Korporativna varnost

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

Letnik 2025, november • št. 39

Bralcem revije želimo miren božič in vse dobro v letu 2026

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

VAŠA 360° VARNOST 365 DNI V LETU

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

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

CENTER KIBERNETSKE VARNOSTI IN ODPORNOSTI

TelekomSlovenije
Vedno na boljše.

Telekom Slovenije, d.d., Ljubljana.

Korporativna varnost

Spoštovane bralke in bralci!

Izdajatelj:
Institut za korporativne varnostne študije, ICS-Ljubljana

Naslov izdajatelja in uredništva:
Cesta Andreja Bitenca 68
1000 Ljubljana

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

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

Oblikovanje in DTP:
Robert Mostar

Tisk:
tiskano v Sloveniji

Datum izida:
november 2025

Izvod revije je brezplačen

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

ISSN 2232-6170

Sodobno varnostno okolje postaja vse bolj zapleteno, prepleteno in nepredvidljivo. Organizacije se soočajo z izzivi, ki presegajo tradicionalne okvire razumevanja varnosti od kibernetskih groženj, geopolitičnih napetosti, vplivov podnebnih sprememb pa do motenj v dobavnih verigah in hitro razvijajočih se tehnologij. Vse to zahteva nov, celovit pogled na korporativno varnost, ki presega posamezne sektorje in povezuje različne deležnike, tako v javnem kot zasebnem sektorju.

Pomemben mejnik na tem področju predstavlja implementacija novega Zakona o informacijski varnosti, ki prinaša številne spremembe in zahteve, zlasti za subjekte, ki opravljajo ključne storitve. Zakon postavlja temelje za vzpostavitev enotnih standardov informacijske in kibernetske varnosti ter krepi odgovornost organizacij za zaščito podatkov, informacijskih sistemov in digitalne infrastrukture. Njegova učinkovita izvedba bo v prihodnjih mesecih in letih ključno vplivala na stopnjo odpornosti države ter družbe kot celote.

V tej številki revije poleg ostalih prispevkov izpostavljamo zlasti intervjuja z dvema ministricama, ki s svojega področja pomembno sooblikujeta nacionalno odpornost Republike Slovenije. Ministrica za digitalno preobrazbo osvetljuje izzive digitalne preobrazbe, pomen kibernetske varnosti in strateške usmeritve države na področju digitalne odpornosti. Ministrica za kmetijstvo, gozdarstvo in prehrano pa izpostavlja pomen varovanja prehranske varnosti, trajnostnega upravljanja z naravnimi viri ter odpornosti ključnih sistemov, ki zagotavljajo preskrbo prebivalstva v kriznih razmerah.

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

Prepričani smo, da bo predstavljena vsebina bralkam in bralcem nudila dodatno strokovno podporo ter jih spodbudila k nadaljnjemu razmisleku o pomenu usklajenega, sistematičnega in celostnega pristopa k obvladovanju varnostnih tveganj. S tem si želimo prispevati k dvigu splošne varnostne kulture in krepitvi odpornosti organizacij ter družbe kot celote v sodobnem in izzivov polnem varnostnem okolju.

V uredništvu revije Korporativna varnost upamo, da boste tudi v 39. številki našli ustrezne strokovne vsebine, ki vam bodo pomagale pri vašem zahtevnem delu.

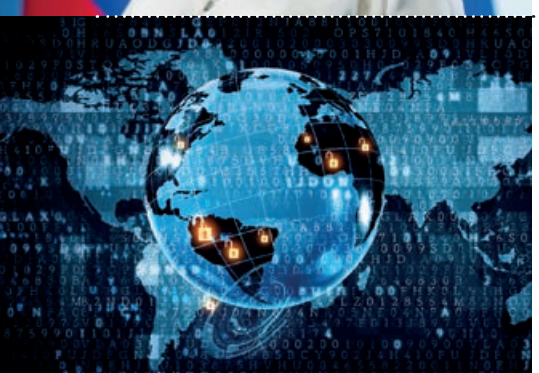
izr. prof. dr. Denis Čaleta
Glavni urednik

INTERVJU
mag. Ksenija Klampfer,
ministrica za digitalno preobrazbo

DIGITALNA PREOBRAZBA KOT TEMELJ PRIHODNOSTI DRUŽBE

INTERVJU
Mateja Čalušić,
ministrica za kmetijstvo, gozdarstvo in prehrano

KAKO SLOVENIJA KREPI ODPORNOST PREHRANSKE VERIGE V ČASU KRIZ



DEJAVNIKI KIBERNETSKE ODPORNOSTI ELEKTROENERGETSKE KRITIČNE INFRASTRUKTURE – ALIENS-SOC

Kibernetska varnost energetske kritične infrastrukture postaja vse zahtevnejši izziv zaradi kompleksnih integriranih informacijskih in procesnih omrežij, medsebojnih odvisnosti z drugimi sektorji, geopolitičnih razmer, vse naprednejših tehnologij in vektorjev napadov, resnih posledic potencialnih napadov ter privlačnosti za napadalce.

INTERVJU
Tone Stanovnik,
Špica International, d.o.o.

OBLAK JE NOVA KRIVULJA RASTI, NE ZGOLJ TEHNOLOŠKI TREND

INOVATIVNA UPORABA UMETNE INTELIGENCE ZA KREPITEV PREISKOVALNE ANALITIKE V OKVIRU PROGRAMA HORIZON EUROPE

V zadnjih letih se vse policije pri preiskovanju kaznivih ravnanj soočajo z vedno večjimi količinami heterogenih podatkov. Tradicionalni pristopi za učinkovito odkrivanje sumljivih povezav in vzorcev v podatkih so postajali nezadostni za podporo operativnim preiskavam.

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

INTERVJU
mag. Ksenija Klampfer, ministrica za digitalno preobrazbo

DIGITALNA PREOBRAZBA KOT TEMELJ PRIHODNOSTI DRUŽBE

Digitalna preobrazba ni več zgolj tehnološki proces, temveč temelj sodobne družbe, ki oblikuje način dela, življenja in medsebojnega povezovanja. V Sloveniji se ta preobrazba odvija hitro, kar potrjujejo tako evropska poročila kot konkretni projekti v javnem in zasebnem sektorju. V ekskluzivnem intervjuju z mag. Ksenijo Klampfer, ministrico za digitalno preobrazbo, smo se pogovarjali, kako država s strateškimi investicijami, inovativnimi rešitvami in programsko podporo gradi digitalno prihodnost, hkrati pa skrbi za varno ter etično rabo tehnologij, kot je umetna inteligenca.

Najprej nam dovolite, da vam in vašim sodelavcem čestitamo za odlično delo. Digitalizacija ni več samo tehnični proces, temveč družbena sprememba. Kako ocenjujete stopnjo digitalne razvitosti Slovenije in kaj so vaše ključne prioritete v tem mandatu?

Najlepša hvala. Če pogledamo junijsko Poročilo o stanju digitalnega desetletja Evropske komisije, se Slovenija uvršča med države z visoko stopnjo ambicioznosti: vseh 13 nacionalnih ciljev je usklajenih z EU do 2030, kar 63 % ciljev sledi časovnici, naslovili pa smo že 82 % priporočil za 2024. Posebej izstopa širitev 5G – tudi na podeželju – in pospešena gradnja optike. V podjetjih vidimo skoraj podvojeno uporabo umetne inteligence glede na leto prej, zelo aktivni smo tudi pri strateških tehnologijah, kot so kvantno računalništvo, polprevodniki, oblak in umetna inteligenca. Digitalne javne storitve so dostopne in blizu povprečja EU. Naš fokus je pospešiti podporo MSP-jem pri uvajanju naprednih tehnologij, dvigovati osnovne in napredne digitalne spretnosti ter povečati delež IKT-strokovnjakov. To pomeni: konkretna pomoč podjetjem, sistematična krepitev znanj in stalna nadgradnja javnih storitev.

Pogosto lahko slišimo, da digitalizacija včasih prehiteva potrebe ljudi. Kako boste zagotovili, da bo digitalni razvoj usmerjen v uporabnika in ne zgolj v tehnologijo?

V središče postavljamo človeka. Vizija Digitalne Slovenije 2030 se v Strategiji digitalnih javnih storitev 2030 prevaja v pet smeri: soustvarjanje z uporabniki, preprostost, vključenost, podpora in izobraževanje ter aktivna promocija. Ne želimo storitev, ki so samo “na voljo” - želimo, da jih ljudje z veseljem uporabljajo. Zato poenostavljamo uporabo digital-

Varnost gradimo celostno in preventivno. Varnostno-operativni center MDP, ob sodelovanju vodilnih slovenskih podjetij s področja kibernetske varnosti grožnje zaznava in blaži, še preden prerastejo v incidente.

*avtor je član Slovenskega združenja korporativne varnosti

ne identitete, povezujemo najpogostejše storitve na enem mestu in krepimo pomoč uporabnikom prek Enotnega kontaktnega centra (tudi prek Viberja in WhatsAppa) ter mreže Digi info točk. Med resorji standardiziramo uporabniško izkušnjo, da je pot uporabnika kratka, jasna in predvidljiva.

Digitalna izključenost ostaja velik izziv v Sloveniji. Kako boste poskrbeli, da digitalizacija ne bo povečala družbenih razlik med mestom in podeželjem ter mladimi in starejšimi?

Digitalizacija je orodje za bolj povezano, vključujočo in trajnostno družbo. Naš cilj je odgovorna raba tehnologij, ki povečuje odpornost skupnosti, pospešuje dostop do ključnih informacij in storitev ter ljudem olajša življenje tam, kjer to najbolj šteje.

Zavedamo se tveganj, zato z deležniki sistematično dvigujemo digitalne kompetence. Po Zakonu o spodbujanju digitalne vključenosti se trenutno izvajata dva javna razpisa. Za otroke in mlade (6–29 let) poteka 36 projektov, v katere bo vključenih skupno 38.500 udeležencev. Za odrasle (30+ let) izvajamo 2.553 izobraževanj s skupno 25.530 udeleženci - nov razpis sledi konec leta. Posebej naslavljamo starejše od 55 let na ruralnih območjih, in sicer z mobilnimi enotami projekta Mobilni heroji, kjer so usposabljanja brezplačna in prilagojena ciljni skupini. Sofinanciramo tudi Center za varnejši internet, ki ščiti otroke in mlade ter ozavešča o varni in odgovorni rabi interneta. Cilj je jasen: nihče ne sme ostati zadaj.

Digitalne kompetence so ključne za prihodnost. Ali Slovenija dovolj vlaga v digitalno izobraževanje v šolah in programe za digitalno usposabljanje zaposlenih?

Čeprav za formalno izobraževanje in interno usposabljanje zaposlenih nismo neposredno pristojni, delamo usklajeno z resorji in partnerji. Ob naših programih digitalnega opismenjevanja pripravljamo razpis za prekvalifikacije v IKT v prihodnjem letu - namen je povečati število IKT strokovnjakov na trgu dela. Hkrati gradimo dinamičen sistem, ki poveže delodajalce in sprotno posodabljanje programov, da potrebe

trga hitreje prepoznamo in zapolnimo - tako dosegamo trajne rezultate in večjo prilagodljivost.

Slovenska podjetja imajo še veliko rezerv pri uporabi naprednih digitalnih tehnologij. Kako bo vaše ministrstvo podprlo digitalno konkurenčnost gospodarstva in malih podjetij?

Gradimo močan podporni ekosistem. Evropski digitalni inovacijski stičišči DIGI-SI in SRC-EDIH MSP-jem in javnemu sektorju ponujata testiranja, svetovanja, izobraževanja, ocene digitalne zrelosti in pomoč pri iskanju financiranja - od prve ideje do uvedbe. Z razvojem Slovenske tovarne umetne inteligence (SLAIF) pa podjetjem in raziskovalcem odpiramo dostop do visokozmogljivih računalniških kapacitet in naprednih UI-orodij. To pomeni hitrejši razvoj, nižje vstopne stroške in večjo konkurenčnost, zlasti pri uvajanju UI v procese, storitve in produkte.

Mediji poročajo o kibernetskih prevarah, zlorabah podatkov in širjenju dezinformacij. Kako krepite digitalno varnost in zaupanje v digitalne storitve pri državljanih?

Varnost gradimo celostno in preventivno. Varnostno-operativni center MDP, ob sodelovanju vodilnih slovenskih podjetij s področja kibernetske varnosti grožnje zaznava in blaži, še preden prerastejo v incidente. Z deležniki si sproti izmenjujemo informacije o grožnjah in ranljivostih, izvajamo proaktivne preglede in odpravljamo tveganja. Na sistemskem nivoju delujemo preventivno na način, da so vse rešitve v Državnem računalniškem oblaku pred uporabo varnostno preverjene, kar krepi zaupanje tako v javni upravi kot med državljani in zagotavlja, da so podatki obdelani varno.

Digitalizacija je postala tudi vprašanje odpornosti družbe, tako ob naravnih nesrečah kot ob kibernetskih motnjah in krizah. Kako bo digitalizacija prispevala k večji odpornosti in povezljivosti skupnosti po vsej državi?

Digitalizacija je orodje za bolj povezano, vključujočo in trajnostno družbo. Res je, da večja odvisnost od tehnologije prinaša nova tveganja, hkrati pa omogoča hitrejše zbiranje informacij in boljše, podatkovno podprto odločanje - tudi ob naravnih nesrečah. Naš cilj je odgovorna raba tehnologij, ki povečuje odpornost skupnosti, pospešuje dostop do ključnih informacij in storitev ter ljudem olajša življenje tam, kjer to najbolj šteje.

Slovenija je letos testirala nov sistem javnega obveščanja prek mobilnih omrežij. So bili rezultati testiranja zadovoljivi in kakšne so naslednje izboljšave?

Zadnja leta so jasno pokazala, kako nujen je učinkovit sistem javnega obveščanja. V Sloveniji je že vzpostavljen zelo dober in učinkovit sistem prek siren ter radijskih in televizijskih obvestil, ki mu dodajamo še sistem množičnega obveščanja preko mobilnih naprav. Ta bo dodatno prispeval k večji varnosti in obveščenosti prebivalcev.

Zadnja leta so jasno pokazala, kako nujen je učinkovit sistem javnega obveščanja. V Sloveniji je že vzpostavljen zelo dober in učinkovit sistem prek siren ter radijskih in televizijskih obvestil, ki mu dodajamo še sistem množičnega obveščanja preko mobilnih naprav. Ta bo dodatno prispeval k večji varnosti in obveščenosti prebivalcev. Prvo javno testiranje, ki smo ga izvedli v soboto, 27. septembra 2025, je bilo namenjeno prav temu - da se preveri tehnično delovanje sistema na eni strani in preizkusi delovanje uporabniških naprav na drugi, preden gre sistem v produkcijsko delovanje. Med testiranjem se je pokazala težava pri enem od operaterjev, ki pa je bila hitro odpravljena, ugotovili pa smo tudi, da nekatera sporočila zaradi neposodobljenih operacijskih sistemov niso bila prikazana. Pozvali smo Apple in Google, da v najkrajšem možnem času zagotovita avtomatsko nadgradnjo svojih operacijskih sistemov na način, da bo vključena funkcionalnost SI-ALARM ustrezno delujoča. S tem bomo zagotovili, da bo ob prihodnjih preizkusih sistema delež dostavljenih in prikazanih sporočil višji. Cilj je jasen: robusten, zanesljiv in vsem dostopen sistem opozarjanja.

Vaše ministrstvo je vključeno v številne evropske projekte digitalne preobrazbe. Katere konkretne koristi prinaša to sodelovanje Sloveniji?

Evropska partnerstva nam omogočajo skupne standarde, infrastrukturo in prenos znanja — korist za javne storitve, gospodarstvo, raziskave in državljane. Ključno vlogo imajo Evropski digitalni infrastrukturni konzorciji (EDIC).

Sodelujemo v treh:
– ALT-EDIC za jezikovne tehnologije in večjezičnost, ki spodbuja razvoj UI, ki razume in uporablja slovenščino;
– CitiVERSE EDIC za pametna in trajnostna mesta s podatkovnimi prostori in digitalnimi dvojčki;
– Europeum EDIC na osnovi EBSI in digitalnih identitet, za interoperabilnost, varnost in zaupanje.

Aktivno soustvarjamo tudi dva nova EDIC-a: za agroživilstvo ter Digital Commons, ki bo razvijal odprtokodne gradnike za digitalne storitve. Rezultat sodelovanja v teh evropskih konzorcijih je hitrejši in bolj usklajen digitalni razvoj, močnejša strateška avtonomija in lažji prenos rešitev v prakso.

Umetna inteligenca bo močno vplivala na nadaljnji razvoj družbe. Kako boste zagotovili, da bo njen razvoj pri nas varen, odgovoren in človeku prijazen?

Tu imamo zelo jasen pristop — strateško-zakonodajni in razvojno-infrastrukturni. Ker se to področje hitro razvija, ministrstvo trenutno pripravlja posodobitev Nacionalnega programa spodbujanja razvoja in uporabe umetne inteligence – NpUI 2030, ki bo prilagojen novim razvojnim trendom in usmerjen v spodbujanje zaupanja vredne umetne inteligence, podporo inovacijam ter krepitev znanja in digitalnih kompetenc. Strateški okvir dopolnjuje Uredba (EU) o umetni inteligenci, ki je začela veljati avgusta 2024 in predstavlja prvi celovit zakonodajni okvir za zanesljivo uporabo umetne inteligence. Na njeni podlagi je bil 23. oktobra 2025 v Državnem zboru sprejet Zakon o izvajanju Uredbe (EU) o določitvi harmoniziranih pravil o umetni inteligenci, ki je poznana tudi kot Akt o umetni inteligenci. Zakon vzpostavlja celovit sistem nadzora in etičnega upravljanja, ki vključuje več ministrstev in nadzorne organe (AKOS, Informacijskega pooblaščenca, Tržni inšpektorat, Banko Slovenije ipd.). Določa tudi vzpostavitev regulativnih peskovnikov, kjer bodo podjetja in raziskovalne organizacije lahko varno preizkušale inovativne rešitve UI pod strokovnim nadzorom regulatorjev, HelpDesk za podjetja in javni sektor ter Nacionalni svet za etiko v UI, kar bo okrepilo zaupanje v varno in odgovorno rabo tehnologij.

Pomembno vlogo pri uresničevanju teh ciljev imata tudi projekta Slovenska tovarna umetne inteligence (SLAIF) in Kompetenčni center za umetno inteligenco (KCUI), ki krepita raziskovalne, razvojne in kadrovske zmogljivosti ter omogočata dostop do napredne infrastrukture in znanja. Projekt Slovenska tovarna umetne inteligence (SLAIF) je nacionalna naložba do 150 milijonov evrov, ki jo sofinancirata EU in RS. V Mariboru — v sodelovanju z IZUM-om, Institutom Jožef Stefan in Arnesom — vzpostavljamo visokozmogljivo superračunalniško infrastrukturo, optimizirano za razvoj in uporabo umetne inteligence. 6. maja 2025 smo položili temeljni kamen za podatkovni center. SLAIF bo enotna vstopna točka za podjetja, raziskovalce in javni sektor: dostop do računskih kapacitet, naprednih orodij za UI, izobraževanj in podpore pri razvoju velikih jezikovnih modelov ter drugih rešitev UI. Projekt je medresorski — Ministrstvo za digitalno preobrazbo, Ministrstvo za visoko šolstvo, znanost in inovacije ter Ministrstvo za gospodarstvo, turizem in šport vodimo usklajen pristop, sodelovanje in financiranje. Ob tem z ARIS in partnerji vzpostavljamo Kompetenčni center za umetno inteligenco (KCUI) kot nacionalno stičišče znanja, tehnologij in strokovnega potenciala. KCUI bo konzorcij akademskih, raziskovalnih in industrijskih partnerjev ter bo ponujal dostop do vrhunskih kompetenc, storitev in infrastrukture; skrbel bo za prenos znanja v gospodarstvo in javni sektor, za strokovne delavnice, programe usposabljanj in druge aktivnosti za krepitev kadrovskih zmogljivosti.

Naš cilj je preprost: umetna inteligenca v službi ljudi — za napredek, inovacije in višjo kakovost življenja — ob doslednem spoštovanju etike, varnosti in človekovih pravic. ■

Foto: arhiv Ministrstva za digitalno preobrazbo RS

UČINKOVITO OBVLADOVANJE TVEGANJ ZA ZAŠČITO KRITIČNE INFRASTRUKTURE IN INFORMACIJSKIH SISTEMOV

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

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

Ekipa Silver Bullet Risk (SBR) vam nudi:

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

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

info@silverbulletrisk.com - www.silverbulletrisk.com

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

INTERVJU
Mateja Čalušić, ministrica za kmetijstvo, gozdarstvo in prehrano

KAKO SLOVENIJA KREPI ODPORNOST PREHRANSKE VERIGE V ČASU KRIZ

V času, ko svet vse glasneje zaznamujejo podnebne spremembe, naraščajoče geopolitične napetosti in pogoste motnje v globalnih dobavnih verigah, postaja vprašanje prehranske varnosti ena osrednjih strateških tem. Slovenija se pri tem sooča s svojimi posebnostmi: omejenimi kmetijskimi površinami, precejšnjo odvisnostjo od uvoza ter nujo po okrepitvi samooskrbe in odpornosti prehranskega sistema. O tem, kako država krepi pripravljenost na prihodnje izzive, katere ukrepe že izvaja in kakšno vlogo pri tem igra sodelovanje znotraj Evropske unije, smo se pogovarjali z Matejo Čalušić, ministrico za kmetijstvo, gozdarstvo in prehrano.

Spoštovana ministrica, najprej nam dovolite, da vam in vašim sodelavcem čestitamo za pomembne korake, ki jih delate pri razumevanju pomena odpornosti prehranske verige. Pandemija covid-19 in vojna v Ukrajini sta pokazali, kako ranljiva je lahko prehranska veriga. Kako danes ocenjujete odpornost slovenskega prehranskega sistema?

Lahko rečem, da je slovenski prehranski sistem kot celota, v normalnih razmerah, dokaj odporen. Njegova ranljivost pa se zelo poveča ob pojavu kakršnih koli kriznih razmer. Prehranski sistem mora biti zasnovan tako, da omogoča prehransko varnost. To pomeni zadostno razpoložljivost in ustrezno kakovost hrane, kakor tudi stabilno preskrbo oziroma ustrezno infrastrukturo, zato da prebivalstvo lahko oskrbimo s hrano.

Stabilnost slovenskega prehranskega sistema je zelo odvisna od uvoza hrane, velik vpliv pa imajo tudi podnebni vplivi – suše in visoke temperature na eni, izjemne količine padavin in posledično poplavni dogodki na drugi strani. Za povečanje odpornosti in zagotavljanje stabilnosti prehranskega sistema je ključno zagotavljanje strateških zalog osnovnih živil in semen. Nadaljevati moramo s spodbujanjem večje pridelave ter povečanjem samooskrbe predvsem z zelenjavo in žiti, kakor tudi z digitalizacijo in krepitvijo lokalnih prehranskih verig.

Veseli nas, da potrošniki vse bolj cenijo lokalno pridelano hrano, kar krepi notranji trg, ohranja slovensko podeželje in ima pozitiven učinek na celotno agroživilsko verigo. Za obstoj in razvoj slovenske živilskopredelovalne industrije je informiranje potrošnika o pomenu in kakovosti slovenskih prehranskih izdelkov zelo pomembno.

Na Ministrstvu za kmetijstvo, gozdarstvo in prehrano izvajamo kar nekaj projektov, s katerimi želimo povečati odpornost prehranskega sistema oziroma prehransko varnost. Ključna področja so povečanje stopnje samooskrbe, krepitev kratkih dobavnih verig, povečevanje deleža porabe lokalno pridelane hrane, povezovanje pridelovalcev na lokalnih trgih (tržnice, zadruge, konzorciji), zmanjševanje okoljskih in podnebnih vplivov, agrotehnološki razvoj in inovacije.

Ali Slovenija pri zagotavljanju prehranske varnosti še vedno preveč računa na uvoz? Kako povečati samooskrbo pri ključnih prehranskih izdelkih?

Slovenija je še vedno neto uvoznica hrane, odvisni smo predvsem od uvoza zelenjave, sadja, sladkorja in olj, kakor tudi od uvoza semen in s tem od tujih

*avtor je član Slovenskega združenja korporativne varnosti

semenarskih družb. Zelo velika je tudi odvisnost od uvoza repromaterialov za kmetijsko pridelavo, fitofarmacevtskih sredstev, mineralnih gnojil in rastlinskih hranil.

V Strateškem načrtu za obdobje 2023–2027 se je poudarjalo le doseganje in ohranjanje ustrezne stopnje samooskrbe s hrano in zagotavljanje prehranske varnosti. Pri pripravi novega načrta pa se na ministrstvu zavzemamo, da se določijo konkretnejši cilji. Zavedamo se, da je vprašanje prehranske samooskrbe izrazito horizontalno in posega v vse ključne politike v državi, ne zgolj v kmetijsko. V razpravo moramo vključiti vse člene prehranske verige: od proizvajalca, predelovalca, odkupovalca ter distributerja in trgovine do končnega potrošnika. Vsakršno ukrepanje skupaj s strokovnjaki mora temeljiti na kompleksni ekonomski, okoljsko-podnebni in družbeni oceni.

Večja stopnja samooskrbe odpira vrsto vprašanj, od optimalne rabe in zaščite omejenih kmetijskih zemljišč, prostorskega razvoja, vrste kmetijske proizvodnje, ki jo v prihodnje želimo strateško razvijati in vanjo usmerjati javna sredstva, do perspektive prihodnjega razvoja kmetijstva v Sloveniji v kontekstu vedno bolj kompleksnih okoljskih in podnebnih izzivov prehranskega sistema. Prav tako je treba najti odgovore na vprašanje, kako optimizirati delovanje celotne prehranske verige in navsezadnje, kako spodbujati več trajnostne potrošnje in zmanjšati delež odpadne hrane.

Prehranska veriga je prepoznana kot del kritične infrastrukture. Katere ukrepe je ministrstvo sprejelo za povečanje njene varnosti in delovanja v kriznih razmerah?

Prehranska varnost je pomemben del varnosti države, njen pomen je še posebej izrazit v kriznih razmerah. Kmetijska zemljišča so temelj proizvodnje hrane, zato jih je nujno treba trajno zavarovati pred spremembo namenske rabe in poskrbeti za ohranjanje proizvodnega potenciala. Kmetijska zemljišča moramo obravnavati z enako pozornostjo kot vodo in zrak, saj so nujna za preživetje slehernega posameznika in družbe kot celote. Zaščita kmetijskih zemljišč ni le naloga pristojnega ministrstva, temveč naloga celotne družbe. Vsak hektar, ki ga spremenimo v nekmetijsko rabo, pomeni dolgoročno ogrožanje naše prehranske varnosti. Ko se bo začela naslednja kriza – bodisi zaradi zaprtja meja, vojne ali naravne nesreče – se bomo spraševali, kje bomo dobili hrano, če smo že zdaj izgubili pomembne kmetijske površine. Te so namreč neobnovljiv naravni vir, do katerega se moramo obnašati trajnostno. Zato so nujno potrebna vlaganja v namakalne sisteme, komasacije, ekosistemske storitve tal, hkrati pa je treba na državnih kmetijskih zemljiščih v prihodnosti določiti prioritetne proizvodne kulture (na primer krompir, pšenica, zelenjava).

Ukrepi, ki jih je treba izvesti v primeru kriznih razmer, so takojšnja aktivacija vseh kmetijskih zemljišč, vključno z zaraščenimi degradiranimi zemljišči; uvedba kmetijskih praks, pri katerih se rabi manj fitofarmacevtskih sredstev in mineralnih gnojil; uporaba najboljših kmetijskih zemljišč za pridelavo hrane za ljudi, na primer hmeljišča, ki so skoraj v celoti pod namakalnimi sistemi, v pridelavo stročnic (kot nadomestek beljakovin) in žit; pregled in aktivacija zalog

semen v semenarskih hišah, v prodajni verigi in na kmetijah; zmanjšanje staleža živali, predvsem pitancev, katerih reja je locirana v ravnini in je močno odvisna od uvoza krme; povečanje pridelave v zavarovanih prostorih, ki se sedaj uporabljajo za hortikulturo, v pridelavo zelenjadnic.

Končni strateški cilj Ministrstva za kmetijstvo, gozdarstvo in prehrano je neprekinjena, odporna, sonaravna in konkurenčna pridelava in predelava hrane, ki se bo dosegala z mnogimi aktivnostmi v okviru naslednjih sklopov: zagotavljanje visokih standardov varne in kakovostne hrane; krepitev agroživilskih verig in izboljšanje položaja kmeta v verigi; spodbujanje trajnostne pridelave, predelave in porabe hrane z višjo dodano vrednostjo, vključno s porabo v javnih zavodih; krepitev tržne naravnanosti in podjetništva vseh deležnikov v verigi preskrbe s hrano in spodbujanje generacijske prenove – z namenom ohranitve kmetijstva in povečanje interesa za kmetovanje ter krepitev vključevanja sonaravnih rešitev v pridelavo.

Kako pripravljeni smo na večje motnje v oskrbi – npr. zaradi naravnih nesreč, podnebnih ekstremov ali motenj v logistiki?

Podnebne spremembe v Sloveniji že povzročajo pogostejše in intenzivnejše vremenske ekstreme – vročinske valove, suše, poplave, neurja in požare. Ti pojavi močno vplivajo na kmetijstvo, gozdarstvo, vodne vire, zdravje ljudi, biotsko raznovrstnost in infrastrukturo. Čeprav je Slovenija v preteklosti veliko vlagala v blaženje podnebnih sprememb, je področje prilagajanja ostajalo zapostavljeno. S projektom LIFE4ADAPT to vrzel zapolnjujemo.

Med ključnimi aktivnostmi projekta so vzpostavitev nacionalnega centra za podnebne analize in projekcije (ARSO), okrepitev medresorskega sodelovanja in usklajevanja politik, širitev delovanja Podnebne pisarne (Skupnost občin Slovenije), nadgradnja portala www.samo1planet.si z vsebinami o prilagajanju, izboljšanje kmetijskega informacijskega sistema in upravljanja z vodami, izvedba 14 pilotnih projektov na področjih kmetijstva, gozdarstva, zdravja, gospodarstva in narave, razvoj izobraževalnih programov za učitelje, študente, strokovnjake in javno upravo ter oblikovanje sistema spremljanja, vrednotenja in financiranja ukrepov.

Ministrstvo za kmetijstvo, gozdarstvo in prehrano bo v okviru projekta razvilo spletno aplikacijo za »prvo odzivanje« na škodne dogodke na kmetijskih zemljiščih (suše, toče, pozebe ipd.), ki

bo omogočila hiter pretok informacij med kmeti, svetovalno službo in državno upravo. Prav tako pa bo ministrstvo koordiniralo vzpostavitev petih regionalnih demonstracijskih centrov za prilagajanje kmetijstva, povečanje odpornosti kraške regije z uvajanjem trajnostnih praks v gozdarstvu in kmetijstvu ter izvedbo prilagoditvenih ukrepov za krepitev odpornosti nižinskih hrastovih in smrekovih gozdov.

Ali država načrtuje strateške rezerve hrane ali surovin za predelovalno industrijo za primer daljših kriz?

Za strateške rezerve, ki jih načrtuje država, skrbi Zavod RS za blagovne rezerve v pristojnosti Ministrstva za gospodarstvo, turizem in šport. Osnovna naloga zavoda je med drugim tudi zagotavljanje preskrbe z osnovnimi živili. Ministrstvo za kmetijstvo, gozdarstvo in prehrano sodeluje pri pripravi Petletnega programa o državnih blagovnih rezervah, v katerem so določene tudi vrste in količine živil, ki morajo biti na razpolago za potrebe preskrbe ob naravnih in drugih nesrečah večjega obsega, kriznih razmer, vojnega ali izrednega stanja v Republiki Sloveniji, ko je ogroženo javno zdravje ljudi in zdravje živali v skladu z zakoni, ki urejajo področje zdravja ljudi in živali, pomanjkanje blaga na trgu, kadar ni možnosti preskrbe z ustreznim nadomestnim blagom. Ministrstvo za kmetijstvo, gozdarstvo in prehrano v okviru svoje pristojnosti pripravi seznam in potrebne količine blaga oziroma živil, za katere oceni, da so potrebne za zagotavljanje osnovne preskrbe prebivalstva v zgoraj navedenih okoliščinah.

Digitalizacija in kibernetska varnost postajata pomembna tudi v agrosektorju. Ali ocenjujete, da je sektor pripravljen na kibernetske grožnje, ki bi lahko ohromile oskrbo s hrano?

Težko je predvideti posledice resnega kibernetskega napada na celoten sistem v državi, enako velja tudi za agroživilski sektor. Sodobna kmetijska gospodarstva so na to pripravljena s primernimi sistemi za zaščito, prav tako tudi podjetja v živilskopredelovalni industriji. Za manjša kmetijska gospodarstva, kjer procesi v večini niso digitalizirani, pa to težko rečem.

Na Ministrstvu za kmetijstvo, gozdarstvo in prehrano imamo že od leta 2009 uvedeno t. i. politiko varovanja podatkov in informacij, ki upošteva pravila dobre prakse pri zagotavljanju informacijske varnosti, kot so opredeljena v standardu ISO/IEC 27002. Vsakoletna preverjanja IT-pooblaščenih revizorjev (na pobudo Urada za nadzor proračuna) omogočajo sprotno odpravljanje ugotovljenih pomanjkljivosti. Vseskozi tudi zagotavljamo posodabljanje ključne strojne opreme. Ob centralizaciji informatike v državni upravi smo postali del t. i. državnega računalniškega oblaka, kar pomeni, da imamo zagotovljeno ločeno, varovano informacijsko omrežje.

Kako pomembno je sodelovanje s sosednjimi državami in EU pri zaščiti prehranske verige in stabilnosti agroživilske oskrbe?

Stabilnost prehranske verige je za Republiko Slovenijo strateškega pomena. Ker so naravni viri omejeni, naš trg pa zaradi svoje majhnosti zelo občutljiv, kakršnakoli nihanja v agroživilskem segmentu v EU ali širše zelo močno občutimo. Zato je učinkovito sodelovanje s sosednjimi državami in EU ključnega pomena, saj omogoča večjo odpornost prehranskega sistema ter dolgoročno varnost oskrbe prebivalstva.

Države članice EU so medsebojno povezane v dobavnih verigah hrane, krme in energentov. Slovenija je odvisna od uvoza določenih vhodnih surovin, hkrati pa izvozi pomemben delež predelanih agroživilskih izdelkov. Ohranitev odprtega pretoka blaga in storitev znotraj enotnega trga EU je zato ključna za preprečevanje motenj v preskrbi. Še posebej je to pomembno v kriznih situacijah – na primer ob pandemiji SARS-CoV-2 (covid-19) ali ekstremnih dogodkih, kot so poplave ali požari. Usklajeni ukrepi znotraj EU in s sosednjimi državami so ključni za nemoteno delovanje logističnih poti, preprečevanje izvoznih omejitev ter zagotavljanje humanitarne in tehnične pomoči. Nadaljnja krepitev partnerstev s sosednjimi državami in aktivna vloga Slovenije v oblikovanju evropskih politik, ki spodbujajo odpornost, trajnost in varnost prehranskih sistemov, je zato nujna.

Kateri so po vašem mnenju trije ključni ukrepi, ki jih mora Slovenija sprejeti do leta 2030, da okrepi prehransko varnost in odpornost celotne prehranske verige?

Prvi in najbolj ključen ukrep, ki državi in prebivalstvu zagotavlja prehransko varnost, je trajna zaščita kmetijskih zemljišč. Določiti moramo trajno varovana zemljišča in vanje sistematično vlagati z ukrepi, kot so izgradnja namakalnih sistemov, ustrezne komasacije in sočasno skrbeti za ekosistemske storitve na zemljiščih. Drugi ukrep je vzpostavitev regijskih prehranskih verig za oskrbo s hrano. Sem spada tudi oskrba s semeni, pridelava, predelava, skladiščne in logistične kapacitete ter distribucija do javnih zavodov (vrtcev, šol, bolnišnic, domov za ostarele, vojašnic) in končnega potrošnika. Zelo pomembna je tudi vloga države v živilskopredelovalni industriji, kjer je treba okrepiti njeno vlogo. Tretji ukrep je zmanjšanje odpadne hrane, saj to neposredno vpliva na obseg preskrbe s hrano. V Sloveniji na prebivalca v povprečju letno zavržemo skoraj 80 kilogramov hrane. Na svetu vsak dan zavržemo več kot milijardo obrokov, medtem ko več kot 730 milijonov ljudi živi v lakoti. Tako visok delež odpadne hrane ni samo predmet ozaveščenosti o pomenu in vlogi hrane, temveč tudi okoljski problem. Zavržena hrana po nekaterih informacijah povzroči petkrat več emisij, kot jih izpusti letalski sektor. Zmanjševanje količine odpadne hrane je zato bistvenega pomena.

V Slovensko združenje za korporativno varnost so vključene tudi pomembne državne institucije, ki so posredno in neposredno odgovorne za posamezne kritične sektorje. Menite, da je čas, da se tudi Ministrstvo za kmetijstvo, gozdarstvo in prehrano priključi tej pomembni varnostni platformi?

Da, menimo, da je čas, da se tudi mi priključimo tej varnostni platformi. Na ministrstvu že pripravljamo Vizijo »Kmetijstvo in hrana v 2040«, ki predvideva tudi investicijske projekte za dvig prehranske varnosti države. Država je dolžna zagotavljati stabilno, kakovostno in cenovno dostopno oskrbo prebivalcev s hrano. Osnova za to je trajnostni prehranski sistem, ki v kontekstu krepitve zmogljivosti upošteva okoljski, družbeni in upravljavski vidik glede na razvoj in krepitve zmogljivosti. Aktivnosti z vsemi ključnimi deležniki že nekaj časa potekajo. ■

Foto: arhiv Ministrstva za kmetijstvo, gozdrastvo in prehrano RS

Slovensko združenje korporativne varnosti

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

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

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

Namen združenja je uresničevanje interesov članstva, ki so:

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

www.ics-institut.si

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

Ugodnosti za člane združenja:

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

Dodatne ugodnosti za korporacijske člane združenja:

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

NOVARTIS

sbr

Mestna občina Ljubljana

GASILSKA ZVEZA LJUBLJANA

Občina Slovenska Bistrica

Melamin

Mercator

telemach

SIEMENS

SKUPINA

SMART COM

URSIV

Onkološki inštitut Institute of Oncology Ljubljana

ELEKTRONČEK

MINISTRSTVO ZA INFRASTRUKTURO

TEB

JAVNI MEDOBČINSKI STANOVANJSKI SKLAD MARIBOR

Telekom Slovenije

Pošta Slovenije

CAA

PETROL

Energija za življenje

AKRAPOVIČ

4AJPES

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.

INFORMATIKA

interblock

LUXURY GAMING PRODUCTS

triglav

otpbanka

Elita i.b. d.o.o.

SPICA

tenzor

ZARJA ELEKTRONIKA

UNISTAR PRO

smartis

PAMETNI INFORMACIJSKI SISTEMI

LON

CINKARNA

Slovenske železnice

energetika ljubljana

www.ics-institut.si

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

KOLUMNA

VARNOST KOT KLJUČNA STORITEV DOBAVNE VERIGE

Varnost v vseh svojih pojavnih oblikah postaja ena od ključnih storitev sodobnih dobavnih verig zlasti za upravljavce kritične infrastrukture in izvajalce bistvenih storitev. Če smo jo nekoč razumeli kot podporno funkcijo ali »nepotreben strošek«, danes postaja eden glavnih stebrov odpornosti, zaupanja in konkurenčnosti. Svet, v katerem živimo, je izrazito medsebojno povezan. Motnja v eni točki lahko v nekaj urah sproži verižno reakcijo po celotni oskrbovalni verigi – od energetske oskrbe do zdravstvenega sistema. Pandemija, vojne, kibernetski napadi, podnebne spremembe in migracijski tokovi so nas naučili, da varnost ni le notranja skrb podjetja, temveč strateški element delovanja družbe kot celote.

Varnost v dobavnih verigah ni več omejena na fizično in tehnično zaščito ali digitalne sisteme. Gre za sistem medsebojno povezanih dejavnosti, ki morajo delovati usklajeno, da se zaščitijo ljudje, procesi, podatki, infrastruktura in premoženje. Zasebno varovanje v skladu z Zakonom o zasebnem varovanju (ZZasV-1) danes vključuje varovanje ljudi in premoženja, javnih zbiranj, nadzor na vstopnih točkah, varnostno načrtovanje, prevoz gotovine ter drugih vrednostnih pošiljk, tehnično varovanje, upravljanje varnostno-nadzornih centrov in varnostno-svetovalne storitve.

Varnost ni strošek – je investicija v odpornost celotne družbe. Organizacije, ki jo vključijo v strategijo dobavne verige, bodo bolj zaupanja vredne, odporne in konkurenčne. Potrebna je sprememba miselnosti: od najcenejšega ponudnika k najzanesljivejšemu partnerju.

Zasebno varovanje danes ni zgolj fizično prisotno – uporablja napredne tehnologije, video analitiko, umetno inteligenco in oddaljeno spremljanje dogodkov na varovanih območjih, kar omogoča učinkovitejše prepoznavanje ter zaznavanje varnostnih pojavov in pravočasno preprečevanje tveganj. Hitro razvijajoče se tehnologije pomenijo tudi stalno potrebo po usposabljanju in nadgradnji kompetenc kadrov, ki varujejo kritično infrastrukturo ter izvajalce bistvenih storitev.

Informacijska in kibernetska varnost sta dve ločeni, a neločljivo povezani področji. Prva ščiti vse informacije, ne glede na obliko in zagotavlja zaupnost, integriteto ter razpoložljivost podatkov. Vključuje upravljanje dostopov, varovanje fizičnih in digitalnih dokumentov ter arhivov, implementacijo politik in po-

*avtor je član Slovenskega združenja korporativne varnosti

stopkov za ravnanje s podatki ter informacijami in izobraževanje zaposlenih o zavedanju pomena varovanja informacij. V dobavnih verigah to pomeni, da so osebni in tajni podatki, poslovne skrivnosti, intelektualna lastnina ter načrti neprekinjenega poslovanja in kriznega odziva ustrezno zaščiteni. Pomanjkanje usposobljenih kadrov na tem področju pa lahko bistveno poveča ranljivost celotne verige.

Kibernetska varnost varuje digitalne sisteme, omrežja in aplikacije pred zlonamernimi napadi. Nanaša se na zaščito omrežij, strežnikov in aplikacij pred vdori, upravljanje varnostnih incidentov, uporabo tehničnih rešitev, kot so požarni zidovi, šifriranje ali IDS/IPS sistemi in VPN ter redno testiranje ranljivosti z penetracijskimi testi in skladnost z regulativami ter standardi. V kontekstu dobavne verige to pomeni, da morajo tudi dobavitelji izpolnjevati enake kibernetske standarde, saj lahko šibek člen postane izhodišče za sistemske motnje, vdore ali krajo podatkov. Hitro spreminjajoče se tehnološke grožnje in kompleksnost digitalnih ekosistemov zahtevajo stalno prilagajanje ter inovativne rešitve.

Poleg informacijske in kibernetske so za odpornost pomembne tudi druge oblike varnosti. Okoljska varnost zajema preprečevanje in obvladovanje tveganj, ki jih povečujejo podnebne spremembe, ekstremni vremenski dogodki in migracijski tokovi, saj ti vplivajo na logistiko ter oskrbo. Požarna varnost se nanaša na zaščito objektov, infrastrukture in ljudi pred tveganji zaradi požarov, kar je zlasti pomembno pri objektih kritične infrastrukture. Varnost in zdravje pri delu sta ključnega pomena tam, kjer pomanjkanje kadrov ali obremenjenost zaposlenih lahko povzročita sistemske motnje. Poseben poudarek zahteva tudi varstvo intelektualne lastnine, ki vključuje zaščito inovacij, patentov in poslovnih skrivnosti pred kibernetskimi grožnjami ter nepooblaščenim razkritjem.

Varnost je danes integrirana komponenta dobavne verige. Upravljavci kritične infrastrukture in izvajalci bistvenih storitev ne morejo zagotoviti lastne varnosti, če njihovi strateški dobavitelji in podizvajalci ne delujejo po enakih standardih. Zato varnost postaja skupna odgovornost vseh deležnikov v verigi, tako vertikalno kot horizontalno. Tu pa se pojavljajo ključni izzivi, ki vplivajo na odpornost celotnega sistema.

Eden izmed njih je javno naročanje, kjer cenovni kriterij pogosto prevlada nad kakovostjo in varnostjo. Posledica je, da storitve varovanja ali informacijske varnosti prevzemajo ponudniki brez ustreznih certifikatov ali kadrov in brez zagotovil o tem, kako bodo delovali ob izrednih dogodkih. Rešitev je v izbiri ustreznih postopkov in pripravi povabil ponudnikom, ki temeljijo na ekonomsko najustreznejši, ne zgolj najcenejši ponudbi. Pomembno je tudi, da pogodbe vključujejo jamstva za zagotavljanje neprekinjenosti delovanja v primeru incidentov, ustrezno število usposobljenih kadrov, kritične zaloge in dogovorjene odzivne čase.

Drug izziv je zagotavljanje neprekinjenosti dobav, ki ni le pravočasna dostava, temveč odpornost procesa ob izrednih dogodkih. Podnebne spremembe, migracije, pandemije ali kibernetski napadi lahko ustavijo celotno verigo. Zato so načrti neprekinjenega delovanja in kriznega odziva nujni, kar dokazujejo tudi dobre prakse iz tujine, kjer od dobaviteljev zahtevajo pripravo scenarijev delovanja v izrednih razmerah.

Tretji izziv je odpornost strateških dobaviteljev. Odpornost je lastnost celotnega ekosistema – če šibek člen odpove, trpi celoten sistem. Organizacije zato uvajajo ocenjevanje varnostne zrelosti dobaviteljev, preverjajo skladnost, kadre, zaščito podatkov in krizne načrte. Pri tem pa se pojavljajo še dodatni izzivi, kot so pomanjkanje kadrov, hitro razvijajoče se tehnologije, geopolitična tveganja, migracije in podnebne spremembe, ki lahko povzročijo resne motnje v oskrbi.

Ključno vprašanje ostaja, kako zagotoviti, da vsi strateški dobavitelji – ne glede na velikost, lokacijo ali področje delovanja – izpolnjujejo enake standarde varnosti. Rešitev je v uvedbi minimalnih obveznih standardov, ki zahtevajo certifikate, usposobljenost kadrov in skladnost z relevantnimi standardi, v rednih revizijah ter penetracijskih testih, pa tudi v sistemu nagrajevanja zanesljivosti. Strateški dobavitelji, ki dokazano izpolnjujejo varnostne kriterije in se uspešno odzivajo na incidente, postajajo prednostni partnerji. Pomembno je tudi izobraževanje in testiranje scenarijev, saj skupni treningi ter izmenjava dobrih praks dvigujejo varnostno zrelost vseh deležnikov. Napredni sistemi za digitalni nadzor in transparentno poročanje pa dodatno zmanjšujejo tveganja ter odkrivajo šibke člene. Sistematičen pristop k usklajevanju standardov tako pomeni, da varnost postane konkurenčna prednost in ne le regulativna obveznost.

Varnost ni strošek – je investicija v odpornost celotne družbe. Organizacije, ki jo vključijo v strategijo dobavne verige, bodo bolj zaupanja vredne, odporne in konkurenčne. Potrebna je sprememba miselnosti: od najcenejšega ponudnika k najzanesljivejšemu partnerju. Sistemskih sprememb v javnem naročanju, obveznih certifikatov, oceni tveganj dobaviteljev in stalnem prilagajanju globalnim varnostnim izzivom ne moremo preskočiti. Prav te spremembe bodo ključne za zagotavljanje večje odpornosti in neprekinjenosti delovanja organizacij, zlasti tistih, ki upravljajo kritično infrastrukturo in izvajajo bistvene storitve. Če smo se iz zadnjih kriz kaj naučili, je to, da bo ravno odpornost tista valuta, ki bo ločevala uspešne od ranljivih. ■

ZAŠČITITE PROCESNA OKOLJA PRED KIBERNETSKIMI NAPADI

2-dnevni tečaj

Spoznajte, kako učinkovito poskrbeti za kibernetsko varnost in zagotoviti neprekinjeno delovanje v okoljih kritične infrastrukture ter industrijskih in procesnih okoljih.

PREVERI PROGRAM

https://bit.ly/3WRKuJg

info@smart-com.si

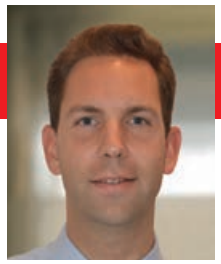
01 561 16 06

SMART COM

UDEJANJAMO VAŠE VIZIJE

www.smart-com.si

Avtorja: dr. Andrej Bregar, Alexander Schmelev / Informatika d.o.o.*



DEJAVNIKI KIBERNETSKE ODPORNOSTI ELEKTROENERGETSKE KRITIČNE INFRASTRUKTURE – ALIENS-SOC

Kibernetska varnost energetske kritične infrastrukture postaja vse zahtevnejši izziv zaradi kompleksnih integriranih informacijskih in procesnih omrežij, medsebojnih odvisnosti z drugimi sektorji, geopolitičnih razmer, vse naprednejših tehnologij in vektorjev napadov, resnih posledic potencialnih napadov ter privlačnosti za napadalce. V prispevku podajamo izsledke analize ekosistema v okviru evropskega projekta ALiEnS-SOC

Kibernetski napadi in tehnične odpovedi distribucijskih električnih omrežij kažejo na varnostne izzive, ki smo jim bili nedavno priča tako v Sloveniji kot v širšem evropskem prostoru. Ti primeri so jasno izpostavili občutljivost družbe in korporativnih sistemov na večje motnje v energetskem ekosistemu. Zato deležniki v slovenskem elektroenergetskem sektorju in nekateri ključni nosilci nacionalne kibernetske varnosti sodelujemo na evropskem projektu ALiEnS-SOC (Artificial Intelligence for Slovenian Electro-Energy Sector Security Operation Centre), katerega cilj je povečati odpornost elektroenergetskega ekosistema. Projekt se osredotoča na sektorski varnostni operativni center (VOC), ki prevzema vlogo temeljne entitete za zagotavljanje kibernetske varnosti. Krepi ga z napredno platformo, ki podpira izmenjavo obveščevalnih informacij (CTI – Cyber Threat Intelligence) in povečuje učinkovitost zaznavanja kibernetskih napadov ter odzivanja nanje z uporabo umetne inteligence. Ključno je, da takšna platforma pokriva karseda popoln obseg raznolikih dejavnikov in scenarijev, ki povečajo zrelost ekosistema z vidika kibernetske varnosti ter odpornosti.

Ocenitev zrelosti sistema kibernetske varnosti

Za analizo kibernetske varnosti energetskega ekosistema je najprimernejši model C2M2 (Cybersecurity Capability Maturity Model), ki je bil razvit posebej za ta sektor na podlagi priporočil varnostnih strokovnjakov iz prakse. V izhodišču sledi standardom organizacije NIST (National Institute of Standards and Technology), zlasti ogrodju CSF (Cybersecurity Framework), ki pa je zastavljeno širše in pokriva različna okolja ter industrije. Ogrodje CSF predpisuje šest varnostnih funkcij (identifikacija, zaščita, zaznava, odziv, okrevanje in obvladovanje), ki so izpeljane iz faz življenjskega cikla kibernetske varnosti. Model C2M2 razdela te funkcije v deset specifičnih varnostnih domen, ki pokrivajo upravljanje tveganj, ranljivosti, virov, konfiguracij in dobavnih verig, odzivanje na incidente, usposabljanje ter ozaveščanje, obvladovanje skladnosti, neprekinjen nadzor in druge vidike. Ob uporabi modela C2M2 ocenjujemo zrelost na štirih nivojih, od nepodprtih varnostnih praks, prek ad hoc in dokumentiranih praks do standardiziranih ter upravljanih aktivnosti.

Dejavnike kibernetske varnosti obravnavamo in izboljšujemo v iterativnem življenjskem ciklu. Organizacija najprej izvede prvo samoocenitev po modelu C2M2. Na njeni podlagi identificira razkorak v zrelosti, oblikuje akcijski načrt izboljšav ter ga implementira. S tem se dvigne nivo zrelosti, kar vodi k spremembi poslovnih ciljev in ponovni samoocenitvi.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Identifikacija dejavnikov in scenarijev kibernetske odpornosti

Projekt ALiEnS-SOC vpeljuje metodologijo za pregled in ocenitev stanja kibernetske varnosti ekosistema, analizo razkoraka ter oblikovanje dejavnikov, akcij in scenarijev za povečanje kibernetske odpornosti na podlagi identificiranega razkoraka. Metodologija prevzema življenjski cikel in dobre prakse modela C2M2, vendar jih bistveno nadgrajuje, saj mora upoštevati informacijsko, procesno in fizično kritično infrastrukturo na eni strani, kot tudi učinkovitost delovanja varnostnih operativnih centrov, ki ščitijo to infrastrukturo na drugi strani. Prav tako mora nasloviti več kompleksnih in kritičnih vidikov kibernetske varnosti, kot sta izmenjava obveščevalnih informacij (CTI) in transparentno poenoteno zaznavanje anomalij v IT on OT omrežjih. Metodologija sestoji iz več korakov:

- Identifikacija vidikov krepitve kibernetske odpornosti postavlja osnovo za analizo razkoraka. Upoštevati mora zakonodajo in tehnološke zmožnosti. Ključni vidiki so zmanjšanje površine napadov, zgodnje zaznavanje in preprečevanje tveganj, hiter odziv na incidente ter njihova zajezitev, učinkovito okrevanje kritičnih storitev in virov, zmanjšanje časa nerazpoložljivosti ter ozaveščanje in krepitev znanja.
- Samoocenitev nosilcev kritične IT in OT infrastrukture temelji na modelu C2M2. Njen namen je identificirati področja s primanjkljajem v zrelosti in tako izpostaviti relevantne dejavnike za krepitev kibernetske odpornosti.
- Analiza razkoraka je izvedena na podlagi predhodne analize ekosistema kritične infrastrukture, samoocenitve nosilcev kritične infrastrukture in analize aktualnega stanja VOC. Pri tem je lahko zajetih več VOC za različne segmente infrastrukture, npr. za ločeno varovanje prenosnega in distribucijskega omrežja.
- Načrtovanje akcij in scenarijev za krepitev kibernetske odpornosti mora izhajati iz zaznanega razkoraka in identificiranih dejavnikov odpornosti. Cilj tega koraka je postavitev formalnih osnov za vzpostavitev enotnega odpornega okolja, katerega kibernetsko varnost zagotavlja sektorski VOC.
- Implementacija akcij in scenarijev na osnovi vzpostavitve platforme je tehnični del projekta ALiEnS-SOC. Je končni cilj krepitve kibernetske odpornosti sektorja.
- Ponovna ocenitev sledi iterativnemu življenjskemu ciklu modela C2M2. Zagotovi, da so upoštevani in uspešno realizirani vsi dejavniki kibernetske odpornosti.

Kako povečati kibernetsko odpornost kritične infrastrukture?

Z analizo razkoraka smo določili cilje krepitve kibernetske odpornosti slovenskega elektroenergetskega sektorja, ki naslavljajo več različnih plasti zaščite pred kibernetskimi incidenti. Večplasten pristop k zaščiti kritične infrastrukture je potreben ne samo zaradi njene pomembnosti za družbo, temveč tudi, ker se tehnike kibernetskih napadov nenehno razvijajo in postanejo vse bolj kompleksne. Z več nivoji zaščite imamo na razpolago več možnosti, da preprečimo kibernetske incidente.

Poleg zmanjšanja površine napada pripomore k preprečevanju kibernetskih incidentov in s tem povečanju kibernetske odpornosti tudi izboljšanje situacijskega zavedanja, torej preslikava globalnega in regijskega dogajanja v kibernetskem prostoru na slovenski elektroenergetski sektor. Izmenjava aktualnih podatkov o varnostnih dogodkih omogoča hitrejši in učinkovitejši odziv na kibernetske grožnje. Ključno je aktivno sodelovanje in povezovanje več deležnikov, ki imajo na tem področju različne zmogljivosti in izkušnje.

Čimprejšnje zaznavanje kibernetskih incidentov je naslednji vidik krepitve kibernetske odpornosti. Incident, ki je zaznan v zgodnji fazi, bo lahko rešen z manjšimi posledicami in manj škode. Vendar je hitro in učinkovito zaznavanje anomalij mogoče samo, če imamo zadostno vidljivost in je poznano normalno (neogroženo) stanje. Varnostna orodja na podlagi modelov strojnega učenja so lahko zelo učinkovita pri zaznavanju anomalij v IT in OT omrežjih, ker spremljajo in obdelujejo ogromne

količine podatkov, potrebujejo pa pomoč pri učenju, zlasti pri začetni vzpostavitvi in konfiguraciji takšnih sistemov.

Ljudje so običajno prva in zadnja obrambna linija pred/med kibernetskim incidentom. Prepoznavanje poskusa kraje poverilnic ali drugih podatkov lahko prepreči incident, še preden se ta začne. V elektroenergetskem sektorju je ozaveščanje o kibernetski varnosti že na visokem nivoju na osnovi rednih in pogostih izobraževanj zaposlenih ter testiranj. Kljub temu razvoj strategije za ozaveščanje in izobraževanje osebja o kibernetski varnosti ostaja še en temelj za krepitev kibernetske odpornosti.

Kako povečati učinkovitost VOC?

Enega ključnih vidikov kibernetske odpornosti predstavljajo varnostni operativni centri. Projekt ALiEnS-SOC zajema pregled zahtevane zrelosti VOC za elektroenergetski sektor. Oceno zrelosti VOC lahko razdelimo na tri vidike: kader, postopke in tehnologijo.

Pri ocenitvi kadrovske zrelosti je ključno, kakšno je strokovno znanje posameznikov in kako dobro so definirane vloge ter odgovornosti. Izziv manjših okolij VOC je zagotoviti zadostno strokovno znanje na različnih področjih, omogočiti specializacijo in razdeliti odgovornosti. V takšnih primerih se poveča odvisnost od zunanjih izvajalcev. Za VOC, ki deluje v sektorju energetske kritične infrastrukture je zato bistvenega pomena zagotoviti dobro kadrovsko zmogljivost in širok vpogled v kibernetsko dogajanje v sektorju ter širše.

Veliki del postopkov v VOC lahko avtomatiziramo in s tem povečamo pripravljenost ter odzivnost na kibernetske incidente. Za avtomatizacijo so med drugim primerni postopki za odkrivanje, dokumentiranje in spremljanje ranljivosti uporabljenih IT ter OT sredstev, zaznavanje anomalij, izvajanje odzivnih procedur in izmenjavo obveščevalnih podatkov. Poleg avtomatizacije ima pozitiven učinek na delovanje VOC tudi definicija standardnih, dobro opredeljenih in praktično naravnanih odzivnih procedur. Ob odzivu na incident mora VOC oceniti vpliv incidenta na celoten elektroenergetski sektor zaradi povezanosti deležnikov in virov ter kaskadnih učinkov. Deljenje obveščevalnih podatkov in pravočasno obveščanje deležnikov znotraj sektorja je tako zelo pomembno za zajezitev in reševanje incidenta. Uporabno pa je tudi po incidentu, npr. za namen ozaveščanja in izobraževanja.

Izboljšanje postopkov delovanja VOC in razvoj strokovnega znanja posameznikov je treba podpreti z uporabo naprednih tehnologij. Avtomatizacija zgoraj omenjenih postopkov zahteva uporabo orodij, kot so SOAR, SIEM, NDR in EDR. Tudi za izmenjavo obveščevalnih informacij je potrebna ustrezna platforma. Izpostaviti velja še uporabo sistema vab (honeypot) za dodaten vpogled v vektorje napadov, situacijsko zavedanje in odkrivanje anomalij, kot tudi peskovnike (sandbox) za forenzične raziskave.

Kaj smo torej ugotovili?

Analiza ekosistema v sklopu projekta ALiEnS-SOC je dala zelo dober vpogled v dejavnike in scenarije za krepitev kibernetske odpornosti elektroenergetske kritične infrastrukture. Dobili smo tudi jasno sliko, kako mora biti organiziran in tehnološko podprt učinkovit sektorski VOC ter kako mora sodelovati z deležniki znotraj sektorja in širše. Z vpeljavo tehnološke platforme, ki bo omogočila avtomatizacijo na osnovi umetne inteligence in napredne mehanizme izmenjave obveščevalnih informacij o kibernetskih grožnjah, pa bodo ti vidiki celovito podprti ter realizirani v praksi. ■

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.

INFORMATIKA

Varnostni operativni center za sektor energetike

Celovito obvladovanje kibernetskih varnostnih tveganj

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

Vplivi kibernetskih napadov na različna področja v energetiki:

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

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

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

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

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

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

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

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

ČAS JE ZA ODLOČILEN KORAK

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

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

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

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

www.informatika.si

Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Tone Stanovnik, Špica International, d.o.o.*

OBLAK JE NOVA KRIVULJA RASTI, NE ZGOLJ TEHNOLOŠKI TREND

Podjetje Špica International že več kot tri desetletja ostaja sinonim za zanesljive rešitve na področju tehničnega varovanja, kontrole pristopa in evidence delovnega časa. S svojimi sistemi podpira ključne organizacije v Sloveniji in širši regiji, pri čemer strateško stavi na prihodnost v oblaku. O viziji digitalne preobrazbe, pomenu varnosti in vlogi umetne inteligence smo se pogovarjali z g. Tonetom Stanovnikom, direktorjem podjetja, ki poudarja, da je oblak nova krivulja rasti, ne zgolj tehnološki trend.

V vašem primeru gre za visoko tehnološko podjetje, ki podpira na področju tehničnega varovanja s poudarkom na kontroli pristopa in evidenci delovnega časa zelo širok spekter pomembnih organizacij v Sloveniji. Kako bi opisali strategijo prehoda vaših rešitev v oblak in kateri ključni cilji stojijo za to odločitvijo?

Vsaka tehnologija ima svojo S-krivuljo: najprej hitro raste, nato se izravna ter začne pešati in padati. Na vrhu stare krivulje podjetja pogosto vlagajo vedno več za vedno manj učinka. Optimizirajo in se trudijo z izpopolnjevanjem znanega, namesto da bi pravočasno zagrabili za novo.
Mi v Špici smo se zato odločili za zgodnji prehod v oblak – še preden postane prepozno. Zakaj? Ker nam oblak omogoča hitrejše uvajanje novih funkcionalnosti in zanesljivejše delovanje. Našim uporabnikom pa oblak tehnologija prinaša preprostejši in hitrejši dostop do storitev ter višjo razpoložljivost in varnost.

Zavedamo se, da je taka sprememba za kupce zahtevna, zato naša strategija ni »veliki pok«, temveč prehod peljemo postopno in hibridno. Tako si vsaka organizacija izbere svoj tempo in ne ogrozi kontinuitete. To je še posebej pomembno za naše velike regijske kupce med katerimi so mnogi s področja kritične infrastrukture.

Oblak torej ni modna muha, temveč naslednja krivulja rasti, na kateri želimo napredovati skupaj z našimi uporabniki.

Kaj prinaša prehod v oblak vašim strankam — predvsem z vidika zanesljivosti, učinkovitosti in dostopa do storitev?

Prehod v oblak našim strankam prinese predvsem miren spanec, hitrost in odzivnost ter preprost dostop do storitev.

Zanesljivost je naša prva prioriteta, zato so naše storitve podvržene rednim penetracijskim testom in so razvite z najnovejšimi tehnologijami, ki znižujejo tveganja na minimum. Storitve delujejo tudi, ko se kaj zalomi, saj imamo vzpostavljeno neprekinjeno spremljanje delovanja 24/7 in načrt neprekinjenega poslovanja. Ne samo produkti in storitve, temveč tudi kot podjetje in procesi smo dolga leta pod neodvisnimi presojami. ISO 9001 imamo kot eno prvih slovenskih računalniških podjetij že od leta 1995. Zadnjih 10 let imamo vzpostavljen tudi sistem upravljanja informacijske varnosti po standardu ISO 27001.

Področje varnosti je bilo vedno podvrženo predvidljivosti, standardizaciji in stabilizaciji. V zadnjem obdobju pa se vedno bolj kaže potreba po rednih nadgradnjah sistemov tehničnega varovanja z novosti ki jih preko oblačne tehnologije

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

dobite hitreje, brez izpadov ob nadgradnjah. Sistem se uči in prilagaja, ko je poraba procesorske moči na vrhu, se oblačna infrastruktura sistemsko ojači in zmore več; ko se situacija umiri, se skrči in ne troši po nepotrebnem. To pomeni visoko učinkovitost in manj čakanja ter več uporabne vrednosti.

Dostop je preprost. Do storitev lahko dostopate od kjerkoli, z eno prijavo in na vseh napravah. Ker danes veliko dela teče na mobilnih telefonih, je to za ekipe na terenu ali na več lokacijah velika razbremenitev. Oblak je hkrati prijazen do vaših obstoječih sistemov prek API vmesnikov se povežemo z ERP, HRM, CNS in drugimi orodji, zato je manj ročnega dela in napak.

In nenazadnje je tu še ekonomika, saj ni potrebne investicije in spremljajočih stroškov za vzdrževanja lastnih strežnikov. Plačate tisto, kar in kolikor uporabljate, kar pomeni, da se strošek naročnine prilagaja glede na dejanski obseg storitve, ki jo v določenem obdobju potrebujete in uporabljate. Če povzamem, oblačna tehnologija torej prinaša več zanesljivosti, več hitrosti, manj zapletov pri dostopu in elastična ter preprostejša ekonomika.

Kako ta prehod vpliva na zaposlene v podjetju Špica, tako na tehnični kot organizacijski ravni? Ali zahteva nova znanja in prilagoditve delovnih procesov?

Prehod v oblak pri nas ni le tehnološka selitev, temveč razvoj ljudi in načina dela. To smo povzeli kar v formuli **K5** – kadri, ključni procesi, kupci, ključni kazalniki in kultura. Najprej **kadri**: zagnali smo novo ekipo mlajših sodelavcev, tako imenovan kontaktno svetovalni center. Ekipa hitro raste, ker smo spoznali da imamo tehnološko že postavljeno odlično podlago. Namreč že leta 2002 smo v oblaku ponudili www.myhours.com in ga dolgo držali kot brezplačen servis, a se sedaj odlično prodaja. Drugo področje so **ključni procesi**: delamo agilno in v veliki meri na daljavo, razen pri postavitvi naših HW kontrolerjev in čitalcev za kontrolo pristopa. Nadgradnje uporabniki dobijo v manjših valovih, odzivni časi so kratki in se lahko hitro prilagajamo, kot na primer, ko smo v času covida podaljšali brezplačno uporabo v duhu digitalne solidarnosti. Tretji element so **kupci**: klasična prodaja in izvedba je usmerjena na največje kupce v Adria regiji, KSC ekipa pa cilja na srednja podjetja, kjer je nakupno implementacijski proces krajši, bolj preprost in dobrodošel. Opažamo, da se za implementacijo v oblaku opogumljajo vedno večja podjetja, še posebej na zahodu, kjer je tak pristop domač. Četrti sklop so **ključni kazalniki**: gradimo podatkovno vodeno (data driven) organizacijo. V storitve vgrajujemo merjenja, da podatke pretvarjamo v informacije in z zanko povratnih vplivov izboljšujemo uporabniško izkušnjo ter usmerjamo trženje, da bolje razumemo, zakaj nas kupci izberejo, kje smo dobri in kje imamo še prostor za odlično. In končno **kultura**: kultura te mlajše ekipe je bolj

agilna, naš izziv pa je, da s to energijo prepojimo vso Špico in naša podjetja v Adriatic regiji (Zagreb, Beograd, Sarajevo, Skopje, NY) . To je dolgoročen proces, ki potrebuje jasnega nosilca, zato se osebno angažiram in dajem tempo, da celotno ladjo obrnemo proti novim priložnostim, ki jih prinaša oblačna tehnologija. Na kratko: manj zidov med ekipami, več odgovornosti in podatkovne jasnosti – in kultura, ki ljudem omogoča, da skupaj rastejo hitreje kot tehnologija (Best Together).

Kako nove zakonodajne zahteve, kot je Zakon o informacijski varnosti (ZInfV-1), vplivajo na vaše poslovanje kot dobavitelja digitalnih storitev?

Nove zakonodajne zahteve kot sta NIS-2 oziroma ZInfV-1 dvigujejo letvico informacijske varnosti v celotnem ekosistemu, kar naši Špici kot podjetju, ki v to področje ves čas vlaga enormne napore, seveda koristi. Mnogi tudi pomembni kupci so pogosto do sedaj pri izbiri dobavitelja kot ključno in včasih celo edino merilo imeli ceno. Varnost je relativno težko ovrednotit kot ROI - povračilo investicije in jo je treba oceniti skozi tveganja, ki jih moramo zmanjšati na razumno mejo. Ta nova zakonodaja bo sistematično vplivala, da se bo uveljavilo tudi to novo merilo pri izbiri dobaviteljev. Certifikati, ki smo jih pridobili na tem področju in jih, seveda, prek rednih vsakoletnih presoj tudi vzdržujemo in nadgrajujemo, so pomemben dokaz, da imamo tako proizvode in storitve kot tudi ustroj podjetja, skupaj z zaposlenimi, podvržene najvišjim standardom kakovosti in informacijske varnosti. Regulative torej ne vidimo kot breme, temveč kot pomemben nov standard na trgu, ki vzpostavlja določen red in ščiti stranke ter dviguje zrelost naše ekipe in nam dviguje konkurenčno prednost, ker delujemo varno, predvidljivo in transparentno. Zato izvajamo redna izobraževanja ter imamo sistematično določene odgovornosti in postopke ter z rednimi presojami preverjamo, ali procesi in sodelavci delujemo tako, kot je zapisano in kot od nas zahteva dobra praksa. Že pri planiranju naših informacijskih rešitev upoštevamo koncept »security by design« in tako so varnostni elementi vgrajeni v DNK naše ponudbe.

Kako se vaše podjetje pripravlja na prihod umetne inteligence in kakšen vpliv pričakujete na razvoj rešitev ter podporo uporab nikom?

Naši začetki na področju umetne inteligence segajo v leto 2007, ko smo skupaj z Institutom Jožef Stefan in prof. dr. Gams Matjažem razvili sistem CIVaBiS – Celovit inteligentni varnostni biometrični sistem. Projekt sta sofinancirala ARRS in MORS z namenom dvonivojskega nadzora vstopa v prostore, rezultat pa smo zaščitili s patentom pri Uradu RS za intelektualno lastnino (št. 22822). Danes, ko je UI del vsakdana, se osredotočamo na pristop *"management by exception"*: v svetu naraščajoče kompleksnosti tehnologija vodjem pomaga, da svoj čas posvetijo res pomembnim primerom, rutino pa prevzame informacijski sistem. Drugo področje, kjer vidimo veliko vrednost, je programiranje z omejitvami (*constraint programming*). Po domače: človek določi cilje in pravila, UI sistem pa predlaga najboljše možnosti, ki ta pravila upoštevajo. Tako lahko, denimo, pri razporejanju dela ali pri dodeljevanju pravic dostopa UI, hitro izračuna več smiselnih predlogov, človek pa izbere in potrdi optimalnega. Rezultat so hitrejše in preglednejše odločitve, manj rutinskega računanja in več časa za tisto, kar res šteje.

Kako vidite vlogo vašega podjetja v naslednjih petih letih v kontekstu povezovanja oblačnih tehnologij, informacijske varnosti in umetne inteligence?

V naslednjih petih letih se vidimo kot partner našim strankam, tako da svoje oblačne storitve lepo zaokrožimo v 360 stopinjsko uporabniško izkušnjo. Najgloblji in temeljni stebri, na katerih bo slonela naša ponudba, bodo ravno oblačna tehnologija, informacijska varnost in umetna inteligenca. To zaokroženo ponudbo lahko prikažemo zelo plastično skozi zelo popularen Demingov življenjski krog stalnih izboljšav (PDCA Plan-Do-Check-Act). Demingov krog najdemo kot podlago tudi ISO standardom, tako 9001 kot 27001 in ga mnogi štejejo kot praočeta sodobnega agilnega pristopa, ki ga čislajo informatiki.

V fazi **Planiranja** je tu naša rešitev *Dynamic Scheduling*, ki hitro sestavlja razporede in urnike dostopov, ob upoštevanju vseh pravil in posebnosti. V fazi **Izvedbe** z www.myhours.com preprosto beležimo čas po projektih, kjer nastaja vrednost in jo nato tudi uspešno zaračunamo kupcem. Sledi **Merjenje**: Evidentiranje posameznih segmentov delovnega časa *www.allhours.com* ter **Registriranje** ob vstopanju in zapuščanju prostorov *www.doorcloud.com*. Krog zaključimo z **Analiziranjem ter ukrepi** za izboljšave, kjer levji delež prispeva tudi umetna inteligenca, ki na podlagi obilice zbranih podatkov omogoča preko prediktivne analitike v ponovni krog planiranja.

Naš cilj ni "AI zaradi AI", temveč merljiv učinek: manj napak, hitrejše odločanje, varnejši dostopi in razporedi, ki delujejo v praksi. Oblak nam daje hitrost in razširljivost, varnost jemljemo kot našo privzeto razvojno mantro, človek pa ostane tisti, ki izbere in potrdi ključne odločitve, ki jih na seznam naniza umetna inteligenca. Tako uporabniki porabijo manj časa za operativno delo in več za upravljanje in postavljanje strategije.

Kako ocenjujete vaše delovanje znotraj Slovenskega združenja za korporativno varnost?

Zelo smo veseli, da lahko kot član združenja tvorno prispevamo dobro prakso na našem kompetenčnem področju. Vesel sem tudi, da se slovensko združenje proaktivno vključuje tudi v regijska srečanja, saj je za Špico Adriatic regija tako rekoč domač teren. Svoja podjetja imamo namreč v vseh glavnih mestih bivše Jugoslavije. Časi, ki nas obkrožajo, vse hitreje prinašajo nove varnostne izzive na naše mize in srečanja ter izmenjave informacij, ki jih spodbuja združenje, so nepogrešljive na poti ki je pred nami. Kot je dejal naš znani alpinist Nejc Zaplotnik »Cilj je pot« in zato želim vsem bralcem »Srečno na poti«! ■

Foto: arhiv Špica International, d.o.o.

Avtorica: Jasmina Mešić / vodja programa ozaveščanja Varni na internetu, SI-CERT*

NACIONALNI PROGRAM OZAVEŠČANJA VARNI NA INTERNETU V SREDIŠČE KIBERNETSKE OBRAMBE POSTAVLJA POSAMEZNIKA

Letos mineva štirinajsto leto odkar je zaživel nacionalni program ozaveščanja o informacijski varnosti Varni na internetu. V dobrem desetletju – kar je v svetu informacijske tehnologije, kjer še komaj lovimo vse spremembe, preboje in novosti, že precej dolgo obdobje, smo na Nacionalnem odzivnem centru za kibernetsko varnost SI-CERT izluščili pomembni lekciji, ki nas vodita pri nadaljnjih aktivnosti ozaveščanja in izobraževanja.

Uvod

Najprej je dejstvo, da moramo v ospredje postaviti posameznika - uporabnika, ki je več kot zgolj floskula »najšibkejši člen v verigi kibernetske varnosti«. Po natanko 30. letih delovanja centra SI-CERT in tisoče obdelanih incidentih, še vedno trdimo, da so v samem vrhu napadi družbenega oziroma socialnega inženiringa. V mislih imamo različne oblike spletnih goljufij in predvsem napadov z zvabljanjem (ang. phishing), ki so v zadnjih nekaj letih zabeležili globalen skok ter so trenutno najpogostejša grožnja, ki preti povprečnemu spletnemu uporabniku. V največ primerih je vektor napada elektronska pošta, velik skok pa je v porastu phishing napadov z SMS sporočili in prek aplikacij za hipno sporočanje. V zadnjih letih smo priča trendu, da se nevarnosti selijo na pametne telefone v obliki SMS sporočil, ki pod pretvezo „preverjanja podatkov“, „potrjevanja transakcij“ ipd. želijo izvabiti avtentikacijske podatke za dostop do elektronske banke (t.i. smishing).

Gre za incidente, kjer napadalci izkoristijo naše ranljivosti, podobno kot bi poiskali in izkoristili napako v programski kodi. In v svetu kibernetske varnosti nas ravno lastnosti, ki so imanentno človeške, delajo tako ranljive – radovednost, strast, sočutje, strah, če naštejemo le nekatere. Zaupanje v programske rešitve nas pred takimi zlorabami ne bo vedno obvarovalo, še vedno je glavna rešitev izobraževanje spletnih uporabnikov. Ne zgolj s komunikacijskimi akcijami, ki naslavljajo posameznika v njegovem domačem okolju, temveč tudi s kontinuiranim, hkratnim izobraževanjem v poslovnem okolju. V SI-CERT že leta opozarjamo, da je še vedno (pre)pogosto prepričanje, da manjša podjetja niso zanimiva za spletne napadalce, kar pa ne

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti

drži. Zaradi omejenih finančnih in kadrovskih virov so vlaganja v informacijsko varnost tam velikokrat pomanjkljiva, zato so manjša podjetja lažja tarča. Tudi v večjih podjetjih in organizacijah, kjer je stopnja zavedanja o kibernetski varnosti mnogo višja, težavo še vedno predstavlja nezadostno izobraževanje zaposlenih. Vlaganje zgolj v programsko in omrežno opremo ne reši vseh težav, saj gre v večini primerov za tehnično nezahtevne napade, ki temeljijo na družbenem inženiringu. Če zaposleni nimajo ustreznih znanj in veščin, da bi prepoznali nevarnost, so napadalci pogosto uspešni. Vendar se tudi na tem področju v zadnjih letih dogajajo intenzivne spremembe.

Nove spletne platforme prinašajo nove priložnosti za napadalce

Če je zadnjih deset let glavni motiv napadalcev ostal enak - prepričati uporabnike v nakazilo denarja, pa so se močno spremenile komunikacijske poti, kako pridejo do svojih žrtev. Nove spletne storitve, nove oblike plačevanja na spletu, predvsem pa nove platforme družbenih omrežjih so prinesle številne priložnosti za spletne goljufe. Pred desetletjem smo opozarjali večinoma na spam oziroma neželeno pošto, krajo Gmail gesel in nekaj prevarantov na spletnih oglasnikih. Danes pa obravnavamo povsem druge problematike, ki se odražajo v resni finančni in poslovni škodi. Opozarjamo na vrivanje v poslovno komunikacijo, direktorske prevare, phishing kraje kreditnih kartic, številne prevare pri spletnem nakupovanju, izsiljevanje z intimnimi posnetki, lažne kredite, investicijske kripto prevare, ki se končajo z več deset tisoč evri škode. Pogosto so skupni imenovalec ravno družbena omrežja, kjer napadalci vzpostavijo prvi stik – postavijo lažno nagradno igro, oglas za lažno spletno trgovino ali lažni profil osamljenega marinca. Domišljija spletnih goljufov praktično ne pozna meja, kar pa terja nove pristope pri izobraževanju, torej kako nagovoriti spletne uporabnike, pritegniti njihovo pozornost in jim pojasniti, kje tiči nevarnost.

Ob letošnjem mesecu kibervarnosti smo v ospredje postavili osebne zgodbe žrtev spletnih prevar, ki se skrivajo za neosebnimi statistikami. Žal še vedno pogosto slišimo stavek »Meni se pa to ne more zgoditi!«

Kibernetska varnost se tiče vseh

Drugo pomembno zavedanje je, da kibernetska varnost ni neprijetna naloga enega oddelka znotraj podjetja ali

ene organizacije znotraj države. Hkrati se kibernetske grožnje tudi ne ustavijo na nacionalnih mejah. Kibernetska varnost se tiče vseh - *Cyber Security Is Everyone's Business* in najti učinkovit odziv na kibernetske grožnje je globalni izziv naše dobe. Varnost in zaupanje sta predpogoja, da uporabniki usvojimo vse spletne storitve, ki so nam na voljo. Zato s programom ozaveščanja Varni na internetu aktivno sodelujemo tudi v širših pobudah in smo slovenski predstavnik oziroma koordinator v kampanji Evropski mesec kibervarnosti. Vseevropsko pobudo usklajujeta Agencija Evropske unije za kibernetsko varnost ENISA in Evropska komisija, ob podpori članic EU ter čez 300 drugih partnerjev in podpornikov. Evropski mesec kibervarnosti se prične vsako leto oktobra in v mesecu dni intenzivnega dogajanja doseže milijone Evropejcev. Poglavitni cilj iniciative je okrepiti odpornost sistemov in storitev EU, opolnomočiti državljane ter narediti korak naprej k bolj kibernetsko varni in ozaveščeni družbi.

EVROPSKI MESEC KIBERNETSKE VARNOSTI

V ospredju letošnjega meseca kibervarnosti osebne zgodbe žrtev

Ob letošnjem mesecu kibervarnosti smo v ospredje postavili osebne zgodbe žrtev spletnih prevar, ki se skrivajo za neosebnimi statistikami. Žal še vedno pogosto slišimo stavek *»Meni se pa to ne more zgoditi!«* Toda spletne prevare in povzročena finančna škoda v Sloveniji iz leta v leto naraščata. V prvi polovici 2025 je SI-CERT obravnaval 1089 spletnih goljufij, od tega so tretjino predstavljale lažne investicijske sheme v kriptovalute. Gre za obliko prevare, pri kateri žrtve nasedejo obljubam o hitrem zaslužku in ob tem pogosto izgubijo vse svoje prihranke. Opazen je bil tudi porast lažnih spletnih trgovin, kjer uporabniki plačajo za naročene izdelke, ki jih nato nikoli ne prejmejo.

Za temi številkami se skrivajo resnične zgodbe ljudi, ki so utrpeli finančno škodo in pogosto doživeli občutke nemoči, sramu ali krivde. Žrtev lahko postane vsakdo, saj napadalci ciljajo na čustva – bodisi z vzbujanjem strahu in občutka nujnosti bodisi z obljubami o hitrem zaslužku ali prihranku. Naše osrednje sporočilo je jasno: nihče ni imun na spletne prevare.

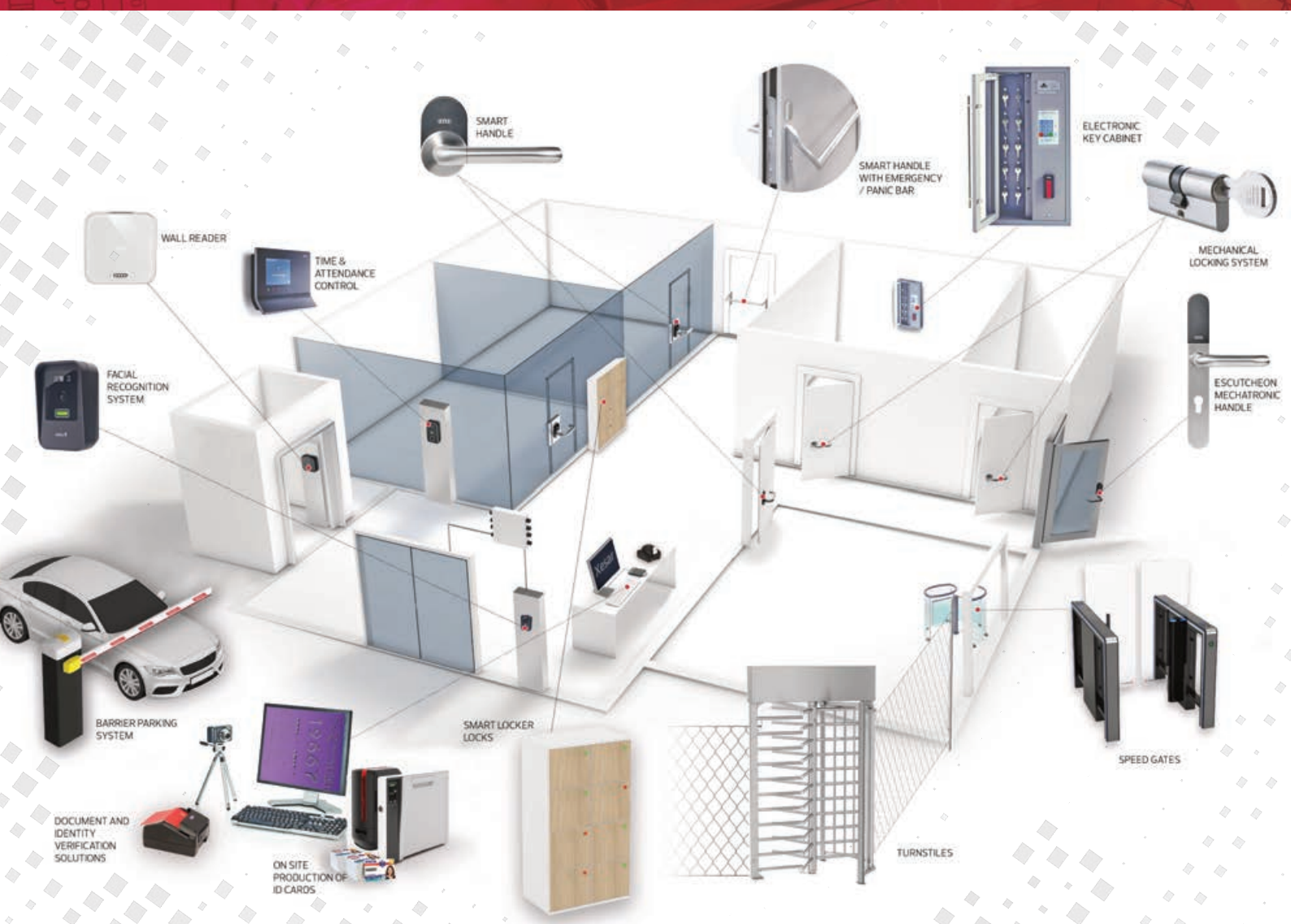
Veliko prevar bi lahko preprečili z nekaj dodatne previdnosti in znanjem. Ključno je, da ostanemo mirni ob sporočilih, ki zahtevajo takojšnje ukrepanje. Ne ustrašimo se groženj, da moramo nemudoma vnesti svoje geslo ali bančne podatke. Ustavimo se, preden vnesemo finančne podatke (geslo za e-banko ali kreditno kartico) in preverimo verodostojnost spletnega mesta. Predvsem pa ne zaupajmo obljubam o hitrih zaslužkih.

Ker se lahko zgodi tudi vam. ■

CELOVITE REŠITVE KONTROLE DOSTOPA ZA SODOBNE ORGANIZACIJE

ID Shop – Povezujemo tradicionalno varnost in pametne tehnologije.

Kontrolo dostopa razumemo kot sistem, ki raste skupaj z organizacijo.
Več kot oprema - za vas načrtujemo, montiramo in vzdržujemo sisteme za zagotavljanje varnosti.
Ker varnost ni le tehnična rešitev, temveč del zanesljivega delovanja vaše organizacije.
Vse na enem mestu, z enim partnerjem!



Rešitve za celovito kontrolo dostopa na vseh vrstah objektov:

mehanski in mehatronski sistemi zaklepanja, on-line/off-line kontrola dostopa, pametni sistemi zaklepanja garderobnih omaric, hitri prehodi (bariere) za nadzorovana območja, nizka in visoka vrtljiva vrata, parkirni sistemi, ticketing sistemi, naprave za preverjanje istovetnosti dokumentov, elektronske omarice za ključe, oprema za tiskanje ID kartic, ...

IDealni partner za identifikacijo in varnost

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

Avtorica: Mateja Mirtič Zelič / vodja Marketinga in PR, ID Shop, d.o.o.

POMEN ZAGOTAVLJANJA VARNOSTI KOT NOVI STANDARD GRADNJE

Sodobni poslovni objekti zahtevajo varnostne rešitve, ki so hkrati učinkovite, estetsko dovršene in digitalno povezane. Podjetje ID Shop zato naročnikom zagotavlja celostno podporo na področju kontrole pristopa, mehanskega zaklepanja in tehničnega varovanja, pri čemer se vključuje že v začetnih fazah projektiranja novogradenj ter prenov.

Celovit pristop k varnosti in estetiki

Pri izbiri partnerja za izvedbo varnostnih rešitev je bilo naročniku ključnega pomena sodelovanje s podjetjem, ki ne zagotavlja le dobave opreme, temveč ima tudi lastno ekipo za strokovno vgradnjo. Poleg tega je ID Shop aktivno vključen v projektiranje, usklajevanje z različnimi izvajalci na objektu in nudi podporo tudi po izvedeni montaži ter implementaciji sistemov. Takšen pristop zagotavlja, da so rešitve optimalno integrirane, funkcionalno dovršene in zanesljivo delujejo tudi po predaji objekta, hkrati pa omogoča, da varnostne rešitve niso rezultat kompromisov, temveč del premišljene zasnove objekta. V praksi to pomeni, da bodo sistemi, ki jih zagotavljamo v ID Shop, hkrati zanesljivi, digitalno napredni in estetsko usklajeni z arhitekturo.

Varnost in digitalizacija kot temelj trajnostne gradnje

V središču Rogaške Slatine nastaja **Mednarodni center za trajnostno gradnjo (MCTG)** – projekt skupine GIC, ki bo v prihodnosti predstavljal model pametne in trajnostne gradnje v Sloveniji ter širše.

Objekt bo združeval načela trajnostne gradnje, digitalizacije, energetske učinkovitosti in celostne varnosti, v njem bodo zaživele napredne rešitve, nastale pod okriljem »G Zero« vizije, ki bodo zagotavljale samooskrbo, multimodalnost in trajnostnost z minimalnim vplivom na okolje. Eden izmed ključnih ciljev projekta je preseči trenutno nizko stopnjo digitalizacije gradbene panoge, ki povzroča organizacijske, kadrovske in finančne izgube. Z uvedbo naprednih tehnologij bo MCTG pokazal, kako digitalizacija izboljša ne le učinkovitost, temveč tudi varnost in preglednost delovanja poslovnih objektov.

Integriran varnostni koncept podjetja ID Shop - združevanje mehanske in digitalne varnosti

V podjetju ID Shop smo sisteme kontrole pristopa in mehanskega zaklepanja za MCTG razvijali v tesnem sodelovanju z naročnikom, GIC GRADNJE, že v fazi projektiranja. Skupaj smo analizirali varnostne potrebe objekta, arhitekturne zahteve in estetski koncept, da bi oblikovali rešitve, ki so hkrati učinkovite, digitalno napredne ter vizualno usklajene z zasnovo stavbe. Takšen sodelovalni pristop zagotavlja, da varnostni sistemi niso le dodatek, temveč integralni del objekta, kar omogoča popolno sinergijo med mehanskimi in digitalnimi elementi ter ostalimi zalednimi sistemi. Rezultat so premišljeno zasnovani elegantni črni cilindri, stekleni podometni čitalci in brezkontaktne biometrične rešitve, ki subtilno dopolnjujejo sodobno arhitekturo centra ter hkrati zagotavljajo vrhunsko varnost.

Mehanska osnova – sistem EVVA ICS

Temelj varnostne ureditve predstavlja mehanski sistem zaklepanja EVVA ICS s cilindričnimi vložki v črni barvi, ki se bodo estetsko dopolnjevali z izbranim okovjem. V ID Shop vedno zagovarjamo, da je sistem zaklepanja osnovni varnostni gradnik za vsako digitalno kontrolo pristopa, saj zagotavlja:

- natančen pregled nad obtokom ključev in njihovimi nosilci,
- onemogočeno nepooblaščeno kopiranje – dodatni ključi se izdelajo le z varnostno kartico,
- sledljivost fizičnih dostopov in integracija z digitalno kontrolo dostopa.

EVVA ICS sistem zaklepanja tako preprečuje, da bi se dostop do prostorov izvajal mimo elektronske evidence, s čimer se zagotavlja popolna skladnost med mehansko in digitalno varnostjo.

Elektronska kontrola pristopa – sistem SALTO XS4

Elektronski del sistema temelji na rešitvah Salto, ki omogočajo napredno, brezkontaktno in estetsko usklajeno kontrolo pristopa.
V objektu bodo nameščeni podometni XS4 stekleni čitalci –

minimalistična in arhitekturno dovršena izvedba, ki se zlije z ambientom. Salto Face Recognition – sistem za prepoznavo obraza bo nameščen na glavnem vhodu in vhodu za zaposlene ter bo omogočal biometrično prepoznavo brez kartic ali mobilnih identifikatorjev. Na ostalih prostorih bodo nameščene XS4 One baterijske komponente.
S Salto XS4 kontrolo dostopa bo poskrbljeno za:
- preprosto vpisovanje uporabnikov prek mobilne naprave ali računalnika,
- popolnoma šifrirano shranjevanje biometričnih podatkov (vključno s komunikacijo med napravami),
- anti-spoofing zaščita (preprečevanje zlorab s fotografijami ali maskami),
- revizijske sledi in poročila v realnem času o dostopih in prisotnosti,
- enostaven izbris ali deaktivacija uporabnikov, kar zmanjšuje tveganje nepooblaščenega dostopa,
- možnost uporabe tudi za evidenco delovnega časa in povezavo s kadrovskimi sistemi.

Ko bo rešitev implementirana, bo zagotavljala sledljivost dogodkov, redne varnostne posodobitve in šifriranje vseh podatkov, kar je skladno z zahtevami sodobnih varnostnih standardov.

Integracija sistemov – digitalna sinergija

Vsi podsistemi v objektu bodo povezani z avtomatiziranim sistemom Nioma/Loxone, kar bo omogočalo centralno upravljanje in energetsko optimizacijo. Sistem bo združeval funkcije razsvetljave, prezračevanja, ogrevanja in kontrole dostopa, ki bodo delovale glede na prisotnost oseb v prostorih.

Dodatno bo kontrola dostopa povezana s Schindler dvigali, kar pomeni, da lahko uporabniki izberejo le tista nadstropja, za katera imajo dovoljenje – tako je zagotovljen popoln nadzor gibanja v objektu.

Takšna integracija bo zagotavljala visoko stopnjo varnosti, funkcionalnosti in energetske učinkovitosti.

Varnost v skladu z evropskimi smernicami NIS2

Pri projektih, kot je MCTG, kjer se združujejo elementi pametne zgradbe, digitalne kontrole pristopa in avtomatiziranega upravljanja, je ključno, da so vsi sistemi zasnovani tudi v skladu z načeli NIS2. Ta evropska uredba ne velja zgolj za kritično infrastrukturo, temveč tudi za pomembne in bistvene subjekte, med katere spadajo gradbena podjetja, investitorji in upravljavci digitaliziranih objektov.

Za gradbeni sektor to pomeni, da mora biti varnost vgrajena že v fazi načrtovanja (načelo »Security by Design«). To vključuje odpornost komunikacijskih sistemov, ločitev kritičnih omrežij od javnih povezav in uporabo certificirane, redno posodobljene opreme. Ključno vlogo ima tudi upravljanje dostopov in identitet, saj je treba zagotoviti sledljivost vseh fizičnih ter digitalnih dostopov, individualne pravice in dvofaktorsko avtentikacijo.

V praksi bo to pri MCTG pomenilo:
- integracijo sistemov Salto, EVVA, Loxone in Schindler in ostalih prek šifriranih povezav ter ločenih uporabniških pravic,
- šifrirano obdelavo biometričnih podatkov v sistemu Salto Face Recognition,
- sledljivost in revizijske sledi vseh dostopov,
- usposabljanje osebja in postopki za odziv na morebitne incidente.

S takšnim pristopom MCTG uresničuje načelo “Security by Design” – varnost ni dodatek, temveč sestavni del arhitekturne, digitalne in organizacijske zasnove objekta.

V sodelovanju z ID Shop in drugimi tehnološkimi partnerji bo MCTG postal primer, kako lahko mehanska, digitalna in biometrična zaščita ter ostali digitalni sistemi delujejo v sinergiji – estetsko, učinkovito in skladno z evropskimi varnostnimi smernicami. ■

Foto: arhiv ID Shop, d.o.o.

ACTUAL I.T. UNISTAR PRO astec ITELIS

www.actual-it.si

Avtor: Matic Čaleta / Institut za korporativne varnostne študije*

INTERVJU
Uroš Strnišek, vodja SOC & skladnost v skupini ACTUAL I.T.

NAJVEČJA GROŽNJA JE TISTO, ČESAR NE VIDIMO

Digitalna napadalna površina organizacij se širi iz dneva v dan. Podatki so v oblaku, infrastruktura razpršena, uporabniki delajo od kjerkoli, dobaviteljske verige pa povezujejo podjetja v neločljivo celoto. Kibernetska varnost zato ni več le zaščita omrežja, temveč upravljanje izpostavljenosti, ki se neprestano spreminja. O tem, kako to vidljivost ohraniti in zakaj je varnost danes predvsem poslovna funkcija, smo se pogovarjali z Urošem Strnišnikom, vodjo SOC & skladnosti v skupini ACTUAL I.T.

Napadalna površina organizacij raste hitreje od njihove sposobnosti nadzora. Kako jo opredeljujete in merite v praksi?

Napadalno površino moramo razumeti kot vse tisto, kar je izpostavljeno navzven. Vse, kar je povezano v digitalni svet in bi lahko nekdo izkoristil za vdor. To niso samo strežniki in spletne aplikacije, ampak tudi uporabniški računi, oblačne storitve, partnerji in celo delovni procesi. Največji izziv danes ni v tem, da teh stvari ne bi znali zaščititi, temveč da pogosto sploh ne poznamo vseh. V praksi zato najprej poskrbimo za popolno vidljivost. Mi moramo vedeti, kaj vse je dejansko "tam zunaj". Šele nato lahko govorimo o nadzoru in zmanjševanju tveganj. Tu ne gre za enkratno akcijo, temveč za stalni proces, saj se digitalna površina podjetja spreminja vsak dan – z novimi aplikacijami, uporabniki in storitvami.

Najpogosteje so spregledani ravno deli okolja, ki niso več uradno v uporabi, a so še vedno aktivni v ozadju. Katera območja napadalne površine podjetja se po vaših izkušnjah najpogosteje zanemarijo in zakaj?

Najpogosteje so spregledani deli okolja, ki jih nihče več "uradno" ne uporablja, a še vedno delujejo v ozadju. Govorim o starih sistemih, pozabljenih aplikacijah ali testnih okoljih. To so taki tihi kotički IT-ja, kjer se pogosto skriva največ tveganj. Veliko vrzeli nastaja tudi pri API-jih, ki povezujejo aplikacije med seboj. Ker jih je težko slediti in pogosto nimajo jasnega lastnika, hitro postanejo neviden, a zelo privlačen cilj za napadalce. Podobno velja za shadow IT, kjer zaposleni po lastni presoji uporabljajo različna orodja ali oblačne storitve, s čimer nehote povečajo digitalno izpostavljenost podjetja. Vedno večjo težavo pa predstavlja dobaviteljska veriga. Podjetja danes niso več izolirani sistemi, temveč so povezana z množico zunanjih partnerjev, ponudnikov storitev in podizvajalcev. Napadalci to dobro izkoriščajo in napadejo tam, kjer je varnostna kontrola najšibkejša – pri partnerju, ki ima dostop do naših sistemov. Zato je zaupanje v dobavitelje treba dopolniti z rednim preverjanjem in jasnimi varnostnimi zahtevami.

Vidljivost mora biti stalna in celovita, sicer o varnosti ne moremo govoriti. Katere pristope in orodja priporočate

*avtor je član Slovenskega združenja korporativne varnosti

za učinkovito in neprekinjeno vidljivost v razpršenih IT in OT okoljih?

Zelo pomembno je, da podjetje najprej dobro pozna samo sebe. Da pozna vse svoje sisteme, aplikacije, naprave in uporabnike. Brez tega ne moremo govoriti o varnosti. Zato je prvi korak vzpostavitev popolne vidljivosti, ki mora biti stalna, ne le občasna. V IT okolju pri tem pomagajo orodja za neprekinjeno spremljanje sredstev in ranljivosti, medtem ko je v OT okolju pristop bolj nežen – tam uporabljamo pasivne metode, ki ne posegajo v delovanje industrijskih sistemov. Pomembno je, da se vsi podatki zbirajo na enem mestu, kjer jih lahko varnostna ekipa analizira in razume v kontekstu celotnega okolja. To je edini način, da lahko organizacija hitro zazna spremembe, poveže dogodke med seboj in se pravočasno odzove.

Multi-cloud, edge in IoT so odprli vrata fleksibilnosti, hkrati pa tudi bistveno večji kompleksnosti. Kako ta premik vpliva na varnostno arhitekturo in širino napadalnih vektorjev?

Premik v multi-cloud in edge okolja je podjetjem prinesel veliko fleksibilnosti, hkrati pa tudi precej večjo kompleksnost. Podatki in aplikacije so danes razpršeni med več ponudnikov in lokacij, kar pomeni, da klasični model varovanja "enega omrežja" preprosto ne deluje več. Vsako okolje ima svoje varnostne mehanizme, zato je izziv predvsem v tem, kako vse skupaj povezati v enoten, pregleden sistem. Na primer, tudi IoT-naprave so dodale nov sloj tveganj, saj pogosto nimajo osnovnih varnostnih zaščit in se hitro znajdejo v vlogi šibkega člena. Zato se moramo držati načela ničelnega zaupanja (zero trust), kar pomeni, da nikomur in ničemur ne zaupamo samodejno, temveč preverjamo vsako povezavo, dostop in prenos podatkov. Le tako lahko v razpršenih okoljih ohranimo nadzor in zmanjšamo možnosti za zlorabo.

Identiteta je danes najpomembnejša točka nadzora. Kako lahko celovito upravljanje identitet in privilegijev zmanjša dejansko izpostavljenost podjetja?

Danes meje omrežja praktično ni več – zaposleni dostopajo do podatkov od kjerkoli, prek različnih naprav in oblačnih storitev. V takem okolju je identiteta postala glavni varnostni element. Če nekdo prevzame račun uporabnika, ima pogosto na široko odprta vrata do podatkov podjetja. Zato je celovito upravljanje identitet in privilegijev izredno pomembno, saj le tako v vsakem trenutku vemo, kdo ima dostop do česa in zakaj. To vključuje preverjanje pristnosti z več faktorji, redne revizije dostopov in načelo najmanjših privilegijev, kjer ima vsak uporabnik samo toliko pravic, kot jih res potrebuje za svoje delo.

Zero Trust danes ni več koncept rezerviran za največje. Kako realistična je njegova uvedba v srednje velikih podjetjih in kateri koraki prinašajo največje organizacijske izzive?

Zero Trust je povsem dosegljiv tudi za srednje velika podjetja, če se ga lotijo postopno. Največji izziv ni tehnologija, temveč sprememba miselnosti – od zaupanja do preverjanja. Začeti je treba pri

upravljanju identitet in dostopov, nato pa pristop postopno razširjati na celotno okolje.

Kakšen pomen ima po vašem mnenju prehod k neprekinjenemu upravljanju napadalne površine, podprtemu z avtomatizacijo, CTI in napovedno analitiko?

To je naraven in predvsem potreben premik. Penetracijski testi so še vedno pomembni, vendar pokažejo le trenutno sliko, torej stanje na določen dan. V resnici se okolje spreminja vsak trenutek, saj se sistemi posodabljajo, storitve dodajajo, uporabniki prihajajo in odhajajo. Zato danes govorimo o stalnem upravljanju napadalne površine, kjer avtomatizacija, obveščevalni viri (CTI) in analitika omogočajo sprotno zaznavanje sprememb in groženj. Tak pristop organizacijam omogoča, da tveganja ne le prepoznajo, temveč jih tudi aktivno zmanjšujejo – še preden pride do incidenta.

Na katere metrike se velja osredotočiti, da organizacija resnično razume, ali postaja bolj odporna in ne zgolj skladna?

Najbolj zgovorni so kazalniki, ki merijo učinkovitost odziva, ne le količine aktivnosti. To so predvsem čas zaznave (MTTD), čas odziva (MTTR) in delež incidentov, ki jih uspemo obvladati avtomatizirano. Pomembno je tudi spremljati, kako se skozi čas zmanjšuje število kritičnih ranljivosti. Administrativna skladnost je nujna, a ne pomeni varnosti. Prave izboljšave vidimo takrat, ko se podjetje zna hitreje in pametneje odzvati – ne le izpolnjevati obrazcev.

Modeli SOC-a se razvijajo v smeri upravljanih ali hibridnih pristopov. V katerih primerih je za podjetje smiselnejši interni SOC in kaj je ključno za učinkovito integracijo procesov, ljudi in tehnologije?

Interni SOC ima smisel, kadar podjetje potrebuje visoko stopnjo nadzora in ima dovolj kadrovskih ter finančnih zmožnosti, da ga vzdržuje 24/7. Večina organizacij pa se danes odloča za upravljane ali hibridne modele, kjer zunanja ekipa dopolnjuje interno znanje in skrbi za stalno pokritost. Zelo pomembno pri tem je sodelovanje – jasna delitev odgovornosti, izmenjava podatkov in usklajeni postopki odziva. Šele ko procesi, ljudje in tehnologija delujejo kot enoten sistem, SOC resnično prinaša vrednost, ne glede na to, ali je interni ali upravljan.

Na kakšen način morajo varnostne operacije prilagoditi svoj pristop širjenju digitalne površine, da zagotovijo pravočasen in kontekstualiziran odziv?

Varnostne operacije se morajo premakniti od zgolj zbiranja podatkov k razumevanju konteksta. Sam alarm danes ne pove veliko – pomembno je vedeti, kaj pomeni v širši sliki in kakšen vpliv ima na poslovanje. Tu pomembno vlogo prevzema umetna inteligenca, ki pomaga prepoznati vzorce v ogromni količini podatkov in izpostavi tiste dogodke, ki resnično zahtevajo pozornost analitika. S tem varnostne ekipe prihranijo čas in se lahko osredotočijo na tisto, kar je zares pomembno. V praksi se tako povezujejo SIEM, SOAR, CTI in AI sistemi, ki omogočajo avtomatizirano korelacijo dogodkov in hiter, kontekstualiziran odziv glede na stopnjo tveganja. A kljub naprednim orodjem ostaja ključen človeški dejavnik. Govorim o analitiku, ki zna tehnične signale prevesti v poslovni pomen in se odločiti, kdaj ter kako ukrepati.

V kolikšni meri je v podjetjih že uveljavljeno razumevanje, da kibernetska varnost neposredno podpira poslovne cilje in presega okvire klasičnega IT-ja?

Varnost se počasi, a vztrajno premika iz tehničnega v poslovni kontekst. Številna podjetja danes že razumejo, da gre pri varnosti predvsem za upravljanje tveganj in zaupanja, ne le za požarne zidove in posodobitve sistemov. Kljub temu je v mnogih okoljih še vedno prisotno razmišljanje, da je varnost nekaj, kar "ureja IT". Ključna sprememba nastopi, ko vodstva spoznajo, da varnost neposredno vpliva na poslovno stabilnost, ugled in konkurenčnost podjetja. Takrat postane varnost del strateškega odločanja – in ne več samo strošek, temveč naložba v zanesljivo prihodnost.

Kateri pristopi vodstvom omogočajo, da digitalno širitev podjetja usklajujejo z učinkovitim nadzorom izpostavljenosti in tveganj v dobavni verigi?

Digitalizacija prinaša hitrost in učinkovitost, a hkrati odpira nova vrata za napadalce. Ključ je v tem, da varnost ne zavira inovacij, temveč jih spremlja od začetka – po načelu »secure by design«. Uprave morajo razumeti, da vsak nov projekt, sistem ali partner vstopa v digitalni ekosistem podjetja in s tem vpliva na njegovo izpostavljenost. Zato mora biti varnost del vsakega strateškega pogovora, ne naknaden popravek. Tu moram ponovno izpostaviti vlogo dobaviteljske verige. Zaupanje v partnerje mora spremljati tudi preverjanje njihovih varnostnih praks. V sodobnem poslovnem okolju je namreč veriga močna le toliko, kot njen najšibkejši člen.

Poslovna stabilnost in ugled sta danes neposredno vezana na varnost. Kako ekonomsko utemeljiti investicije v varnost skozi prizmo upravljanja poslovnega tveganja?

Na varnost ne smemo gledati kot na strošek, temveč kot na naložbo v zanesljivo poslovanje. Varnostni incident danes ne pomeni več samo tehnične težave. Lahko ustavi proizvodnjo, prekine dobavne verige ali trajno načne ugled podjetja. Ko varnost postavimo v kontekst poslovnih tveganj, postane hitro jasno, da so preventivni ukrepi cenejši od posledic napada. Vlaganje v varnost je pravzaprav vlaganje v odpornost in kontinuiteto poslovanja, kar je dolgoročno ena najbolj racionalnih odločitev, ki jih lahko podjetje sprejme.

Digitalna napadalna površina se bo z nadaljnjo digitalizacijo še širila. Kateri tehnološki in taktični pristopi bodo najpomembnejši za njeno učinkovito obvladovanje ter zmanjševanje tveganj, povezanih z izpostavljenostjo?

Da, digitalna površina se bo širila, to je neizogibno. Pomembno bo predvsem, da podjetja razumejo, kaj je izpostavljeno in zakaj, ter da se znajo na spremembe odzivati sproti. Na tehnološki ravni bo vedno več poudarka na umetni inteligenci, avtomatizaciji in boljšem povezovanju varnostnih rešitev, ki skupaj omogočajo hitrejše odkrivanje ranljivosti in primeren odziv na dogodke. Na taktični ravni pa bo uspeh odvisen od sodelovanja med ljudmi in procesi. Tu mislim na sodelovanje varnostnih ekip, IT-oddelkov, vodstva in zunanjih partnerjev. Tehnologija sama po sebi še ne zagotavlja varnosti. Tisto, kar res šteje, je usklajeno in premišljeno delovanje vseh, ki skrbijo za varno poslovanje. ■

Foto: arhiv Actual I.T., d.d.

PODELITEV NAGRAD

SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 19. MAJ 2026

17. mednarodna konferenca Dnevi korporativne varnosti

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

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

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

Avtor: članek je skupno delo zaposlenih v podjetju Zarja Elektronika, d.o.o.*

POŽARNA VARNOST SONČNIH ELEKTRARN

V zadnjem času se tudi v Sloveniji povečuje število požarov, povezanih s sončnimi elektrarnami, kar razkriva pomanjkljivosti v njihovi požarni zaščiti. Med najpogostejšimi vzroki strokovnjaki navajajo mehansko poškodovane module, oksidirane spoje, neustrezne kable, pregrete razsmernike in električne obločne pojave na visokonapetostnih enosmernih vodih. K tveganju dodatno prispevajo vremenski vplivi in živali, ki lahko poškodujejo napeljavo ali povzročijo kratke stike.

Čeprav so fotonapetostni sistemi pomemben del energetske tranzicije, njihova hitra rast razkriva potrebo po boljšem načrtovanju varnostnih ukrepov. Sončne elektrarne so običajno nameščene na strehah, kjer je dostop otežen, kar dodatno zaplete intervencijo v primeru požara. Zato je ključnega pomena pravočasno zaznavanje nevarnosti in ustrezno delovanje sistemov za zgodnje obveščanje.

V podjetju Zarja Elektronika že več kot pet desetletij razvijamo inovativne sisteme za zgodnje zaznavanje požara. Avgusta 2025 smo skupaj z Zavodom za gradbeništvo Slovenije (ZAG) in proizvajalcem tehnologije Protectowire izvedli eksperiment požarne varnosti sončnih elektrarn, namenjen investitorjem, projektantom ter strokovnjakom s področja aktivne požarne zaščite (APZ).

V okviru dogodka smo predstavili linearni sistem toplotnega javljanja Protectowire LHD–CTI (Linear Heat Detection – Conductive Thermal Interface), zasnovan posebej za zaščito fotonapetostnih (FV) sistemov. Gre za napredno tehnologijo, pri kateri toplotno občutljiv kabel omogoča hitro in natančno zaznavanje pregrevanja ali začetnega požara vzdolž celotne dolžine sistema. Eksperiment je potrdil, da lahko sodobna tehnologija bistveno poveča požarno varnost in omogoči zanesljivo zaznavanje že v začetni fazi požara.

Kljub napredku pa požarna zaščita PV sistemov v Sloveniji ostaja delno neurejena in pogosto podcenjena. V praksi ni jasno določenih minimalnih zahtev za načrtovanje sistemov požarnega javljanja, zato so številne elektrarne brez ustrezne zaščite. To predstavlja tveganje tako za objekte kot za ljudi, ki jih upravljajo ali vzdržujejo.

Načrtovanje požarne varnosti fotonapetostnih sistemov

Fotonapetostni (PV) sistemi (angl. *Photovoltaic*) pretvarjajo sončno energijo neposredno v električno s pomočjo polprevodniških celic. So eden ključnih gradnikov prehoda v trajnostno energetiko, saj omogočajo čisto in obnovljivo proizvodnjo električne energije.

V Sloveniji je bilo do leta 2024 nameščenih že več kot 64.000 sončnih elektrarn s skupno močjo prek 1.400 MW, povprečna

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

velikost posamezne naprave pa znaša okoli 22 kW. Po prenovljeni Direktivi EU o energetski učinkovitosti stavb (EPBD – Solar Standard) bodo od leta 2026 naprej morale vse nove in večje obstoječe stavbe vključevati sončne elektrarne. To pomeni, da se bo v prihodnjem desetletju število PV sistemov skoraj zagotovo podvojilo.

Čeprav so sončne elektrarne okolju prijazne, se v primeru požara njihova prednost hitro spremeni v tveganje. Pri gorenju PV modulov lahko pride do sproščanja strupenih plinov, taljenja plastičnih materialov, poškodb električnih vodov in onesnaženja okolja. Zaradi električnega potenciala na enosmernih vodih gasilska intervencija pogosto predstavlja dodatno nevarnost. Zato je celovito načrtovanje požarne zaščite ključno za varno delovanje PV sistemov in zaščito ljudi, opreme ter okolja.

Eksperiment v Logatcu 2025

Avgusta 2025 smo v laboratoriju Zavoda za gradbeništvo Slovenije (ZAG) v Logatcu izvedli obsežen požarni preizkus fotonapetostnih sistemov v sodelovanju s podjetjem Protectowire FireSystems (ZDA). Namen eksperimenta je bil preveriti učinkovitost različnih tehnologij za zaznavanje požara in

analizirati vpliv konstrukcijskih razlik med PV moduli na širjenje ognja.

Tehnična ekipa je pripravila realistične mock-up modele delujočih PV polj, ki so omogočali varno simulacijo različnih požarnih scenarijev. Uporabljeni so bili CTI LHD detektorji (Conductive Thermal Interface – Linear Heat Detector), ki delujejo na principu zaznavanja toplotnih sprememb vzdolž detekcijskega kabla. Ko temperatura preseže določeno mejo (npr. 68 °C, 88 °C ali 105 °C), se toplotno občutljiva izolacija med prevodnikoma zmehča, kar povzroči stik in sproži alarm.

V eksperimentu so bili CTI kabli nameščeni pod sončnimi moduli v treh linijah – zgornji, srednji in spodnji – kar omogoča zaznavanje lokalnih pregrevanj ter t. i. vročih točk. Rezultati so pokazali izjemno odzivnost: detektorji so požar zaznali že v manj kot 20 sekundah po začetku vžiga. Sistem je deloval stabilno, z zelo nizko verjetnostjo lažnih alarmov.

Preizkušeni so bili tudi XCR detektorji (Extreme Condition Rated), namenjeni delovanju v zahtevnih okoljih z visoko temperaturo, vlago in UV-obremenitvami. Njihova robustna izvedba z ovojem iz fluoropolimera omogoča zanesljivo delovanje tudi v ekstremnih razmerah. Primerjava med CTI LHD in XCR sistemi je pokazala, da so CTI detektorji učinkoviti zlasti pri natančni zaznavi toplote, XCR pa izjemno vzdržljivi za uporabo pod moduli ali v bližini razsmernikov.

Predavanja in strokovni prispevki

Pomemben del dogodka je bil strokovni program, namenjen izmenjavi znanja in izkušenj s področja požarne varnosti sončnih elektrarn. Udeleženci so spremljali več zanimivih predstavitev, med njimi tudi predavanje prof. Grundeja Jomaasa, ki je predstavil mednarodni pogled na požarno varnost PV sistemov in poudaril pomen sodelovanja med gradbeniki, elektrotehniki ter požarnimi strokovnjaki. Njegov nastop je spodbudil razpravo o tem, kako lahko povezovanje znanja in tehnologije izboljša varnost prihodnjih energetskih rešitev.

Dogodek sta obiskala tudi predstavnika podjetja Protectowire (ZDA) – Brooke Fishback, direktor mednarodne prodaje in Brian Harrington, podpredsednik proizvodnje ter izumitelj CTI sistema. Predstavila sta razvoj linearnih toplotnih detektorjev in izkušnje z njihovo uporabo v zahtevnih industrijskih okoljih po svetu. Dogodek je bil hkrati priložnost za povezovanje strokovnjakov, proizvajalcev in raziskovalcev, ki si prizadevajo za varnejšo ter trajnostno rabo sončne energije.

Vloga investitorjev in zavarovalnic

Odločitev za vgradnjo dodatne požarne zaščite pri PV sistemih je pri nas večinoma v rokah investitorjev. Strošek vgradnje predstavlja le 2–10 % celotne vrednosti elektrarne, ven-

dar lahko bistveno zmanjša tveganje za večjo materialno škodo. V tujini zavarovalnice, kot so Zurich, FM Global in Allianz, že spodbujajo uvedbo dodatnih varnostnih ukrepov z nižjimi zavarovalnimi premijami, medtem ko slovenski trg na tem področju še nekoliko zaostaja.

Smernice in zaključek

Za PV sisteme z nazivno močjo do 1 MW trenutno ni zakonsko določenih predpisov, zato se pri načrtovanju uporabljajo strokovne smernice, kot so SZPV-512:2016 (Smernica o požarni varnosti fotonapetostnih elektrarn), pregled IZS (2022) in tehnična smernica TSG-1-001:2019. Čeprav ne zahtevajo obvezne vgradnje sistemov za samodejno zaznavanje požara, se ti vedno pogosteje uporabljajo kot nadstandardna rešitev.

Eksperiment v Logatcu je jasno pokazal, da z ustrezno tehnologijo lahko bistveno zmanjšamo požarno tveganje in izboljšamo varnost sončnih elektrarn. Požarna varnost PV sistemov ni več vprašanje prihodnosti, temveč sedanjosti. Le s sodelovanjem raziskovalcev, proizvajalcev, projektantov in investitorjev bomo zagotovili, da bo sončna energija resnično varna, trajnostna ter zanesljiva rešitev prihodnosti. ■

Foto: arhiv Zarja Elektronika, d.o.o.

Smart Fire / Gas Safety for Energy Transition Sites.

SENSIA

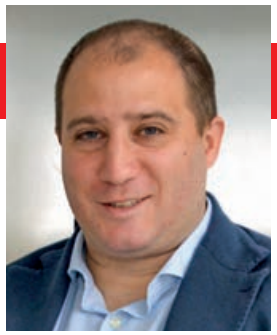
AI Thermal Cameras for Methane/SO_2 Leak Detection – EU Ready

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

ZARJA ELEKTRONIKA

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

Avtor: Jan Veršnik / vodja poslovnega razvoja v ASSA ABLOY Slovenija, d.o.o.



NEPREKINJENO DELOVANJE V POVEZANEM SVETU: KAKO DIREKTIVA NIS 2 POGANJA NOVO ERO VARNOSTI

Sodobni svet temelji na povezovanju med ljudmi, podatki in tehnologijo. A z večjo povezanostjo raste tudi ranljivost. Od kibernetskih napadov do motenj v dobavnih verigah današnje grožnje ne sodijo več v jasne kategorije. Nova direktiva NIS 2 priznava to realnost.

Uvod

Po vsej Evropi in v Sloveniji novi Zakon o informacijski varnosti (ZInfV-1) poziva upravljavce bistvenih in pomembnih storitev, da varnost obravnavajo ne kot izdelek, temveč kot proces, ki združuje fizično zaščito ter kibernetsko varnost v enotno strateško vizijo. Za slovenske organizacije ta premik pomeni več kot zgolj skladnost. Gre za zaščito tistega, na kar se družba najbolj zanaša: neprekinjeno delovanje bistvenih storitev, varovanje sredstev in zaupanje državljanov, ki so od teh storitev odvisni.

Nov standard odpornosti

NIS 2 ni zgolj regulativa, temveč načrt za odpornost, ki preoblikuje način upravljanja tveganj, poročanja o incidentih in zagotavljanja odgovornosti v organizacijah po Sloveniji in EU. Z višjimi standardi postavlja varnost kot skupno odgovornost od vodstva do operativnega nivoja in vseh ravni organizacije.

Za upravljavce v energetiki, prometu, telekomunikacijah, oskrbi z vodo, rudarstvu in naftni ter plinski industriji slovenski okvir zdaj odraža evropske ambicije. Gre za poziv k prehodu od reaktivnih ukrepov k proaktivni zaščiti z integracijo tehnologije, procesov in ljudi za predvidevanje tveganj, še preden se ta stopnjujejo.

Integracija: jedro sodobne varnosti

Sodobna varnost ni več stvar izoliranih sistemov. Ena šibka točka, bodisi napačno konfigurirana dostopna točka ali pomanjkanje preglednosti med lokacijami, lahko ogrozi celotno delovanje.

Za številne slovenske upravljavce bistvenih storitev nove obveznosti iz direktive NIS 2 poudarjajo pomen integracije: usklajevanje fizičnih in digitalnih varnostnih ukrepov, povezovanje lokalnih ter oddaljenih lokacij in zagotavljanje varnega pretoka informacij v vseh delih organizacije.

Takšen povezan pristop izboljšuje situacijsko zavedanje, pospešuje odziv na incidente in podpira skladnost z nacionalnim Zakonom o informacijski varnosti, hkrati pa poenostavlja vsakodnevno delovanje.

Neprekinjeno delovanje v negotovem svetu

Neprekinjeno delovanje pomeni več kot zgolj razpoložljivost, pomeni zaupanje. V kritičnih okoljih, kot so slovenska energetska omrežja, vodovodni sistemi in prometna infrastruktura, lahko že kratka prekinitev pomeni varnostna tveganja, izgubo prihodkov ali vpliv na javnost.

Za izpolnjevanje zahtev direktive NIS 2 in nacionalne zakonodaje morajo slovenski varnostni vodje zdaj uravnotežiti zaščito ter učinkovitost. Prilagodljive, razširljive in dobro integrirane rešitve, podprte z zaupanja vrednimi lokalnimi ter evropskimi partnerji, organizacijam omogočajo prilagajanje spreminjajočim se zahtevam brez motenj v delovanju.

Cilj je jasen: ne le obramba pred incidenti, temveč ohranjanje kontinuitete tudi pod pritiskom.

Od skladnosti do zaupanja

Izpolnjevanje zahtev direktive NIS 2 ni zgolj formalnost. Predstavlja priložnost za slovenske organizacije, da zgradijo pravo varnostno kulturo, takšno, kjer vodstvo obravnava varnost kot strateško prednost, ne le kot tehnično nujnost. Ko vodstvo spodbuja ozaveščenost, usposabljanje in sodelovanje, zaposleni postanejo aktivni soustvarjalci odpornosti. Ta kulturni premik, ki ga spodbuja posodobljen slovenski Zakon o informacijski varnosti je ključen za trajne spremembe.

Organizacije lahko k temu cilju pristopijo z naslednjimi praktičnimi koraki:

1. Razumevanje tveganj:
Začnite oceno ranljivosti v fizičnem in digitalnem okolju. Pregled ključnih sredstev in njihovih povezav pomaga prepoznati, kje bi se lahko pojavile hibridne grožnje.

2. Določanje prioritet:
Vsi sistemi ne predstavljajo enakega tveganja. Najprej se osredotočite na sredstva, ki podpirajo bistvene storitve, zagotavljajo varnost ali obravnavajo občutljive podatke. Jasno določene prioritete olajšajo učinkovito razporejanje virov in dokazovanje skladnosti.

3. Integracija sistemov:
Poiščite priložnosti za povezovanje obstoječih rešitev za kontrolo dostopa in upravljanje ključev. Integracija zmanjšuje kompleksnost, povečuje preglednost in podpira hitrejše ter usklajeno odločanje.

4. Pripravljenost na incidente:
Dobro preizkušen načrt odzivanja opredeljuje vloge, odgovornosti in poti eskalacije. Redne vaje zagotavljajo, da so ekipe pripravljene hitro in odločno ukrepati ob incidentih.

5. Nenehno izboljševanje:
Varnost in skladnost sta stalni prizadevanji. Redni pregledi, revizije in posodobitve organizacijam pomagajo ostati usklajene z razvijajočimi se grožnjami ter regulativnimi pričakovanji.

Zaključek: pogled v prihodnost

Varnost danes pomeni povezovanje med tehnologijami, ekipami in med vizijo ter izvedbo. Direktiva NIS 2 spodbuja to preobrazbo in postavlja višje standarde za to, kako organizacije ščitijo tisto, kar je najpomembnejše.

Odpornost bo v prihodnosti vse bolj temeljila na napovednih zmogljivostih, ki jih poganjajo umetna inteligenca, avtomatizacija in analiza podatkov. Te tehnologije bodo organizacijam omogočile zgodnejše zaznavanje anomalij, hitrejše odzivanje in učinkovitejše delovanje, kar bo okrepilo tako nacionalno kot evropsko odpornost.

V podjetju ALCEA verjamemo, da je kontinuiteta pravo merilo varnosti. Naše poslanstvo je pomagati operaterjem bistvenih storitev pri gradnji trajne odpornosti z združevanjem vpogleda, integracije in partnerstva za varno, pametno ter neprekinjeno delovanje. Več odkrijte v naši e-knjigi »NIS 2 in prihodnost varnosti infrastrukture z ALCEA« ter spoznajte, kako skladnost spremeniti v trajno odpornost. ■

ALCEA
ASSA ABLOY

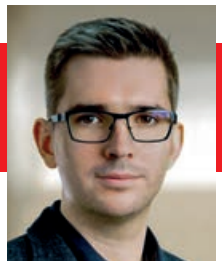
vaša vstopna točka v revolucijo povezljivosti.

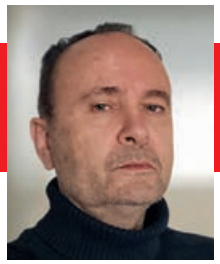
ALCEA GATEWAY

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

alceaglobal.com/gateway

Avtorja: dr. Niko Lukač / Univerza v Mariboru, FERI,
dr. Aleksander Pur / Ministrstvo za notranje zadeve, Policija





INOVATIVNA UPORABA UMETNE INTELIGENCE ZA KREPITEV PREISKOVALNE ANALITIKE V OKVIRU PROGRAMA HORIZON EUROPE

V zadnjih letih se vse policije pri preiskovanju kaznivih ravnanj soočajo z vedno večjimi količinami heterogenih podatkov. Tradicionalni pristopi za učinkovito odkrivanje sumljivih povezav in vzorcev v podatkih so postajali nezadostni za podporo operativnim preiskavam. Zato se je pokazala nujna potreba po razvoju novih inteligentnih orodij za podporo preiskovanj kaznivih ravnanj, zlasti pri napredni obdelavi velikih podatkovnih zbirk, njihovi vizualizaciji in integraciji heterogenih podatkovnih tokov.

Začetki sodelovanja: od nacionalnih projektov do Horizon Europe

Policija v Republiki Sloveniji rešuje te izzive tudi v okviru sodelovanj v nacionalnih in evropskih raziskovalnih projektih. Začetki tesnejšega sodelovanja med Uradom za informatiko Policije in Fakulteto za elektrotehniko, računalništvo in informatiko Univerze v Mariboru (UM FERI) segajo prav v ta kontekst. Pomemben člen pri tem predstavljajo raziskovalci iz laboratorija GeMMA, Inštituta za računalništvo (UM FERI), ki s svojim strokovnim znanjem omogočajo razvoj rešitev, neposredno uporabnih za potrebe Policije na področju podatkovne in preiskovalne analitike.

Tesnejše sodelovanje se je najprej oblikovalo znotraj dveh ciljnih raziskovalnih projektov (CRP), sofinanciranih s strani Agencije za raziskovalno in inovativno dejavnost Republike Slovenije (ARIS). Uspešno sodelovanje v okviru CRP-jev je ustvarilo trdno podlago za prijavo in vključevanje v evropske razpise programa *Obzorje Evropa* (Horzion Europe, HE)[1], kjer je sofinanciranje v celoti zagotovljeno iz evropskih raziskovalnih sredstev. V zadnjih petih letih je preboj umetne inteligence (UI) še dodatno izpostavil potrebo po novih rešitvah za podporo preiskovalni analitiki, ki temeljijo na metodah in orodjih UI. Znotraj programa HE smo se uspešno priključili dvema mednarodnima projektoma:

- **ARIEN** (*ARtificial IntelligencE in fighting illicit drugs production and trafficking*) – projekt, ki se je začel novembra 2023 in bo trajal do oktobra 2026. Njegov cilj je razvoj rešitev na osnovi UI za boj proti nezakoniti proizvodnji in trgovini s prepovedanimi drogami[2].

ARIEN
ARtificial IntelligencE in fighting illicit drugs production and trafficking

"The project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121329".

- **ORION** (*Optimized Risk-based Intelligence-driven Operations for Next-generation Secure, Reliable and Privacy-preserving Border Management*) – projekt, ki se je začel septembra 2025 in se bo zaključil avgusta 2028. Namenjen je razvoju naprednih, z UI podprtih rešitev za varno, zanesljivo in zasebnosti prijazno upravljanje evropskih meja[3].

"The project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101225611".

Znotraj obeh projektov sodeluje tudi slovenski Inštitut za korporativno varnost (ICS), kjer ima pomembno vlogo za izvedbo demonstracijskih scenarijev za ovrednotenje tehnologij v realnih okoljih. Komplementarno tem programom ima Policija sofinanciran razvoj tovrstnih programskih rešitev tudi iz sredstev evropskega Sklada za notranjo varnost.

Potreba po naprednih rešitvah umetne inteligence

Odkrivanje koristnih informacij v podatkih za podporo preprečevanju in preiskovanju kaznivih dejanj ni novost. Adriano Balbi in André-Michel Guerry sta že leta 1829 izdelala zemljevide, ki prikazujejo razmerja med izobrazbo ter nasilnim in premoženjskim kriminalom v Franciji[4]. Joseph Fletcher (1849) in Henry Mayhew (1861) sta prav tako pripravila zemljevide, na katerih sta prikazala deleže zaprtih moških ter stopnje kriminala po posameznih območjih[5]. Pomembna prelomnica se je začela v šestdesetih letih prejšnjega stoletja s prvimi računalniki, ki so podpirali preprečevanje in preiskovanje kaznivih dejanj. Že leta 1967 je Inštitut za obrambne analize opisal možnosti uporabe računalnikov za obdelavo ogromnih količin podatkov (The Institute for Defense Analyses, 1967)[6]. Dve leti pozneje je Arthur R. Miller že opozoril na vprašanja zasebnosti v računalniški dobi. Tudi uporaba metod UI v organih pregona ni novost, saj so bili v osemdesetih letih prejšnjega stoletja že zabeleženi številni primeri uporabe ekspertnih sistemov[7].

Zadnja desetletja je eksponentna rast podatkov, njihova heterogenost in kompleksnost preiskovalnih primerov, razkrila omejitve tradicionalnih ekspertnih sistemov, ki niso več zadostni. Vse večji obseg digitalnih sledi, komunikacijskih zapisov, finančnih transakcij, slikovnih in video podatkov ter podatkov iz odprtih virov (OSINT) zahteva orodja, ki omogočajo samodejno obdelavo in analizo na način, ki je hiter ter zanesljiv. UI ponuja nabor naprednih pristopov, ki omogočajo:

- **Samodejno odkrivanje vzorcev in anomalij** v velikih podatkovnih zbirkah, kjer so ročne metode neizvedljive.
- **Integracijo heterogenih podatkov** (besedilo, slike, video, senzorni podatki, socialna omrežja) v enotne analitične platforme.
- **Napredno vizualizacijo in interpretacijo rezultatov**, kar omogoča hitrejše in bolj utemeljene odločitve v preiskavah.
- **Podporo pri odločanju v realnem času**, kjer sta odzivnost in točnost ključnega pomena.

Posebno pomembno vlogo imajo nevronske mreže, ki omogočajo obdelavo kompleksnih in visokodimenzionalnih podatkov ter veliki jezikovni modeli (LLM-ji), ki lahko analizirajo velike količine besedilnih virov, samodejno izluščijo relevantne informacije, prepoznajo semantične povezave in podpirajo pripravo poročil ter analitičnih povzetkov. Pri tem dobivajo ključno vlogo tudi grafi znanja, ki omogočajo strukturirano predstavitev entitet (osebe, organizacije, dogodki, lokacije) in njihovih povezav. Na teh osnovah se uporabljajo grafovske nevronske mreže (GNN), ki omogočajo učinkovito klasifikacijo sumljivih vzorcev in odkrivanje anomalij v kompleksnih kriminalnih mrežah ter podporo pri odkrivanju skritih povezav. Taki pristopi odpirajo možnosti za boljše prepoznavanje kriminalnih mrež, učinkovitejše odkrivanje finančnih goljufij, hitrejše prepoznavanje tveganih vedenjskih vzorcev v komunikacijah in proaktivno zaznavanje groženj v zgodnjih fazah.

V tem kontekstu sta evropska projekta ARIEN in ORION naravna nadaljevanja nacionalnih raziskovalnih prizadevanj. Raziskovalci UM FERI so znotraj projekta ARIEN razvili rešitev za odkrivanje sumljivih vozlišč z uporabo grafov znanja in GNN. Prav tako pa v projektu ORION, ki se šele začenja, načrtujejo razvoj varnih in zasebnosti prijaznih rešitev za upravljanje evropskih meja, pri čemer bodo uporabili napredne metode UI, kot so LLM-ji za analizo virov in gradnjo grafov znanja ter GNN za zaznavanje sumljivih vzorcev pri mejnih prehodih. Pri tem je ključnega pomena, da se vse razvite rešitve ovrednotijo v realnem okolju: s strani slovenske Policije in partnerskih varnostnih organov iz celotne EU, ki sodelujejo v obeh projektih. Tak pristop zagotavlja, da so rezultati ne le raziskovalno relevantni, temveč tudi praktično uporabni, preverjeni in prilagojeni dejanskim potrebam varnostnih organov.

Regulativni okvir: AI Act

Pri razvoju rešitev UI za podporo na področju preiskovanja kaznivih ravnanj raziskovalci dajejo poudarek zlasti zagotavljanju pravnih norm, temeljnih človekovih pravic in etičnih pristopov. Tako je ključnega pomena upoštevanje Uredbe EU o umetni inteligenci (AI Act)[8], ki določa pravila glede varnosti, preglednosti, odgovornosti in varovanja temeljnih pravic pri razvoju ter uporabi sistemov UI. Zlasti relevantna so poglavja, ki opredeljujejo prepovedane prakse UI in sisteme z visokim tveganjem, kamor sodijo tudi rešitve za področje kazenskih preiskav, varovanja meja ter javne varnosti. Projekta ARIEN in ORION se na ta izziv odzoveta s pristopi, ki vključujejo:

- **vgradnjo načel zaupanja vredne UI** (*trustworthy AI*) v vse razvojne faze,
- **mehanizme za sledljivost in razlago odločitev modelov**, da se zagotovi transparentnost,
- **upoštevanje varstva podatkov (GDPR)** in znižanje tveganj pri obdelavi osebnih podatkov,
- **ocenjevanje vplivov na človekove pravice**, zlasti pri uporabi rešitev v realnih preiskovalnih in mejnih postopkih.

Ekipa iz UM FERI s svojim raziskovalnim delom aktivno razvija metodološke okvire in tehnične rešitve, ki omogočajo skladnost s smernicami AI Act. To vključuje tudi uporabo grafov znanja in GNN na način, ki je razložljiv ter preverljiv in uporabo lokalnih LLM-jev v obliki prilagojenih, varnostno preverjenih modelov, ki spoštujejo zahteve po zasebnosti ter odgovorni rabi.

Zaključne misli

Razvoj inovativnih pristopov UI je postal globalni trend, ki določa prihodnost varnostnih politik in praks. Eksponentna rast podatkov, njihova heterogenost in naraščajoča kompleksnost preiskovalnih primerov so izzivi, s katerimi se danes soočajo varnostne institucije po vsem svetu. V tem kontekstu sodelovanje med UM FERI in slovensko Policijo ponazarja, kako lahko povezovanje raziskovalnega znanja ter praktičnih potreb varnostnih organov vodi v rešitve, ki krepijo preiskovalno analitiko in omogočajo hitrejše, natančnejše ter bolj utemeljene odločitve.

Pomemben razvojni korak v tej smeri predstavlja uvedba **agentov UI:** specializiranih in avtonomnih enot, ki lahko delujejo kot digitalni pomočniki preiskovalcev. Taki agenti ne avtomatizirajo zgolj rutinskih nalog, temveč omogočajo aktivno spremljanje dogajanja v realnem času, proaktivno prepoznavanje vzorcev in anomalij ter integracijo heterogenih virov podatkov (od satelitskih posnetkov, komunikacijskih tokov do finančnih transakcij). S tem se preiskovalna ekipa razbremeni ponavljajočih se nalog in se osredotoči na strateške vidike odločanja.

V prihodnje bodo ključni izzivi v Evropi povezani s skladnostjo z regulativnimi in etičnimi okviri, kot je AI Act, ter z zagotavljanjem razložljivosti, zaupanja in zaščite temeljnih pravic. Globalno se bo tekmovanje med različnimi pristopi k uporabi UI v varnostne namene še stopnjevalo: Kitajska in Rusija krepita razvoj lastnih rešitev za množični nadzor ter geopolitični vpliv, ZDA vlagajo v kombinacijo komercialnih in vojaških aplikacij, Evropa pa gradi model zaupanja vredne ter človeku prijazne UI. Tak pristop je v skladu z evropskimi vrednotami in krepi zaupanje javnosti, hkrati pa lahko pomeni tudi morebitno slabost, saj pretirana regulacija ter stroga etična merila upočasnjujejo razvoj in implementacijo novih tehnologij. To ustvarja nevarnost, da Evropa v globalni tekmi za tehnološko premoč na področju UI zaostane za bolj agresivnimi ali manj reguliranimi pristopi drugih velesil.

Uspešno sodelovanje med raziskovalci UM FERI in Policijo v okviru projektov HE je primer dobre prakse, ki temelji na povezovanju končnih uporabnikov ter tehničnih partnerjev iz Slovenije. Pri tem morajo imeti končni uporabniki jasno opredeljene potrebe in cilje, tehnični partnerji pa znanje ter inovativne ideje, s katerimi naslavljajo tudi pomanjkanje strokovnega tehničnega kadra v državni upravi. Kljub dobrim rezultatom izziv predstavljajo predvsem številne birokratske ovire. Zaradi pomena tehnološkega razvoja in sofinanciranja s strani EU v Sloveniji lahko v prihodnosti pričakujemo več podpore ter manj administrativnih ovir pri sodelovanju v tovrstnih projektih. Navsezadnje pa tovrstni inovativni pristopi, ki jih sofinancira EU, vodijo k višji varnosti za vse državljane, kar je osnovno vodilo slovenske Policije.

1 Program HE: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

2 Projekt ARIEN: https://cordis.europa.eu/project/id/101121329

3 Projekt ORION: https://cordis.europa.eu/project/id/101225611

4 Borden. 2000. „Brief History of Crime Mapping.“ In Atlas of Crime: Mapping the Criminal Landscape, Phoenix, AZ: Oryx Press.

5 Sharon. 2006. „The History of Crime Mapping and Its Use by American Police Departments.“ Alaska Justice Forum 23, no. 3: 1.

6 Institute for Defense Analyses. 1967. Task Force Report: Science and Technology. Washington, DC: U.S. Government Printing Office.

7 Miller. 1969. „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society.“ Michigan Law Review 67, no. 6.

8 EU AI Act: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence ■

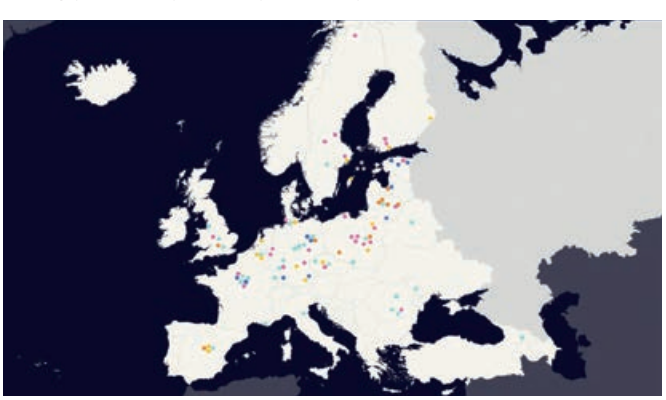
Avtorica: mag. Sabina Muratović / Oddajniki in zveze RTV Slovenija*

ODPORNOST NACIONALNIH MEDIJEV NA HIBRIDNE GROŽNJE

Julija 2025 je Evropska unija izdala enotno opozorilo: javni mediji so v prvi liniji hibridne vojne. Napadi nanje niso več osamljeni incidenti, temveč del širše strategije destabilizacije evropskih demokracij. Svet Evropske unije je Rusijo tedaj vnovič obtožil nenehnih zlonamernih dejavnosti. Te so del širših, usklajenih in dolgotrajnih hibridnih napadov, namenjenih ogrožanju ter spodkopavanju varnosti, odpornosti in demokratičnih temeljev Evropske unije. Ruske aktivnosti vključujejo ciljanje na kritično infrastrukturo, volilne procese v posameznih državah in zlasti medije.

Poročilo EBU 2025: več kot 60 hibridnih napadov

Le nekaj mesecev pred tem, marca 2025, je Evropska radiodifuzna zveza (EBU) objavila preiskovalno poročilo *Playing with Fire*, ki niza več kot 60 hibridnih napadov, pripisanih ruskim ali proruskim akterjem. Šlo je za kibernetske vdore, sabotaže, vandalizem, požige, vplivne operacije in ciljno dezinformiranje evropskih javnosti – zlasti v predvolilnih obdobjih ali v državah, ki javno podpirajo Ukrajino. Poročilo posebej izpostavlja javne servise in medije, ki so bili tarče DDoS napadov, poskusov vdorov, kampanj diskreditacije novinarjev in infiltracije lažnih informacijskih kanalov. Napadi so bili usmerjeni tudi v tehnično infrastrukturo za oddajanje in prenos informacij. Taki incidenti so se med drugim zgodili v Belgiji, Nemčiji, Španiji, Estoniji, Litvi.



Na zemljevidu so prikazani hibridni napadi – od fizičnih (vandalizem, sabotaža, požigi), označenih z modro, rdečo in oranžno barvo, do digitalnih (vplivne in kibernetske operacije), prikazanih z vijoličnimi, turkiznimi in sivimi pikami. Vir: European Broadcasting Union - EBU, Playing With Fire, marec 2025.

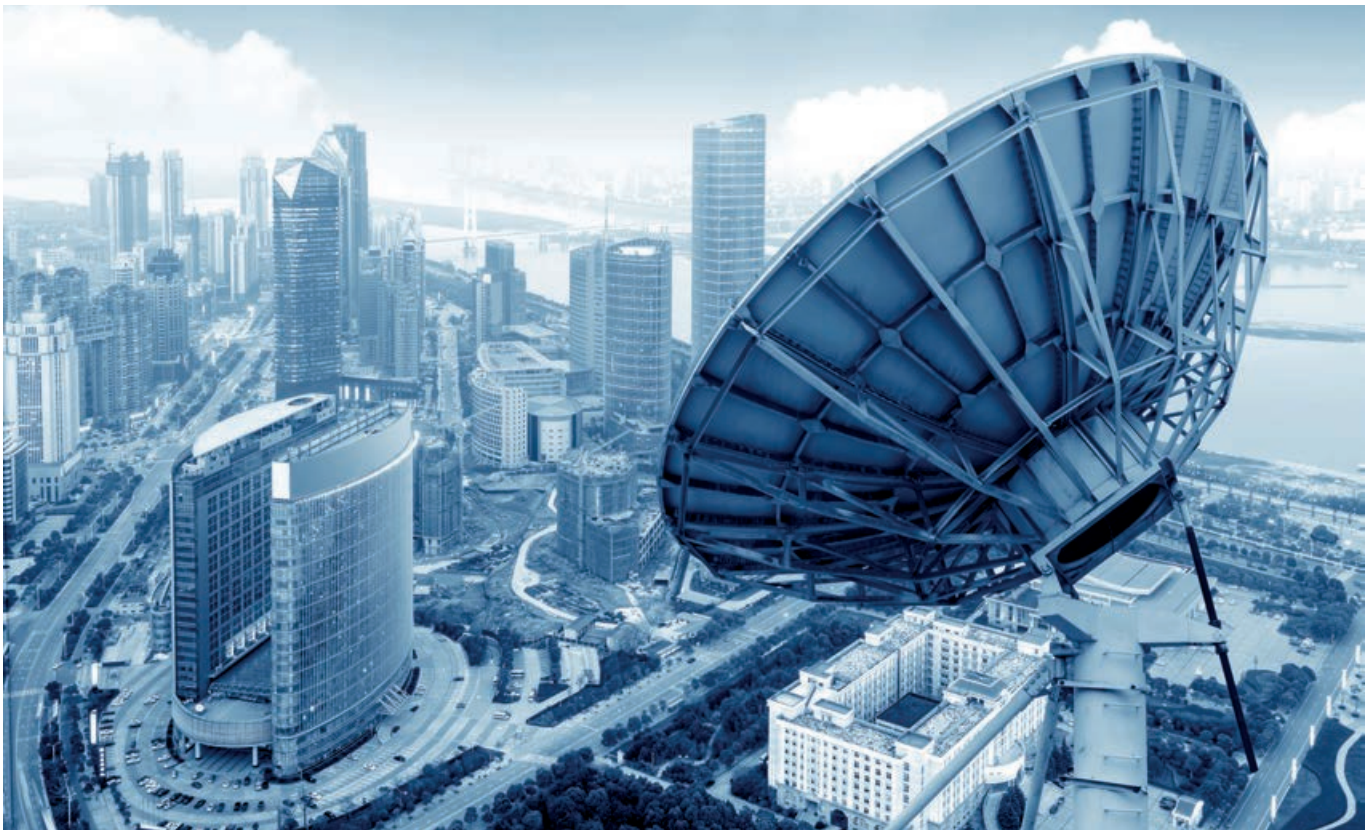
TV5Monde: prvi večji kolaps javnega medija v Evropi

Aprila 2015 se je v Evropi zgodil prvi primer, ko je osrednji javni medij skoraj v celoti onesposobila kibernetska operacija. Francoska televizijska mreža TV5Monde je doživela programski kolaps. Dvanajst programov je ugasnilo, spletna stran je bila nedosegljiva, na družbenih platformah TV5Monde so se začele pojavljati grožnje pod zastavo ISIS. Pozneje se je izkazalo, da je za napadom ruska hekerska skupina APT28. Primer TV5Monde je referenčni primer kibernetskega napada na javni medij z geopolitičnim ozadjem.

Od BBC do Imprese: primeri napadov na evropske medije

Temu napadu so sledili številni drugi. Tako javni kot komercialni mediji so postali žrtev in strateški cilj. Konec leta 2015 so DDoS napadi onesposobili spletne portale britanske BBC. V začetku leta 2022 je na Portugalskem skupina Lapsus$ vdr-

*organizacija je korporacijski član Slovenskega združenja korporativne varnosti



la v strežnike medijske hiše Impresa in zlorabila njihov uradni Twitter račun za razpošiljanje lažnih novic. Leta 2024 je nemški lokalni radio Geretsried zaradi ransomware napada izgubil dostop do svojega digitalnega arhiva in moral več dni oddajati zgolj avtomatizirano glasbo.

Fizične sabotaže: oddajniki in napadi na infrastrukturo

Ob kibernetskih napadih se je kot tarča fizičnih sabotaž izkazala tudi evropska telekomunikacijska infrastruktura, ki omogoča oddajanje radijskih in televizijskih programov. Leta 2016 se je na Švedskem porušil 300-metrski stolp pri mestu Borås, preiskava pa je potrdila sabotažo. V istem obdobju so v regiji zaznali še presekanje komunikacijskih kablov, kar so obravnavali kot širši varnostni incident. Med rusko invazijo na Ukrajino so oddajniki postali vojaški cilji – raketni napad je leta 2022 poškodoval televizijsko stavbo v Kijevu, v Harkovu pa oddajnik dvakrat (2022 in 2024). V Pridnestrju sta bili uničeni dve radijski anteni.

Vsi ti primeri potrjujejo ranljivost telekomunikacijske infrastrukture, zlasti v kriznih obdobjih, ko se dezinformacije in strahovi širijo z močnejšim psihološkim učinkom.

Psihološki učinki hibridnih napadov na javne medije

Skupni imenovalec hibridnih napadov na medije ni zgolj spodkopavanje zaupanja v demokracijo in njene ustanove, temveč dokazovanje moči. Vsak uspešen vdor razgali tehnično ranljivost sistemov in skuša ustvarjati vtis, da so napadalci ves čas korak pred obrambo. Zlasti uspešno širjenje dezinformacij ima dvojni učinek: na eni strani vpliva na percepcijo dogodkov in javno mnenje, na drugi pa psihološko deluje na posameznika, v katerem se ob programskem izpadu ali manipuliranih vsebinah sproži naraven odziv strahu, dvoma ali izgube občutka varnosti. Vsak napad je sporočilo, da noben sistem ni zares varen in da lahko sovražnik vstopi v jedro zaupanja, kadar koli želi. Prav zato hibridni napadi na medije presegajo naravo tehničnega incidenta – postanejo strateško orožje, ki cilja na več tarč hkrati - na sisteme, na ljudi, s tem pa spodkopava odpornost celotne družbe.

Primer RTV Slovenija: medijska vloga in kritična infrastruktura

Vloga RTV Slovenija je dvojna, ker nastopa kot javni medijski servis na eni strani in kot ključni subjekt kritične infrastrukture na drugi. Upravlja obsežno mrežo oddajnikov in pretvornikov na 208 lokacijah po vsej Sloveniji. Telekomunikacijski stolpi omogočajo prenos radijskih in televizijskih signalov ter oddajanje v uporabo mobilnim operaterjem, Ministrstvu za obrambo, Ministrstvu za notranje zadeve, kontroli zračnega prometa in drugim uporabnikom radiodifuznega spektra. Vsak izpad oddajanja neposredno ogroža obveščanje prebivalstva, v kriznih trenutkih pa lahko pomembno zamaje občutek varnosti.

Vojna za Slovenijo leta 1991 je pokazala, da oddajniška infrastruktura sodi med prve tarče agresorja. JLA je z letalskimi napadi na ključne oddajniške lokacije (Krvavec, Nanos, Kum, Domžale) hotela preprečiti obveščanje prebivalstva v Sloveniji, s poškodovanjem evrovizijskih zvez pa tudi širše evropske javnosti. Že tedaj se izkazala izjemna komunikacijska vloga javnega medija, saj je bila nacionalna radiotelevizija nepogrešljiva pri obveščanju prebivalstva doma in po svetu.

Skupni imenovalec hibridnih napadov na medije ni zgolj spodkopavanje zaupanja v demokracijo in njene ustanove, temveč dokazovanje moči. Vsak uspešen vdor razgali tehnično ranljivost sistemov in skuša ustvarjati vtis, da so napadalci ves čas korak pred obrambo.

Oddajniški center Nanos je bil ena osrednjih tarč letalskih napadov JLA leta 1991, ko je agresor nameraval uničiti evrovizijske zveze proti Avstriji in Italiji. Vir: Arhiv RTV Slovenija.

Ne glede na skokovit tehnološki napredek, pojave komercialnih televizij in družbenih omrežij se v kriznih trenutkih vloga RTV Slovenija vsakič potrjuje kot ključna. Žledolom 2014, požari na Krasu 2022, katastrofalne poplave avgusta 2023 – v takih situacijah je prav RTV Slovenija tisti kanal, prek katerega država v ključnih trenutkih najbolj nagovarja državljane in mu državljani najbolj zaupajo. Takšna infrastruktura je posledično eden ključnih stebrov nacionalne odpornosti.

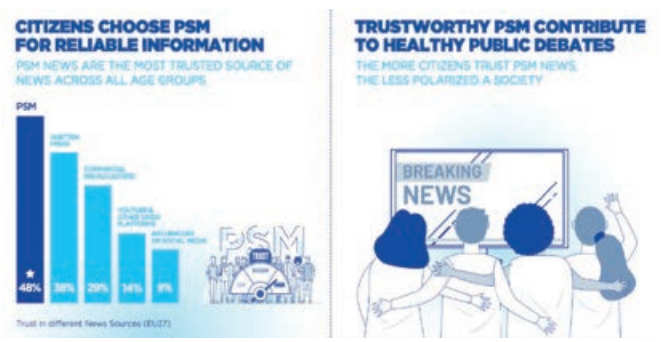
Napad marca 2024: odziv in pomen nacionalnega javnega medija

Zato je RTV Slovenija kibernetski napad, ki se ji je zgodil marca 2024, ko je bila tarča DDoS napada**,** vzela izjemno resno. Napad so hitro zajezili in sistem zaščitili, zato večje programske škode ni bilo. Po podatkih Urada vlade za informacijsko varnost je bil napad verjetno politično motiviran**,** podobno kot drugi tedanji napadi na spletne strani državnih institucij, vključno z Uradom predsednice Republike Slovenije. Napade naj bi izvajala ruska hekerska skupina Cyber Army Russia Reborn**,** ki je v videu Slovenijo označila za tarčo zaradi njene podpore Ukrajini.

Zaupanje v javne medije – ključni podatek za prihodnost

Konec leta 2024 je začel veljati novi Zakon o kritični infrastrukturi (ZKI-1), ki uvaja koncept aktivne odpornosti – poudarja funkcionalno vzdržnost, redundanco in informacijsko varnost kot temelje nacionalne varnosti. RTV Slovenija je bila v tem okviru prepoznana kot subjekt najvišje nacionalne pomembnosti, saj njeno neprekinjeno delovanje neposredno vpliva na varnost prebivalcev, kar so potrdili tudi uradni dokumenti o poplavah leta 2023.

Na evropski ravni podatki poročila EBU Trust in Media (2024) kažejo, da so javni mediji najbolj zaupanja vreden vir novic – v povprečju jim zaupa skoraj polovica evropskih državljanov, med mladimi pa so med dvema najbolj zanesljivima viroma informacij. Razlika v zaupanju med javnimi in drugimi mediji presega 20 odstotnih točk, kar potrjuje, da je zaupanje ključen varnostni dejavnik, ne le medijski.



Javni mediji (PSM) so v državah EU najzanesljivejši vir informacij – zaupa jim skoraj polovica prebivalcev, bistveno več kot tiskanim, komercialnim ali spletnim virom. Zaupanje v javne medije hkrati zmanjšuje družbeno polarizacijo in prispeva k bolj zdravim javnim razpravam. Vir: European Broadcasting Union - EBU, Trust in Media Report 2024.

Človeški obraz odpornosti

Za številkami in napadi stojijo ljudje – novinarji, inženirji in gledalci. Novinar, ki mu vdrejo v elektronsko pošto, inženir, ki ponoči vzdržuje oddajnik, ali gledalec, ki v kriznih razmerah išče informacije – vsi so del istega bojišča. Odpornost javnih medijev se ne gradi le s tehnologijo, temveč z zaupanjem državljanov, ki pričakujejo, da bodo informirani tudi takrat, ko odpove vse drugo.

Hibridni napadi kot strategija destabilizacije

Hibridni napadi na medije so sestavni del strategije destabilizacije – razkrivajo ranljivosti sistemov in hkrati rušijo občutek varnosti. Primeri od TV5Monde do BBC potrjujejo, da mediji niso tarča zaradi šibkosti, temveč zato, ker predstavljajo jedro zaupanja v demokraciji. RTV Slovenija je v krizah, od vojne leta 1991 do poplav 2023, ohranjala verodostojne informacije in s tem stabilnost skupnosti.

Zaupanje postaja strateški vir – ščiti pred manipulacijo, zmanjšuje polarizacijo in krepi odpornost družbe. Ko zaupanje popusti, popusti tudi obramba. Odpornost medijev zato ni le tehnično vprašanje, temveč pogoj za odpornost same demokracije. ■

YOUR ORGANIZATION COULD BE NEXT.

Welcome to Tessa Sec, where your security is our priority.

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

tessa
SEC - SKOPJE

Avtorica: Eva Čaleta / Institut za korporativne varnostne študije

INTERVJU
Matjaž Kocjančič, Reisswolf, d.o.o.*

KO IZBRIS NI DOVOLJ: VARNO UNIČENJE PODATKOV KOT DEL KORPORATIVNE ODGOVORNOSTI

Podjetja pogosto vlagajo ogromno v varnostne sisteme, šifriranje in digitalno zaščito, pozabljajo pa na zadnjo, pogosto najšibkejšo fazo življenjskega cikla podatkov tj. uničenje. Od pozabljenih diskov in odprodane računalniške opreme do odsluženih uniform ter promocijskih materialov. Vsak od teh nosilcev podatkov lahko postane varnostno tveganje z vidika zlorabe podatkov, ki jih vsebuje. O tem, zakaj varno uničenje podatkov ni zgolj tehnična naloga, temveč del širše korporativne odgovornosti in varnosti, smo se pogovarjali z Matjažem Kocjančičem iz podjetja REISSWOLF, ki se že vrsto let strokovno ukvarja s celovitim ter varnim upravljanjem dokumentacije in varnostjo podatkovnih nosilcev v njihovem celotnem življenjskem ciklu ter v vseh njihovih pojavnih oblikah.

Podjetja pogosto veliko pozornosti namenjajo zaščiti in obdelavi podatkov, manj pa njihovi končni fazi tj. uničenju. Zakaj je prav ta faza tako ključna?

Vsak podatek ima svoj življenjski cikel, ki je od nastanka, njegove uporabe, hrambe in vse do njegovega končnega uničenja. Prav zadnja faza, ko podatek postane nepotreben, pa je pogosto tista, kjer se zgodi največ napak. Podjetja pogosto domnevajo, da z izbrisom ali prenosom dokumentacije na odpad zaključijo svojo odgovornost, kar pa ne drži. Podatek obstaja, dokler ni dokazljivo in nepopravljivo uničen. V praksi to pomeni, da mora biti proces uničenja dokumentiran, sledljiv in izveden skladno z zakonodajo in standardi. Samo tako lahko podjetje zagotovi skladno uničenje podatkov in prepreči njihovo ponovno uporabo in zlorabo.

Ko govorimo o uničenju podatkov, mnogi pomislijo le na papirne dokumente. Katere druge nosilce v praksi pogosto spregledamo?

Danes podatki niso več vezani le na papir. Podatkovni nosilci so lahko različni kot npr.: trdi diski, magnetni trakovi, CD-ji, DVD-ji, USB-ključki, SD kartice, pametne kartice, GSM telefoni, pomnilniki tiskalnikov ipd. Vsi ti podatkovni nosilci so potencialni viri informacij. Zanimivo pa je, da se tveganja pojavljajo tudi tam, kjer jih najmanj pričakujemo, na primer pri uniformah, akreditacijah, ID-karticah ali promocijskih materialih, ki nosijo logotip podjetja ali osebne podatke posameznikov. Ko taki podatkovni nosilci končajo v nepravih rokah, ne gre le za zlorabo opreme kot take, temveč zlorabo podatkov, ki se nahajajo na podatkovnih nosilcih. Gre torej za širši problem, gre za resno varnostno vprašanje, vprašanje korporativne integritete in vprašanje ugleda blagovne znamke in podjetja kot celote. V preteklosti smo že videli primere, ko so rabljene uniforme ali reklamni materiali povzročili varnostne incidente, saj

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

so omogočili nepooblaščeno predstavljanje podjetja ali prodajo na črnem trgu.

Veliko uporabnikov še vedno misli, da zadostuje formatiranje diska ali brisanje datotek. Zakaj to ne drži?

Formatiranje podatkovnega nosilca ne pomeni fizičnega uničenja podatkov pomeni le odstranitev povezav do njih. V praksi je takšne podatke mogoče obnoviti z relativno enostavnimi in dostopnimi orodji. Zato se v profesionalnih okoljih uporabljajo postopki, ki temeljijo na popolnem mehanskem ali digitalnem uničenju podatkovnega nosilca, ne zgolj brisanju vsebine. Le na ta način se zagotovi, da podatki postanejo neobnovljivi.

Pri tem se pogosto omenjajo različni standardi – GDPR, ISO 27001 in tudi DIN 66399. Kako ti standardi vplivajo na prakso uničevanja podatkov? Ali se tukaj standardi kako spreminjajo ali dopolnjujejo?

Standardi določajo, kako varnostno zahtevno mora biti uničenje glede na vrsto podatkov in medija, na katerem se ti nahajajo. DIN 66399 je bil dolgo osnova za razvrščanje varnostnih stopenj pri mehanskem razrezu dokumentov in elektronskih nosilcev. Danes ta pristop nadgrajuje **ISO/IEC 21964**, ki je nastal iz DIN-a, a ga postavlja v širši, mednarodni okvir. Nekatere evropske države ta standard že uporabljajo kot osnovo za certificiranje izvajalcev uničenja, saj določa strožje zahteve glede sledljivosti, postopkov in revizijske sledi procesov uničevanja. Gre za evolucijo v smeri večje odgovornosti izvajalcev in večje transparentnosti procesa uničevanja.

Kako se varno uničenje podatkov povezuje z okoljskimi in trajnostnimi vidiki poslovanja?

Varno uničenje podatkov ne pomeni, da mora vse končati na odlagališču. Prav nasprotno. Sodobni postopki omogočajo, da se materiali po uničenju reciklirajo in ponovno uporabijo. Tako podjetje hkrati zaščiti podatke in prispeva k zmanjšanju okoljskega odtisa. V tem smislu ima odgovorno uničenje dvojno vrednost: varnostno in okolijsko. V zadnjih letih postaja to pomemben del **ESG-poročanja**, saj vlagatelji, partnerji, dobavitelji ali pa kupci vse bolj pričakujejo transparentnost tudi pri ravnanju s podatkovnimi nosilci in občutljivimi materiali. Podjetja, ki se tega zavedajo, s tem gradijo zaupanje in dokazujejo, da varnost ni samo tehnična, temveč tudi etična kategorija.

Katere so po vaših izkušnjah najpogostejše napake, ki povzročajo resne varnostne incidente?

Največ težav povzročajo neorganizirani, nesledljivi ali improvizirani postopki. Odprti zabojniki na hodnikih, neustrezni prevozi podatkovnih nosilcev od lokacije prevzema do lokacije uničenja, vreče brez varnostnih oznak ali pa odsotnost revizijske sledi postopkov in procesa uničevanja. Vse to so situacije, kjer lahko pride do tveganj nepooblaščenih dostopov do podatkovnih nosilcev in podatkov, ki se na njih nahajajo. Ko se to združi s pomanjkanjem ozaveščenosti in varnostne kulture zaposlenih, lahko hitro pride do uhajanja informacij, kraje podatkov, kraje identitete in posredno negativnih objav v medijih. Rešitev je v standardiziranih postopkih in sodelovanju s certificiranimi izvajalci, ki zagotavljajo popolno sledljivost od trenutka prevzema podatkovnega nosilca do njegovega trajnega uničenja ter izdaje potrdila o varnem in sledljivem uničenju. To podjetju omogoča dokazljivo skladnost in varnost, obenem pa zmanjšuje tveganja, povezana z zlorabo podatkov.

Kako vidite prihodnji razvoj tega področja? Bo uničenje podatkov postalo še bolj avtomatizirano in regulirano?

Vsekakor. Digitalizacija bo prinesla še večjo sledljivost, saj bo vsak korak procesa elektronsko zabeležen, od prevzema do reciklaže (revizijska sled). Standardi se bodo še naprej razvijali v smeri povezovanja varnosti, okoljske odgovornosti in skladnosti. Podjetja bodo morala tudi procese uničevanja obravnavati kot integralni del upravljanja s podatki, ne kot obrobno tehnično nalogo. Največjo prednost pa bodo imela tista, ki bodo združila naslednje elemente: varnost, transparentnost, skladnost in trajnost. To je prihodnost korporativne varnosti in odgovornega ravnanja s podatki v vseh njihovih pojavnih oblikah in v vseh fazah njihovega življenjskega cikla.

Če bi morali podjetjem dati en sam nasvet glede ravnanja s podatki, ne glede na njihovo obliko – kaj bi izpostavili kot najpomembnejše?

Podatek ima vrednost le, dokler je pod nadzorom. Ko izgubimo sled nad njim zaradi slabe hrambe, neustreznega uničenja ali nepozornosti zaposlenih le-ta postane tveganje. Zato naj podjetja vsak korak življenjskega cikla podatka obravnavajo z enako resnostjo. Varnost ni projekt, temveč odgovornost, ki povezuje tehnologijo, procese in ljudi. ■

Foto: arhiv Reisswolf, d.o.o.

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

ZAKLJUČEK EU PROJEKTA SUNRISE

Pandemija COVID-19 je izpostavila pomen organizacijske odpornosti in sposobnosti zagotavljanja nemotenega delovanja ključnih poslovnih procesov tudi v najzahtevnejših trenutkih. Posledično potreba po boljšem sodelovanju in skupnem duhu pri iskanju rešitev še nikoli ni bila tako očitna in nujna. Vendar pa je zaradi pomanjkanja virov, zlasti v začetnem obdobju zadnje pandemije, namesto sodelovanja med različnimi kritičnimi infrastrukturami (KI) ter med državami (celo regijami in lokalnimi skupnostmi) prišlo celo do konkurence. EU projekt SUNRISE[1] je omogočil preseganje navedenega ter aktivno sodelovanje nacionalnih in evropskih KI – pri tem jim je pomagal in jih podprl, da so bolje pripravljene in opremljene za ustrezno oceno in skupno obvladovanje prihodnjih tveganj, ki jih povzročajo pandemije.

Uvod

Ker so sistemi in operaterji KI ključni za delovanje družbe in gospodarstva ter vitalni pri podpiranju vsakodnevnih življenj, kot tudi pri zagotavljanju nacionalne in mednarodne varnosti, je še posebej pomembno, da so cilji takšnih projektov usmerjeni v združevanje strokovnega znanja, izboljševanje učinkovitosti ter izkoriščanje vzajemnih prednosti. Za ohranjanje odpornosti in stabilnosti KI so potrebni novi pristopi in rešitve, ki ne bodo zgolj izboljšali zaščite fizičnih infrastrukturnih komponent, temveč bodo upoštevali tudi družbene vidike, vključno z državljani, delovno silo in oblikovalci politik.

Motnje v teh sistemih lahko imajo resne posledice, kot so izguba življenj, gospodarske izgube ter zmanjšana stopnja varnosti. Zato je izjemno pomembno vedno znova poudariti, da mora biti KI ustrezno zaščitena, odporna ter pravilno vzdrževana v skladu z najvišjimi standardi.

Ozadje in poslanstvo projekta

Kompleksnost in dinamika delovanja človeške družbe in tehničnih sistemov zahteva nenehno iskanje novih načinov uvajanja najnovejših praks in novih tehnoloških rešitev za operativno delovanje zahtevnih tehnoloških in družbenih sistemov, predvsem tistih, ki upravljajo KI, kar omogoča boljše situacijsko dojemanje in uvajanje sistematičnih pristopov za obvladovanje tveganj.

Pandemija COVID-19 je glede razsežnosti in posledic presenetila ves svet. Povzročila je negotovost, prepletanje resničnih in lažnih informacij, omejevanje gibanja in s tem poseg v temeljne človekove pravice in svoboščine ter družbene nemire v času čakanja družbe na izboljšanje razmer. Reševanje tovrstnih kriznih situacij zahteva kompleksen pristop k njihovemu reševanju, angažiranje vseh družbenih sil, veliko materialnih, finančnih in človeških virov. Organizacije KI temeljijo na soodvisnosti in so medsebojno močno povezane, kar ustvarja zahteve po celostnem upravljavskem pristopu v normalnih in še bolj v kriznih situacijah, kot je pandemija. Zagotoviti je treba ustrezno raven varnosti in usklajenosti med organizacijo družbe in gospodarskim razvojem ter doseči optimalno ravnotežje med tveganjem, stroški in zahtevami glede varnosti in odpornosti. Raziskave in nastajajoče rešitve se osredotočajo na zaščito posameznih KI, čeprav so medsebojni odnosi med posameznimi sektorji kritične infrastrukture postali zelo kompleksni.

Dodaten izziv je nova doba realnosti, v kateri smo se znašli. Digitalne tehnologije pomagajo ljudem razumeti in preoblikovati svoje okolje. Tehnološka infrastruktura je postala bolj zapletena in povezana, njena gostota in kompleksnost pa prinašata dodatna tveganja. Eden od njih je, da se manjše začetne napake zlijejo v veliko večje in bolj škodljive z nepredvidljivimi posledicami. Drugo tveganje je, da so zapleteni, tesno povezani sistemi lahko vabljive tarče za kriminalce in druge dejavnosti, ki lahko povzročijo okvaro ali odpoved sistema. Med varnostnimi izzivi prihodnosti velja izpostaviti tudi nedvomno tveganje, povezano s kadrovskim potencialom v organizacijah kritične infrastrukture. Nakopičen stres in potlačene travma-

[1] https://sunrise-europe.eu/

*avtor je član Slovenskega združenja korporativne varnosti

tične izkušnje iz obdobja pandemije se lahko stopnjujejo, ko se družba poskuša naglo vrniti v približno realnost, ki smo jo poznali pred pandemijo. Poleg kibernetskih tveganj bodo nestrpnost, konflikti in nasilje na delovnem mestu postali varnostni dejavniki, ki jim bo treba v prihodnosti še posebej posvetiti pozornost. Pospešena digitalizacija družbe pa kibernetska tveganja že dlje časa postavlja na vrh varnostnih izzivov, ki jim bo morala korporativna varnost posvetiti vso potrebno pozornost. Evropske družbe in gospodarstva so odvisni od zanesljivega zagotavljanja vitalnih storitev, zlasti v času pandemije. Ker se ključne storitve zagotavljajo prek KI, to pomeni, da morajo biti evropski KI odporni, tj. sposobni se prilagajati nenehno spreminjajočim se tveganjem in hitro okrevati po pričakovanih ali nepričakovanih motnjah.

Rezultati projekta ter aktivno sodelovanje nacionalnih in evropskih kritičnih infrastruktur

Med vitalnimi rezultati projekta SUNRISE, zlasti v delovnem paketu 1 (Work package 1 - WP1), ki ga je vodil in koordiniral Institut za korporativne varnostne študije (ICS), velja izpostaviti implementiran okvir sodelovanja za izmenjavo znanja in aktivno sodelovanje evropskih KI – v tem delovnem paketu je bilo vključenih vseh 41 partnerjev projekta SUNRISE – z namenom povečanja stopnje statusa odpornosti delovanja KI. Pandemija COVID-19 je bila zlasti v najhujšem poteku globalna izkušnja, med katerim so vsaka država in vsak sektor izvajali posebne protiukrepe, namenjene ohranjanju zdravja svojih državljanov in neprekinjenosti zagotavljanja osnovnih storitev. KI so imele pri tem ključno vlogo na evropski, nacionalni in lokalni ravni. Izredne razmere zaradi COVID-19 so organe in operaterje KI prisilile k izvajanju in hitremu sprejetju zdravstvenih protokolov in operativnih modelov v skladu z nacionalnimi predpisi. V projektu SUNRISE je bila implementirana poglobljen analiza in razvoj strategije, tehničnih rešitev ter orodij, ki so aktualno na voljo; operaterji KI so se tekom projekta imeli možnost primerjati z drugimi ter izmenjevati izkušnje in najboljše prakse.

V skladu z načrtom in cilji projekta SUNRISE so bile v organizaciji ICS Ljubljana v tri letnem poteku projekta uspešno in produktivno implementirane štiri nacionalne delavnice. Na delavnicah so sodelovali vsi slovenski projektni partnerji s številno udeležbo - poleg ICS Ljubljana kot vodje delavnic in XLAB kot ko-moderatorjev delavnic še Ministrstvo za infrastrukturo, UKC Ljubljana, Plinovodi, ELES, Slovenske železnice, Slovenske železnice-infrastruktura, Prometni inštitut in Telekom Slovenije. Namen produktivnih razprav je bil zbiranje izkušenj, prepoznavanje pomanjkljivosti, pričakovanj in dobrih praks za izboljšanje odpornosti organizacij KI in vitalnih storitev v času pandemije. Poudarek je bil na formiranju odgovorov, kako lahko podpremo druge in kako lahko bolje sodelujemo v krizah, povezanih s pandemičnimi razmerami. Poseben poudarek je bil na razumevanju javno-zasebnega partnerstva ter kaj je že v operativnem okolju, kaj manjka in kako lahko dosežemo strateške in sistemske izboljšave. Zbrane informacije, izkušnje in dobre prakse so podprle nadaljevanje razprav, analiz in raziskav EU projekta SUNRISE v nacionalnem in mednarodnem okolju ter v znatni meri prispevale k rezultatom projekta.

V teku projekta so bile tovrstne nacionalne delavnice projektnih partnerjev izvedene tudi v Italiji in Španiji. Zatem smo skupno predstavili in opredelili rezultate - skupne izzive in dobre prakse, ki so bile ugotovljene v treh državah, kjer so potekale delavnice. V vseh navedenih državah je obstajala splošna težava pri pridobivanju zanesljivih informacij z najvišjih ravni. To je bilo periodično povezano s pogostim in pretiranim spreminjanjem strateških odločitev. V vseh treh državah so se norme in zakoni včasih spreminjali čez noč ali čez vikend, kar je KI prisililo, da hitro analizirajo izvedene spremembe in nato prilagodijo svoje politike ter ukrepe. V nekaterih državah je bilo to vprašanje dodatno problematično zaradi pomanjkanja nacionalnih načrtov za centralizacijo in koordinacijo kriznega upravljanja, kadar je to potrebno, ter za boljše usklajevanje in komuniciranje z regionalnimi/lokalnimi vladami. Za nekatere operaterje KI je bilo problematično tudi pomanjkanje in neustreznost načrtov za soočanje s pandemijo. Nekatere organi-

zacije, večinoma največje/mednarodne, so imele pripravljene obsežne načrte neprekinjenega poslovanja, vendar praktično nobena ni bila pripravljena soočiti se z danim obsegom situacije. Zato so se mnogi soočili s pomanjkanjem predvidevanja scenarija pandemije. To je na primer povzročilo, da kritični procesi in bistveni delavci niso bili identificirani dovolj hitro. Poleg tega je bila vedno, ko je bilo kritično osebje okuženo in ni bilo več na voljo, njihova zamenjava težavna, deloma zaradi pomanjkanja strokovne razpoložljivosti ali premalo usposobljenega osebja. Na nekaterih področjih strokovnjaki, čeprav so bili na voljo (npr. zdravstvo), niso smeli delati, ker niso bili ustrezno akreditirani in je postopek akreditacije zastal. Ena od rešitev med pandemijo je bilo delo na daljavo, ko je bilo to mogoče, vendar se je tudi ta rešitev soočila z novimi izzivi. Na primer, delo na daljavo je bilo težko upravljati (in je ponekod še vedno), saj vodstvene ekipe niso bile usposobljene/pripravljene nanj in ni bilo vzpostavljenih postopkov. Poleg tega je primanjkovalo opreme (npr. prenosnikov) in infrastrukture (npr. strežnikov) za podporo delu na daljavo, razen za zelo velike organizacije in organe. Poleg tega, da organizacije niso bile pripravljene na delo na daljavo, tudi njihovi načrti kibernetske varnosti niso bili pripravljeni, zato so bile politike kibernetske varnosti omejene, kibernetska tveganja pa so se povečala zaradi uporabe neustrezne opreme in praks.

Vendar pa je bilo sprejetih tudi veliko dobrih praks. Na primer, KI so imenovale odbore za odločanje (za nujne primere, krizno načrtovanje). Postavili so tudi izolirane operativne in rezervne ekipe. Izpostavljeno je bilo, da javno-zasebno in medsektorsko komunikacijo ter sodelovanje ob tovrstnih krizah večkrat uspešno podpirajo osebna poznanstva (kot pa ustaljeni protokoli).

Na podlagi navedenih ugotovitev implementiranih nacionalnih delavnic smo na treh implementiranih evropskih delavnicah in periodičnih sestankih Generalne skupščine SUNRISE podrobneje analizirali področje nacionalnega kot tudi področje meddržavnega sodelovanja s ciljem nadaljnjega iskanja ustreznih rešitev in dobrih praks ob upoštevanju relevantnih evropskih direktiv.

Vse to je rezultiralo v pripravljeni strategiji projekta SUNRISE, ki vključno s tehničnimi rešitvami in orodji ustrezno naslavlja prihajajoče izzive naslednjih pandemij ter ob njeni uporabi omogoča pravočasno pripravljenost in boljšo odpornost nacionalne in evropske KI.

Zaključek

V projektu SUNRISE je bil uporabljen multidisciplinaren pristop, ki je rezultiral, da so se pri načrtovanju ukrepov v času pandemije upoštevale tako kratkoročne kot dolgoročne spremembe v naših družbah. Glavni cilji projekta so bili doseženi in sicer: (1) Okrepljeno aktivno sodelovanje KI v Evropi za izmenjavo najboljših praks in združitev kapacitet v pandemijah. (2) Opredeljene ključne storitve in kritične storitve, specifične za pandemijo, njihove soodvisnosti, tveganja, kaskadni učinki in učinkoviti ukrepi za njihovo obravnavo na evropski ravni. (3) Razvita strategija in orodja, ki zagotavljajo razpoložljivost, zanesljivost in kontinuiteto kritičnih storitev, specifičnih za pandemijo v Evropi. (4) Pilotno testiranje rezultatov v operativnih okoljih evropskih KI ob hkratnem odpravljanju nekaterih največjih težav, ki jih je razkrila pandemija COVID-19. (5) Usklajen pristop po vsej Evropi, s ciljem zagotoviti enotno fronto in odpornost naših KI v pandemijah. Pri vsem našem delu smo skrbno upoštevali pravne, etične, družbene, gospodarske in podnebne vidike ter zagotovili, da naši rezultati niso naslovili le potreb KI, temveč tudi potrebe naše družbe. ■

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

SUNRISE

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

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

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

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

ICS INSTITUT ZA KORPORATIVNE VARNOSTNE ŠTUDIJE

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

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

ISO 27001

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

BUREAU VERITAS

DPO

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

17. mednarodna konferenca

Dnevi korporativne varnosti

PODELITEV NAGRAD SLOVENIAN GRAND SECURITY AWARD

BRDO PRI KRANJU, 18. - 19. MAJ 2026

DODAJTE DELČEK ZNANJA V MOZAIK VAŠEGA USPEHA!

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

WWW.ICS-INSTITUT.SI