ensured infrastructure resilience in case of Pandemics« izbran projekt SUNRISE - Strategies and technologies for united and resilient critical infrastructures and vital services in pandemic-stricken Europe. Posebej nas lahko veseli, da so organizacije, kot so Institut za korporativne varnostne študije, Ministrstvo za infrastrukturo, Telekom Slovenije in Slovenske železnice, edine evropske organizacije, ki so prisotne v obeh projektih. To je seveda dokaz odličnosti in prodornosti slovenskega znanja in seveda priznanje za odlično delo v fazi priprave na objavljen razpis. V nadaljevanju si podrobneje oglejmo vsebino in glavne cilje obeh navedenih projektov.

ATLANTIS

Mednarodni konzorcij obsega 39 partnerjev iz 11 držav. V okviru tega projekta je zelo velik del slovenskih partnerjev, katere poleg Instituta za korporativne varnostne študije predstavljajo še Inštitut Jožef Štefan Luka Koper, PETROL, Slovenske železnice, DARS, Telekom Slovenije, Ministrstvo za infrastrukturo in Urad RS za informacijsko varnost.

Zanesljivo, robustno in prožno delovanje kritičnih infrastruktur (KI) je predpogoj za celovitost vitalnih elementov v naši družbi ter varnost, dobro počutje in gospodarsko blaginjo Evrope, njenih državljanov in podjetij. Strategija varnostne unije EU za obdobje 2020–2025 opredeljuje zaščito KI kot eno glavnih prednostnih nalog EU in njenih držav članic. Vendar pa so KI postale zelo zapletene in delujejo v hitro razvijajočem se družbenem, tehnološkem in poslovnem okolju.



Slika 1: Partnerji projekta ATLANTIS

"The project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073909".

*avtorica je članica Slovenskega združenja korporativne varnosti

Posebej nas lahko veseli, da so organizacije, kot so Institut za korporativne varnostne študije, Ministrstvo za infrastrukturo, Telekom Slovenije in Slovenske železnice, edine evropske organizacije, ki so prisotne v obeh projektih. To je seveda dokaz odličnosti in prodornosti slovenskega znanja in seveda priznanje za odlično delo v fazi priprave na objavljen razpis.

Naraščajoča digitalizacija in medsebojna povezljivost KI, ki temeljijo na novih tehnologijah in tehnološko dovršenih aplikacijah, ustvarjajo potencialno nove ranljivosti, vključno s tistimi, ki jih namerno prenašajo ljudje in zaposleni (npr. notranja grožnja, ki jo predstavljajo sedanji ali nekdanji zaposleni, ki lahko zlorabijo svoje pravice dostopa do informacij znotraj organizacij in s tem škodujejo in povzročajo škodo) ali ne namerno (npr. nesreča, človeška napaka, socialni inženiring). Poleg tega, ker so KI bolj omrežne, medsebojno povezane in odvisne druga od druge, imajo lahko resne motnje v eni od njih in v nekaterih primerih dolgotrajne kaskadne učinke v drugih KI in storitvah, ki so bistvenega pomena za vzdrževanje kritičnih družbenih in gospodarskih dejavnosti, celo v več sektorjih in čezmejno (nekatere KI zagotavljajo bistvene storitve prek državnih meja ali celo po vsej EU, kot so npr. vesoljske storitve). To poveča površino napadov in vpliv napadov, ki se lahko hitro stopnjujejo in negativno vplivajo na druge KI in širše dele vitalnih družbenih funkcij. V tem nastajajočem varnostnem okolju evropske kritične infrastrukture (EKI) vse bolj postajajo tarče novih kategorij hibridnih groženj in napadov, ki jih podpirajo tehnološke inovacije, kot so zloraba/napadi na orodja/metode umetne inteligence in hitri razvoj drugih sofisticiranih tehnologij (kot so vozila brez posadke, 5G).

Več projektov CIP/INFRA se v glavnem ukvarja z zaščito in odpornostjo posameznih sektorjev KI (ali celo posameznih komponent znotraj njih), pri čemer zagotavlja le predhodno analizo in modele soodvisnosti in kaskadnih učinkov med njimi, v primeru kritičnih dogodkov. Vendar so bile v takšnih projektih opravljene omejene raziskave o obsežnih, transnacionalnih in med domenskih usklajenih napadih. Še pomembneje, obsežna ocena ranljivosti in analiza tveganja na sistemski ravni, ki se sooča s tveganjem zloma celotnega sistema, še nikoli nista bili obravnavani. Medtem, ko so bile grožnje (tako fizične kot kibernetske) obravnavane z različno stopnjo učinkovitosti, sistemsko tveganje, ki pa izhaja iz velikih nevarnosti in kompleksnih groženj, ni bilo dovolj upoštevano in razumljeno. Napadi so lahko kiber-fizični, usklajeni (med različnimi akterji, tudi v različnih državah), mešani (z uporabo različnih taktik), moteči (vodijo v propad celih sistemov, sektorjev ali regij), nepričakovani, subverzivni in jih je težko zgodaj prepoznati, kot tudi pripisati določenim akterjem (tudi zaradi novih kriminalnih poslovnih modelov). Naraščajoče večje naravne nevarnosti (npr. poplave, požari v naravi, pogosto nepričakovani in nepredvidljivi) so prav tako velike skrbi, ki lahko povzročijo motnje v delovanju kritične infrastrukture in tako vplivajo na širše funkcije naše družbe. To lahko zahteva dolgoročne analize in predvidevanja. Pomembno je omeniti, da sistemska tveganja v veliki večini ne sledijo običajni porazdelitvi tveganja, temveč se širijo z izjemno visokimi stopnjami, kar pomeni visoko verjetnost sprožitve anomalij, nestabilnosti in potencialno katastrofalnih, kaskadnih učinkov na ugnezdene ali medsebojno povezane sisteme, organizacije, regionalna gospodarstva, države ali celo na ravni EU. Temeljni izziv za obvladovanje sistemskega tveganja v takšnem mrežnem scenariju je, da razumemo sistem kot kompleksno mrežo posameznih in institucionalnih akterjev z različnimi in pogosto nasprotujočimi si interesi, vrednotami in pogledi na svet. To bo zahtevalo preglednost in odgovornost procesa obvladovanja tveganja ter učinkovitost in trajnost rezultata.

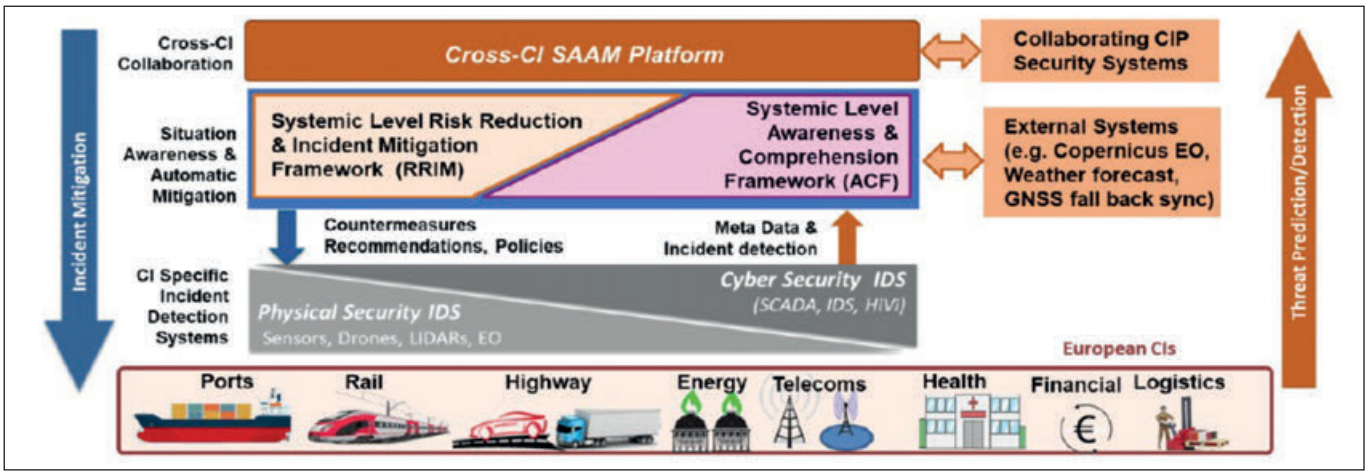


Slika 2: Large Scale Pilot: Cross-Border/Cross Domain Large Scale Pilot in Transport, Energy and Telecoms v katerega je vključeno 10 slovenskih organizacij

Poslanstvo ATLANTIS bo doseženo z zasledovanjem naslednjih 4 strateških ciljev (SG):

SG1: DVIGOVANJE ZAVESTI. Izboljšati znanje o obsežnih ocenah ranljivosti in dolgoročnih sistemskih tveganjih. ATLANTIS bo prispeval k izboljšani obsežni oceni ranljivosti ter ustvarjanju ustreznega znanja in ozaveščenosti o odpornosti EKI na sistemska tveganja. To bo zagotovilo višjo raven znanja in razumevanja tveganj/hibridnih groženj, ki jih morajo obravnavati KI, varnostnih strategij za pripravo, predvidevanje, preprečevanje, odkrivanje, blaženje, odzivanje na takšne grožnje in okrevanje. ATLANTIS bo omogočil polno izkoriščanje svojih tehnoloških inovacij s kulturo varnosti EKI in izvajanjem na človeka osredotočenega pristopa, ki združuje podporo pri odločanju in človeško strokovno znanje.

SG.2: ZMOGLJIVOST. Izboljšati sistemsko odpornost EKI z novimi, prilagodljivimi, prožnimi in prilagodljivimi varnostnimi ukrepi (»po zasnovi«) in orodji (»po inovaciji«). Zagotavljanje sistematičnih metod, postopkov in no-



Slika 3: Arhitektura projekta Atlantis

vih orodij za ocenjevanje, upravljanje in ublažitev sistemskega tveganja, ki izhaja iz hibridnih groženj in zapletenih kibernetskih fizičnih napadov. To bo vključevalo orodja usmerjena v odpornost za oceno ranljivosti, oceno tveganja, načrtovanje odziva, obveščanje o grožnjah, napovedovanje in predvidevanje, sanacijo in ublažitev, odkrivanje (hibridnih, sistemskih napadov), upravljanje odzivanja, oceno škode, okrevanje s ciljem povečanja operativnega in sistemskega neprekinjenega poslovanja.

SG.3: SODELOVANJE. Učinkovito sodelovanje med operaterji KI in vladnimi varnostnimi deležniki ob ohranjanju avtonomije in suverenosti KI. Omogočiti učinkovito sodelovanje, da bi: 1) pripravili in izvedli skupne in usklajene načrte odpornosti, ublažitve in odzivanja za obvladovanje sistemskih tveganj; 2) ustvarjanje in upravljanje skupne situacijske »slike« ter izmenjava ustreznih informacij in obveščevalnih podatkov; 3) ovirati širjenje kaskadnih učinkov: a) med fizičnim in kibernetskim svetom; b) med medsebojno povezanimi in soodvisnimi KI.

SG.4: TEHNOLOGIJA. Zagotavljanje odprtega tehnološkega okvira, ki bo EKI zagotovil rešitve, ki temeljijo na umetni inteligenci, za večjo ZAVEST, ZMOGLJIVOST in SODELOVANJE pri obvladovanju sistemskih groženj. ATLANTIS bo omogočil preprosto integracijo prihodnjih varnostnih tehnologij, podatkovnih virov/analiz, storitev za podporo odločanju in učinkovito integracijo obstoječih rešitev, ki so že nameščene v KI. Okvir bo temeljil (kadar koli je to primerno) na odprtokodni tehnologiji in/ali tehnologiji EU, da bi prispeval k strateški neodvisnosti EKI in EU glede kritičnih storitev.

Sunrise

Mednarodni konzorcij obsega 41 partnerjev iz 13 držav. V okviru tega projekta je zelo velik del slovenskih partnerjev, ki so poleg Instituta za korporativne varnostne študije še XLAB, ELES, Slovenske železnice, UKC Ljubljana, Telekom Slovenije, Ministrstvo za infrastrukturo in Plinovodi.

SUNRISE bo olajšal aktivno sodelovanje evropskih KI in jim pomagal, da bodo bolje pripravljeni in opremljeni za ustrezno oceno in skupno obvladovanje prihodnjih tveganj, ki jih povzročajo pandemije. Evropske države članice se razlikujejo glede storitev, infrastruktur, subjektov in sektorjev, ki so uradno priznani kot kritični. Na ravni EU ni enotnega priznanega seznama sektorjev KI. Na primer, direktiva EKI zajema dva sektorja, medtem ko jih direktiva NIS pokriva sedem. Na nacionalni ravni se tudi sektorska pokritost razlikuje. Večina držav članic formalno priznava energijo, promet in bančništvo kot kritične sektorje, nekatere države pa uradno ne priznavajo zdravja, digitalne infrastrukture, hrane ali javne uprave – nekaterih najpomembnejših storitev v pandemiji – kot kritičnih. To pomeni, da v več državah članicah obstajajo bistvene storitve, za katere ne veljajo enaki postopki ocenjevanja tveganja in ublažitve ter tako ne upoštevajo ustrezno novih groženj, ki jih povzroča pandemija.

In ker je naša močno prepletena evropska KI močna le toliko, kolikor je močan njen najšibkejši člen, moramo zagotoviti, da so vse vitalne storitve, specifične za



Slika 4: Geografska razporejenost partnerjev projekta SUNRISE

"The project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073821".

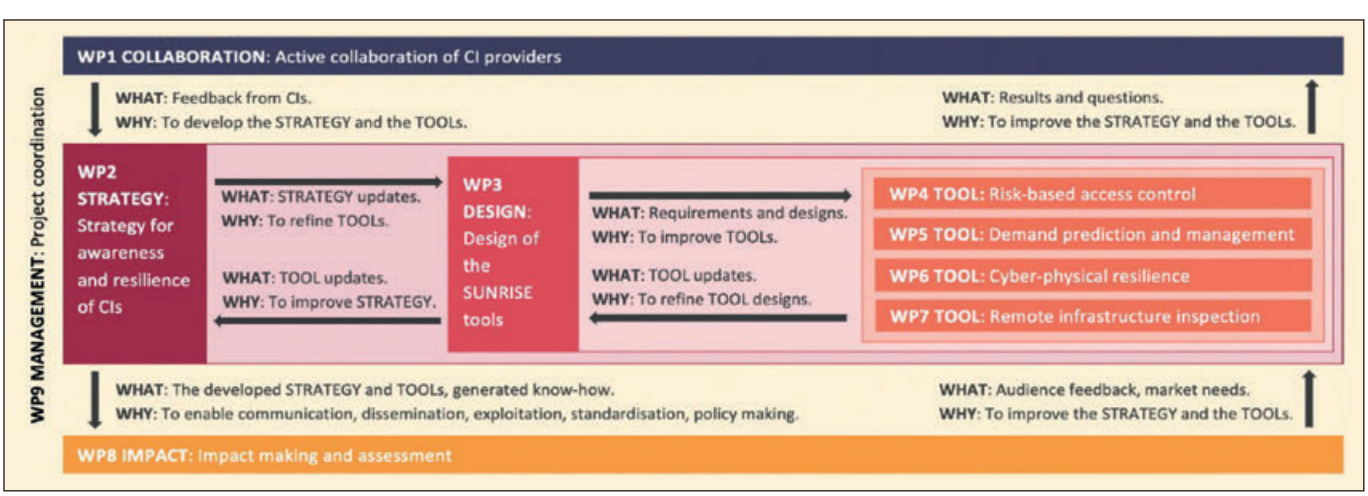
Razvojno raziskovalni projekti na področju kritične infrastrukture, financirani v okviru projektov HORIZON EUROPE, so ključni za boljše razumevanje zahtevnega varnostnega okolja, zagotavljajo temelj za analizo možnih kaskadnih vplivov med soodvisnimi kritičnimi infrastrukturami in na koncu zagotavljajo odlično podlago za boljše sodelovanje med različnimi pomembnimi deležniki, tako na nacionalnem kakor tudi mednarodnem okolju. Institut za korporativne varnostne študije ima v tem mednarodnem okviru vedno pomembnejšo koordinativno vlogo.

pandemijo, po Evropi odporne, ne glede na njihov formalni status. SUNRISE bo identificiral ključne storitve, specifične za pandemijo, in zagotovil sredstva za izenačitev in povečanje njihove odpornosti. Če se ne bodo ustrezno lotili, bodo zgoraj opisane težave postale še bolj pereče zaradi vse pogostejših ekstremnih vremenskih pojavov in vse pogostejših pandemij. Naraščajoče krčenje gozdov, spremembe rabe zemljišč in podnebne spremembe bodo povzročile izgubo življenjskega prostora za živali, zaradi česar bodo morale migrirati in se srečevati z drugimi živalmi, kar se običajno ne bi, to pa bo ustvarilo več možnosti za patogene, da pridejo v nove gostitelje, se prenesejo iz živali na ljudi ter povzročajo pogostejše izbruhe bolezni in s tem skrajšajo intervale med različnimi pandemijami. Podnebne spremembe bodo vplivale tudi na povpraševanje po energiji in oskrbi z vodo, ekstremno vreme pa bo vse pogostejše in hujše. V prihodnosti bodo morale biti KI sposobne upoštevati negotovosti, se prilagoditi podnebnim spremembam in pogostejšim zdravstvenim krizam ter zagotoviti zanesljivost zagotavljanja storitev v različnih možnih prihodnjih scenarijih. SUNRISE vključuje modeliranje podnebnih sprememb in širjenja bolezni, analize kaj če, in povezano celovito oceno tveganja za KI. Tudi družba se spreminja. Tehnološki napredek v zadnjem desetletju in kriza, v kateri smo danes, trajno preoblikujejo našo družbo. V pisarnah ne delamo več s polnim delovnim časom in hibridni delovni model bo v prihodnosti postal norma. Digitalno smo povezani bolj kot kdaj koli prej – naše družbeno življenje, izobraževanje in zdravstvo so postali digitalni. Manj potujemo, več nakupujemo. Več je polarizacije, več je nezaupanja v institucije, razlika v neenakosti pa se povečuje. Vsi ti trendi vplivajo na KI, ker so ljudje tisti, ki oblikujejo, upravljajo in uporabljajo njihove storitve. Da bi zagotovili odpornost in stabilnost KI, potrebujemo pristope in rešitve, ki ne bodo zagotavljali le boljše odpornosti naših fizičnih infrastruktur, ampak bodo upoštevali tudi naše družbeno kritične infrastrukture: državljane, delovno silo in oblikovalce politik. SUNRISE uporablja interdisciplinarni pristop, ki zagotavlja, da se dolgoročne in kratkoročne spremembe v naših družbah med pandemijo načrtno upoštevajo.

Glavni cilji projekta SUNRISE: (1) Okrepiti aktivno sodelovanje KI v Evropi za izmenjavo najboljših praks in združevanje moči v primeru pandemij. (2) Opredeliti ključne storitve in KI, specifične za pandemijo, njihove odvisnosti, tveganja, kaskadne učinke in učinkovite ukrepe za njihovo obravnavo na evropski ravni. (3) Razviti strategijo (TRL8) in orodja (TRL7), ki v Evropi zagotavljajo razpoložljivost, zanesljivost in kontinuiteto kritičnih storitev, specifičnih za pandemijo. (4) Rezultate pilotnih testnih okolij prenesti v operativna okolja evropskih KI tako, da bodo odporna in sposobna učinkovitega odzivanja na stanja različnih pandemij. (5) Spodbujanje implementacije vse evropskega pristopa, da se zagotovi enotne in celovite ukrepe za dvigovanje odpornosti naših KI na pandemije.

Iz zapisanega lahko ugotovimo, da imamo pred seboj dva izredno zahtevna evropska projekta, ki pa sta usmerjena v center reševanja izzivov s katerimi se sooča evropska kritična infrastruktura. Vabimo vas, da skozi naslednja tri leta spremljate razvoj obeh projektov, saj vas bomo tekoče seznanjali z dobrimi praksami in najnovejšimi spoznanji, do katerih bomo prišli skupaj s sodelujočimi partnerji na obeh projektih. ■

SUNRISE



Slika 5: Procesna opredelitev projekta SUNRISE

Avtor: mag. Miran Novak / vodja projektov digitalizacije / CDO, Melamin d.d.*



VAROVANJE INTEGRITETE BLAGOVNIH ZNAMK IN SLEDENJE POREKLA IZDELKOV

Problematika varovanja blagovnih znamk pred ponaredki je bila izpostavljena na nedavnem srečanju slovenskega združenja za korporativno varnost. Podobno se zastavlja vprašanje, ali kaže zaupati deklaracijam na izdelkih, ki opisujejo poreklo le-teh. Pogosto ugotovimo, da je v primerih ponaredkov, deklaracija o poreklu ravno tako lažna in se v bistvu srečujemo z istim problemom. Pričujoči prispevek nakazuje možnosti uporabe tehnologij veriženja blokov za preprečevanje omenjenih zlorab.

Uvod

Običajno si kupec zavestno ne želi kupiti ponarejenega izdelka. Resnici na ljubo, se to včasih dejansko dogaja, še zlasti pri izdelkih prestižnih modnih znamk, ki veljajo za statusni simbol. Prestižne švicarske ure po 20 EUR na istanbulski tržnici očitno najdejo svoje kupce. Tako ali drugače, je lastnik blagovne znamke oškodovan v obeh primerih, v prvem pa poleg njega še kupec. Za preprečevanje takšnih zlorab so države sprejele bolj ali manj restriktivno zakonodajo, inšpekcije in organi pregona pa ta dejanja preiskujejo in skušajo v kar največji meri to preprečevati. Je pa to, roko na srce, bolj kot ne, boj z mlini na veter, saj so zaslužki v tem poslu vse preveč mamljivi. Kot piše Handfield v [1], je bila po navedbah OECD ocenjena vrednost trga s piratskimi in ponarejenimi izdelki v letu 2013 okrog 1 bilijona USD, v letu 2022 pa naj bi ta vrednost narastla na 3 bilijone USD. Isti vir navaja, da so med najbolj izpostavljenimi blagovnimi skupinami potrošniško blago, tobačni izdelki, komponente za letalsko industrijo (!), elektronske naprave, farmacevtski izdelki, ... Ne gre torej zgolj za pridobitništvo, temveč za resen kriminal, ki neposredno ogroža življenja. Malce nelagodno bi stopili na letalo, če nismo gotovi, ali so v njem vgrajeni originalni deli.

Veriženje blokov

O tehnologiji veriženja blokov, oziroma angleško *BlockChain* je bilo v zadnjih letih napisanega zelo veliko. Največ v povezavi s kripto valutami. Študij tehnologije veriženja blokov ni namen tega prispevka. Za njegovo razumevanje zadošča poljuden opis, ki ga najdemo na primer v [2].



*podjetje je korporacijski član Slovenskega združenja korporativne varnosti



Tehnologija temelji na veriženju neprodornih algoritmov, na katerih je zapisana vsota podatkov o neki transakciji – lahko gre za prenos zneska, izvršljivo pogodbo ali prenos drugih podatkov. Vsaka transakcija dobi svoj blok – algoritem, ki se postavi v vrsto z drugimi algoritmi in tako tvori sistem verige blokov, ki prenaša informacije o valuti, njeni vrednosti, nekdanjih in sedanjih lastnikih. Koncept je prvič leta 2008 predstavila oseba z vzdevkom Satoshi Nakamoto, leto dni kasneje pa se je sistemu pridružila trenutno najbolj poznana digitalna valuta bitcoin.

Radovednejši bralec bo obširnejšo, a še vedno dovolj poljudno razlago, našel v članku iz revije Monitor, oktober 2017 [3].

Zaenkrat tehnologija velja za varno, torej takšno, ki se je z razumnimi sredstvi ne da razbiti, oziroma kompromitirati. Monitor v [3] sicer navaja tveganje, da bi razvoj kvantnih superračunalnikov utegnil privesti do dovoljšnje procesorske moči za razbitja verig blokov, a v dogledni prihodnosti tega še ni pričakovati.

Blokovna veriga za izdelke

Predstavljajmo si torej, da namesto kripto transakcije kateregakoli-že-coina, transakcijo predstavlja proizvodni proces, kjer iz ene ali več surovin, oz. polizdelkov, sestavimo izdelek. To verigo lahko začnemo že pri osnovni surovini, na primer, železovi rudi. Tako bi lahko v vsakem nadaljnjem koraku predelave ustvarili blok, ki bi produkt spremljal v proizvodnem zaporedju. Na enak način, kot transakcijske verige kripto valut vsebujejo informacije o »rojstvu« kripto kovanca in o vseh njegovih naslednjih lastnikih (tu seveda ne govorimo o osebnih podatkih!), bi na tak način opisan izdelek vseboval celovito in ne ponaredljivo informacijo o njegovem poreklu ter pristnosti. Zraven bi lahko vključili še poljubne informacije o, recimo, porabi energije za izdelavo, morda celo o sproščenem ogljikovem dioksidu v procesu izdelave, ali pa, če hočete, številu kilometrov, ki jih je polizdelek prepotoval do mesta vgradnje.

Uporaba tehnologije veriženja blokov v tak namen ne bi bila uporabna zgolj za končnega kupca, ki lahko kadarkoli preveri poreklo in pristnost blaga, ki ga je kupil, ampak tudi za udeležence v proizvodnem procesu, na koncu pa še za regulatorne organe, ki bi na ta način lahko sledili atribute izdelka in ga uvrstili v ustrezne kategorije (npr. davčne).

Tak sistem bi na globalni ravni lahko deloval le, če bi vse v verigi udeležene prepričali (ali pa prisilili), da svojo aktivnost v verigi popišejo v bloku. Verjamem, da bi marsikdo raje skril poreklo surovine, kot pa jo navedel na tak način, zato menim, da masovne uporabe podobnega sistema še nekaj časa ne bomo imeli priložnosti videti.

Da bi bil sistem uporaben, seveda ni potrebno, da se vanj vključijo vsi v proizvodnjo-trženjski verigi. Že dva ali trije deležniki, ki ocenijo, da bi od tega imeli korist, lahko ustvarijo blokovno verigo s podatki. Verjetno bi kupec bil pripravljen plačati nekaj več, če bi imel na voljo neovrgljiv dokaz o poreklu izdelka, ki ga kupuje. Pa tu ne mislim zgolj na blagovne znamke, ampak tudi na živilske in kmetijske izdelke.

Lastniki blagovnih znamk, ki se, kot uvodoma povedano, borijo proti ponarejevalcem, bi na ta način v roke dobili močno orožje za zaščito svojih zakonitih interesov.

Kaj pa praksa?

Teoretična izhodišča tehnologije veriženja blokov so tudi v slovenskem prostoru zelo dobro obdelana skozi številne zanimive doktorske, magistrske in seminarske naloge na fakultetah in visokih ter višjih šolah. Je pa tudi pri nas kar nekaj podjetij, ki razpolagajo s potrebnim znanjem in orodji, da opisane ideje dejansko tudi v praksi implementirajo. Tehnologija veriženja blokov je namreč poleg omogočanja kripto valut, našla precej aplikativnih področij, opisani primer je zgolj en primer uporabe. V okviru platforme Industrija 4.0 je, kot se vidi iz [4], nabor praktične uporabe tehnologije veriženja blokov zelo širok, kar obeta njeno še intenzivnejšo praktično rabo v prihodnosti.

Viri

[1] https://scm.ncsu.edu/scm-articles/article/counterfeiting-is-on-the-rise-projected-to-exceed-3-trillion-in-2022 , zajeto 14. 11. 2022

[2] https://iprom.si/slovar/14-tehnologija-verizenja-blokov-veriga-podatkovnih-blokov/ , zajeto 14. 11. 2022

[3] https://www.monitor.si/clanek/verizenje-blokov-in-razprsene-evidence/181948/ , zajeto 14. 11. 2022

[4] https://www.indu40.io/?utm_source=traffus_google&utm_medium=search&utm_campaign=blockchain&utm_term=blockchain%20use%20cases , zajeto 15. 11. 2022 ■

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 23. MAJ 2023

14. 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!

14. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 23. - 24. MAJ 2023



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