ISSN 2820-6029

PODJETNA VARNOST

ZA vrhunsko in odgovorno podjetništvo

Št. 57 | letnik 9 | Junij 2026 www.podjetnaslovenija.si

Kibernetski spopad 2030:
Predator vs. Terminator

Etični heker **Milan Gabor** med drugim o tem, kakšni bodo kibernetski spopadi že v bližnji prihodnosti.

62

OBRAMBNA VARNOST

Bi kupili lastno zaklonišče?

Kdo v Sloveniji izdeluje hibridne pametne zgradbe in zaklonišča za varno prihodnost?

48

UF PRO

PART OF MEHLER SYSTEMS

LIMITS ARE A MINDSET

WWW.UFPRO.COM

Kibernetska varnost

Finance & varnost

Kibernetski napadi

Obrambna industrija

Podjetja za varovanje

PODJETNA SLOVENIJA

Št. 57 | Letnik 9 | Junij 2026

Izdajatelj:
Izziv X, d. o. o.
Gorenjesavska cesta 13b
4000 Kranj
info@podjetnaslovenija.si

Uredništvo

Odgovorni urednik:
Goran Novković
urednistvo@podjetnaslovenija.si

Izvršna urednica:
Maja Virant

Zasnova:
Nenad Bebić

Oblikovanje in prelom:
Mitja Pogorevc, Spotnet d.o.o.

Lektoriranje:
Nina Drašler

Trženje oglasnega prostora:
trzenje@podjetnaslovenija.si
01 5130 832
marketing@podjetnaslovenija.si
01 5130 824

Fotografija na naslovnici:
Barbara Reya & Ai

Podjetna Slovenija je namenjena ambicioznim, odgovornim in vrhunskim slovenskim podjetnikom, starejšim in mlajšim, malim, srednjim in tudi največjim podjetjem ter vsem drugim podpornikom vrednote podjetnosti. Vsem, ki po svojih močeh podpirajo podjetno Slovenijo.

ISSN 2820-6029

Prevod oglasa na str. 2 in 3:
Meje so stvar miselnosti

Partnerji Podjetne Slovenije

Partnerji Podjetne Slovenije so organizacije, s katerimi sodelujemo pri načrtovanju vsebin. Za sodelovanje se jim iskreno zahvaljujemo.

SVET PREDATORJEV IN TERMINATORJEV

Goran Novković

Milan Gabor, etični heker: *»Po mojem mnenju se bo leta 2030 napadalni agent umetne inteligence kibernetsko boril z obrambnim agentom umetne inteligence.«* Tako bo v vojni in v miru. Poleg agentov umetne inteligence (UI) bodo v realnem svetu namesto rojev kobilic ali čebel na sceni roji dronov.

To ni fikcija, pač pa realnost, o kateri lahko veliko preberete v tokratni Podjetni varnosti, drugi posebni izdaji Podjetne Slovenije na temo različnih oblik napadov in varnosti.

Svet se spreminja hitro. Poleg zgoraj omenjenega so značilnosti sedanjega trenutka in bližnje prihodnosti še nekatere novosti:

1. Obrambno-vojaško področje postaja vse bolj podobno običajnemu biznisu: vsi iščejo poceni in učinkovito, ne pa glomazno in drago. Iščejo drone namesto tankov.

2. Kriminalno ozemlje je organizirano kot podjetje. Tam so vodje skupine, pisci kod, denarne mule, ki skrbijo za pranje denarja …

Zmagovalec spopadov v prihodnje ne bo več tisti z najdražjo opremo, temveč tisti, ki najbolje razume omejitve tehnologije in jo zna pametno kombinirati s človeškim odločanjem. Tisti, ki uporablja cenovno dostopne, množične in operativno odporne rešitve, lahko pogosto nevtralizira bistveno dražjo tehnologijo.

Kako zelo hitro se spreminja svet, kažejo naslednji podatki:

1. Število kibernetskih incidentov se je lani povečalo za 35 odstotkov. Glavni razlog je hitrejša priprava sporočil ob pomoči UI, brez očitnih slovničnih in slogovnih napak.

2. Napadalci so izvedli približno 36.000 zlonamernih pregledov na sekundo, kar je 16,7-odstotno povečanje v primerjavi z letom 2024.

3. Ukradena sredstva se po izvedeni transakciji skoraj takoj razpršijo prek mreže mednarodnih denarnih mul.

Bodite pozorni na kibernetsko varnost. A ne pozabite na finančno varnost!

Na obrambnem in kibernetskem področju lahko vsak dan spremljamo konkretne primere napadov v novicah na svojih telefonih, računalnikih, TV in radijskih sprejemnikih – vse v realnem času. A to za podjetja ni največja nevarnost.

Največjih finančnih izgub namreč ne povzročajo hekerski vdori, temveč so to še vedno vsakodnevni poslovni procesi. Finančno izčrpavanje podjetij je danes redko videti kot spektakularen napad; pogosteje gre za tihe, postopne odlive, skrite v legitimnih procesih. Slovenska policija in Združenje bank Slovenije redno beležita primere korporativnih prevar, kjer posamezna oškodovanja podjetij dosegajo – več sto tisoč ali celo milijone evrov!

Paziti moramo na splet različnih varnosti: obrambne, kibernetske, finančne, fizične, tehnične, požarne, potresne … Informacije in nasvete o tem najdete v reviji, ki jo imate v rokah.

POSTAVILI SO SE OB BOK NAJBOLJŠIM

Guardiaris se uspešno kosa z največjimi na svetu v obrambni industriji, na nekaterih področjih je celo vodilen. Razloge za njihovo rast in uspešnost nam je zaupal direktor Primož Peterca, ki je predstavil tudi njihove najbolj obetavne projekte.

Lansko leto smo se na istem mestu pogovarjali o podjetju Guardiaris in dejavnikih, katerih posledica je vaša hitra rast.

Kako ocenjujete stanje danes in katere tehnološke preskoke ter nove usmeritve podjetja ste dosegli v enem letu?

Guardiaris v enem letu definitivno ni več tisto, kar je bil lani (smeh). Predvsem pa ni več eno podjetje. Postal je sicer največji del skupine podjetij, tako ali drugače, povezanih v manjši ekosistem, kjer sinergija ljudi različnih znanj z neizmerno motivacijo razvija v Sloveniji in pošilja v svet nove in nove produkte. V ožji skupini so podjetja Carboteh, Cerasynth, Panna Plus, naše sodelovanje pa se je tudi s pomočjo razvojnih programov slovenske vojske (SV) razširilo do podjetij RTC Maribor, Keko oprema, SK, d. o. o. in še nekaj drugih. Kot skupina delamo tudi na popolnoma novih proizvodih, ki bodo predstavljali del rešitve prihodnjih konfliktov in Slovenijo postavile ob bok velikim. To je družina radarjev za identifikacijo dronov, proizvodnja elektrike iz vodika in še nekaj briljantnih rešitev za izzive, ki prihajajo.

»Kot skupina delamo tudi na popolnoma novih proizvodih, ki bodo predstavljali del rešitve prihodnjih konfliktov in Slovenijo postavili ob bok velikim,« pravi Aleš Perko, direktor Cerasyntha.

Ko ste lani omenili idejo o prvih začetkih razvoja radarja za detekcijo dronov in energijske kocke, nas je zanimalo, kako je možno, da lahko oba sicer tako različna projekta temeljita na podobni in čisto slovenski tehnologiji?

Mogoče se res sliši enostavno, ampak vsak od projektov je izredno kompleksen in kot tak sestavljen iz več podsistemov in modulov. Res pa je, da je tehnologija na nekaterih modulih pri obeh projektih izvorno enaka in tudi med proizvodnjo zelo sorodna. Tukaj govorimo o res posebnih keramičnih plasteh, katerih razvoj in izdelava je plod slovenskega znanja. V tem trenutku v Evropi samo v Sloveniji obvladamo fundamentalno tehnologijo takih nanosov. Upam si trditi, da nobena evropska korporacija ni na tej ravni oziroma jih dobavljajo iz Kitajske.

Ali lahko razložite malo bolj podrobno, kaj bo dejansko narejeno v Sloveniji in kaj boste kupovali od dobaviteljev ter ali bodo vključeni tudi proizvodi, narejeni na Kitajskem?

Od mnogoterih podsistemov in modulov bodo vsi narejeni pri nas. Gre tudi za evropsko direktivo na obrambnem področju, ki nam je s tem dala celo neko prednost. Vsak tak podsistem je mehanski ter kombinacija mehanike in kemije ali elektronike in programske opreme. Zato je veliko priložnosti za vključitev slovenskega znanja, razvoja, izdelave, integracije in testov. Razen pri nas razvitih keramičnih materialov so komponente od dobaviteljev, ki jih kupujemo na evropskem trgu, ki imajo certificirane logistične verige, kar je ključno, da se prepreči vgradnja ponaredkov.

Kje točno sta projekta in kako ste se jih zastavili v razvojnem, proizvodnem in komercialnem smislu? Splošno je namreč znano, da so tokovi v obrambni industriji obrnjeni v smeri velikih korporacij in da podjetje iz Slovenije z novo tehnologijo verjetno nima referenc, ki bi zadostile prodoru na zahtevne in velike trge.

Oba projekta sta prešla fazo minimalnega produkta, prototipa, tako da smo v integracijskem delu podsistemov in testiranjih na terenu. Pri velikih projektih je največja dodana vrednost povezovanje partnerskih podjetij in akademskih institucij, saj tako lahko dosežemo kritično maso možganov in proizvodnih zmogljivosti. In ko to pogledamo kot celoto, se lahko pohvalimo s primernimi referencami. Za uspeh projektov proti uveljavljenim igralcem je pomemben element tudi svež pristop in možnost razvoja iz skoraj čistega koncepta, ki ni obremenjen z zgodovino in kompatibilnostmi. Naša največja prednost pa je hitrost. Sorazmerno majhen ekosistem, ki obvladuje tehnologije in je finančno podkrepljen, z lahkoto prehiteva vse velike in okorne sisteme.

Mikro dopler radar zaznava vrtinčenje elis dronov in ne drona kot objekta. S tem novim pristopom so drastično izboljšali razdaljo vidnosti drona.

Kot vidim, v bistvu Guardiaris postaja korporacija, saj ste aktivno vključeni v popolnoma različne procese, ki rezultirajo v produktih, za katere ne vidimo enakih prodajnih poti.

Ali obstajajo še kakšna podjetja v Sloveniji ali v tujini, s katerimi ste vključeni v razvojne, oziroma v komercialne procese in kakšne so vaše vloge v teh povezavah?

Naš najmočnejši prodajni adut, ne boste verjeli, je podjetje Panna Plus, ki že 20 let na celotnem področju nekdanje države zastopa svetovne korporacije na področju obrambe. Ekipa, ki jo sestavlja 35 strokovnjakov, je tako kakovostno vpeta v mednarodno sodelovanje, da ji tuje korporacije popolnoma zaupajo, ko predlagajo, da namesto tujega umestijo v svoje projekte slovenski produkt. Tako smo čez celotno zgodovino tudi postavili na noge Guardiaris, ki je letos prvo leto že samostojen. Na isti način tudi financiramo vse ostale projekte. Dejstvo je, da je obrambna industrija še vedno zaprta in da so novinci, sploh iz malih držav, drugače skoraj brez možnosti uspeha. Res pa je tudi, da brez podpore slovenske vojske ne bi imeli možnosti pridobitve financiranja, znanja in testiranja, kar nam posledično omogoča, da se hitro bližamo svetovnemu vrhu.

Kje vidite Guardiaris v naslednjih letih in kako trenutna situacija v svetu vpliva na razvoj podjetja? Kljub temu da vaši podatki še niso bili javno objavljeni, delate dobro.

Tako Guardiaris kot Panna Plus sta srednje veliki podjetji in zato zavezani k reviziji. Rezultati bodo objavljeni šele v drugem delu leta. Je pa dejstvo, da smo uspešni. Kot skupina smo precej zrasli. Guardiaris je podvojil svoj promet glede na lansko leto. Ni pa to posledica dogodkov okoli nas, ampak trdega dela in vlaganj zadnjih 20 let in dejstva, da je 90 % našega prometa ustvarjeno v tujini. Svet je res velik, in dokler si tega ne vtisnemo v gen, smo pač omejeni na domače, velikokrat nepredvidljivo okolje. Seveda pa se ta rast in na papirju prikazani dobički ne vidijo v likvidnosti. Večja rast zahteva tudi večja vlaganje v razvoj, ljudi in proizvodnjo, ki pa se zadnje čase ne cenijo. A po nekaj temačnih letih se je vsaj začel razvijati bančni trg, ki ga prej za našo dejavnost praktično ni bilo, in lahko pohvalim tako državno SID kot privatni Gorenjski banki (GB) in Unicredit banki, ki nam res stojijo ob strani.

Kako vidite trenutno politično situacijo v Sloveniji in kako lahko vpliva na vaše poslovanje?

Predvsem ni dobro, da se pogled na dolgoročno vizijo razvoja države menja kot noč in dan. Je pa kot kaže to del naše mentalitete in mi je žal, saj bi bili danes res lahko že Švica. Žal mi je tudi, ko ekstremne skupine mladih fantov in deklet redno mažejo fasade stavb, v katerih delujemo, in jih onečaščajo z neprimernimi grafiti in letaki. Mogoče se bo slišalo smešno, ampak če v svetu primerjamo število smrti, povzročenih z alkoholom, in tistimi z vojnami, je to razmerje skoraj 20:1. In verjetno več gorja in posledic nastane okoli družin alkoholikov kot v vseh vojnah skupaj. Razlika je le, da se to dogaja skrito za štirimi stenami in ne na televiziji. Čas je, da bi te isti mladi ljudje nehali iskati le politične točke, ampak začeli ustvarjati nov svet na drugačnih postulatih in z drugimi mehanizmi. Naša napaka pri vzgoji mladine, vsaj kar se zgodovine tiče, pa je, da danes mladi ne razumejo, da prav revolucije z nasilnim rušenjem obstoječega reda sprožijo vakuum novega reda, v katerem nastane prostor za nove vojne. In kot je davno rekel Nikola Tesla, je boj proti nevednosti veličastnejši od katerekoli zmage v vojni.

Trg UI v obrambi naj bi do 2035 zrasel na skoraj 30–35 milijard USD.

Grafika: Spotnet

NOVA LOGIKA VOJNE: HITROST, KODA IN KONEC KLASIČNE MOČI

- Kako droni in kibernetski napadi spreminjajo vojskovanje?
- Ali bo vojne odločala tehnologija ali prilagodljivost?
- Zakaj so napredni sistemi v vojni lahko tudi šibkost?

Maja Virant

Razmeroma blizu Slovenije potekata dve veliki vojni, ena v Evropi, druga na Bližnjem vzhodu. Čeprav sta geografsko in operativno različni, obe kažeta, kako hitro se spreminja vojskovanje.

V Ukrajini se vojna vse bolj odvija z droni, elektronskim motenjem in v pogojih, kjer komunikacije pogosto ne delujejo zanesljivo. Na Bližnjem vzhodu pa vidimo kombinacijo naprednih raket, kibernetskih napadov in natančnih udarov, ki jih je težko pravočasno zaznati ali ustaviti.

Vojn ne odločajo več klasične platforme, kot so tanki in letala, temveč vse bolj programska oprema, avtonomni sistemi in hitrost odločanja v realnem času.

Tehnologija napreduje zelo hitro, hkrati pa kaže tudi svoje omejitve. Do leta 2035 bodo imeli strateško prednost tisti, ki bodo znali tehnologijo uporabljati pametno in jo združiti z ljudmi. Torej tisti, ki ne bodo zaupali le strojem, navaja ameriški raziskovalno-strateški inštitut Atlantski svet v poročilu Prihodnost vojskovanja 2025–2030.

A. Ključne tehnološke novosti 2030–2035

Do leta 2035 bodo bojišča zaznamovale naslednje ključne tehnološke smernice:

Vojn ne bodo več odločali tanki in letala, temveč algoritmi, roji avtonomnih sistemov, nadzor nad elektromagnetnim spektrom in hitrost odločanja.

1. Avtonomni roji in brezpilotni sistemi (UxV)

Roji dronov (v zraku, na kopnem in pod vodo) bodo delovali samostojno ali v koordinaciji z umetno inteligenco. Omogočali bodo množično izvidništvo, napade, elektronsko vojskovanje in samoobnavljanje (če eden odpove, drugi prevzame nalogo), navaja arXiv. Pričakovati je prehod od daljinsko vodenih k visoko avtonomnim sistemom.

2. Umetna inteligenca in hitro odločanje

Umetna inteligenca (UI) bo drastično pospešila zanko OODA, to je opazuj–orientiraj–odloči–deluj, napoveduje Financial News Media.

Dodaja, da se bo uporabljala za analizo ogromnih količin podatkov, predvidevanje gibov nasprotnika, avtonomno ciljanje in optimizacijo logistike. Trg UI v obrambi naj bi do 2035 zrasel na skoraj 30–35 milijard ameriških dolarjev.

3. Hipersonično orožje in usmerjena energija

Hipersonične rakete (s hitrostjo nad 5 machov, torej petkrat večjo od hitrosti zvoka) bodo omogočale hitre udare, ki jih je težko prestreči.

Sistemi usmerjene energije (visokoenergijski laserji in mikrovalovi) pa bodo postali relativno poceni in učinkovita rešitev za obrambo pred droni, raketami in roji, navaja Kongresna raziskovalna služba v poročilu Hipersonično orožje: Ozadje in vprašanja za Kongres.

4. Večdomenska operacija (MDO)

Prihodnje bojevanje bo potekalo hkrati na vseh področjih: v zraku, na kopnem, na morju, v kibernetskem prostoru in vesolju. Ključna prednost bo sposobnost, da vsi sistemi, senzorji in enote delujejo usklajeno ter si v realnem času izmenjujejo podatke.

Prav hitra povezanost med različnimi deli vojske bo odločala o premoči, ugotavlja Inštitut za sodobno vojskovanje pri ameriški vojaški akademiji West Point v publikaciji Kdo izvaja večdomenske operacije?.

5. Elektronsko vojskovanje in kibernetika

Nadzor nad elektromagnetnim spektrom bo ena ključnih prednosti prihodnjih vojsk. Motenje komunikacij, zavajanje signalov GPS in kibernetski napadi bodo nasprotnika lahko oslepili in zmedli še pred začetkom klasičnega spopada. Vse pogosteje bodo takšne zmogljivosti vgrajene neposredno v drone in druge avtonomne sisteme.

Te tehnologije ne bodo delovale vsaka zase, temveč bodo tesno povezane in usklajene. Prav ta povezanost bo bistveno povečala hitrost odločanja ter spremenila način, kako bodo potekali prihodnji konflikti, poudarja ameriško obrambno ministrstvo v dokumentu Strategija premoči v elektromagnetnem spektru iz leta 2020.

B. Novi načini bojevanja

Prihodnje vojne bodo vse manj podobne klasičnim spopadom velikih armad in vse bolj hibridne, neprekinjene ter pogosto vodene pod pragom formalno razglašenega konflikta.

1. Hibridni spopadi

Meja med vojno in mirom se briše: države se že danes med seboj spopadajo s kibernetskimi napadi, informacijskimi operacijami, elektronskim motenjem, gospodarskim pritiskom in prikritimi tehnološkimi sabotažami, brez uradne vojne napovedi, navaja raziskava Ponovni premislek o poveljevanju in nadzoru Univerze Cornell. Takšne oblike konflikta postajajo novo normalno stanje globalne varnosti.

Poleg tega sodobna bojišča dokazujejo, da prihodnosti ne bodo več določale posamezne drage in kompleksne platforme, denimo tanki, letalonosilke ali lovci pete generacije, temveč množice poceni, hitro proizvedenih in programsko prilagodljivih avtonomnih sistemov.

Konflikti v Ukrajini in na Bližnjem vzhodu potrjujejo, da lahko roji cenovno dostopnih dronov nasprotniku povzročijo nesorazmerno visoke stroške ter izničijo prednosti tehnološko superiornih, a bistveno dražjih sistemov.

Zmagovalec ne bo tisti z najdražjo opremo, temveč tisti, ki najbolje razume omejitve tehnologije in jo zna pametno kombinirati s človeškim odločanjem.

Nasprotnik, ki uporablja cenovno dostopne, množične in operativno odporne rešitve, lahko pogosto nevtralizira bistveno dražjo tehnologijo.

2. Cenejše je učinkovitejše

V ospredje stopa koncept »cenovno vzdržne mase« (affordable mass), kjer zmaga ne pripada nujno tehnološko najnaprednejšemu akterju, temveč tistemu, ki lahko hitreje proizvaja, prilagaja in nadomešča izgubljene zmogljivosti, ugotavlja McKinsey & Company v članku Prihodnje obrambne tehnologije: večdomenske tehnološke plasti za gradnjo cenovno vzdržne množične zmogljivosti.

3. Hitro uvajanje novosti

Ključna konkurenčna prednost prihodnjih vojsk bo zato predvsem hitrost prilagajanja. Zmagovale bodo sile, ki bodo sposobne v realnem času spreminjati programsko opremo, prilagajati taktiko, integrirati UI ter uvajati nove sisteme hitreje, kot jih nasprotnik uspe analizirati in nevtralizirati, pojasnjuje globe Newswire v članku Prihodnost avtonomnega bojevanja je zapisana v kodi. Programska oprema tako postaja enako pomembna kot strojna oprema, razvojni cikel pa pomembnejši od same velikosti arzenala.

4. Navigacija brez GPS signala

Poseben izziv bo delovanje v tako imenovanem degradiranem okolju, kjer bodo satelitska navigacija, komunikacijska omrežja in klasični sistemi poveljevanja pogosto moteni ali popolnoma nedosegljivi, poudarja AINewsWire v članku Konec zanesljivosti GPS-ja spreminja sodobno vojaško strategijo (2026).

V takšnem prostoru bodo odločali sistemi, ki lahko delujejo avtonomno, navigirajo brez GPS signala, sprejemajo odločitve z omejenimi podatki in ohranjajo operativno učinkovitost tudi v pogojih intenzivnega elektronskega bojevanja. Prav odpornost na izgubo povezljivosti postaja ena ključnih lastnosti prihodnjih obrambnih tehnologij.

Poseben izziv bo delovanje v tako imenovanem degradiranem okolju, kjer bodo satelitska navigacija, komunikacijska omrežja in klasični sistemi poveljevanja moteni ali nedosegljivi.

C. Ranljivosti pametnih tehnologij

Vendar tehnološka superiornost sama po sebi ne zagotavlja več vojaške prednosti. Izkušnje iz Ukrajine in z Bližnjega vzhoda jasno kažejo, da so tudi najnaprednejši sistemi pogosto presenetljivo ranljivi, kadar delujejo v okolju intenzivnega elektronskega bojevanja, piše André Luhmer v članku Elektronsko vojskovanje – ključne lekcije iz Ukrajine.

1. Kdo nadzira elektromagnetni spekter

Motenje satelitske navigacije, prestrezanje komunikacijskih signalov, kibernetski napadi na poveljniške mreže ter manipulacija podatkovnih tokov lahko v trenutku ohromijo tudi najdražje in tehnološko najbolj sofisticirane platforme, opozarja Luhmer. Analize sodobnih konfliktov namreč kažejo, da je nadzor nad elektromagnetnim spektrom postal eden ključnih dejavnikov bojne učinkovitosti.

Posebej ranljivi so sistemi, ki so močno odvisni od neprekinjene povezljivosti in satelitske navigacije. Na ukrajinskem bojišču je elektronsko motenje že večkrat povzročilo, da so droni izgubili orientacijo, zgrešili cilje ali postali popolnoma neuporabni, kar je vojske prisililo k hitremu razvoju alternativnih navigacijskih metod in taktik delovanja brez GPS signala, piše Iryna Levytska v članku »Elektronsko bojevanje onemogoča več kot 50 % ruskih zračnih sredstev – navajajo ukrajinske kopenske sile«.

2. Kako z navigacijo motijo ladje v Hormuški ožini?

Zaradi vse pogostejših motenj so ukrajinski piloti danes usposobljeni za delovanje v razmerah, kjer izguba satelitske navigacije ni več izredna situacija, temveč standarden del sodobnega bojevanja.

Podobni vzorci se pojavljajo tudi na Bližnjem vzhodu, kjer elektronsko motenje ne vpliva le na vojaške operacije, temveč tudi na civilni letalski in pomorski promet. Obsežne motnje GPS signala v Perzijskem zalivu in okolici Hormuške ožine so že povzročile napačne navigacijske podatke za stotine ladij.

To potrjuje, da elektronsko bojevanje danes presega klasično bojišče in neposredno vpliva na globalno logistiko ter energetsko varnost, poroča The Week v članku Kako motenje signala GPS povzroča kaos na Bližnjem vzhodu.

Prihodnost zato ne bo nujno pripadala tehnološko najnaprednejši vojski, temveč tisti, ki bo sposobna razvijati preprostejše, robustnejše in hitro prilagodljive sisteme.

AREX – SLOVENSKO OBRAMBNO PODJETJE Z GLOBALNIM DOSEGOM

AREX predstavlja eno najuspešnejših zgodb slovenske obrambne industrije - z združevanjem lastnega razvoja, naprednih proizvodnih tehnologij in dolgoletnih izkušenj, uspešno konkurira bistveno večjim svetovnim proizvajalcem.

Slovenija morda ni država, ki jo svet najprej povezuje z obrambno industrijo, vendar je podjetje AREX iz Šentjerneja dokaz, da lahko tudi relativno majhno okolje ustvari tehnološko napredno podjetje z mednarodnim ugledom.
V več kot treh desetletjih delovanja se je AREX razvil iz podjetja z močnimi koreninami v orodjarstvu, v enega najpomembnejših proizvajalcev obrambne industrije. Danes produkti podjetja AREX dosegajo kupce po celotnem svetu, podjetje pa sodeluje z vojaškimi, policijskimi in industrijskimi partnerji najvišjega ranga. V Sloveniji je podjetje AREX močno povezano tudi z Ministrstvom za obrambo, Ministrstvom za notranje zadeve in Ministrstvom za pravosodje ter vsemi ostalimi vladnimi institucijami.

Začelo se je z obdelavo kovin in precizno proizvodnjo

Podjetje AREX je bilo ustanovljeno leta 1994 v Šentjerneju. Njegova zgodba temelji na strojništvu, proizvodnji orodij in razvoju proizvodnih tehnologij. Prav znanje s področja obdelave kovin in precizne proizvodnje je podjetju AREX omogočilo postopno širitev v obrambni sektor, kjer so zahteve glede kakovosti, zanesljivosti in sledljivosti med najstrožjimi v industriji.
Danes je AREX del mednarodne skupine, v katero spada tudi podjetje STEYR ARMS, kar omogoča dostop do širših razvojnih, proizvodnih in prodajnih zmogljivosti.

Visoka stopnja vertikalne integracije

Posebnost podjetja AREX je visoka stopnja vertikalne integracije. To pomeni, da vsi razvojni in proizvodni procesi potekajo znotraj podjetja. AREX ne proizvaja zgolj končnih produktov, temveč tudi številne dodatke, orodja in druge ključne komponente povezane z obrambno industrijo. Takšen pristop podjetju AREX omogoča večjo prilagodljivost pri izpolnjevanju specifičnih zahtev kupcev ter hitrejši razvoj novih rešitev.

Glavni produkti...

Med najbolj prepoznavnimi produkti podjetja so pištole kalibra 9 x 19 mm, puške in puškomitraljezi različnih kalibrov, strelivo za usposabljanje, linki in ostali produkti, zasnovani za profesionalne uporabnike, med katere sodijo vojaške in policijske enote, pa tudi športni strelci in drugi zakoniti uporabniki.

Pištole...

Pištole odlikujejo robustna konstrukcija, zanesljivo delovanje in ergonomska zasnova. Podjetje je skozi leta razvilo

več različnih modelov in generacij, ki se razlikujejo po dimenzijah, kapaciteti nabojnikov in namenu uporabe. Pomembna značilnost celotne družine produktov podjetja AREX je poenotena zasnova upravljalnih elementov, ki uporabnikom omogoča enostavno prilagajanje med posameznimi modeli. Podjetje AREX je skupaj s Slovensko vojsko in Ministrstvom za obrambo v letu 2025 dokončalo razvojni projekt pištole AREX DELTA L OR Gen.2 PP za uporabnike Slovenske vojske, kar predstavlja velik korak za skupno sodelovanje tudi v prihodnje.

...puške in puškomitraljezi...

AREX prav tako razvija in proizvaja sodobne jurišne puške in puškomitraljeze, namenjene profesionalnim uporabnikom. Med njimi posebno mesto zasedajo puške platforme AR15 v kalibru 5,56 x 45 mm, ki predstavljajo enega najbolj razširjenih in preizkušenih sistemov na svetu.
Puške na platformi AR15 so zasnovane modularno, kar omogoča prilagajanje različnim operativnim zahtevam.

Uporabniki lahko orožje opremijo z različnimi optičnimi merki, svetilkami, laserskimi označevalci in drugimi dodatki. Zaradi ergonomične zasnove, nizkega odsuna in visoke natančnosti so takšne puške priljubljena izbira vojaških in policijskih enot ter drugih varnostnih organizacij.
Pomemben del ponudbe predstavljajo tudi puškomitraljezi kalibra 5,56 x 45 mm in 7,62 x 51 mm, ki vojaškim enotam zagotavljajo podporo med bojnim delovanjem. Takšni sistemi omogočajo neprekinjeno delovanje z večjimi količinami streliva ter so namenjeni podpori pehotnih enot na različnih vrstah operacij. Zaradi robustne konstrukcije in visoke stopnje zanesljivosti predstavljajo ključen element sodobnih oboroženih sil.
Prednost podjetja AREX je v tem, da ne ponuja zgolj posameznih orožnih sistemov, temveč celovite rešitve, povezovalne člene za strelivo, sisteme za usposabljanje ter druge komponente, potrebne za učinkovito delovanje vojaških in varnostnih organizacij. S tem se podjetje uvršča med pomembnejše evropske ponudnike sodobne obrambne opreme.

...strelivo

Zelo pomemben del proizvodnega programa predstavlja strelivo za usposabljanje v več izvedbah, od markirne izvedbe MT-X do polimernega manevrskega streliva BLAN-X ter do streliva z gumijasto konico NL-X.
AREX je med vodilnimi evropskimi proizvajalci vadbenega streliva, ki omogoča urjenje vojaških ter policijskih enot. Takšno strelivo zmanjšuje obrabo orožja, je lažje od klasičnega streliva in omogoča učinkovito izvajanje različnih oblik treninga. Podjetje proizvaja vadbeno strelivo za več različnih kalibrov, vključno s kalibri, ki jih uporabljajo enote zveze NATO.

Takšni produkti postajajo vse pomembnejši del sodobnih varnostnih sistemov, saj omogočajo stopnjevano uporabo sile in zmanjšujejo tveganje za hujše poškodbe.

Povezovalni členi za puškomitraljeze

AREX je eden največjih svetovnih proizvajalcev povezovalnih členov oziroma linkov (LIN-X) za uporabo pri puškomitraljezih. Gre za ključne komponente, ki omogočajo pravilno podajanje nabojev v orožje. Podjetje proizvaja različne tipe linkov za številne standardne vojaške kalibre. Poleg tega razvija tudi fleksibilne linke za strelivo, ki se uporabljajo v vozilih, plovilih in drugih specializiranih platformah.

Balistična zaščita

V zadnjih letih podjetje širi dejavnost tudi na področje balistične zaščite. V ponudbi so različni zaščitni sistemi, ki vključujejo balistične jopiče, čelade in drugo osebno zaščitno opremo za vojaške ter policijske uporabnike. S tem AREX postopoma postaja ponudnik celovitih rešitev za obrambni in varnostni sektor.

Zanesljiv partner svetovne obrambne industrije

Velik del proizvodnje podjetja AREX je namenjen izvozu. Podjetje sodeluje z mednarodno priznanimi proizvajalci obrambne industrije ter dobavlja produkte in komponente številnim partnerjem po svetu, kar potrjuje visoko stopnjo zaupanja med največjimi igralci v industriji. Certifikati kakovosti ISO in standardi AQAP dodatno potrjujejo skladnost proizvodnje z zahtevami naročnikov.
AREX danes predstavlja eno najuspešnejših zgodb slovenske obrambne industrije. Z združevanjem lastnega razvoja, naprednih proizvodnih tehnologij in dolgoletnih izkušenj podjetje uspešno konkurira bistveno večjim svetovnim proizvajalcem. Njegov razvoj dokazuje, da lahko inovativnost, strokovno znanje in osredotočenost na kakovost ustvarijo globalno prepoznavno blagovno znamko tudi v visoko zahtevni obrambni industriji.

WWW.AREX.SI

Grafika: Spotnet

KJE SO NAJVEČJI PREMIKI SLOVENSKE OBRAMBNE INDUSTRIJE?

- Zakaj ima nišna Slovenija največjo priložnost v obrambni industriji doslej?
- Katera podjetja so naši aduti v obrambni industriji?
- Kako se je obramba razširila in s tem odprla priložnost novim podjetjem?

Kaja Kovič

Slovenija ni vojaška velesila. Nikoli ni bila. Je pa nekaj drugega: država znanja, inženiringa in specializiranih rešitev. In prav v tem je danes vrednost sodobne obrambne industrije.

Če je bila obramba nekoč domena velikih držav, velikih sistemov in velikih tovarn, je danes vse bolj odvisna od naprednih materialov, elektronike, senzorike, umetne inteligence, kibernetske varnosti in logistične odpornosti. Tu Slovenija ni več na robu zgodbe. Postaja del jedra.

V zadnjih letih se je spremenilo nekaj bistvenega: obramba ni več samo postavka v proračunu. Postaja razvojni mehanizem gospodarstva. Evropska unija je za Evropski obrambni sklad v obdobju 2021–2027 namenila skoraj 8 milijard evrov, od tega 2,7 milijarde za skupne raziskave in 5,3 milijarde za skupni razvoj zmogljivosti.

Hkrati globalni obrambni izdatki rastejo najhitreje v zadnjih desetletjih; po podatkih Stockholmskega mednarodnega inštituta za mirovne raziskave (ang. Stockholm International Peace Reasearch Institut, SIPRI) so leta 2024 dosegli 2.718 milijard dolarjev, kar je največ doslej.

To pomeni, da se odpira trg, na katerem ne zmagujejo nujno največji, ampak tudi najbolj specializirani, agilni in tehnološko sposobni. In to je priložnost, ki jo Slovenija lahko razume bolje, kot se zdi na prvi pogled.

A. Kam gre večina od 148 milijonov evrov?

Aprila letos je vlada v razvojne programe Slovenske vojske uvrstila skoraj 148 milijonov evrov novih projektov. Največji delež, dobrih 122 milijonov evrov, je namenjen sistemom brezpilotnih zrakoplovov.

Že ta razporeditev sredstev je zelo zgovorna. Kaže, kam gre sodobna obramba: v brezpilotne sisteme, podatke, povezljivost, avtomatizacijo in natančnost.

To ni zgolj vojaška investicija. To je razvojni projekt, tehnološka platforma in poslovna priložnost. Ko država kupuje drone, v resnici ne kupuje samo letalnikov; kupuje senzoriko, komunikacijske rešitve, programsko opremo, vzdrževanje, podatkovne tokove, usposabljanje in logistiko. Obrambni nakup postaja razvojna veriga.

Če to razumemo pravilno, potem postane jasno tudi nekaj drugega: slovenska podjetja v obrambni zgodbi ne morejo več igrati le vloge pasivnih dobaviteljev. Lahko so soustvarjalci rešitev.

B. Slovenski obrambni projekti so na pragu trga

Najpomembnejša beseda v tem trenutku ni oborožev anje, ampak industrializacija. Po ocenah obrambnega ministrstva in po izjavah državnega sekretarja Boštjana Pavlina so slovenski obrambni projekti v zadnji fazi razvoja in tik pred industrializacijo. To je odločilna točka.

Projekti niso več zgolj ideje in niso več samo raziskovalni koncepti. Prihajajo na prag trga. Prihajajo do točke, ki jo razvojni inženirji poznajo kot TRL 9 – torej do stopnje dejanske uporabe, komercializacije in operativne zrelosti.

A prav tam se v Sloveniji tradicionalno največkrat zalomi: ne pri ideji, ne pri prototipu, ampak pri prehodu v serijo, v proizvodnjo, v dobavno verigo, v trg. Če želimo v obrambni industriji zares uspeti, moramo prvič po dolgem času dokazati, da znamo zaključiti celoten lok – od znanja do izdelka.

Največji aktualni projekt je brez dvoma področje brezpilotnih sistemov.

Odpira se trg, na katerem ne zmagujejo nujno največji, ampak tudi najbolj specializirani, agilni in tehnološko sposobni.

C. 250 slovenskih podjetij v razvojnih projektih

Dobra novica je, da Slovenija ni na začetku. Po besedah Ministrstva za obrambo RS se je grozd slovenske obrambne industrije v kratkem času razširil z okoli 58 na približno 140 članov, v ključnih razvojnih projektih pa sodeluje več kot 250 slovenskih gospodarskih družb. To ni več industrija v nastajanju. To je industrija v aktivaciji.

Ključno je tudi, da današnja obrambna industrija ni več omejena na klasične proizvajalce orožja ali opreme. Vključuje razvojno-raziskovalne institucije, univerze, podjetja iz avtomobilske industrije, proizvajalce elektronike, ponudnike IT-rešitev, logistične igralce in podjetja, ki delujejo na področju energije, komunikacij ali naprednih materialov. Obramba je postala širok tehnološki prostor.

Tu se skriva ena največjih slovenskih prednosti. Kot majhna država nimamo razkošja velikih serij. Imamo pa možnost, da postanemo močni v nišah, v komponentah visoke vrednosti, v razvojnih podsistemih in v povezovanju znanj, ki jih velike korporacije pogosto razvijajo počasneje.

D. Top 3: kje se že vidi premik?

Kateri so najpomembnejši obrambni projekti doma, v Sloveniji?

1. Brezpilotni sistemi

Največji aktualni projekt je brez dvoma področje brezpilotnih sistemov. Vlada je jasno pokazala, da bodo droni eden ključnih stebrov prihodnjih zmogljivosti. To ni presenečenje.

Brezpilotni sistemi so danes hkrati vojaška, varnostna, logistična in civilna tehnologija. Uporabni so v obrambi, pri nadzoru, varstvu pred naravnimi nesrečami, opazovanju terena in podpori odločanju.

Prav zato so idealen primer tako imenovane dvojne rabe. To, kar je danes vojaška rešitev, lahko jutri postane rešitev za civilno zaščito, geodetski nadzor, gozdarstvo ali reševanje.

Ko država kupuje drone, ne kupuje samo letalnikov. Kupuje senzoriko, komunikacijske rešitve, programsko opremo, vzdrževanje, podatkovne tokove, usposabljanje in logistiko.

2. Opremljanje specialnih sil

Drugi pomembni domači projekt je opremljanje specialnih sil Slovenske vojske. Na prvi pogled gre za ožjo nišo, v resnici pa je to zelo zahtevno področje, kjer so pomembne kakovost, zanesljivost, modularnost in interoperabilnost.

Prav tu se pogosto odpirajo vrata za podjetja, ki so sposobna razviti specializirano opremo, komunikacijske sisteme, nosilne elemente, optiko, programsko podporo ali druge napredne rešitve.

Specialne sile so v sodobnih vojskah pogosto laboratorij prihodnje opreme. Kar se dokaže tam, se lahko pozneje razširi tudi širše.

3. Odpornost infrastrukture in digitalizacija

Tretji pomembni domači blok projektov je manj spektakularen, a morda še pomembnejši: infrastruktura, odpornost in digitalizacija. Sem sodijo delavnica za konzervacijo in dekonzervacijo na Vrhniki, prehod Slovenske vojske na IP-telefonijo ter investicije v objekte za večjo odpornost in neprekinjeno delovanje.

Vsi ti projekti na novo opredeljujejo pojem obrambe. Ta zdaj ne vključuje več zgolj orožja, pač pa tudi delujoče omrežje, digitalno povezanost, servisno sposobnost, vzdrževanje, komunikacijo in odpornost institucij. Prav na teh področjih ima slovensko gospodarstvo veliko več kompetenc, kot jih običajno pripisujemo »obrambni industriji«.

E. Top 3 področja v EU, kjer je za Slovenijo največ prostora

Na katerih področjih pa se akterji slovenske obrambne industrije lahko prebijejo v EU?

1. Brezpilotni sistemi

Tu je smer jasna tako na nacionalni kot evropski ravni. Če Slovenija že doma vlaga največ prav v drone, potem je smiselno, da poskuša ta znanja in reference povezati še z evropskimi projekti.

2. Kibernetska varnost in digitalizacija

Srednjeročni obrambni program 2026–2031 izrecno poudarja kibernetsko obrambo, digitalizacijo in nekinetične zmogljivosti kot enega ključnih razvojnih poudarkov.

To je področje, kjer ima Slovenija podjetja, raziskovalce in relativno nizke vstopne ovire v primerjavi s težko oborožitvijo.

3. Vesoljske tehnologije

Morda se sliši futuristično, a ni. Srednjeročni obrambni program prvič jasno opredeljuje tudi nacionalne ambicije na področju vesolja, torej razvoj in uporabo vesoljskih tehnologij za obrambne potrebe ter potrebe varstva pred naravnimi in drugimi nesrečami.

To je izjemno pomembno, ker pomeni vstop v segment, kjer se srečujejo satelitski posnetki, geoinformacijski sistemi, opazovanje Zemlje, krizno upravljanje in digitalna suverenost.

F. Ključni model: konzorciji

Če je treba iz vsega tega izluščiti eno operativno lekcijo, je to naslednja: Slovenija sama po sebi ne bo zmagovala z velikostjo, ampak s povezovanjem.

Kot najbolj obetaven se kaže konzorcijski model, pri katerem država podjetja, raziskovalce, fakultete in razvojne ustanove poveže v konzorcij. Konzorcij razvije produkt. Produkt pride do industrializacije. Industrializacija odpre domači in tuji trg.

To je model, ki zmanjšuje tveganje, pospešuje razvoj in omogoča globalni preboj. Hkrati pa je tudi najbolj realističen za majhno državo, v kateri je znanje razpršeno.

G. Največja nevarnost: da ostanemo podizvajalci

Najlažje je ostati dobavitelj komponent. Najlažje je sodelovati kot podizvajalec. Najlažje je reči, da smo del verige. Najtežje pa je postati razvojni partner, lastnik znanja in nosilec proizvoda.

In prav tu se bo odločalo, ali bo slovenska obrambna industrija v resnici razvojna priložnost ali pa zgolj sezonski val naročil.

Če bomo ostali pri komponentah, bomo vedno zamenljivi. Če bomo razvijali produkte, algoritme, sisteme in specializirane module z lastnim znanjem, pa bomo postali prepoznaven igralec.

H. 30 odstotkov doma: to je nacionalna ambicija

Ena pomembnejših politično-gospodarskih ambicij je, da bi približno 30 odstotkov vrednosti prihodnjih obrambnih investicij ostalo v Sloveniji. To ne pomeni nujno neposrednih nakupov izključno pri slovenskih podjetjih, temveč širši domači učinek: vključevanje slovenskih dobaviteljev, razvojnih ekip, vzdrževalnih zmogljivosti, proizvodnje komponent in raziskovalnih partnerjev v obrambne projekte.

Pomeni namreč naslednje: naj ne odteče vsak evro obrambnih investicij brez sledi, ampak naj pusti razvojni odtis v slovenskih podjetjih, na delovnih mestih, pri znanju in davkih. Če to dosežemo, obrambni proračun postane del industrijske politike.

Če tega ne dosežemo, ostanemo predvsem kupec tujih rešitev.

Globalni in evropski obrambni trg

- Globalni obrambni izdatki: **2.443 milijard USD (2023)**
  Vir: Stockholm International Peace Research Institute
- Evropski obrambni sklad (EDF): **8 milijard EUR (2021–2027)**
  Vir: European Commission
- Trg brezpilotnih sistemov: **več kot 90 milijard USD do 2030**
  Viri: Deloitte, Statista, Fortune Business Insights

Slovenski aduti v dobavnih verigah

Primeri slovenskega znanja v obrambnem okolju in pri produktih dvojne rabe imajo skupni imenovalec – visoka dodana vrednost, nišna specializacija, globalna vpetost:

- **Dewesoft.** Merilni sistemi za letalstvo, vesolje in obrambne aplikacije.
- **Iskra.** Elektronika, energetika, komunikacijske rešitve.
- **Pipistrel.** Napredna letala in električni pogoni (tehnologije dvojne rabe).

Cifre, ki govorijo

- **148 milijonov evrov** za nove projekte Slovenske vojske je vlada potrdila aprila 2026.
- **122,8 milijona evrov** od tega je namenjenih sistemom brezpilotnih zrakoplovov.
- **140 podjetij** približno šteje grozd slovenske obrambne industrije.
- **250+ podjetij** sodeluje v ključnih razvojnih projektih.
- **2.718 milijard dolarjev** so leta 2024 dosegli globalni obrambni izdatki.
- **Skoraj 8 milijard evrov** znaša proračun Evropskega obrambnega sklada za obdobje 2021–2027.
- **3 % BDP do leta 2030** predvideva slovenski srednjeročni obrambni program kot cilj obrambnih izdatkov.

Foto:Barbara Reya

DRONI, SIMULATORJI, AVTONOMNA VOZILA ...

Pogled iz prakse: **Boštjan Skalar,**
Grozd obrambne industrije Slovenije, GOIS

Ali so slovenska podjetja pripravljena?

»Seveda je naša industrija, kar zadeva končne produkte, ki so zreli za komercializacijo, še vedno precej šibka. Je pa treba povedati, da se z razvojnimi sredstvi Ministrstva za obrambo Republike Slovenije (MORS), ki znašajo okoli 23 milijonov evrov letno, ta položaj skokovito izboljšuje.

Kar nekaj izdelkov ima že zelo visoko raven tehnološke pripravljenosti, kar pomeni, da so praktično zreli za komercializacijo. Prav z namenom, da bi bil prehod v industrijsko fazo hitrejši, je bila ustanovljena družba Dovos.«

Kje izgubljamo največ potenciala?

»Izzivi so predvsem v financiranju in koordinaciji. Del odgovora je Dovos, del pa boljša vključenost bank. Slovensko gospodarstvo je zelo močno v dobaviteljskih verigah, manj pa pri razvoju končnih produktov z višjo dodano vrednostjo.«

Kje so konkretne priložnosti?

»Največ na področjih: droni in protidronska zaščita, simulatorji, avtonomna vozila in daljinsko vodene oborožitvene postaje. Priložnosti ostajajo tudi v sodelovanju s tujimi podjetji in vključevanju v dobaviteljske verige.«

Podizvajalci ali razvojni partnerji?

»Razvoj končnih produktov kaže, da se lahko uvrstimo višje v verigi. Cilj je, da se 50–60 odstotkov izdelka proizvede doma. Interes tujih podjetij za sodelovanje je velik.«

Je obrambna industrija tveganje?

»Vsak posel je tvegan. A večina podjetij lahko sodeluje kot del konzorcijev tudi brez posebnih dovoljenj. Podjetja naj se ne bojijo iskati priložnosti.«

Varnost ali gospodarska priložnost?

»Obramba pomeni odpornost družbe. In prav ta odpornost odpira prostor za vključevanje gospodarstva.«

I. Obramba ni več samo vojska

Obrambno industrijo še vedno razumemo preozko.

Sodobna obramba vključuje:

- ★ energijo,
- ★ prehrano,
- ★ logistiko,
- ★ digitalno infrastrukturo,
- ★ kibernetsko varnost,
- ★ satelitske podatke,
- ★ zdravstveno pripravljenost,
- ★ zmogljivost delovanja v krizi.

To ni ideološka razširitev pojma, ampak realnost. Srednjeročni obrambni program se ne osredotoča le na klasične vojaške zmogljivosti, ampak tudi na zračno obrambo, logistične zmogljivosti, letalsko bazo Cerklje ob Krki, digitalizacijo, kibernetsko obrambo, nekinetične zmogljivosti ter razvoj obrambnih in civilno uporabnih vesoljskih zmogljivosti. Hkrati program predvideva postopno povečevanje obrambnih izdatkov do treh odstotkov BDP do leta 2030.

To pomeni, da se gospodarska priložnost odpira mnogo širše, kot si običajno predstavljamo.

Če želimo v obrambni industriji zares uspeti, moramo prvič po dolgem času dokazati, da znamo zaključiti celoten lok – od znanja do izdelka.

J. Zakaj je zdaj pravi trenutek?

V zadnjih treh desetletjih Slovenija za tak premik ni imela boljšega trenutka.

Evropa vlaga. Obrambni proračuni rastejo. Dobavne verige se preoblikujejo. EU išče več lastnih zmogljivosti. Tehnologija je v središču obrambnega razvoja. Slovenija pa ima hkrati dovolj znanja in je dovolj majhna, da se lahko hitro premakne.

To je trenutek, ko lahko iz države podizvajalcev postanemo država razvojnih partnerjev. To je trenutek, ko lahko obrambne projekte razumemo kot industrijske projekte. To je trenutek, ko lahko majhna država zgradi velik položaj – ne s količino, ampak z natančnostjo. Znanje obstaja. Vprašanje ni več, ali lahko sodelujemo. Vprašanje je, ali bomo vodili.

STANDARDIZACIJA KOT MOST DO NOVIH TEHNOLOŠKIH PRILOŽNOSTI

Evropa pospešeno krepi svojo varnostno in obrambno pripravljenost, kar odpira nove razvojne in gospodarske priložnosti za evropska podjetja. V ospredju so inovacije, tehnološka zmogljivost ter vključevanje v skupne evropske dobavne in razvojne verige.

V tem okolju so standardi in standardizacija ključni povezovalni dejavnik. Niso več zgolj tehnična zahteva, temveč temelj interoperabilnosti, zaupanja in učinkovitosti. Standardi omogočajo povezljivost sistemov, zmanjšujejo stroške in odpirajo dostop do evropskih projektov, kjer so usklajene tehnične specifikacije pogosto pogoj za sodelovanje.

Za Slovenijo je to pomembna priložnost za vključevanje v evropske verige vrednosti, razvoj nišnih tehnologij in lažji izvoz. Največji potencial se kaže na področjih elektronike, programske opreme, senzorike, materialov, mobilnosti, kibernetske varnosti in specializiranih komponent.

Slovenski inštitut za standardizacijo (SIST) ima pri tem vlogo ključnega partnerja podjetjem. Omogoča jim dostop do standardov, strokovno podporo in vključevanje v razvoj evropskih standardizacijskih rešitev. Standardizacija tako predstavlja praktično orodje za rast, internacionalizacijo in dolgoročno konkurenčnost slovenskih podjetij.

SIST

OBRANILI SE BOMO LAHKO LE S SKUPNIMI MOČMI

»Slovenija je v letih samostojnosti vzpostavila stabilen in učinkovit obrambni sistem, ki temelji na sodelovanju državnih institucij, lokalnih skupnosti, gospodarstva in družbe,« poudarja Mateja Rokvič, v času pogovora generalna direktorica Direktorata za obrambne zadeve na Ministrstvu za obrambo RS. Dodaja, da sodobna obramba ni več zgolj vojaško vprašanje, temveč sposobnost celotne družbe, da se učinkovito odziva na različne krize.

Kako je danes sestavljen obrambni sistem države in kateri so njegovi ključni stebri?

Obrambni sistem Republike Slovenije sestavljata vojaška in civilna obramba, pri čemer je pomembno poudariti, da je obrambni sistem eden od stebrov sistema nacionalne varnosti, ki vključuje tudi notranjo varnost ter sistem varstva pred naravnimi in drugimi nesrečami. Ključna značilnost slovenskega sistema je medsebojno usklajeno delovanje vseh področij, saj sodobni varnostni izzivi zahtevajo celovit pristop, dobro pripravljenost ter visoko stopnjo odpornosti države in družbe.

Kakšno mesto in pomen ima znotraj obrambnega sistema civilna obramba?

Civilna obramba združuje ukrepe in dejavnosti državnih organov, lokalnih skupnosti, gospodarstva, zavodov, organizacij in državljanov, s katerimi se podpira vojaška obramba, ohranja delovanje države in zagotavljanje delovanja gospodarstva ter oskrbe prebivalstva v krizah, izrednem stanju in vojni.

V kolikšni meri je Sloveniji uspelo oblikovati učinkovit obrambni sistem?

Slovenija je v letih samostojnosti vzpostavila stabilen in učinkovit obrambni sistem, ki temelji na sodelovanju državnih institucij, lokalnih skupnosti, gospodarstva in družbe. Posebej uspešni smo pri medresorskem povezovanju, strateškem načrtovanju, kriznem upravljanju in razvoju nacionalne odpornosti. Direktorat opravlja naloge upravitelja obrambnega načrta države, ima pomembno vlogo pri usklajevanju področja kritične infrastrukture in hibridnih groženj. Nikakor pa ne smemo mimo področja geoprostorske podpore in vesolja. Sodobna obramba namreč ni več zgolj vojaško vprašanje, temveč sposobnost celotne družbe, da se učinkovito odziva na različne krize. Naj poudarim, da je Slovenija na tem področju lahko vzor marsikateri državi.

Kakšna je pri tem vloga Direktorata za obrambne zadeve?

Direktorat skrbi za razvoj civilne obrambe, krizno upravljanje, načrtovanje pripravljenosti države in usklajevanje ukrepov za zagotavljanje neprekinjenega delovanja države in družbe v kriznih razmerah. Med ključnimi nalogami so priprava strateških dokumentov, kot so Strategija civilne obrambe, Strategija odpornosti Republike Slovenije do leta 2030, Strategija za odpornost kritičnih subjektov. Direktorat usmerja in usklajuje aktivnosti za krepitev odpornosti kritične infrastrukture, izvajanje priprav, ukrepov in dejavnosti za pravočasno odzivanje na različne vrste kriz in vojne, na področju odpornosti in civilne pripravljenosti, vojaške mobilnosti, podpore države gostiteljice in izvaja naloge za učinkovito naslavljanje hibridnih groženj. Vse te aktivnosti vključujejo koordinacijo z drugimi ministrstvi, vladnimi službami, lokalnimi skupnostmi, gospodarskimi družbami, zavodi in organizacijami, katerih dejavnost je posebnega pomena za obrambo. Pomembno področje ostaja tudi pridobivanje kadra za Slovensko vojsko in ozaveščanje mladih o pomenu varnosti, pripadnosti in krepitvi vrednot.

Kaj pomeni nacionalna odpornost in zakaj postaja vse pomembnejši del sodobne varnosti?

Nacionalna odpornost pomeni sposobnost države, družbe in posameznika, da se pravočasno pripravijo na krize, jih učinkovito obvladujejo in po njih hitro okrevajo. Gre za celovit koncept, ki vključuje 13 področij, kot so energetika, zdravstvo, prehranska varnost, promet, gospodarstvo, finance. V sodobnem varnostnem okolju, ki ga zaznamujejo hibridne grožnje, kibernetski napadi, motnje v oskrbi in vplivanje na demokratične procese, odpornost postaja ključna za ohranjanje delovanja države in družbe tudi v izrednih razmerah.

»Varnost in odpornost države temeljita na sodelovanju, zaupanju in pripadnosti,« pravi Mateja Rokvič, v času pogovora generalna direktorica Direktorata za obrambne zadeve na Ministrstvu za obrambo RS.

Kako poteka oblikovanje sistema nacionalne odpornosti v Sloveniji?

Slovenija sistem nacionalne odpornosti gradi celovito in medresorsko. Pomemben mejnik je bila nacionalna vaja kriznega upravljanja in odzivanja ODPORNOST24, ki je pokazala dobre temelje sistema in hkrati izpostavila področja za nadgradnjo. Na tej podlagi je bila sprejeta Strategija odpornosti Republike Slovenije do leta 2030, trenutno pa poteka izvajanje akcijskega načrta ter priprava nadaljnjih ukrepov za krepitev pripravljenosti države in družbe. V direktoratu se že intenzivno pripravljamo na izvedbo vaje ODPORNOST26.

Kako ocenjujete vključevanje prebivalstva v sistem varnosti in odpornosti?

Slovenija ima močno tradicijo prostovoljstva, solidarnosti in sodelovanja ljudi ob nesrečah, kar predstavlja veliko prednost naše družbe. Kljub temu ostaja pomembno področje ozaveščanja prebivalcev o osebni pripravljenosti, varnostni kulturi in njihovi vlogi pri odzivanju na krizne dogodke. Nacionalna odpornost namreč ni zgolj naloga institucij, temveč odgovornost celotne družbe.

Za konec – katero sporočilo bi posebej izpostavili?

Varnost in odpornost države temeljita na sodelovanju, zaupanju in pripadnosti. Prav občutek povezanosti, odgovornosti do skupnosti in pripravljenost pomagati drug drugemu krepi družbeno odpornost. Zato je pomembno, da občutek pripadnosti državi krepimo že pri mladih. Lani smo ob prvem šolskem dnevu vsem prvošolčkom podarili slovenske zastavice kot simbol povezanosti in spoštovanja do domovine. V okviru Dneva civilne obrambe smo pripravili tudi okroglo mizo o pripadnosti, prispevek pa je bil objavljen v Zborniku o civilni obrambi, ki ga izdamo vsako leto ob Dnevu Civilne obrambe. Knjižnicam osnovnih šol in njihovim podružnicam po Sloveniji smo podarili knjigo Pravljična Slovenija, s katero želimo že med otroki utrjevati ljubezen do domovine, odnos do skupnosti, vrednot in države – in prav tu, pri najmlajših, se začne izgradnja varne in odporne države, v kateri živimo.

Grafika: Spotnet

DVOJNA RABA: ALI POZNATE VEPKOV IN ALENOS?

- Kako obrambne tehnologije prehajajo v civilno uporabo in gospodarstvo?
- Kateri so konkretni primeri in kateri projekti v Sloveniji so aktualni?
- Kje so poslovne priložnosti za podjetja pri dvonamenskih tehnologijah?

Gregor Lisec

Ko helikopter Slovenske vojske pristane na gorski polici v Alpah, ne gre za vojaško operacijo, ampak za reševanje ponesrečenca. Ko transportno letalo Spartan odvrže vodo nad požariščem na Krasu, ne opravlja obrambne naloge, temveč gasi ogenj. In ko vojaški energetski sistemi zagotavljajo elektriko v kriznih razmerah, postanejo rešitev, ki jo lahko uporabi tudi gospodarstvo.

To so samo nekateri primeri, kako obrambne zmogljivosti prehajajo v civilno uporabo.

V uradni opredelitvi dvojne rabe s strani Evropskega parlamenta je sicer dvojna raba še vedno predvsem zgodba o civilnih izdelkih in tehnologijah, ki se lahko uporabijo tudi vojaško. Ker bi bili v napačnih rokah lahko zlorabljeni, so pod strogim izvoznim režimom, nad katerim v Sloveniji bdi ministrstvo za gospodarstvo, turizem in šport s pristojno komisijo za nadzor izvoza blaga z dvojno rabo.

»Tovrstni izdelki in storitve lahko izboljšujejo življenja ljudi, a jih je mogoče zlorabiti. Avtoritarni režimi bi jih denimo lahko zlorabili za nadzor nad prebivalstvom, teroristične skupine pa za izvedbo napadov,« opozarja Gregor Zupan z ministrstva za obrambo.

Trenutno največji potencial prepoznavamo na področju umetne inteligence, kvantne tehnologije, biotehnologije, vesoljske tehnologije, kibernetske varnosti, naprednih materialov.« Gregor Zupan

No, za slovensko gospodarstvo postaja vse bolj zanimiva obratna smer – kako tehnologije in sistemi, razviti za vojaške namene, dobivajo konkretno vrednost v zdravstvu, energetiki, zaščiti in reševanju ter varovanju kritične infrastrukture ...

Prav na tej točki se srečata razlagi Gregorja Zupana z ministrstva za obrambo (MORS) in Boštjana Skalarja, direktorja Grozda obrambne industrije Slovenije GIZ–GOIS, ki kažeta, da dvojna raba vse bolj postaja razvojni model.

A. Dvojna raba: meja med vojaškim in civilnim se briše

Zupan najprej izpostavi razliko, ki jo v razpravah pogosto spregledamo: »Pri dvojni rabi v osnovi ne gre za tehnologije, ki izhajajo iz obrambnega sektorja in se uporabljajo v civilne namene, pač pa ravno obratno – za proizvode, ki so prvenstveno namenjeni civilni rabi, se pa lahko uporabijo tudi v vojaške namene.« Podobno razlago ponuja tudi Skalar: »Pojem dvojne rabe definira civilno aplikacijo, ki se eventualno lahko uporabi v obrambne namene.«

A za gospodarstvo postaja vse pomembnejši širši koncept dvonamembnosti – ko obrambne zmogljivosti dobijo tudi civilno vrednost.

Ta prehod sicer ni nič novega in to potrjujejo najbolj znani primeri, ki jih našteva Zupan: internet, GPS ter napredni materiali, kot so kevlar, karbon, goreteks in teflon. Vse te tehnologije so bile v osnovi razvite za vojsko, sčasoma pa postale uporabne v civilnem okolju oziroma gospodarstvu.

Danes se ta proces še pospešuje. Razvojni cikli so krajši, tehnologije kompleksnejše, potrebe družbe pa tudi v luči geopolitičnih razmer po svetu vse bolj prepletene z varnostnimi izzivi. Meja med civilnim in vojaškim se zato vse bolj briše – ne le v teoriji, ampak tudi v praksi. V številnih primerih se razvoj že od začetka načrtuje z mislijo na obe uporabi.

Država in mednarodni programi povečujejo financiranje dvonamenskih tehnologij.

B. Ko obrambna zmogljivost dela za bolne

Vojaška infrastruktura danes opravlja številne naloge, ki neposredno vplivajo na življenje ljudi. Eden najbolj očitnih primerov je helikopterska nujna medicinska pomoč (HNMP). Slovenska vojska poleg svojih osnovnih nalog redno sodeluje pri reševanju življenj – od intervencij do prevozov organov in reševanj v gorah. Takšne naloge so del vsakdanjega življenja.

Podoben primer je transportno letalo Spartan, ki ni namenjeno le vojaškim operacijam, temveč tudi gašenju požarov in medicinskim evakuacijam. Dvonamenskost v tem primeru ni naknadna, temveč je bila zamišljena že v osnovi.

Skalar ob tem opozarja, da dvonamenskost ne velja le za tehnologije: »Tudi bolnišnica je lahko objekt z dvojnim namenom, prav tako infrastruktura, še posebej kritična.« Zupan prikima, da so načrtovane gradnje in obnove bolnišnične infrastrukture pomemben projekt dvonamenskosti, pri čemer se že vnaprej razmišlja o uporabi za različne scenarije.

Delež dvonamenskih rešitev v slovenski obrambni industriji je že danes visok, kar pomeni, da podjetja to logiko že prepoznavajo in jo vse bolj vključujejo v svoje razvojne strategije.« Boštjan Skalar

Pomembno področje predstavlja tudi zaščita infrastrukture. Sistemi za zaznavanje in nevtralizacijo brezpilotnih letal lahko poleg vojske ščitijo tudi energetske objekte, bolnišnice ali logistična središča. V času, ko postaja varnost kritične infrastrukture vse pomembnejša, takšne rešitve dobivajo novo vlogo. Niso le obrambni, ampak delujejo tudi kot poslovni produkt.

C. Katere tehnologije kažejo največji potencial?

Vse to kaže, da dvonamenskost v vsakdanjem življenju deluje in je njegov pomemben del, razvoj pa se seveda ni ustavil.

O projektih oziroma tehnologijah v razvoju, ki imajo največji potencial, smo povprašali Gregorja Zupana. »Trenutno največji potencial prepoznavamo na področju najbolj naprednih oziroma prebojnih (ang. disruptive) tehnologij, med katere prištevamo predvsem umetno inteligenco, kvantne tehnologije, biotehnologije, vesoljske tehnologije, kibernetsko varnost, napredne materiale, sisteme brez posadke in učinkovite energetske sisteme,« je naštel ključne primere.

Projekti, kot sta VEPKOV in ALENOS, kažejo neposreden poslovni potencial.

Eden od izstopajočih projektov na Slovenskem je večnamenska platforma na kolesni hibridni pogon VEPKOV brez posadke, ki omogoča uporabo od logistike do gašenja požarov na težko dostopnih območjih. Takšne platforme so zasnovane modularno, kar pomeni, da jih je mogoče prilagoditi različnim potrebam – od vojaških do civilnih.

Podobno velja za razvoj nove gasilske obleke, kjer napredni materiali presegajo obstoječe standarde ter vključujejo vidik trajnostnosti in krožnega gospodarstva. To pomeni, da lahko tehnologije, razvite za zaščito v ekstremnih razmerah, najdejo širšo uporabo tudi v industriji ali vsakdanjih izdelkih.

Najmočnejši slovenski primer pa ostaja ALENOS (Alternativna energetska oskrba), modularni energetski sistem za alternativno oskrbo z energijo.

Zupan poudarja, da njegova uporaba močno presega vojaški okvir, ter ga označuje za izjemno pomemben projekt prepletanja obrambnih in civilnih rešitev na področju energetske učinkovitosti in zelenega prehoda:

»ALENOS zagotavlja dolgoročno energetsko samooskrbo kapacitet Slovenske vojske nižje potrošnje, in sicer z uvajanjem alternativnih virov energije (sončne in vetrne) ter hrambo energije. Rešitev je primerna denimo za energetsko napajanje strelišč in vojaških taborov, začasnih nastanitvenih enot civilne zaščite v primeru naravnih nesreč, pa tudi za energetsko samooskrbo (manjših) gospodarskih družb ali samostojnih stanovanjih objektov, kar bi bilo lahko še posebej pomembno z vidika pričakovanih prihodnjih energetskih negotovosti in kriz.«

Iz tega je mogoče izluščiti bistvo dvonamenskosti: tehnologija, razvita za krizne razmere, postane zanimiva tudi za gospodarstvo, kjer so ključne zanesljivost, odpornost in energetska neodvisnost. Sploh v času energetskih izzivov takšne rešitve niso več le dopolnilo, temveč pomemben del poslovnih strategij.

D. »Potencial slovenskih podjetij je zelo visok.«

Dvonamenskost postaja tudi finančno vse močnejša. Ministrstvo za obrambo bo po napovedih za raziskave, razvoj in inovacije namenjalo več kot 30 milijonov evrov letno na nacionalni in mednarodni

Kaj se uveljavlja ali še prihaja?

- **Umetna inteligenca (UI)** – od vojaške analitike in avtonomnih sistemov do poslovnih odločitev, logistike, zdravstva
- **Avtonomni sistemi in robotika** – vozila brez posadk, logistični roboti, intervencijske platforme
- **Energetski sistemi za samooskrbo (na primer ALENOS)** – iz vojaških baz v podjetja, krizno infrastrukturo in gospodinjstva
- **Sistemi proti dronom (counter-drone)** – zaščita kritične infrastrukture, industrije, letališč
- **Kibernetska varnost** – iz obrambnih sistemov v zaščito podjetij in digitalnih omrežij
- **Napredni senzorji in nadzorni sistemi** – pametna mesta, industrija, promet
- **Kvantne in vesoljske tehnologije** – prihodnja komunikacija, navigacija, obdelava podatkov

Kaj je danes razširjeno v civilni sferi, izšlo pa je iz vojske?

- **Internet** – iz vojaškega omrežja ARPANET v globalno digitalno infrastrukturo
- **GPS navigacija** – prvotno vojaški sistem za pozicioniranje, danes osnova logistike, transporta in mobilnih aplikacij
- **Droni** – od izvidništva do kmetijstva, snemanja, nadzora infrastrukture
- **Napredni materiali (kevlar, karbon, goreteks)** – iz zaščitne opreme v šport, industrijo in vsakdanja oblačila
- **Satelitske tehnologije** – komunikacije, vremenska napoved, upravljanje prometa
- **Medicinske tehnologije** – telemedicina, urgentni transport, sistemi za krizne razmere
- **Simulacije in trening sistemi** – iz vojaškega usposabljanja v industrijo, letalstvo, izobraževanje

Slovenska podjetja imajo nadpovprečen potencial na področju dvojnega namena.

ravni. Ob tem podjetja usmerja in podpira tudi pri projektih Evropskega obrambnega sklada (EDF) ter v okviru mehanizma Nato DIANA (Defence Innovation Accelerator for North Atlantic).

Evropski obrambni sklad in Natov program DIANA spodbujata razvoj tehnologij, ki imajo uporabo v obeh sferah – od umetne inteligence in kibernetske varnosti do energetike in brezpilotnih sistemov. Takšni programi so posebej zanimivi za mala in srednja podjetja, ki lahko s svojo fleksibilnostjo hitro razvijejo in prilagodijo rešitve.

Tudi domači okvir se krepi. Družba za obrambo, varnost in odpornost Slovenije (DOVOS), ki bo s kapitalskimi vložki vlagala v razvoj proizvodnih zmogljivosti domače industrijske in tehnološke baze, je že objavila prvo javno vabilo za kapitalsko sodelovanje s podjetji na področjih obrambe, varnosti in odpornosti, pri čemer kot prednostno področje izpostavlja prav večnamensko rabo.

Zupan ob tem poudarja: »Potencial slovenskih podjetij na področju razvoja naprednih tehnologij, vključno s tehnologijami s potencialno dvojno rabo oziroma namembnostjo, je izjemno visok, zagotovo nadpovprečen v svetovnem merilu.

K temu v prvi vrsti pripomore dejstvo, da večina slovenskih visokotehnoloških podjetij sodi v kategorijo srednjih in malih podjetij, ki zaposlujejo visoko (tehnično) izobražene in motivirane kadre, sam ustroj pa podjetjem omogoča hitre reakcije na tehnološke potrebe iz okolice ter ustrezna in nagla prilagajanja.«

Skalar dodaja, da je delež dvonamenskih rešitev v slovenski obrambni industriji že danes visok, kar pomeni, da podjetja to logiko že prepoznavajo in jo vse bolj vključujejo v svoje razvojne strategije.

Če je bila dvojna raba dolgo razumljena predvsem kot regulativni izziv, je danes vse bolj tudi razvojna in poslovna priložnost. Tehnologije se ne selijo več le iz civilnega v vojaško okolje, ampak vse pogosteje tudi v obratno smer – iz obrambnega sistema v gospodarstvo. In prav v tej smeri, kjer obrambni projekt postane rešitev za trg, se odpira prostor za podjetja.

OŽIČIJO ŠE TAKO ZAHTEVNE ELEKTRONSKE SKLOPE

Družba Elra seti z Andraža nad Polzelo je specializirana za izdelavo kabelske in žične konfekcije ter njihovo sestavo v funkcionalna vezja.

Dejavnost družbe Elra seti vključuje obdelavo kablov in vodnikov (žic) ter izdelavo kabelskih snopov in vezij. Leta 1990 jo je ustanovil Srečko Rajh. Število zaposlenih se čez poslovanje giblje med 5 in 12, trenutno jih je v družbi 5.

V OSPREDJU MALOSERIJSKA NAROČILA

Za svojo dejavnost so zelo dobro tehnološko opremljeni, poleg zanesljivosti jih odlikuje velika prilagodljivost. Izpolnjujejo predvsem maloserijska naročila, ki se jih večja podjetja ne lotevajo. Projekte izvedejo od ideje preko dokumentacije in vzorcev do končnega produkta. Delno avtomatizirana proizvodnja poteka na univerzalnih in namenskih strojih ter napravah z avtomatskim nadzorom parametrov, po potrebi s stoodstotno kontrolo na testnih napravah.

Njihove stranke so uveljavljena slovenska podjetja: Kronoterm, Dewesoft, Omega Air, Alpfrigo ... Zaradi dobre tehnološke opremljenosti so kos tudi velikoserijskim naročilom. Pri večjih naročilih si pomagajo tudi z zunanjimi izvajalci.

VSTOP NA PODROČJE OBRAMBE IN VARNOSTI

V Elra seti želijo vstopiti še na področje obrambe in varnosti. Svoje storitve lahko ponudijo na različnih področjih in za naprave, kjer so potrebne električne povezave med upravljalnimi in izvršilnimi sklopi. V vojnih razmerah, lokacijska razpršenost podjetij za izdelavo podsklopov in komponent pomembno prispeva k zanesljivosti proizvodnje.

ELRA SETI

MIL SISTEMIKA

SLOVENSKO ZNANJE ZA DIGITALNO BOJIŠČE PRIHODNOSTI

Podjetje MIL Sistemika razvija napredno programsko opremo za sodobne obrambne sisteme, namenjeno učinkovitejšemu poveljevanju, hitrejšemu odločanju in boljšemu pregledu nad dogajanjem na bojišču. Rešitve segajo od sistemov poveljevanja in nadzora do podpore brezpilotnim sistemom, elektronskemu bojevanju in jedrsko-radiološko-kemično-biološki obrambi.

Čeprav podjetje formalno deluje od leta 2010, njegove izkušnje na področju obrambnih tehnologij segajo precej dlje. Vodstvena ekipa je prve večje projekte razvijala že leta 2004 v okviru korporacije S&T, kjer so sodelovali pri razvoju taktičnih komunikacij in sistemov poveljevanja v vozilih Slovenske vojske.

DIGITALNA SLIKA SODOBNEGA BOJIŠČA

MIL Sistemika razvija sodobne programske rešitve za poveljevanje in kontrolo, ki združuje komunikacijo, senzorske podatke in lokacijske informacije v enoten operativni sistem. Omogočajo tudi digitalno sliko bojišča v realnem času. Sistem podpira tudi integracijo brezpilotnih in avtonomnih sistemov (UxV). Rešitve vključujejo analizo terena, načrtovanje poti, video prenos v realnem času in uporabo umetne inteligence za analizo podatkov.

Drugo generacijo njihovih sistemov predstavljajo rešitve »Storm«, namenjene uporabi v poveljniških centrih in na višjih ravneh poveljevanja, »Thunder«, namenjene mobilnemu operativnemu poveljevanju ter upravljanju brezposadkovnih in avtonomnih sistemov, ter »Lightning«, namenjene podpori pehoti na terenu. Podjetje pri razvoju uporablja pristop COTS (Commercial Off-The-Shelf), ki omogoča hitrejšo uvedbo osnovne rešitve in njeno prilagoditev operativnim zahtevam uporabnika.

MOČNA PRISOTNOST NA EVROPSKEM TRGU

Podjetje je usmerjeno predvsem na evropski trg, zlasti nemškega. Nepo-

sredno deluje na slovenskem, hrvaškem, avstrijskem in madžarskem trgu, drugje pa sodeluje preko partnerske mreže.

Skupino danes sestavljata dve podjetji v Sloveniji in eno na Hrvaškem. MIL Sistemika Int je v 49-odstotni lasti nemške družbe Blackned, katere večinski lastnik je skupina Rheinmetall. Podjetje MIL Sistemika, d. o. o. ostaja v 100-odstotni slovenski zasebni lasti, prek podjetja MIL Sistemika AI na Hrvaškem pa načrtujejo nadaljnjo širitev v regiji.

SPECIALIZIRANA EKIPA IN RAZVOJ

Podjetje beleži približno 30-odstotno letno rast in trenutno zaposluje okoli 40 razvijalcev, specializiranih za področje obrambnih tehnologij. Razvoj temelji tudi na dobrem razumevanju vojaških operativnih procesov in sodelovanju z domenskimi strokovnjaki z izkušnjami iz obrambnih sil.

Pomemben del njihovega delovanja predstavlja tudi sodelovanje znotraj Grozda obrambne industrije Slovenije (GOIS).

V KORAKU Z RAZVOJEM EVROPSKE OBRAMBNE INDUSTRIJE

V podjetju aktivno spremljajo razvoj evropske obrambne industrije in nove tehnološke trende, predvsem na področju navigacijskih sistemov, odpornih proti motenju, analize frekvenčnega spektra in vključevanja vesoljskih tehnologij v sodobne obrambne sisteme.

Vzpostavili so tudi Center za eksperimentiranje in digitalizacijo vojske, kjer lahko uporabniki v simuliranem okolju preverjajo različne koncepte poveljevanja, nadzora in digitalizacije operativnih procesov. Pohvalijo se lahko tudi s prvo stranko, ki ta center najema: NATO.

DEJAVNOST PODJETJA MIL SISTEMIKA

Razvoj programske opreme za:

- ★ poveljevanje in nadzor (C4I / Battlefield Management Systems),
- ★ NATO povezljivost sistemov poveljevanja in kontrole,
- ★ jedrsko, radiološko, kemično in biološko obrambo (JRKBO),
- ★ ognjeno podporo,
- ★ uporabo in integracijo brezpilotnih sistemov (UxV),
- ★ elektronsko bojevanje,
- ★ taktične in podatkovne komunikacije,
- ★ umetno inteligenco za podporo odločanju,
- ★ video prenos, hranjenje in analizo podatkov v realnem času,
- ★ analizo terena, načrtovanje poti in vojaške geoprostorske rešitve.

Prihaja prva slovenska precizna repetirna puška

NOVA RAZVOJNA ZGODBA IZ KOMENDE

Podjetje Akila iz Komende predstavlja svoj najnovejši razvojni dosežek – precizno repetirno puško Akila Eva. Gre za sodobno puško z neposrednim potegom zaklepa, namenjeno športnim strelcem, lovcem in drugim uporabnikom, ki zahtevajo vrhunsko natančnost, zanesljivost in prilagodljivost.

Podjetje Akila že vrsto let razvija in proizvaja dodatno opremo in komponente za strelno orožje različnih priznanih proizvajalcev. Bogate razvojne in proizvodne izkušnje so zdaj združili v lasten izdelek, ki predstavlja pomemben korak naprej za slovensko orožarsko industrijo.

Puška AKILA Eva je patentiran sistem, zasnovan na Remington 700 inletu, pri njenem razvoju pa je bila posebna pozornost namenjena kakovosti izdelave, natančnosti obdelave posameznih komponent in zanesljivosti delovanja. Rezultat je sodobna modularna platforma, ki omogoča širok spekter uporabniških prilagoditev.

Veliko zanimanje že pred začetkom serijske proizvodnje

V podjetju pripravljajo začetek serijske proizvodnje na podlagi predhodnih naročil. Zaradi dolgoletnega uspešnega sodelovanja s številnimi uporabniki in proizvajalci strelnega orožja so si ustvarili ugled zanesljivega in kakovostnega partnerja, zato je zanimanje za novo puško veliko že pred njenim uradnim prihodom na trg.
Akila Eva je prvenstveno namenjena športnemu strelstvu in lovu, njena modularna zasnova pa omogoča tudi razvoj specializiranih izvedb za zahtevnejše uporabnike v vojski ali policiji.
Dve izvedbi za različne potrebe

Kupcem bosta na voljo dve osnovni izvedbi puške.

Prva različica temelji na sodobni šasiji (chassis) in je namenjena predvsem taktičnemu športnemu strelstvu.
Drugi različici (Eva W in Eva M) temeljita na jeklenem ohišju kratkega sistema (short-action steel receiver). Predstavljata klasično izvedbo precizne puške za športno strelstvo ali lov in prav tako temeljita na Remington 700 inletu, ki se enostavno vgradi v katerokoli kopito na trgu. Zaradi modularne zasnove ju lahko uporabniki nadgradijo in prilagodijo svojim potrebam.

Modularnost in ergonomija

Osnovni model uporablja sodobno šasijo s pištolskim ročajem in zložljivim kopitom. Po želji ga je mogoče opremiti tudi s dvonožnikom, ki izboljša stabilnost pri opazovanju in streljanju na večjih razdaljah. Dvonožniki so na voljo v jekleni ali karbonski izvedbi.

AKILA EVA JE PRVENSTVENO NAMENJENA ŠPORTNEMU STRELSTVU IN LOVU, NJENA MODULARNA ZASNOVA PA OMOGOČA TUDI RAZVOJ SPECIALIZIRANIH IZVEDB ZA ZAHTEVNEJŠE UPORABNIKE V VOJSKI ALI POLICIJI.

Pri razvoju so bile uporabljene dolgoletne izkušnje podjetja na področju izdelave komponent in dodatne opreme za strelno orožje.

Združljivost in prihodnji razvoj

Pomembna prednost sistema Akila Eva je visoka stopnja združljivosti z deli in komponentami drugih proizvajalcev primerljivih pušk. Modularna zasnova omogoča razvoj različnih konfiguracij – od kompaktnih izvedb do visokonatančnih pušk za streljanje na večje razdalje. Poleg izvedbe s šasijo bo na voljo tudi klasična različica s polimernim ali orehovim kopitom, kar uporabnikom omogoča izbiro glede na osebne preference in namen uporabe.

V zložljivem kopitu je integriran monopod za dodatno stabilnost pri streljanju. Sistem omogoča številne ergonomske nastavitve, zato ga je mogoče prilagoditi levičarjem in desničarjem. Omogočena je tudi menjava kopita in drugih sistemskih komponent.

Dovršenost in prilagodljivost

Posebna pozornost je bila namenjena konstrukciji zaklepa, ki zagotavlja zanesljivo delovanje tudi v zahtevnih okoljskih razmerah. Sprožilni mehanizem je združljiv tudi z izdelki drugih priznanih proizvajalcev.
Uporabnik lahko izbira med različnimi vrstami nabojnikov, vključno s krajšimi izvedbami, ki omogočajo hitro menjavo brez spreminjanja strelskega položaja.
Čiščenje in vzdrževanje puške sta enostavna, kar prispeva k zanesljivemu delovanju in dolgi življenjski dobi sistema.
Neposredni poteg zaklepa je zasnovan tako, da omogoča optimalno uporabo različnih vrst streliva in ohranja visoko stopnjo natančnosti.

Korak za korakom do trga

V podjetju trenutno zaključujejo testiranja in priprave na širši nastop na domačem in tujih trgih. Dosedanji rezultati testiranj in nastopov na športnih tekmovanjih potrjujejo zastavljene razvojne cilje, zato v podjetju z optimizmom gledajo v prihodnost.
Pomembna prednost za končne uporabnike bo tudi organizirana servisna podpora, ki jo bodo zagotavljali prek mreže lokalnih partnerjev.
Akila Eva tako predstavlja pomemben razvojni mejnik za slovensko industrijo preciznega strelnega orožja. Dokazuje, da lahko tudi domače znanje in proizvodnja konkurirata najboljšim svetovnim proizvajalcem.

Grafika: Spotnet

EVROPSKE OBRAMBNE MILIJARDE: KJE JE PROSTOR ZA SLOVENIJO?

- Kdo bo pobral milijarde za obrambo?
- Zakaj so priložnosti za podjetja velike, a težje dostopne kot na običajnih trgih?
- Ali ima Slovenija strategijo, da iz tega vala dejansko nekaj pridobi?

Maja Virant

Evropa vstopa v obdobje intenzivnega vlaganja v obrambo. Ne gre več le za varnost, temveč tudi za tehnologijo, industrijo in dolgoročno konkurenčnost. V naslednjem desetletju bodo ključna področja investicij segala od zračne in raketne obrambe do umetne inteligence, kibernetske varnosti in vesoljskih tehnologij.

A ključno vprašanje ostaja: kdo bo te priložnosti znal pretvoriti v razvoj (in kdo bo ostal ob strani)?

1. Od kod se bodo delile obrambne milijarde?

Evropa že danes močno povečuje obrambne izdatke in trend se bo še okrepil. Skupna obrambna poraba držav članic Evropske unije (EU) je leta 2024 dosegla približno 343 milijard evrov, leta 2025 pa naj bi narasla na okoli 381 milijard evrov, kar je že več kot 2 odstotka BDP EU, navaja Evropska obrambna agencija (ang. European Defence Agency, EDA).

Proračun EU za obrambo je manjši, a strateško usmerjen. Po predlogu novega večletnega proračuna za obdobje 2028–34 naj bi EU v sedmih letih za obrambo in vesolje namenila približno 131 milijard evrov.

Slovenska podjetja imajo največjo priložnost v nišnih proizvodih z veliko dodano vrednostjo.«
Erik Kopač

Hkrati EU odpira nove finančne mehanizme, denimo programe za skupno nabavo in proizvodnjo streliva, sredstva za vojaško mobilnost (okoli 1,7 milijarde evrov) in nove programe za razvoj obrambne industrije (ang. European Defence Industry Programme, EDIP), navaja Svet EU (ang. Council of the European Union). Vse to kaže, da obramba postaja eno ključnih investicijskih področij v Evropi.

2. Za kaj se bodo delile obrambne milijarde?

V naslednjem desetletju bodo prioritetna naslednja področja, kot jih našteva nekdanji veleposlanik pri Natu in strokovnjak za obrambno ekonomiko Erik Kopač:

- integrirane zračne in raketne obrambe,
- povečanje industrijskih zmogljivosti za proizvodnjo artilerijskega streliva in raket,
- masovna proizvodnja miniaturnih in taktičnih dronov, izdelava lastnih strateških brezpilotnih sistemov (UAV) ter protidronskih sistemov,
- gradnja prometne infrastrukture z namenom izboljšanja vojaške mobilnosti,
- krepitev zmogljivosti za digitalno bojevanje s pomočjo umetne inteligence (UI), najnovejših komunikacijskih sistemov in kibernetske obrambe,
- proizvodnja satelitov ter drugih vesoljskih zmogljivosti za krepitev nadzora, zgodnjega opozarjanja in komunikacij.

Vodja kabineta evropskega poslanca Mateja Tonina, Vid Meglič, pri tem izpostavlja tudi strateško dimenzijo: »Pomembno vlogo imajo izkušnje z aktualnih svetovnih bojišč in odvisnost EU od ZDA.«

Če se Slovenija kot država določeni pobudi ne pridruži, potem je dostop za slovenska podjetja v veliki meri otežen.«
Klemen Grošelj

Obramboslovec in nekdanji evropski poslanec Klemen Grošelj pravi, da EU že danes vzpostavlja vrsto mehanizmov za krepitev obrambne industrije: »Na ravni EU je več pobud, katerih cilj je krepitev obrambne samozadostnosti EU in izgradnja evropske obrambne industrijske baze.«

Med ključnimi instrumenti so instrument za krepitev evropske obrambne industrije s skupnimi javnimi naročili (EDIRPA), stalno strukturno sodelovanje (PESCO) ter instrument za podporo skupnim obrambnim naložbam (SAFE).

Pri slednjih Grošelj opozarja: »Ne glede na evropsko naravo pa gre še vedno za ključno vlogo držav članic.« To pomeni, da dostop do projektov ni samoumeven: »Če se Slovenija kot država določeni pobudi ne pridruži, potem je dostop za slovenska podjetja v veliki meri otežen.«

3. Kdo lahko vstopi v obrambni posel?

Največje priložnosti za slovenska podjetja niso v velikih sistemih, temveč v specializiranih rešitvah, izpostavlja Erik Kopač: »Slovenska podjetja imajo največjo priložnost v nišnih proizvodih z veliko dodano vrednostjo.« To vključuje programsko opremo, umetno inteligenco, elektroniko, optične senzorje in precizne komponente.

Ob tem dodaja ključno omejitev: »Slovenska podjetja nikakor ne bi bila konkurenčna pri proizvodnji velikih sistemov, kot so tanki, letala in raketni sistemi.«

Pri tem po besedah Vida Megliča ni nujno, da so slovenska podjetja proizvajalec končnih produktov, temveč lahko sodelujejo z deli oziroma programsko opremo: »Ključna formula je jasna: obstoječi ali novi produkti ter partnerstva s podjetji iz drugih držav.«

Hkrati poudarja, da bodo rasli vsi segmenti – od inovacij do proizvodnje in logistike –, a za Slovenijo vidi največ priložnosti prav v inovativnih in kakovostnih nišah.

Grošelj pa opozarja, da je spekter priložnosti širši: »Pravzaprav ni področja, kjer priložnosti ne bo.« Poleg dronov izpostavlja tudi kibernetsko varnost, nove materiale in tehnologije obdelave. A hkrati poudarja realnost trga: »Kupec produktov obrambne industrije je vedno država, in nihče drug.« To pa pomeni drugačno logiko poslovanja in tudi večjo odvisnost od državnih odločitev.

Podjetja naj bodo zato zelo prodorna pri iskanju partnerstev in vstopu v projekte, svetuje Meglič: »Nova finančna perspektiva bo za potrebe obrambe in tudi transportnih poti namenjala znatna sredstva. Ključno je torej že danes iskati nova partnerstva in se pripravljati na novo realnost, ki nas že čaka za vogalom.«

4. Kakšno strategijo potrebuje Slovenija?

Slovenija ima priložnost, da iz tega investicijskega vala pridobi več kot kadarkoli doslej. »Prek Evropskega obrambnega sklada in drugih oblik financiranja lahko pride do izdatnih sredstev za razvoj,« jo izpostavlja Kopač.

Meglič opozarja, da imajo slovenska podjetja že določene izkušnje z evropskimi projekti, a bo prihodnje obdobje še intenzivnejše: nova finančna perspektiva bo namenjala znatna sredstva, pogosto pa bodo projekti zahtevali sodelovanje podjetij iz več držav.

Pri tem Slovenija potrebuje jasno strategijo ter sodelovanje države, vojske in industrije, da se podjetja vključijo v evropske obrambne dobavne verige, je prepričan Meglič.

»Pomembno vlogo imajo izkušnje z aktualnih svetovnih bojišč in odvisnost EU od ZDA.«
Vid Meglič

Obramba ustvarja nove tehnologije

Obrambne investicije imajo tudi širši učinek. »Zgodovinsko gledano so eden glavnih generatorjev civilnih inovacij,« poudarja Kopač. Med primeri navaja internet, GPS, umetno inteligenco, kriptografijo in napredne materiale.

A ta prenos ni samoumeven. Grošelj opozarja, da bo treba razviti sistem, ki omogoča prehod znanja in tehnologij iz vojaške v civilno uporabo: »Ključno bo, da bomo razvili sistem prenosa znanja in tehnologij iz obrambnega sektorja v civilni del gospodarstva.«

5. Zakaj je vstop na obrambni trg težak?

Ob pomoči sogovornikov smo preverili, kje so največje ovire za podjetja pri vstopu v obrambne projekte, in poiskali rešitve zanje.

➔ Izziv: Dostop do trga

Obrambni trgi niso odprti, opozarja Kopač. Postopki so kompleksni, dolgotrajni in pogosto zaprti, trg pa obvladujejo veliki sistemi z zaprtimi verigami.

Rešitev: Vstopa se lahko prek konzorcijev, partnerstev in EU projektov.

➔ Izziv: Fragmentacija evropskega trga

Evropski trg je še vedno razdrobljen z močnimi nacionalnimi interesi.

Rešitev: Rešitev so večnacionalni projekti (EDF, PESCO, EDIRPA).

➔ Izziv: Financiranje

Mala in srednja podjetja se spoprijemajo z izzivi zaradi visokih stroškov, tveganj in dolgotrajnih projektov.

Rešitev: EU instrumenti (EDF, InvestEU) zmanjšujejo tveganje v zgodnjih fazah, vključno s sofinanciranjem R&R, pilotnih projektov in garancij.

Pomembno je tudi povezovanje z večjimi industrijskimi partnerji, ki zagotavljajo stabilnost projektov.

➔ Izziv: Dostop do zaupnih informacij

Kopač ugotavlja, da dostop do varnostnih dovoljenj in zaupnih podatkov pogosto predstavlja dolgotrajno ali celo nepremostljivo oviro za manjša podjetja.

Rešitev: Vstopa se lahko prek večjih integratorjev, MSP pa sodelujejo kot dobavitelji komponent in programske opreme.

➔ Izziv: Certificiranje in izvozne omejitve

Standardi (na primer STANAG), certificiranje in izvozne omejitve so časovno in finančno zahtevni.

Rešitev: Evropska harmonizacija standardov ter vključevanje v certificiranje že v fazi razvoja. Klemen Grošelj pri tem dodaja, da je ključ v sistemskem pristopu države: »Brez povezovanja industrije, države in evropskih projektov preboja ne bomo dosegli.«

»Ključno bo, da bomo razvili sistem prenosa znanja in tehnologij iz obrambnega sektorja v civilni del gospodarstva.«
Klemen Grošelj

Top 5 slovenskih obrambnih projektov/investicij

1. Evropski obrambni sklad (EDF) – slovenski projekti

Vrednost: približno 8 milijard evrov (EU okvir 2021–2027; Slovenija sodeluje v več projektih).

Opis: Slovenija prek podjetij in raziskovalnih institucij sodeluje v evropskih projektih za raziskave in razvoj za obrambne tehnologije (UI senzorji, sistemi dvojne rabe).

2. Nacionalni projekti za raziskave, razvoj in inovacije obrambne industrije

(Ministrstvo za obrambo Republike Slovenije (MORS) + Tehnološki center za električno energijo in sisteme (TECES) + industrija)

Vrednost: približno 23 milijonov evrov letno.

Opis: Razvoj obrambnih tehnologij in tehnologij z dvojno rabo (denimo sistemi, materiali, energija, logistika) v sodelovanju industrije in raziskovalnih organizacij.

3. Slovenska strategija obrambne industrije

(doktrina obrambno-vojaškega sodelovanja + industrijski razvoj)

Vrednost: ni fiksna (strateški investicijski okvir države + EU sredstva).

Opis: Državno usmerjen razvoj obrambne industrije, vključno z državnimi naložbami v podjetja in raziskave, ter razvoj z namenom vključevanja v evropske dobavne verige.

4. Slovenski industrijski vstop v obrambne projekte EU

(talno strukturirano sodelovanje – PESCO)

Vrednost: del širših EU projektov (več milijard evrov skupnih programov).

Opis: Slovenija sodeluje v evropskih skupnih obrambnih projektih (interoperabilnost, razvoj zmogljivosti, skupni sistemi).

5. Industrijsko-razvojni projekti Slovenske vojske

(modernizacija + oprema)

Vrednost: več deset milijonov evrov letno (del širšega investicijskega cikla slovenske vojske).

Opis: Modernizacija vojske, razvoj domače proizvodnje opreme, prototipi in sodelovanje z domačo industrijo (denimo oborožitvene postaje, oprema, sistemi).

Viri: Evropska komisija, Ministrstvo za obrambo RS / investicijski cikli SV, Svet EU, Vlada RS (Strategija obrambne industrije).

kontron

V KONTRONU ZAGOTAVLJAJO POVEZLJIVOST KRITIČNE INFRASTRUKTURE

V kranjskem Kontronu razvijajo digitalne platforme za povezljivost kritične infrastrukture za transport, energetiko, zdravstvo ter javno varnost in obrambo, ki so ključni za delovanje države in celotne družbe.

Njihove rešitve morajo biti visoko zanesljive in suverene, da lahko v sedanjih zahtevnih geopolitičnih razmerah država deluje tudi v izrednih razmerah in da so digitalne zmogljivosti odporne, pri čemer je pomemben nadzor nad podatki in tudi platformami, da so varni. Imajo strokovnjake, ki lahko omenjene rešitve prilagodijo ter zagotavljajo razvoj in podporo čim bližje uporabnikom – v njihovi državi ali vsaj v EU.

»Naše rešitve morajo biti visoko zanesljive in suverene – da lahko v sedanjem zahtevnem geopolitičnem obdobju država deluje tudi v izrednih razmerah,« razlaga Janez Öri, izvršni direktor poslovne enote Komunikacijske rešitve v podjetju Kontron, d. o. o.

Visoko zanesljive telekomunikacijske rešitve

Kontron, d. o. o., nosilec skupine Kontron Slovenija – nekdanji Iskratel - je dolgoletni dobavitelj telekomunikacijskih rešitev, ki delujejo visoko zanesljivo. So tudi dolgoletni dobavitelj na področju komunikacij za železnice; na tem področju so v skupini Kontron AG vodilni dobavitelj.

Janez Öri, izvršni direktor poslovne enote Komunikacijske rešitve v podjetju Kontron, d. o. o., med njihovimi ključnimi rešitvami izpostavlja platformo 5G za zasebna omrežja za kritično infrastrukturo in oblačno platformo.

O Kontronu

Kontron, informacijske in komunikacijske rešitve, d. o. o., nosilec skupine Kontron SI, je vodilni evropski ponudnik celovitih in visoko zanesljivih rešitev za varno, pametno in bolje povezano prihodnost. Skupina je s širokim portfeljem informacijskih, komunikacijskih in poslovnih rešitev v kombinaciji z najhitrejšo in zanesljivo podporo prisotna v več kot 50 državah po svetu. Ima h kupcem usmerjen pristop, lasten raziskovalno-razvojni in proizvodni center ter več kot 1.000 zaposlenih v 10 državah.

Temelji na odprtokodnih tehnologijah, ki jih oblikujejo v izdelek, verificirajo in integrirajo, da so kupci deležni zanesljivih in varnih rešitev, že vnaprej pripravljenih z vsemi vgrajenimi možnostmi (Out of the Box). Na to infrastrukturo integrirajo tudi lastne aplikacije za kritične komunikacije.

Omenjene rešitve so sredi maja prikazali v okviru Demo dni: Kontron je z Demo dnevom pokazal zrelost zasebnih 5G omrežij in evropskih digitalnih tehnologij - kontron.

Digitalna povezljivost naslednje generacije

»Obstaja novi standard MCX (Mission Critical Communications), ki temelji na tehnologijah 4G in 5G, kar razvijamo v Kontronu. Imamo tudi lastne dispečerske rešitve za železnico – operativne komunikacije. Če združimo vse rešitve in platforme, dejansko ponujamo digitalno povezljivost naslednje generacije 5G in digitalno platformo Oblak (Cloud), kjer tečejo kritične aplikacije in podatki. To nadgrajujemo z umetno inteligenco (UI), saj smo prepričani, da se bo del UI preselil bliže uporabnikom in bomo na tem področju morali biti suvereni. Veliki jezikovni modeli (LLM AI) so odprti in jih je mogoče v kritičnih organizacijah usposobiti za želene namene, kar bo omogočala naša platforma,« razlaga Öri.

Avtonomnost za področje obrambe

Vsak segment kritičnih sektorjev ima svoje standarde, ki se jim v kranjskem Kontronu prilagodijo s pomočjo lastnega razvoja. Razvijajo tudi prilagoditve za področje obrambe. Certificirali so se za proizvodnjo elektronskih komponent na področju obrambe in letalske industrije. To je po sogovornikovih besedah zelo pomembno, saj so dobavne verige v kriznih razmerah pretrgane, zato suverenost prispeva k odpornosti. »Kontron lahko ponudi široko paleto sistemov, rešitev in proizvodnje za kritične segmente naše države in družbe,« razlaga Janez Öri.

5G vodilna, prihaja 6G

Ko govori o telekomunikacijski prihodnosti, sogovornik pravi, da je tehnologija 5G – poleg hitrosti – prinesla večjo prilagodljivost implementacije in možnost nadzora nad kakovostjo storitev. Prihajajoče 6G tehnologija pa bo prinesla boljšo identifikacijo lokacije naprav, senzorska omrežja, vpeljavo UI. Do njene polne vpeljave v infrastrukturo pa bo predvidoma minilo deset let.

Promo

PRIDRUŽI SE NAM TUDI TI IN POSTANI DEL EKIPE, KI VARUJE DOMOVINO

Slovenska vojska ima prav posebno poslanstvo – obrambo domovine in zagotavljanje miru. Pripadniki in pripadnice Slovenske vojske z neomajno predanostjo in pogumom branijo domovino in nacionalne interese ter demokratične vrednote. Obenem pa so vojaki nepogrešljivi pri nesebični pomoči prebivalcem ob naravnih nesrečah, kot so poplave, požari, potresi, ter ob zahtevnih reševanjih ponesrečenih v gorah.

Naš cilj je poklic vojaka in vojakinje Slovenske vojske narediti privlačen in v družbi spoštovan, ki mladim lahko ponudi veliko priložnosti za poklicno kariero in osebno rast ter je hkrati ustrezno ovrednoten.

Možnosti sodelovanja s Slovensko vojsko in Ministrstvom za obrambo

Zaposlitev – poklicni vojak, podčastnik, častnik

Vsak, ki je naklonjen dinamičnemu in timskemu delu, je odprt za pridobivanje novih znanj, je polnoleten, ima slovensko državljanstvo in je star do vključno 44. leta, je vabljen v vrste Slovenske vojske. V Slovenski vojski se lahko zaposlite tudi brez dokončane srednje šole.

S pogodbo o izobraževanju ob delu pa lahko srednjo poklicno, splošno ali srednjo strokovno izobrazbo dokončate ob delu. Kandidatke in kandidati, ki se ob sklenitvi pogodbe že izobražujejo, pa so upravičeni do povračila stroškov izobraževanja, ki so nastali pred sklenitvijo pogodbe z ministrstvom.

Slovenska vojska zaposluje več kot 60 različnih poklicev vseh profilov, v svoje vrste vabi kuharje, upravljalce dronov, mehatronike, avtomehanike, letalske tehnike, medicinko osebje, strojnike, informatike, kemike, potapljače in številne druge.

Pogodbeni rezervist

Zelo uspešni smo pri sklepanju novih pogodb za sodelovanje državljank in državljanov v pogodbeni rezervni sestavi Slovenske vojske.

Plačilo za pripravljenost v pogodbeni rezervni sestavi znaša z odsluženim vojaškim rokom 356 € na mesec, brez odsluženega vojaškega roka pa 178 € na mesec.

Prostovoljno služenje vojaškega roka

Povečalo se je tudi število udeležencev prostovoljnega služenja vojaškega roka.

Denarni prejemek za posameznika, ki uspešno v celoti opravi prostovoljno služenje, znaša 4.560 €, urejena ima osnovna zavarovanja ter lahko pridobi določene pogoje za voznika kat. B (prva pomoč, CPP, zdravniško spričevalo).

Štipendije

Izredno dobre rezultate prinaša tudi nova štipendijska politika Ministrstva za obrambo, saj smo v letu 2025 zaposlili večje število kandidatov, ki smo jih štipendirali na različnih stopnjah izobraževanja. Trenutno štipendiramo približno 860 mladih na različnih stopnjah izobraževanja, in sicer tako na visokošolskem študiju kot na srednješolskem izobraževanju.

Štipendije so med višjimi v državi in se letos gibljejo med 370 € – 592 € za dijake in 474 € – 844 € za študente in so dobrodošla finančna podpora v času šolanja ter omogočajo varno in zanesljivo zaposlitev.

Prakse

Ministrstvo za obrambo v zadnjih dveh letih povečuje tudi število mest za opravljanje obveznih praks pri izobraževanju mladih na različnih stopnjah izobraževanj. Tako smo v letu 2025 opravljanje obvezne prakse omogočili kar 115 mladim, pred tem pa je ministrstvo od leta 2017 prakso omogočalo od 5 do 36 mladim na leto.

Za šolsko leto 2025/2026 razpisujemo 69 delovnih področij za prakso v Slovenski vojski in 46 za upravni del na Ministrstvu za obrambo. Praksa je omogočena različnim poklicnim profilom in nivojem izobrazbe.

Tabori za mlade in COD izziv

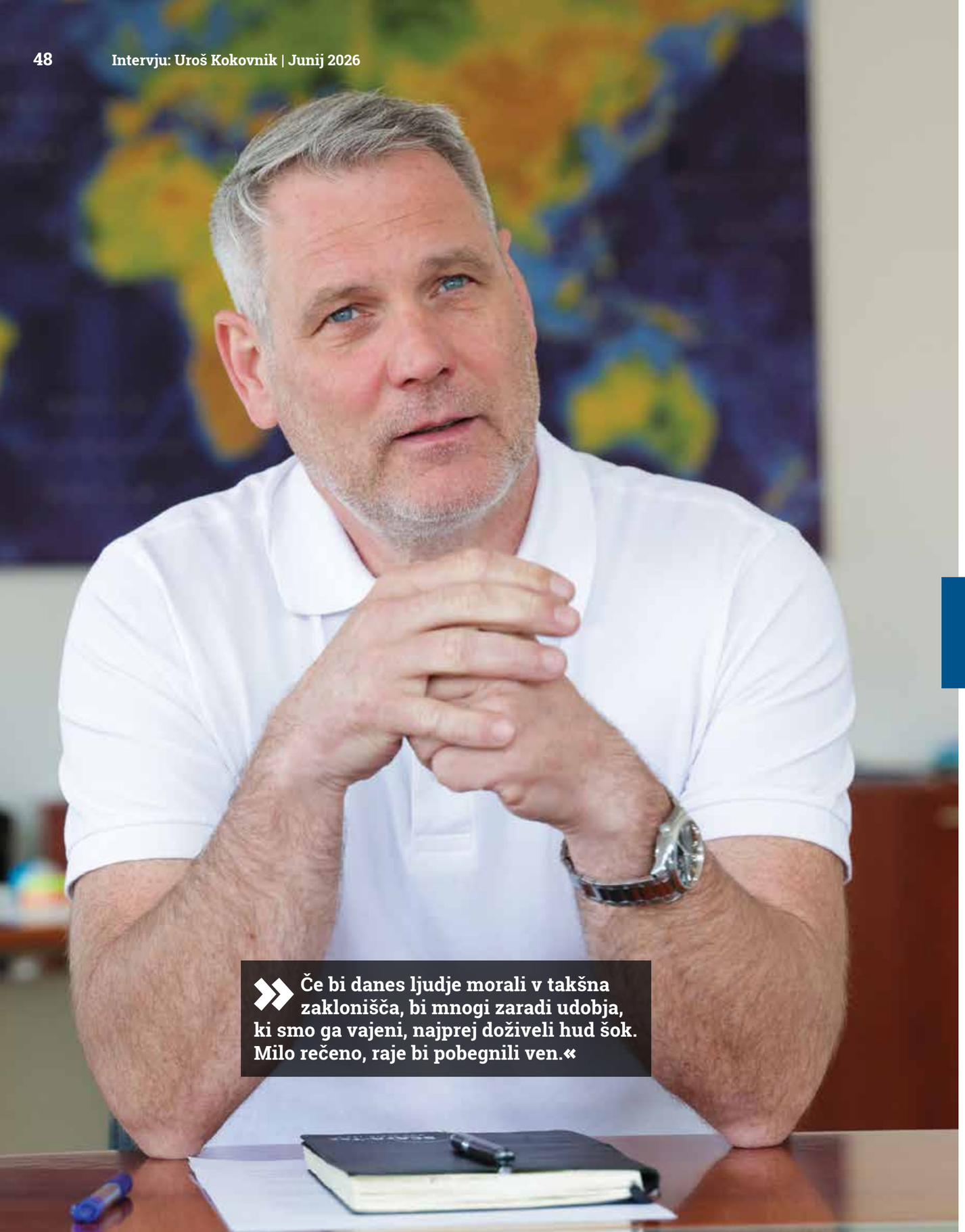
Ena izmed uspešnih oblik približevanja vojaškega poklica mladim so vojaški tabori, ki se izvajajo tako poleti kot pozimi in mladim na izviren ter prijazen način prikažejo raznovrstnost tega poklica. So tudi ena izmed oblik seznanitve s temeljnimi obrambnimi in vojaškimi veščinami za mlade državljane Republike Slovenije.
Veliko zanimanja je tudi za tridnevni vojaški izziv, prenesen iz sveta virtualnih iger v realno okolje – COD izziv, na katerega se lahko prijavijo udeleženci taborov. Predstavlja misijo elitnih vojakov, ki preigravajo različne vojaške scenarije ter preizkušajo samega sebe in svojo psihofizično vzdržljivost.

Udeležba na taborih za mlade in COD izzivu je brezplačna.

»ZAKLONIŠČE JE MOGOČE KUPITI ZA 59.000 EVROV DO 300.000 EVROV.«

- Ali veste, da je mogoče kupiti slovensko zasebno zaklonišče?
- Katero obrambno ministrstvo se zanima za te slovenske produkte?
- Ali bomo v prihodnosti živeli v hišah pod zemljo?

Goran Novković
Foto: Barbara Reya



» Če bi danes ljudje morali v takšna zaklonišča, bi mnogi zaradi udobja, ki smo ga vajeni, najprej doživeli hud šok. Milo rečeno, raje bi pobegnili ven.«

Uroš Kokovnik je direktor in lastnik podjetij Scara-Tec in Scara Group iz Slovenje vasi pri Hajdini. Med drugim se ukvarja s hibridnimi pametnimi zgradbami za varno prihodnost, statičnimi in mobilnimi zaklonišči ter z opremo za vzdrževanje in servisiranje zaklonišč z napredno avtomatizacijo. Z razvojem naprednih balistično odpornih rešitev vstopa tudi v obrambno industrijo.

Kako in zakaj je skupina Scara vstopila na področje obrambnih projektov? Je bila to strateška odločitev ali hipni odziv na razmere na trgu?

Osnovno idejo smo začeli razvijati leta 2019, v času pandemije. Začeli smo razvijati koncept celice, ki bi bila udobna za bivanje, hkrati pa bi zagotavljala visoko stopnjo varnosti, v tem primeru pred virusom covida.

Na podlagi tega je nastala tudi pametna zgradba za varno prihodnost, ki je leta 2023 prejela zlato regijsko priznanje za najboljšo inovacijo, bronasto pa na nacionalni ravni. Takrat je bilo podjetje najperspektivnejše mlado podjetje v Podravski regiji.

Čemu je namenjena pametna zgradba za varno prihodnost?

To je nov koncept vsakodnevnega bivanja ter hibrid med zaklonišcem in klasično hišo.

Zaklonišča se delijo v dve skupini. V prvo skupino sodijo javna zaklonišča, v katera se 40 let ni nič vlagalo. Javna zaklonišča so vedno namenjena minimalnim standardom preživetja. Ta minimalni standard preživetja pomeni, da je treba prilagoditi svoje življenjske funkcije na minimum, se prilagoditi drug drugemu in – tudi vonjavam, ki jih vsakodnevno izločamo.

Če bi danes ljudje morali v takšna zaklonišča, bi mnogi zaradi udobja, ki smo ga vajeni, najprej doživeli hud šok. Tega bi dopolnila panika ali kaos, zato bi mnogi milo rečeno raje pobegnili ven. Kar pa je v luči preživetja danes, ko lahko dron prileti skozi okno, bistveno drugače kot v preteklosti.

» Za naše produkte se zelo zanimajo hrvaško ministrstvo za obrambo, države Bližnjega vzhoda in Nemčija, pobude za sodelovanje pa smo prejeli tudi iz Avstralije.«

Druga skupina so zasebna zaklonišča, tudi preurejene kleti. Naša zaklonišča so tehnološko dovršena in močno presegajo minimalne standarde. Ker se drugi proizvajalci zaklonišcne opreme držijo minimuma, smo razvili tudi lastna kovinska zaklonišcna vrata, ki so zagotovo 10-krat močnejša od zahtev iz pravilnika. S podobno miselnostjo proizvajamo tudi vse druge komponente zaklonišča.

Glavni cilj ni zgolj, da lahko človek preživi nevarno situacijo, ampak da mu to ne povzroča psihološkega pritiska. Zasebno zaklonišče lahko opremimo kot stanovanje ali povsem po želji kupca. Takšno pametno zgradbo bodo navsezadnje uporabljali vsakodnevno.

Kakšno je trenutno povpraševanje po zasebnih zaklonišč doma in v Evropski uniji?

Povpraševanje se je povečalo, pri čemer so se ljudje začeli zavedati, da naše varnosti ne ogrožajo samo vojne, temveč tudi vremenske in podnebne spremembe. Mnogi razmišljajo, da bi zasebno zaklonišče kupili prav zaradi slednjih.

Imate že kupce za zasebna zaklonišča v Sloveniji?

Vsekakor. Kupci povprašujejo po različnih produktih. Eni želijo v zaklonišča preurediti svoje kleti. Drugi se odločijo za vgradnjo prefabriciranega produkta – zaklonišča. V zadnjem obdobju pa opažamo tudi povišano povpraševanje po pametnih zgradbah za varno prihodnost, ki jih načeloma ločujemo od zaklonišč.

Kakšna je hiša za varno prihodnost?

Moja vizija je, da bi gradili drugačne hiše, kot jih poznamo zdaj. Koncept hiše smo postavili na glavo. Najprej želimo, da je vsaj ničenergijska. To je mogoče le tako, da jo vgradimo v zemljo in tja postavimo bolj intimne prostore, kot so spalnice in kopalnice. V nadzemnem delu pa bi ostali prostori, ki jih uporabljamo podnevi, kuhinja z zimskim vrtom, WC in atrij s pogledom v naravo.

V takšni hiši ne potrebujemo presežkov električne energije, s katero bi pozimi morali greti, poleti pa hladiti prostore. To je hkrati pametna hiša in zasebno zaklonišče.

Povpraševanje po zakloniščih se je povečalo. Naše varnosti ne ogrožajo samo vojne, temveč tudi vremenske in podnebne spremembe.«

Kje prodate največ takšnih produktov?

Prestižnejše izvedbe so zanimive za trge Avstrije, Nemčije in Francije. Navadne pa na območjih blizu vojne, torej blizu Ukrajini: v baltskih državah, na Poljskem, tudi na Slovaškem.

Kaj je v takšnih zakloniščih tehnološko pomembno?

Zelo pomembne so tri zadeve: zrak, voda in elektrika. To so trije osnovni pogoji za bivanje človeka v izolaciji. Naša tehnologija s senzorji omogoča avtomatsko spremljanje zraka: ali je čist ali umazan, s čim je kontaminiran ... Lastni zalogovniki vode in energije pa v primeru katastrof zagotavljajo polno samooskrbo tudi v najstrožjih režimih.

Na primer, če senzorji zaznajo grožnjo kemične ali pa biološke kontaminacije, naš objekt UnderPearl obvesti lastnika in druge osebe, naj se umaknejo v zaklonišče in se hermetično zaprejo, kjer se sistem preklopi v režim popolne avtonomije – popolne izolacije od zunanjega sveta.

V popolni izolaciji, podobno kot na vesoljski postaji, sistem odvaja strupene izdihane snovi in dovaja optimalno količino kisika za normalno bivanje. Tudi vsi drugi sistemi se odklopijo iz omrežij in zunanjih sistemov ter preklopijo na polno samooskrbo.

V drugih, manj kritičnih situacijah, kjer ni potrebe po hermetični izolaciji, je zunanji zrak mogoče filtrirati, vodo pa še vedno zajemati iz omrežja. Krmilni sistemi, senzorji in zasloni nam povedo, kaj moramo narediti, tako da je upravljanje otročje lahko. Seveda pa poleg polne digitalne avtomatizacije omogočamo tudi mehansko spremljanje in upravljanje celotnega sistema.

Kdo so zasebni in kdo javni kupci teh izdelkov?

Zasebni kupci so ljudje, ki ta nakup dojemajo kot investicijo za svojo varno prihodnost, zagotavljanje nadaljevanja rodu, hkrati pa želijo povišati vrednost svoje nepremičnine. Pri javnih zakloniščih pa so investitorji večji javni sistemi, kjer investitorje zanima naša oprema, ki bi jo vgradili v ta zaklonišča.

Žal zaradi minimalnih zahtev v pravilnikih o zakloniščih ves ta napredek zasebnih zaklonišč širši javnosti ne bo na voljo, saj v skladu s pravilniki zadošča tudi 40 in več let stara tehnologija. Ljudje pa so morda tudi preveč apatični, ko se govori o njihovi lastni varnosti.

Zaklonišče je mogoče dobiti za 59.000 evrov pa do 300.000 evrov. Cene pametnih hiš za varno prihodnost pa se začnejo pri 300.000, 400.000 evrih.«

Torej želi država javna zaklonišča spraviti na vzdržno raven?

Kaj pa je vzdržna raven? Smiselno bi bilo temeljito posodobiti javna zaklonišča in jih pripraviti na naslednjih 50 let. Ampak preteklo bo še precej vode, preden se bo to zgodilo.

Kakšne želje pa imajo zasebni kupci? Ali ste naleteli na kakšno zelo nenavadno željo?

Imajo različne želje. Mi lahko vsako celico spremenimo v karkoli. Tudi v moški brlog – tam se lahko brezskrbno pokadi cigaro, pa sosed na fotelju ne bo zavohal dima.

Ena od strank je želela imeti zaklonišče z absolutno nadzorovano vlago in temperaturo. Tam je namreč želela shranjevati svoje dragocene predmete. Zaklonišče je v tem primeru služilo kot zaščita pred

kriminalom. V bistvu smo naredili velik trezor, v katerem lahko kupec z družino preživlja prosti čas in uživa v svojih dragocenostih.

Kakšne pa so cene zaklonišč in pametnih hiš za varno prihodnost?

Zaklonišče je mogoče dobiti od tistega za osnovno preživetje za 59.000 evrov pa do 300.000 evrov. Cene pametnih hiš za varno prihodnost pa se začnejo pri 300.000, 400.000 evrih.

Ali kakšna takšna hiša že stoji v Sloveniji?

Stoji. Eno hišo v Sloveniji že imamo.

Ali snujete še kakšne obrambne projekte?

Razvili smo koncept COMPOD – komandne postaje za vodenje brezpilotnih sistemov. Ta celica je balistično odporna, nadzemna, mobilna in drugačne oblike. Z več takšnimi celicami pa bi lahko oblikovali tudi mobilni kamp za dualno uporabo.

Kako sodelujete z drugimi podjetniki na obrambnem področju?

Skupaj smo na trgu močnejši, zato smo se z nekaterimi drugimi člani GOIS povezali v konzorcij. Sodelujemo tudi s podjetji, ki so že aktivna v obrambni industriji. Vsako podjetje ima ekspertize na svojem področju in s tem potencialom, ki ga povežemo skupaj, ustvarjamo izjemne proizvode, namenjene najtežjim razmeram.

Je na vidiku kakšno mednarodno sodelovanje pri takšnih produktih?

Kot skupina smo prisotni že v petih državah, tako da aktivno odpiramo nova mednarodna partnerstva. Za naše produkte se zelo zanimajo hrvaško ministrstvo za obrambo, države Bližnjega vzhoda in Nemčija, pobude za sodelovanje pa smo prejeli tudi iz Avstralije.

Je kakšna možnost, da bi se vključili v veliki evropski obrambni projekt?

Cilj je vsekakor takšen. Z enim od podjetij smo se že pogovarjali, da bi iz modularnih enot razvili visokoodporen vojaški podzemni podatkovni center.

Kaj bi svetovali podjetnikom in poslovnežem, ki razmišljajo o vstopu v obrambno industrijo?

Če se tega lotijo sami, jim ne bo uspelo. Pomembno je, da se pridružijo kakšnemu konzorciju. Zelo pomembno je, da se združita slovensko znanje in proizvodnja.

Poleg tega je to tek na dolge proge. Razmišljati je treba o dualni rabi ali celo o več možnih namenih izdelka. In zavedati se je treba, da so spremembe na tem trgu zelo hitre.

Pred tremi meseci smo imeli produkt, ki je bil takrat še zelo aktualen. Zaradi spremenjene strategije bojevanja danes že ni več tako privlačen.

Kakšno bo zaklonišče v prihodnosti, denimo čez deset let?

Mi imamo zaklonišče prihodnosti, razmere pa bodo dokončno določile, kakšen bo razvoj. Naša zaklonišča že imajo popolno avtonomijo. So povsem avtomatizirana, vsa pa imajo tudi vse potrebne funkcije za ročno upravljanje.

Nadgradnja je potem samo še v komplementarnih produktih in uporabi novih materialov. Eden takih produktov je umetni list za umetno fotosintezo. Ta je že v razvoju. S tem bi rešili vprašanje samooskrbne proizvodnje kisika. Precej pa bo narejeno tudi pri združevanju umetne inteligence in komunikacije ter pri ohranjanju civilizacijskih posebnosti ljudi.

Vrniva se še malo k ničenergijskim hišam, pri katerih bi ljudje živeli pod zemljo. Kako psihološko prepričati ljudi, da bi živeli v takšnih zgradbah?

To smo rešili že v pametnih zgradbah za varno prihodnost. Zgodovinsko gledano, ko ljudje še niso poznali klimatskih naprav in je bilo zunaj vroče, so šli z veseljem v klet, se tam družili in hkrati ohladili.

V takšni hiši ne potrebujemo presežkov električne energije, s katero bi pozimi morali greti, poleti pa hladiti prostore. To je hkrati pametna hiša in zasebno zaklonišče.«

Zdaj lahko pod zemljo že simuliramo dnevno svetlobo, UHD kamere in celostenski zasloni pa nam pričarajo svet kjerkoli nad zemljo. Vzdrževanje je minimalno. Možnost upravljanja kisika v enoti nam lahko poustvari ozračje amazonskega gozda. V ekonomskem smislu bodo v prihodnje kupci iskali rešitve, kot je naša, ker ustvarjajo presežke energije in lahko s tako stavbo celo služijo …

Kdaj bodo torej v modi?

Varnost načeloma ni modna muha, ampak skrb za nadaljevanje vrste. Če temu dodamo še varčnost, je to precej dobra kombinacija. Časovno pa se bomo morda že čez kakšnih pet let še bolj zavedali, kakšne so prednosti takšnega bivanja ob vremenskih, pa tudi geopolitičnih nihanjih.

PRIPRAVITI SE MORAMO TUDI NA ZAHTEVNEJŠE VARNOSTNE SCENARIJE

Slovenija danes deluje v bistveno zahtevnejšem varnostnem okolju kot pred desetletjem. Za večjo varnost bi morala graditi verodostojno odvračalno obrambno sposobnost, znotraj zveze NATO pa smo deležni bistveno višje stopnje varnosti kot jo lahko zagotovimo sami. O varnostnih izzivih, s katerimi se soočata EU in Slovenija, smo se pogovarjali s Katjo Geršak, vodjo Trivelis inštituta.

Katerim varnostnim izzivom je izpostavljena EU?

V Trivelis Inštitutu ugotavljamo, da se EU danes sooča z večplastnimi varnostnimi izzivi. Ruska agresija na Ukrajino je pokazala, da konflikti visoke intenzivnosti in ozemeljske ambicije v Evropi niso preteklost. Evropske države se desetletja niso pripravljale na dolgotrajen konflikt, zato danes ponovno krepijo obrambne in vojaške zmogljivosti. Hkrati pa so odprte demokratične družbe vse bolj izpostavljene hibridnim grožnjam, kot so kibernetski napadi, dezinformacije, gospodarski pritiski in poskusi spodkopavanja zaupanja v demokratične institucije in družbeno stabilnost.

Kateri so največji varnostni izzivi, ki jim je izpostavljena Slovenija?

Ocenjujemo, da tudi Slovenija danes deluje v bistveno zahtevnejšem varnostnem okolju kot pred desetletjem. Poleg možnosti vojaških groženj se sooča predvsem s hibridnim delovanjem, kot so kibernetski napadi, dezinformacije in poskusi spodkopavanja zaupanja v institucije, demokracijo in zavezništva. Takšne aktivnosti pogosto izvajajo nedemokratične države in ekstremistične skupine z namenom oslabitve evropskih družb. Zato je pomembno, da se Slovenija pravočasno pripravi tudi na zahtevnejše varnostne scenarije in okrepi obrambno pripravljenost.

»KLJUČNI SO RAZVOJ ZRAČNE OBRAMBE KRATKEGA DOSEGA, KIBERNETSKE ZAŠČITE, SAMOVODLJIVIH AVTONOMNIH SISTEMOV TER LOGISTIČNE IN ENERGETSKE ODPORNOSTI NAŠE DRŽAVE.«

»Poleg možnosti vojaških groženj se Slovenija sooča predvsem s hibridnim delovanjem, kot so kibernetski napadi, dezinformacije in poskusi spodkopavanja zaupanja v institucije, demokracijo in zavezništva,« razlaga Katja Geršak, vodja Trivelis inštituta.

Čemu bi morala Slovenija pri svoji vojaški varnosti in civilni odpornosti posvetiti največjo pozornost? Kaj bi morala razvijati?

Civilne odpornosti brez vojaške zmogljivosti ni. Zato ocenjujemo, da mora Slovenija graditi verodostojno odvračalno obrambno sposobnost z modernimi, tehnološko podprtimi in hitro odzivnimi vojaškimi zmogljivostmi. Ključni so razvoj zračne obrambe kratkega dosega, kibernetske zaščite, samovodljivih avtonomnih sistemov ter logistične in energetske odpornosti naše države. Pomembna sta tudi krepitev rezervne sestave in oblikovanje prostorskih sil ter sposobnost hitrega povečanja vojske v kriznih razmerah. Varnost danes ni le vprašanje vojske, ampak celotne odpornosti družbe in države.

V čem so razlike, če je Slovenija vključena v sistem kolektivne varnosti in če bi morala za svojo varnost poskrbeti sama? Naj se pripravlja tudi na to možnost?

Članstvo v NATO po našem mnenju Sloveniji zagotavlja bistveno višjo raven varnosti, kot bi jo lahko dosegla sama. Kolektivna obramba temelji na skupnih zmogljivostih, delitvi bremen in sodelovanju z najnaprednejšimi vojskami. Samostojna obramba bi bila dražja in manj učinkovita, kar je še posebej izrazito pri majhnih državah, kot je Slovenija. Članstvo v NATO Sloveniji zagotavlja pomembno varnostno oporo, vendar nas to ne sme uspavati. Tudi znotraj zavezništva mora vsaka država skrbeti za lastno pripravljenost, zaščito prebivalstva, ključnih sistemov in ozemlja ter aktivno prispevati k skupni varnosti.

Na kakšen način lahko k sistemu varnosti in odpornosti Slovenije prispevate v Trivelis Inštitutu?

V Trivelis Inštitutu želimo prispevati k razvoju resnega razmisleka o varnosti, odpornosti in obrambe v Sloveniji. Povezujemo domače in mednarodne strokovnjake ter pripravljamo poglobljene strokovne analize, spodbujamo sodelovanje in odpiramo razprave o vprašanjih, ki bodo odločala o dolgoročni varnosti tako slovenske države kot celotne družbe. Verjamemo, da je varnost skupna družbena odgovornost, zato želimo krepiti razumevanje sodobnih varnostnih izzivov in prispevati k razvoju zanesljivega in učinkovitega sistema varnosti Slovenije.

ČLANSTVO V ZVEZI NATO SLOVENIJI ZAGOTAVLJA VIŠJO RAVEN VARNOSTI, SAJ TEMELJI NA KOLEKTIVNI OBRAMBI, SKUPNIH ZMOGLJIVOSTIH IN SODELOVANJU Z ZAVEZNIŠKIMI DRŽAVAMI.

Grafika: Spotnet

Lani so zabeležili že več kot 97 milijard poskusov izkoriščanja.

INTENZIVNOST KIBERNETSKIH NAPADOV JE ŠOKANTNA!

- Kako pripravljena so slovenska podjetja na povečano število kibernetskih napadov?
- Zakaj postajajo napadi vse bolj prepričljivi in nevarni, tudi za izkušene zaposlene?
- Kaj lahko podjetja naredijo takoj, da zmanjšajo tveganje za resno škodo?

Simona Drevenšek

Aprila letos je javna Agencija za civilno letalstvo doživela nepooblaščen vdor v spletno aplikacijo UAS repozitorij, pri katerem naj bi napadalci pridobili osebne podatke pilotov in operaterjev dronov. To odpira vrata za morebitne zlorabe. Leta 2024 sta bila tarča napadov tudi slovenska zdravstvena ustanova in podjetje LTH Castings, napadi pa so povzročili motnje v delovanju sistemov.

Od vojaških sistemov do e-trgovine in zdravstvenih sistemov – kibernetski napadi predstavljajo eksistenčno grožnjo za vsako organizacijo. Če tem nevidnim sovražnikom do zdaj niste posvečali pozornosti, bi jo verjetno morali. Kibernetski napadi so v porastu in strokovnjaki pričakujejo, da se bodo v prihodnjih letih le še stopnjevali.

V digitalni dobi, kjer so podatki in povezljivost srce poslovanja, postaja varnost ključni dejavnik konkurenčnosti in stabilnosti. Kako kibernetsko varna so slovenska podjetja? Kaj lahko storijo, da zaščitijo svoje poslovanje pred vedno bolj prefinjenimi napadi?

Trenutno izstopajo napadi na oblačne storitve, kot je Microsoft 365, ki so postale osrednja infrastruktura poslovanja.«
Matej Matija Grobelšek

1. Zlonamernih pregledov na sekundo kar 36.000: pritisk na podjetja narašča

Življenjski cikel kibernetskih groženj se hitro krajša, napadi pa postajajo vse bolj usmerjeni v ključne poslovne platforme, kot so oblačne storitve, denimo Microsoft 365, ki danes predstavljajo osrednjo infrastrukturo številnih podjetij.

Intenzivnost napadalnih aktivnosti je šokantna. Avtomatizirano kibernetsko izvidništvo je močno naraslo, kaže Fortinetovo poročilo FortiGuard Labs 2025 o globalnih kibernetskih grožnjah. Napadalci so izvajali približno 36.000 zlonamernih pregledov na sekundo, kar je 16,7-odstotno povečanje v primerjavi z letom 2024. Zabeležili so tudi več kot 97 milijard poskusov izkoriščanja.

Na te izzive odgovarja tudi evropska regulativa. Direktiva NIS2, sprejeta leta 2022, od srednjih in velikih podjetij v ključnih sektorjih zahteva bolj sistematično upravljanje kibernetskih tveganj, zaščito informacijskih sistemov in učinkovito odzivanje na incidente. V praksi to pomeni uvajanje preverjenih pristopov, kot jih opredeljujejo mednarodni standardi za upravljanje informacijske varnosti in neprekinjenega poslovanja.

Vendar, kot opozarja direktor za poslovni trg v A1 Slovenija Matej Matija Grobelšek, sama skladnost z regulativo še ne zagotavlja dejanske odpornosti: »Organizacije pogosto izpolnijo zahteve zgolj formalno, ne da bi bistveno izboljšale svoje varnostne prakse.« Ključna razlika se pokaže šele ob incidentu.

Glavna napaka podjetij je, da varnost obravnavajo kot enkraten projekt, ne kot stalen proces. Med najpomembnejšimi ukrepi so:

Število incidentov se je povečalo za 35 odstotkov. Glavni razlog je hitrejša priprava prepričljivejših sporočil s pomočjo UI, brez očitnih slovničnih in slogovnih napak.«
Gorazd Božič

- redni in poglobljeni varnostni pregledi, ki razkrijejo dejanske ranljivosti,
- kombinacija tehničnih zaščitnih mehanizmov in ozaveščenosti zaposlenih,
- sprotno spremljanje novih groženj ter hitro posodabljanje sistemov,
- sodelovanje s specializiranimi ponudniki in odzivnimi centri.

Kot kaže praksa, je največ težav še vedno povezanih z osnovami – od neustrezno upravljanih dostopov do zastarelih sistemov. Prav tu pa so tudi največje in najhitreje dosegljive izboljšave.

2. IT slovenskih MSP je še vedno omejen na ...

V Sloveniji podjetja niso nujno pogosteje tarča napadov kot drugod po Evropi, razlika pa se kaže v pripravljenosti in odzivnosti. Kot pojasnjuje Matej Matija Grobelšek, imajo večja podjetja sicer pogosto vzpostavljene osnovne varnostne mehanizme, vendar med formalno skladnostjo in dejansko operativno odpornostjo ostaja pomemben razkorak.

»Prava odpornost se pokaže šele ob incidentu – pri hitrosti zaznave, jasnosti odločanja in sposobnosti omejevanja škode,« poudarja sogovornik.

Ta razkorak je še izrazitejši pri malih in srednje velikih podjetjih. Kot opozarja Gorazd Božič iz SI-CERT, imajo ta pogosto omejene vire in znanje: IT je praviloma omejen na osnovno vzdrževanje, celostno upravljanje varnosti pa ostaja zapostavljeno. Omrežja so pogosto slabo segmentirana, zaznavanje incidentov pomanjkljivo, odzivni načrti pa neobstoječi.

Prav manjša podjetja so zato med bolj ranljivimi; ne zato, ker bi bila manj pomembna, temveč ker imajo šibkejše varnostne temelje. Odpornejša so podjetja iz strogo reguliranih panog, kot so bančništvo, kritična infrastruktura in drugi sektorji z jasno določenimi varnostnimi zahtevami, kjer so postopki, nadzor in dobre prakse vzpostavljeni bolj sistematično.

Napadalci so lani izvajali približno 36.000 zlonamernih pregledov na sekundo, kar je 16,7-odstotno povečanje v primerjavi z letom 2024.

3. Ko kliče »direktor«, pa je to v resnici umetna inteligenca ...

Kljub tehnološkemu napredku ljudje pogosto ostajajo najšibkejši člen v varnostnem sistemu. Uporaba umetne inteligence (UI) je močno spremenila način izvedbe kibernetskih napadov, predvsem phishinga in spletnih goljufij.

Gorazd Božič, vodja Nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, ki deluje v okviru javnega zavoda Arnes, pravi, da se je število incidentov lani povečalo za 35 odstotkov v primerjavi z letom 2024. K temu je nedvomno pripomogla tudi uporaba orodij UI. »Glavni razlog je hitrejša priprava prepričljivejših sporočil brez očitnih slovničnih in slogovnih napak, zaradi česar prejemniki lažje nasedejo,« pojasnjuje Božič.

Dodatno k uspešnosti prispeva množična personalizacija, ki je bila prej težje izvedljiva: »Napadalci lahko danes avtomatizirajo velik del procesa – od priprave vsebine in zbiranja podatkov do lokalizacije in množičnega pošiljanja sporočil.« Zato bistveno lažje izvajajo napade večjega obsega na več trgih hkrati.

V dobi generativne UI postaja kombinacija ozaveščenih zaposlenih in tehničnih zaščitnih ukrepov ključni pogoj za kibernetsko odpornost, poudarja Grobelšek.

Gorazd Božič še dodaja, da so do zdaj zaznali dva primera, kjer so tehnologijo ponarejenega posnetka z UI (deepfake) uporabili za simuliranje glasov: »V obeh primerih so uporabili glas direktorja, a so v podjetju hitro ugotovili, da se izraža nenavadno.« V dobi generativne UI je zato kombinacija ozaveščenih posameznikov in ustreznih tehničnih zaščitnih ukrepov ključna za kibernetsko odpornost.

KAKO Z RADIJSKIM SISTEMOM ZARE NEPOSREDNO KOMUNICIRATI Z ZRAKOPLOVI?

Slovensko podjetje Elektronika Naglič je z razvojem vmesnika RAIM-4000 omogočilo neposredno komunikacijo med ekipami na terenu in posadkami zrakoplovov prek sistema ZARE. Gre za rešitev, ki pomembno izboljšuje usklajevanje med intervencijami in povečuje varnost vseh sodelujočih.

Izziv komunikacije med tlemi in zrakom

Reševalci in gasilci za komunikacijo med intervencijami uporabljajo radijski sistem ZARE, ki ga načrtuje, gradi in nadgrajuje URSZR. Že dlje časa se je pojavljal izziv, kako vzpostaviti neposredno komunikacijo z zrakoplovi, ki jih v Sloveniji upravljata SV in Policija.

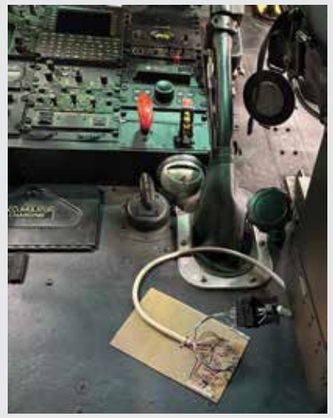
Med postopno digitalizacijo sistema ZARE se je ob prenovi helikopterjev Slovenske vojske pojavila ideja o učinkoviti rešitvi – vgradnji radijske postaje Motorola DM4600e neposredno v zrakoplove. Posadka bi tako lahko neposredno komunicirala z gasilci in reševalci prek istih kanalov, ki jih uporabljajo ekipe na terenu.

Po uspešno izvedenih postopkih certificiranja za vgradnjo radijske postaje v helikopter pa se je ob prvem preizkusu pokazala pomembna težava: ko je pilot komuniciral prek nove radijske postaje, ga kopilot ni slišal, kar je z vidika varnosti predstavljalo nesprejemljivo tveganje.

S tem izzivom so predstavniki SV stopili v stik z Miroslavom Nagličem, ustanoviteljem in prokuristom podjetja Elektronika Naglič, ki je kot izkušen pilot dobro razumel težavo. V podjetju so razvili tehnično rešitev in jo prek videokonference predstavili družbi RUAG v Švici, ki izvaja predelave zrakoplovov.

Tehnična rešitev za večjo varnost in učinkovitost

»Predlagana rešitev je bila dobro sprejeta, zato smo v najkrajšem možnem času pristopili k razvoju vmesnika. Prvi razvojni model smo izdelali na prototipni ploščici, julija 2025 pa sem osebno sodeloval pri prvem preizkusu koncepta v Švici, kjer je sistem deloval natanko tako, kot smo si zamislili.« pojasnjuje sogovornik.



Prototip, ki je bil preizkušen v Švici.

Končni produkt v ohišju iz kromatiranega aluminija.

Sledili so razvoj do končne izvedbe, priprava obsežne tehnične dokumentacije in zahtevni postopki certificiranja, saj mora vsak element letalske opreme ustrezati strogim varnostnim in tehničnim standardom. Podjetje RUAG je pred vgradnjo izvedlo podroben pregled vmesnikov in dokumentacije ter nato odobrilo in izvedlo njihovo integracijo v zrakoplove. »Komunikacija bo s tem vmesnikom hitrejša, zanesljivejša in brez nepotrebnih zapletov, kar predstavlja pomemben doprinos k učinkovitosti intervencij in predvsem k večji varnosti ekip na terenu in posadk v zrakoplovih,« ob tem še dodaja Naglič.

Razvita rešitev ne predstavlja le povezave med zrakoplovi in sistemom ZARE. Z ustreznimi prilagoditvami bi jo bilo mogoče uporabiti tudi za komunikacijo z radijskimi napravami v sistemu TETRA, s čimer se odpirajo dodatne možnosti uporabe v varnostnih, reševalnih in drugih kritičnih okoljih.

Miroslav Naglič, ustanovitelj in prokurist podjetja Elektronika Naglič.

SLOVENSKA OBRAMBNA INDUSTRIJA SE VZTRAJNO KREPI

Država ji pomaga s spodbujanjem razvoja specializiranih in nišnih proizvodov, ki dosegajo visoko raven tehnološke razvitosti ter usmerja s strategijo obrambne industrije in tehnološke baze.

Obrambna industrija ima v Sloveniji dolgo tradicijo, čeprav po obsegu nikoli ni bila primerljiva z nekaterimi drugimi gospodarskimi panogami. Geopolitične spremembe in aktualna krizna žarišča so tudi pri nas povzročili velike premike v zavedanju, da se moramo opreti predvsem na domače znanje in sposobnosti ter pospešen razvoj obrambnih proizvodov razumeti kot novo realnost ter poslovno priložnost na širšem evropskem in svetovnem trgu. Tako bo Ministrstvo za obrambo Republike Slovenije (MORS), skladno s Srednjeročnim obrambnim programom 2026–2031, samo letos za podporo raziskovalno-razvojnim in inovacijskim (RRI) aktivnostim na nacionalni in mednarodni ravni namenilo več kot 29 milijonov EUR, tovrstna sredstva pa se bodo v prihodnih letih še dodatno zviševala.

Razvoj specializiranih in nišnih proizvodov

MORS si z RRI aktivnostmi prizadeva spodbujati podjetja, da samostojno ali v okviru projektnih konzorcijev razvijajo specializirane in nišne proizvode, ki dosegajo visoko raven tehnološke razvitosti (TRL). Tako lahko hitreje prestanejo potrebna testiranja in se uvedejo v operativno uporabo enot Slovenske vojske ali sistema zaščite in reševanja. Na ta način pridobijo ustrezne in pogosto zahtevane reference, saj imajo izpolnjene pogoje za prehod v serijsko proizvodnjo in so pripravljeni za lansiranje na mednarodnih trgih.

Treba je združiti moči

Generalno gledano (tudi) v Sloveniji zaznavamo negativne učinke velike razdrobljenosti (evropske in svetovne) obrambne industrije ter prepoznavamo smiselnost in racionalnost njenega poenotenja, ki bi se izvajalo skozi napore in procese skupnega razvoja, skupne proizvodnje in skupnega vzdrževanja (co-development, co-production and co-sustainment). Na ta način bi prišlo do poenotenja velikega števila različnih platform na posameznih segmentih, kar bi v smislu standardizacije znatno prispevalo k izboljšanju interoperabilnost in izmenljivosti (interchangeability).
Na MORS verjamejo, da na vseh naštetih področjih pomembno vlogo lahko prevzamejo tudi slovenska podjetja obrambne industrije, saj se številna visokotehnološka, mala in srednje velika podjetja naglo prilagajajo, z visoko usposobljenim, izobraženim in motiviranim kadrom pa se lahko specializirajo ter pospešujejo in spodbujajo inovacije.

Vpeti v evropske ustanove

V mednarodnem okolju MORS aktivno sodeluje v Evropskem obrambnem skladu (EDF), ki ima pomembno vlogo pri spodbujanju inovacij in sodelovanja pri razvoju obrambnih tehnologij in zmogljivosti. EDF vsako leto objavi razpis, na katerem redno kandidirajo slovenska podjetja in različne institucije, ki jih MORS podpira z organizacijo informativnega dne in pismi podpore.
V letu 2025 je bilo v okviru EDF izbranih 57 raziskovalnih projektov in razvojnih aktivnosti, pri čemer pri šestih sodelujejo slovenski deležniki, usmerjeni pa so na posamezna ključna področja, ki obsegajo umetno inteligenco, kibernetsko obrambo ter brezpilotna letala in sisteme za boj proti njim.
Podobno velja tudi za RRI v okviru Evropske obrambne agencije (EDA), pri čemer MORS ozavešča o priložnostih in spodbuja vključevanje novih prodornih podjetij. Različne naložbe so zasnovane z namenom, da EU (p)ostane vodilna na področju napredne obrambne tehnologije.
Tehnološko suverenost, naprednost in kakovost so slovenska podjetja dokazala tudi v okviru razpisa Nato pospeševalnika DIANA (Defence Innovation Accelerator for the North Atlantic), saj je bilo med več kot 3.600 prijavami nekaj manj kot 100 slovenskih. Izbrali so 150 podjetij, od katerih tri prihajajo iz Slovenije. Hkrati nekateri slovenski laboratoriji prevzemajo vlogo t. i. DIANA testnih centrov.

Krepitev odpornosti države

Vzporedno pa nacionalne RRI aktivnosti podpirajo predvsem izgradnjo zmogljivosti in operativno delovanje obrambnih sil, s čimer imajo pomemben vpliv tudi na odpornost države. Večje število projektov pa je tudi t. i. dvojne rabe (dual-use), torej namenjenih tako vojaški kot civilni rabi, kar prinaša dodano vrednost za širšo družbeno skupnost. Hkrati se neposredni učinki izvajanja RRI dejavnosti kažejo v medsebojnem sodelovanju države, znanstveno-raziskovalnih sferah in nacionalni obrambni industriji.
Nedavno zaključeni RRI projekti, kot so daljinsko vodene oborožitvene postaje, aktivne prikolice za taktična vozila, trenažerji in simulatorji, multispektralna kamuflaža in večnamenska platforma na hibridni pogon (VEPKOV, na sliki) so primeri dobre prakse, kako znanje, kreativno razmišljanje, inovativnost, prodornost in močna partnerstva prinašajo napredne in prebojne proizvode, ki postajajo prepoznavni in zanimivi tudi na mednarodnem trgu.

Strategija razvoja obrambne industrije in tehnološke baze v Republiki Sloveniji

Lani je bila sprejeta prva Strategija razvoja obrambne industrije in tehnološke baze v Republiki Sloveniji, katere namen je spodbujanje in krepitev slovenske obrambne industrije, njenega vključevanja v širše mednarodno okolje oz. globalne dobavne verige ter njenega prispevka k Evropski obrambni tehnološki in industrijski bazi (EDTIB).

Močna obrambna industrija bo trgu ponudila večjo razpoložljivost obrambnih proizvodov in storitev, s čimer se bodo skozi zanesljivost dobavnih verig in oskrbe dodatno okrepile samozadostnost, neodvisnost in odpornost države.

Strategija postavlja jasne usmeritve za prihodnji razvoj nacionalne obrambne in varnostne industrije s poudarkom na industrializaciji razvojnih projektov. Hkrati spodbuja vključevanje malih in srednjih podjetij (SME) v mednarodni prostor in ustvarjanje konkurenčnih pogojev, še posebej z različnimi oblikami financiranja in strateškimi vlaganji v domača podjetja v obrambni panogi.

DOVOS za razvoj in trženje novih izdelkov

Na podlagi Strategije je bila ustanovljena gospodarska družba DOVOS (Družba za obrambo, varnost in odpornost Slovenije), katere namen je s strateškimi naložbami v ključna slovenska podjetja v obrambni panogi podpirati razvoj, industrializacijo in trženje proizvodov ter storitev s področij obrambe, varnosti in odpornosti, s tem pa krepiti obrambne in varnostne sposobnosti države ter pozitivno prispevati k splošnemu gospodarskemu razvoju.

SIDEC 2026 letos v novembru

Slovenska podjetja se ob podpori GOIS in SPIRIT redno udeležujejo mednarodnih oborožitvenih sejmov – tako bodo sredi junija prisotni na sejmu EUROSATORY v Parizu. V mesecu novembru pa se ponuja ponovna priložnost za razstavljanje na domačih tleh. Ob izjemnem uspehu lanskega sejma, ki je po številu razstavljavcev in obiskovalcev močno presegel pričakovanja, bo mednarodni oborožitveni sejem s spremljajočim konferenčnim delom – SIDEC ponovno potekal letos, in sicer od 10. do 12. novembra na Celjskem sejmišču.

KIBERNETSKI NAPAD 2030: »VIDETI BO KOT SPOPAD PREDATORJA IN TERMINATORJA.«

- Ali veste, da vaša ukradena gesla na črnem trgu stanejo le 10 evrov?
- Kaj vse bo omogočala umetna inteligenca pri kibernetskih napadih?
- Zakaj ste v nevarnosti, četudi ste majhen dobavitelj kritične infrastrukture?

Goran Novković
Foto: Barbara Reya

Milan Gabor je etični heker, direktor in lastnik podjetja Viris, ki skrbi za informacijsko varnost: simuliranje kibernetskih vdorov, preglede aplikacij in sistemov, varnostno testiranje ter izobraževanje ljudi in podobno. Odlično pozna kibernetsko varnost in trende kibernetskih napadov.

Katere so tri največje kibernetske grožnje za slovenska podjetja v bližnji prihodnosti?

Vsekakor bo to izsiljevalska škodljiva koda, torej kraja in odtujevanje podatkov, njihovo šifriranje in potem izsiljevanje glede odkupnine. Druga grožnja bo še naprej kraja identitete in dostop do podatkov.

Močnejša grožnja kot doslej pa bo posreden napad na dobaviteljsko verigo. V tem primeru je napaden dobavitelj, ki je lahko dobavitelj programske ali strojne opreme za kritično infrastrukturo, namesto same kritične infrastrukture.

Koliko so danes na črnem trgu vredni podatki osebe, ki so ukradeni s hekerskim napadom?

Podatki za dostope, kot so gesla in uporabniška imena, ki nam jih napadalci poberejo, so na črnem trgu vredni okoli deset dolarjev. Podatki ključnih oseb pa so seveda lahko dražji.

Ali to pomeni, da so naši identitetni podatki najcenejši v zgodovini? 🙂

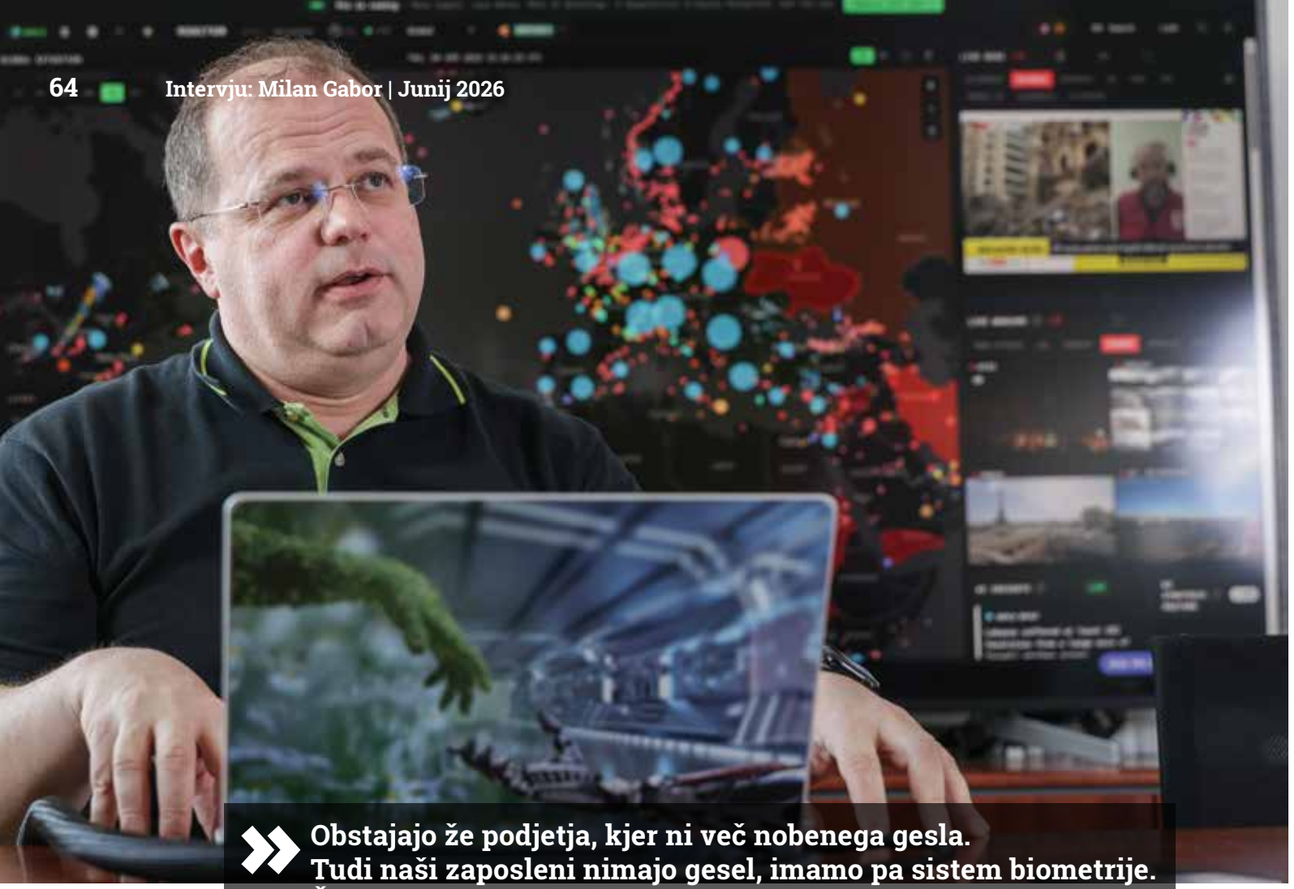
Lahko bi tako rekli, saj so dejansko zelo poceni. Kadar ljudi vprašamo, koliko so po njihovem mnenju vredni takšni podatki na črnem trgu, navadno rečejo, da okoli sto dolarjev. Realnost pa je seveda drugačna.

Ali podjetniki in podjetja v Sloveniji kibernetsko varnost še vedno podcenjujejo? Katere so njihove največje napake, kar zadeva skrb za kibernetsko varnost?

Obstajata dva tipa podjetij: regulirana, ki morajo za kibernetsko varnost skrbeti po zakonu, ali na primer finančne ustanove, in druga podjetja, ki za to večinoma začnejo skrbeti, ko se kaj zgodi. Pred dvema letoma smo imeli dobro pobudo države, ki je podjetjem za spodbudo ponudila kibernetske vavčerje. Tako smo poskrbeli za varnost mnogih malih in srednjih podjetij (MSP). Zdaj že skoraj tri leta čakamo na nove vavčerje.

Ali so prav ta podjetja največja rak rana naše kibernetske varnosti? Koliko hekerji napadajo kritično infrastrukturo, koliko pa MSP in samostojne podjetnike?

»Po mojem mnenju se bo leta 2030 napadalni agent UI kibernetsko boril z obrambnim agentom UI.«



Obstajajo že podjetja, kjer ni več nobenega gesla. Tudi naši zaposleni nimajo gesel, imamo pa sistem biometrije. Če greste stran od računalnika, se ta samodejno zaklene.«

Hekerji pri internetnem napadu na velika ali mala podjetja uporabljajo isto programsko opremo; napadejo lahko vse. Prav pri MSP je še vedno veliko šibkih gesel, kibernetska varnost in kibernetska higiena pa sta tam slabši. Še vedno ni povsod večfaktorskih avtentifikacij. Veliko je tudi starejše programske opreme, ki ni vedno posodobljena.

Ampak vsa ta gesla in avtentifikacije postajajo digitalizacijska džungla, ki gre uporabnikom vse bolj na živce. Bi bilo zaščito mogoče nekako standardizirati z uporabnikom prijaznejšimi rešitvami, ne pa da nenehno menjavamo gesla in podobno?

Zdajle je moj računalnik zaklenjen. Zdaj pa je odklenjen. Ste vmes videli, da sem vpisal geslo?

Ne. Torej tehnologijo imamo?

Da, tehnologijo imamo, brez gesel. Vstopimo lahko s prepoznavo obraza, s prstnim odtisom in tako naprej. Obstajajo že podjetja, kjer zaposleni nimajo več nobenih gesel. Imamo pa sistem biometrije; če greste stran od računalnika, se ta samodejno zaklene, vendar to uporabljajo le redki.

Kako se spreminja profil napadalcev? So vse bolj poslovno organizirani?

Veliki igralci v kriminalnem podzemlju so organizirani kot prava podjetja. Tam so vodje skupine, pisci škodljivih kod, iskalci ranljivih žrtev, tudi denarne mule, ki skrbijo za pranje denarja. Okrevanje žrtev kibernetskih napadov takšnih napadalcev lahko traja tudi mesece. Univerza v Mariboru je po kibernetskem napadu potrebovala mesec dni, da si je opomogla.

Kako pomembna bo umetna inteligenca (UI) pri hekerskih napadih in obrambi pred njimi?

Napadalci lahko uporabljajo UI brez omejitev. Vemo, da se zdaj pripravljajo pravila etične uporabe UI. A napadalci jih ne bodo upoštevali, zato so vedno malo v prednosti. UI uporabljajo predvsem zato, da izboljšajo napade in da so hitrejši.

Zdaj vas lažje napadejo z eno verzijo napada, mene pa z drugo. Napadi postajajo bolj prilagojeni posamezni žrtvi, prej pa so eno vrsto napada uporabili za vse. Zdaj lahko vsakega zaposlenega napadejo drugače, in sicer tako, da se podučijo o vsakem posamezniku. To bo zanimivo, ker tudi na obrambni strani z UI prihajajo nova orodja za obrambo.

Kdo bo z uporabo imel večjo prednost? Napadalci ali obramba?

Napadalci, ker nimajo regulatornih in etičnih omejitev. Pri obrambi morate denimo upoštevati varstvo osebnih podatkov, zakonodajo in druga priporočila.

Kateri kibernetski scenarij vas najbolj skrbi v naslednjih treh do štirih letih?

Kraje gesel, nato pa se z UI ta gesla na vse možne načine izrabi za dostop do kritičnih sistemov in obide tudi najboljše zaščite. Nihče ne ve, kako se bodo kibernetski napadi razvijali z UI.

Danes imamo UI agente, ki vse korake naredijo v enem. Lahko celo izpeljete hekerski napad na podjetje, ne da bi kaj vedeli o tehnologiji. Agentu UI poveste, kdo je primarna tarča, on pa zna napad pripraviti in izpeljati sam.

Ali vse to pomeni, da lahko pričakujemo bolj množične napade kot doslej?

Ja, napadi bodo bolj množični. Ena od verzij UI je denimo našla ranljivosti v 26 let stari programski opremi, ki jih doslej ni našel nihče. Ne bodo je dali niti v javno uporabo, ampak so jo dali določenim pomembnim podjetjem, na primer Applu, Microsoftu, Googlu, da najdejo vse ranljivosti pri sebi. Napisala je namreč takšno izkoriščevalsko kodo, da se je bojijo. To verzijo bodo uporabili za reševanje problemov. A nekoč bi lahko kaj takšnega kdo uporabil za drugačne namene.

Ali je morda dobra novica vendarle ta, da so z UI vojaški cilji merjeni bolj natančno in bo tako manj žrtev vojn? Ker z napadi na kritično infrastrukturo se tako doseže velik učinek.

Ukrajinci so ob ruskem napadu na Krim leta 2014 uspešno izklopili četrtino tamkajšnjega električnega omrežja. A tudi danes v vojnah ljudje umirajo ob napadih z droni. Z njimi bi bilo možno napasti Maribor ali Ljubljano tako, da je žrtev več, kot bi jih bilo pri napadu s kasetno bombo.

Kako lahko podjetja poskrbijo za najbolj učinkovito kibernetsko varnost?

Ni se veliko spremenilo. Še vedno je treba paziti pri geslih; ta so najšibkejši člen. Podjetje mora biti zaščiteno z nekim požarnim zidom … V zadnjih letih pa so napadalci bolj pozorni na arhive. Podjetjem pogosto poskušajo odvzeti celoten arhiv, torej 'backup', in jim ga pobrisati, tako da podjetje ne more okrevati.

Danes imamo UI agente, ki vse korake naredijo v enem. Izpeljete lahko celo hekerski napad na podjetje, ne da bi kaj vedeli o tehnologiji.«

Močnejša grožnja kot doslej bo posredni napad na dobaviteljsko verigo. Napaden bo dobavitelj programske ali strojne opreme za kritično infrastrukturo.«

Kaj je rešitev: ločeno shranjevanje arhiva ali kaj drugega?

Ja, ločeno omejevanje dostopa do arhiva in več načinov arhiviranja.

Je varno, da ga imajo podjetja v oblaku?

Ne ravno. Tudi to je možnost, vendar je arhiv oziroma 'backup' dobro najprej imeti nekje shranjen lokalno, še bolje dislocirano. Nekateri jih shranjujejo celo na kasetah na dislocirani enoti. Res pa to pomeni, da mora nekdo to fizično početi sproti, tudi vsak dan.

Malo analogne telovadbe v digitalni dobi. 😊

Lahko se zgodi, da boste pri hrambi v oblaku zaradi omejene pretočnosti potrebovali dva tedna, da iz njega potegnete vso količino podatkov. Vse to so izzivi, ki jih je treba upoštevati.

Kolikšna pa je cena kibernetske varnosti?

Američani pravijo, da je ta cena nekaj odstotkov letnih prihodkov, če želite biti zaščiteni z najsodobnejšimi sistemi zaščite. A večinoma podjetja za ta namen uporabljajo zunanje partnerje. Če oprema, ki ste jo kupili, ni primerno konfigurirana, ni nujno, da pomaga. Sicer pa najdražje ni vedno najboljše.

Na kaj naj bodo v svojem kolektivu pozorni direktorji, ki niso strokovnjaki za kibernetsko varnost?

Malo naj se sprehodijo in pogledajo, kje imajo zaposleni na delovnem mestu kaj zapisano. Pod tipkovnicami ali na monitorjih so morda še nalepljeni listki z gesli. Prav na enem zadnjih testov smo ga našli na robu mize.

Na koliko časa je dobro menjati gesla?

Odvisno od tega, kako dolga so gesla. Če imajo po osem znakov, jih je treba menjati redno, vsakih nekaj mesecev. Če pa imate daljša gesla in druge začetne mehanizme, potem je dovolj enkrat na leto oziroma je to seveda odvisno tudi od varnostne politike, občutljivosti gesel in drugih dejavnikov.

Veliki igralci v kriminalnem podzemlju so organizirani kot podjetja. Tam so vodje skupine, pisci škodljivih kod, iskalci ranljivih žrtev in tudi denarne mule, ki skrbijo za pranje denarja.«

Kateri je bil najbolj nenavaden ali presenetljiv napad, ki ste ga videli v praksi?

Od tistih, o katerih smem govoriti, bi omenil napade, ki niso prišli od zunaj. Podjetje lahko napade tudi kdo od znotraj, ki ima dostop do sistema: slabo plačani in nezadovoljni sistemski administrator; nekdo, ki mu niso podaljšali pogodbe, pa je izbrisal del baze; razvijalec, ki je vgradil logično bombo in jo vsake toliko podaljševal, ko pa je odšel iz podjetja, se je ta sprožila …

Videli smo tudi že takšno izsiljevanje, da je nekdo prinesel novo verzijo programske opreme, ki je imela hrošča, nato pa zaračunaval dodatne ure za njegovo reševanje. Nekdo je imel celo dostop do posnetkov klicev za nujno medicinsko pomoč in jih je poskusil unovčiti na črnem trgu.

Treba pa je paziti tudi, da se forenzično raziskavo izpelje zakonito in pravilno. Zgodilo se je že, da so zaradi forenzičnih postopkovnih napak v podjetju morali ponovno zaposliti osebo, ki so jo zaradi tega nepravilno odpustili.

Kakšen pa bo hekerski napad leta 2030?

Po mojem mnenju se bo napadalni agent UI boril z obrambnim agentom UI. Rdeči proti modremu. Na eni strani imamo namreč obrambno strojno opremo, v katero se že vgrajuje UI, a napadalci so v prednosti, ker se ne ozirajo na spoštovanje zakonodajnih predpisov.

To bo pa malce hollywoodsko. V bistvu bo kot bitka virtualnih transformerjev …

Da, tako nekako bo videti. Ali pa kot bitka virtualnega Predatorja in virtualnega Terminatorja. Vsak bo imel svojo tehnologijo in opremo. Tisti, ki bo vanju vlagal več, bo zmagal.

Kaj pa bo ostalo nam, ljudem? Da spremljamo, kakšen bo rezultat boja?

Ljudje bomo lahko gledali in upali, da bo naš agent UI zmagal. In seveda bomo odločali o tem, koliko bomo investirali v tehnologijo. Mi bomo izbirali UI, ki bo čim boljša za obrambo.

Več napadov bo na manj kritične deležnike v dobavni verigi. Če nekdo vdre v majhno knjižnico, lahko hitro prodre do drugih knjižnic. Če vdre v eno elektrarno, pa kmalu lahko pride do jedrske elektrarne. Če obramba ni dovolj hitra …

Pred kratkim se denimo v nekem napadu z UI znaki v škodljivi kodi sploh niso videli. Takšnih kod, generiranih z UI, bi lahko bilo v prihodnje veliko.

Grafika: Spotnet

KDO BO Z RAZVOJEM UMETNE INTELIGENCE ZMAGAL: NAPADALCI ALI ŽRTVE?

- Kako umetna inteligenca spreminja kibernetske napade?
- Zakaj današnje varnostne rešitve niso vedno dovolj?
- Kako se lahko podjetja pripravijo na prihodnost, ko napada umetna inteligenca?

Simona Drevenšek

Kibernetska varnost je postala tekma, v kateri napadalci narekujejo tempo. So hitrejši, natančnejši in vse bolj avtomatizirani, pogosto tudi ob pomoči umetne inteligence. Obramba sicer razvija nove tehnologije, vendar razkorak ne izginja, le spreminja se. Gre za digitalno oboroževalno tekmo, kjer odločajo hitrost, učinkovitost in prilagodljivost.

Ključno vprašanje pa ostaja: kako lahko podjetja sploh še ostanejo korak pred njimi?

Vse se začne s klicem nekoga, ki trdi, da kliče z banke, kjer imate odprt račun. Poznajo vaše ime in celo številko vaše kreditne kartice. Povedo vam, da je na vašem računu prišlo do »nenavadne aktivnosti«. Pravkar so vam poslali enkratno geslo za potrditev vaše identitete, da bi vam lahko pomagali.

To ni nišna ali osamljena prevara, pač pa del vzorca, ki ga opažajo po svetu. Kibernetski kriminalci združujejo digitalne in realne taktike tako, da so prevare bolj prepričljive in tudi veliko bolj škodljive.

Organizacije in podjetja medtem širijo svoj digitalni vpliv v oblačnih okoljih, omrežjih interneta stvari (IoT) in zapletenih dobavnih verigah. To prinaša tudi vse večje tveganje za kibernetske napade, ki postajajo vse bolj sofisticirani in pogosto podprti z umetno inteligenco (UI).

> **Pričakujemo, da bodo agenti UI kmalu sposobni samostojno zaznati in izolirati napade v milisekundah, še preden jih človek sploh opazi.«**
> Gorazd Božič

1. Kako napadalci razmišljajo danes?

S stališča napadalcev so pomembne predvsem tehnologije, ki jim pomagajo oceniti, katere tarče se bolj »izplačajo«, ter tehnologije, ki maksimalno pohitrijo in avtomatizirajo napade, navaja direktor za poslovni trg A1 Slovenija Matej Matija Grobelšek: »Napadalci namreč iščejo čim boljši izkoristek svojega časa. To pomeni, da bodo še bistveno učinkovitejši, natančnejši in hitrejši, kot so danes.«

Razvoj sistemov za zaznavanje in razvoj procesov v varnostno-operativnem centru morata temu slediti. Enako velja za razvoj obrambnih tehnologij in procesov v varnostno-operativnih centrih, dodaja Grobelšek.

Takšen pristop pa postavlja obrambne sisteme pred vse večje izzive, saj morajo slediti hitrosti in prilagodljivosti napadalcev.

2. Zakaj obramba pogosto ne zadostuje?

Na drugi strani organizacije že uporabljajo napredne rešitve, kot so EDR, XDR in SIEM, ki v realnem času analizirajo ogromne količine podatkov in zaznavajo anomalije. A ključni problem ostaja: vsi signali ne pomenijo tudi dejanskega napada.

Grobelšek to ponazori s preprosto primerjavo: »Če nekdo s kladivom tolče po ključavnici, je jasno, da gre za napad. Če pa nekdo sredi noči odklene vrata, ni nujno jasno, ali gre za vlomilca ali zaposlenega. Podobno velja v digitalnem svetu, saj tehnični signal še ne pove celotne zgodbe.«

Veliko opozoril je lažnih ali pa zahtevajo dodatno razlago. Prav tu nastopi največja omejitev današnjih sistemov: pomanjkanje razumevanja konteksta.

Ta vrzel med količino podatkov in razumevanjem konteksta je razlog, da v ospredje vse bolj stopa UI.

3. Zakaj je uporaba UI nujna, ni pa čudežna rešitev?

Uporaba UI v kibernetski varnosti ni več futuristična ideja, temveč nuja. Matej Matija Grobelšek pojasnjuje: »Zaradi ogromnega števila varnostnih dogodkov bi bilo zanašanje zgolj na človeške vire neučinkovito. Avtomatizacija omogoča, da se delo začetnikov preusmeri na bolj rutinska opravila, medtem ko izkušeni strokovnjaki ostajajo ključni za razumevanje poslovnega konteksta in sprejemanje kompleksnih odločitev.«

Prav razumevanje konteksta bo ena ključnih nalog prihodnjih agentov UI, dodaja Grobelšek, saj bodo ti sposobni sprejemati natančnejše odločitve. »Brez UI sodoben varnostni operativni center (SOC) danes ne more učinkovito delovati,« poudarja, ob tem pa opozarja, da uporaba UI prinaša tudi izzive.

Občutljive podatke je treba skrbno varovati. Ne smemo jih nekritično prenašati med različnimi okolji. Zato se vse pogosteje uporabljajo zaprta okolja UI, kjer je mogoče varno analizirati podatke strank in izboljševati zaznavanje vzorcev napadov.

Kljub hitremu napredku pa je treba ohraniti realna pričakovanja. Kot opozarja vodja Nacionalnega odzivnega centra za kibernetsko varnost SI-CERT Gorazd Božič: »Nismo še dosegli stopnje, ko bi sistemi UI lahko sami, brez človeškega posega, izolirali napad v milisekundah.« Trenutno UI predvsem pomaga pri prepoznavanju vzorcev in opozarjanju strokovnjakov, ki nato sprejmejo končne odločitve.

4. Zakaj so nova orodja UI lahko nevarna, če pridejo v napačne roke?

A enaka tehnologija, ki krepi obrambo, odpira tudi nova tveganja. UI ni le orodje obrambe, ampak tudi potencialno orožje napadalcev. Svet se tako postopoma premika proti scenariju, kjer se bodo napadi in obramba odvijali na ravni UI proti UI.

Ena izmed pozitivnih lastnosti UI danes je, da so sistemi še relativno pod nadzorom glede tega, kje in kako se uporabljajo. Pri »klasičnih« modelih UI, kot je ChatGPT, poskusi zlonamerne uporabe hitro naletijo na omejitve, zato bi moral napadalec razviti lasten model, to pa je zahtevno, pojasnjuje Grobelšek in dodaja: »To za zdaj deluje kot pomemben obrambni mehanizem in pomeni, da UI še ni ključen dejavnik pri napadih.«

Kljub temu pa obstajajo tveganja, denimo model Claude Mythos, namenjen iskanju varnostnih lukenj, ki je raziskovalce presenetil z učinkovitostjo, opozarja Grobelšek: »Takšni primeri kažejo, kako hitro bi se lahko razmere spremenile, če bi taka orodja prišla v napačne roke.«

5. Kako hitro se razvija avtomatizirana obramba?

Prihodnost kibernetske varnosti bo temeljila na še večji stopnji avtomatizacije in uporabi agentov UI, ki bodo sposobni razumeti tudi poslovni kontekst.

Božič poudarja, da se že razvijajo sistemi za boljšo korelacijo podatkov in zaznavanje kompleksnih napadov, kot so phishing in napadi socialnega inženiringa. »Pričakujemo, da bodo agenti UI kmalu sposobni samostojno zaznati in izolirati napade, še preden jih človek sploh opazi.«

Na ta pospešen razvoj se odziva tudi tehnološka industrija. IBM je aprila letos napovedal nove ukrepe za kibernetsko varnost, ki naj bi organizacijam pomagali pri boju proti novi generaciji kibernetskih groženj. V ta boj se je podal tudi OpenAI, ki razvija nov AI model GPT 5.4-Cyber, vendar pa ta še ni na voljo širši javnosti.

Trenutno je z omejitvami dostopen le preverjenim strokovnjakom za kibernetsko varnost, ki ga preizkušajo z namenom odkrivanja ranljivosti in izboljševanja odpornosti proti zlorabam. Ta pristop je del programa Trusted Access for Cyber, ki omogoča zgoden dostop varnostnim strokovnjakom za razvoj obrambnih rešitev.

To kaže, da se obramba vse bolj premika na raven naprednih sistemov UI, ki bodo igrali ključno vlogo pri zaznavanju in preprečevanju napadov.

Primeri velikih tveganj že obstajajo – denimo model Claude Mythos, namenjen iskanju varnostnih lukenj, ki je raziskovalce presenetil z učinkovitostjo.«
Matej Matija Grobelšek

Zaradi ogromnega števila varnostnih dogodkov bi bilo zanašanje zgolj na človeške vire neučinkovito.«
Matej Matija Grobelšek

6. Kje podjetja najpogosteje zaostajajo?

Za učinkovito zaščito ni dovolj le tehnologija. Ključna je kombinacija osnovne varnostne higiene, pravih orodij in ustreznih procesov. Grobelšek poudarja minimalen tehnološki higienski standard, ki vključuje urejeno in varno informacijsko okolje, ustrezno tehnologijo za zaznavanje napadov in predvsem vzpostavljene procese za hiter in pravilen odziv ob incidentu.

Dodaja, da je brez integracije v dober varnostno-operativni center skoraj nemogoče zagotoviti ustrezno zaščito: »Prvi pogoj lahko podjetja delno uredijo sama, drugi je že zahtevnejši, tretji pa skoraj nemogoč brez podpore strokovnjakov in varnostnega operativnega centra, ki zagotavlja stalen nadzor in hitro ukrepanje.«

Božič meni, da je poleg minimalnega tehnološkega standarda v podjetju pomembno imeti kompetentno osebo, ki bo pregledovala omrežje in svetovala, kaj lahko izboljšajo.

Tehnologija sama po sebi ni največji problem. Večji izziv predstavlja zrelost varnostnih praks. Grobelšek pojasnjuje: »Manj ko uporabljajo večnivojsko avtentikacijo, manj stalnega varnostnega nadzora imajo in manj sistematično izobražujejo zaposlene.«

Razlika postane očitna ob varnostnem incidentu. Najbolj pripravljena podjetja imajo poleg tehnologije vzpostavljene in preizkušene postopke za odzivanje in okrevanje, kar jim omogoča hitrejšo vrnitev v normalno poslovanje, dodaja Grobelšek.

7. Kdaj bi lahko prišli nevidni varuhi pred napadi?

Čeprav UI postaja osrednji element kibernetske varnosti, ne nadomešča ljudi. Nasprotno, njihova vloga postaja še pomembnejša. Prihodnost namreč ne bo temeljila na popolni avtomatizaciji, temveč na učinkovitem sodelovanju med tehnologijo in strokovnjaki.

Kot poudarja Božič, v sklopu evropskih projektov že razvijajo in testirajo modele, ki bodo omogočili naprednejšo korelacijo podatkov ter zaznavanje vse bolj sofisticiranih napadov, kot so phishing in napadi socialnega inženiringa.

V bližnji prihodnosti bi lahko takšni sistemi delovali kot nevidni varuhi, ki podjetjem omogočajo, da se osredotočijo na svoje poslovanje brez stalnega strahu pred kibernetskimi grožnjami. V tej tekmi pa si podjetja pasivnosti preprosto ne morejo več privoščiti.

IZPOVED ŽRTVE KIBERNETSKEGA NAPADA: »BILI SMO ZAPRTI IN BREZ STIKA.«

- Česa jih je bilo najbolj strah?
- Zakaj so se zaposleni počutili huje kot v času epidemije?
- Koliko zdaj namenjajo za dobro kibernetsko varnost?

Goran Novković
Foto: Barbara Reya

Prvi teden smo bili vsi tako rekoč brez vsega.«

Najtežje je bilo vse ljudi poslati domov in jim reči, naj sploh ne prihajajo v službo.«

Angelo Žigon je direktor in partner podjetja Elea IC v Ljubljani ter partner mednarodne skupine iC. Lansko jesen je doživel kibernetski napad na skupino in na ljubljansko podjetje. Napadena je bila skupina iC, ki ima sedež na Dunaju, lokacije pa na Dunaju, v Salzburgu, Ljubljani, Beogradu, Zagrebu, Sarajevu, Ukrajini in drugje. Skupina zaposluje 800 ljudi, od tega 130 v Ljubljani.

Elea iC se ukvarja s tehničnim svetovanjem, projektiranjem visokih in nizkih gradenj, predorov in druge infrastrukture, arhitekturo, gradbenim nadzorom, projektnim vodenjem, geologijo, geotehniko … Lahko si torej predstavljate količino in vrsto podatkov, ki so bili tarča napada.

Kdaj so vas napadli?

Sredi oktobra, neko nedeljo. Fizično smo morali iztakniti kable iz vseh električnih vtičnic in vseh računalnikov. Pozneje smo ugotovili, da so v naše sisteme prišli že maja lani. Do oktobra so se pripravljali, vse dokler niso bili toliko gotovi, da so zaklenili podatke.

Vdor je bil izveden na neki precej neopazni lokaciji naše mednarodne skupine, najverjetneje v Avstriji. Ko hekerji enkrat pridejo v en računalnik v sistemu, imajo dostop do vseh. So na vseh računalnikih in strežnikih, kjer so podatki shranjeni.

Vse naprave smo zato odklopili, da smo zavarovali podatke, ker takrat še nismo vedeli, katere so napadalci zaklenili in katerih ne. To je prvo, kar kot direktor narediš v primeru napada.

Kaj pa ste storili potem?

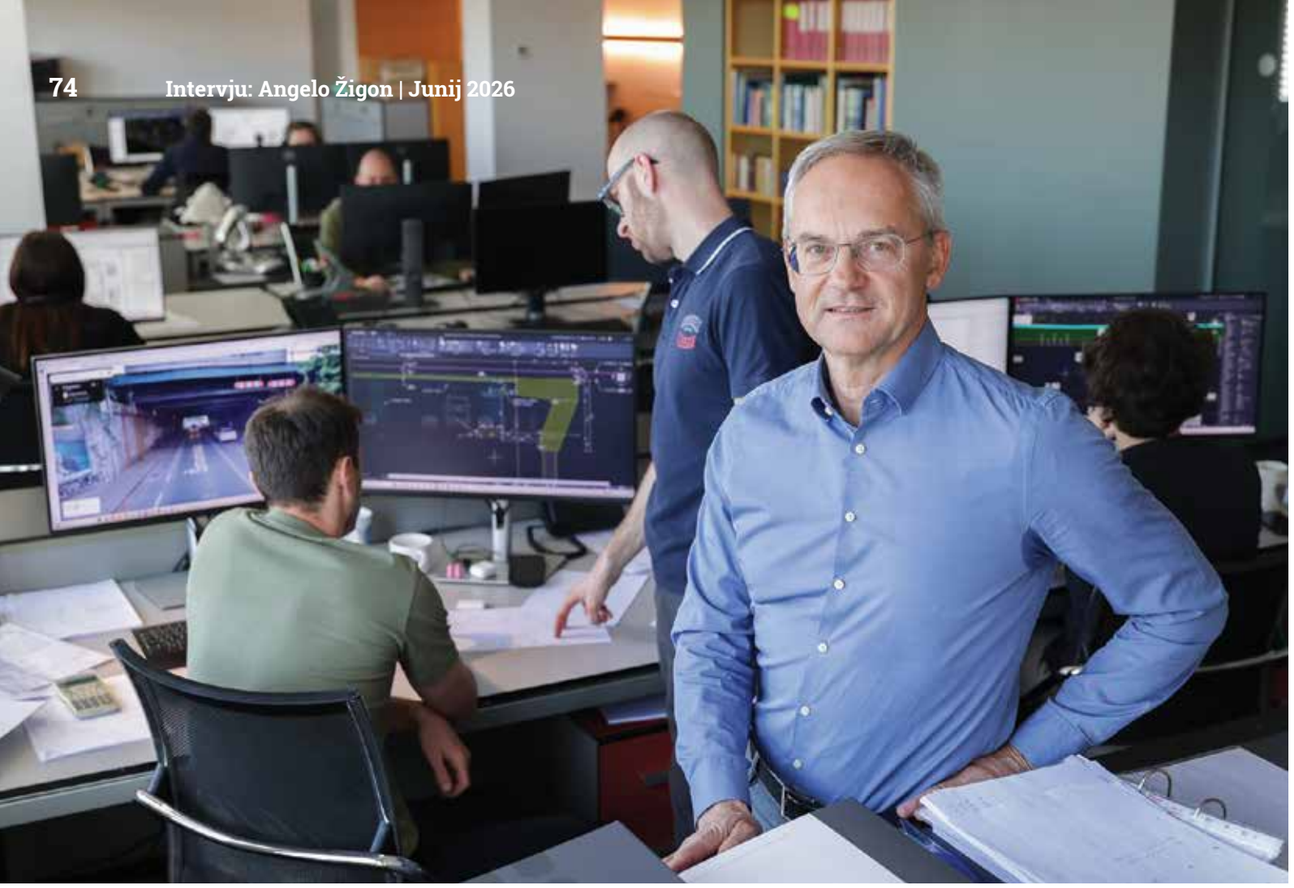
Treba je bilo diagnosticirati, kateri podatki so zaklenjeni in kateri so na voljo. Počasi smo vzpostavljali sisteme, hkrati pa smo se pogajali z napadalci. Tako nam niti niso odvzeli podatkov niti niso vseh zaklenili. Ne vemo, zakaj so tako ravnali.

Ste se pogajali sami ali ste klicali policijo?

Obvestili smo vse, ki jih je v takšnih primerih treba obvestiti. Glede na to, da se vdor ni zgodil pri nas, ampak v Avstriji, smo sodelovali z našimi tamkajšnjimi kolegi. Pri ponovnem oživljanju celotne skupine smo v Avstriji angažirali približno 40 ljudi, ki so nam pomagali s forenziko in pri ponovnem vzpostavljanju sistema.

Koliko časa pa je trajalo vzpostavljanje sistema?

To se je dogajalo postopno. Prvi teden smo bili vsi tako rekoč brez vsega; opravljali smo lokalne naloge v službi. Gradbeni nadzor je še vedno funkcioniral, projektiranje pa zelo malo, razen pri tistih, ki smo imeli podatke na svojem lastnem računalniku.



Da smo se postavili na noge, je trajalo približno en mesec ... V drugih podjetjih je trajalo tudi do štiri mesece.«

Najprej smo vse računalnike poslali skozi čistilno cesto in tako s posebnim programom preverili, ali je vsak računalnik čist. To je skupno trajalo nekaj dni. Računalnike smo lahko vklopili, nismo pa jih smeli povezati z internetom.

Koliko časa je trajalo to obdobje?

Da smo se postavili na noge, je trajalo približno en mesec. Šele po enem mesecu smo vse sisteme vzpostavili nazaj, vendar smo bili od podjetij, ki se jim je to zgodilo, še vedno med najhitrejšimi. V drugih podjetjih je lahko trajalo tudi do štiri mesece.

Česa vas je bilo najbolj strah? Izgube podatkov, poslovanja, ugleda ali denarja?

Najbolj nas je bilo strah izgube podatkov. Pri projektih smo pogodbeno vezani z roki. Če bi pri projektu na primer delali več mesecev, potem pa bi vsi podatki izginili, bi vse skupaj morali začeti znova in zamudili bi roke.

Kaj pa so napadalci zahtevali?

Denar. Odškodnino. Imeli smo dva pogajalca med 40 ljudmi v krizni ekipi. Pomagali so nam strokovnjaki iz Kopernikusa, Dataplexa in Certainityja. To so specialisti za kibernetsko varnost.

Katera odločitev je bila v prvih 24 urah najtežja?

Najtežje je bilo vse ljudi poslati domov in jim reči, naj sploh ne prihajajo v službo.

Ste imeli krizni načrt za kaj takšnega?

Ne, nismo ga imeli. Tega res nismo pričakovali. Naša IT skupina šteje 17, 18 ljudi. Vso programsko opremo, pogodbe, varovanja, vse rezervne kopije – vse to smo imeli urejeno. Ampak kljub temu nas je zadelo.

Kako pa ste komunicirali s strankami, partnerji?

Partnerje smo obvestili, da imamo problem. Pomagali so nam tako, da smo od njih dobili dokumente, ki smo jih že oddali. Največji izziv so bila gradbišča, ker se tam dela odvijajo. Prosili smo jih, naj nam vrnejo naše dokumente, potem pa smo jih začeli nadgrajevati ali uporabljati kako drugače. Kmalu smo začeli delati s polovično intenzivnostjo.

Kaj bi naredili drugače, da bi bili bolj pripravljeni?

Moje prvo sporočilo je, da nihče ni varen. Popolne varnosti ni. Kibernetski napad lahko prizadene vsakogar. Toda varnost je mogoče izboljšati in to smo tudi naredili.

Požarni zid smo zamenjali z novim, zelo naprednim in kompleksnim. Drugi zelo pomemben ukrep je zagotoviti, da so vsi sistemi znotraj podjetja zaprti, da torej zunanji akterji nimajo nikakršnega dostopa do našega sistema. Pomembno je, da tretjim osebam onemogočimo dostop do svojih strežnikov. Kot tretji korak pa smo vse računalnike, pri katerih smo to storili že dvakrat, očistili še tretjič. Pri tem smo našli še več stranskih vrat napadalcev. In to na vseh lokacijah.

Kaj ste se naučili, da boste v prihodnje preprečili tak napada?

Po vsem omenjenem smo naložili program, ki spremlja dohodne poti do računalnikov in omogoča MDR spremljavo podjetja 24 na dan. MDR je kratica za Managed Detection Response – sistem, ki zaznava kibernetske napade in jih upravlja. To pomeni, da potrebujemo program in podjetje, ki to področje spremlja 24/7.

Nadvse pomembno je tudi izobraževanje zaposlenih, sicer ne pomaga niti najboljši sistem varnosti. V preteklem mesecu smo detektirali že dva nova napada, ki so ju zaradi pridobljenega izobraževanja zaznali sodelavci, naš IT pa ju je izoliral.

Vsak lahko izračuna, kaj pomenijo 1 do 3 meseci brez dela, izgubljeni podatki in zamude rokov. Potem lahko hitro izračuna, koliko je smiselno vložiti v kibernetsko varnost.«

Kako pa jih izobražujete? Ste pripravili seminar ali imate tudi vaje v slogu 'nič nas ne sme presenetiti'?

Imeli bomo tudi test na kibernetski napad. To ne bo napovedana vaja. Predvsem pa morajo zaposleni pravilno ravnati s svojimi podatki, v prvi vrsti z gesli in uporabniškimi imeni. Če nekaj pride na njihov računalnik, je na vseh računalnikih, ker so med sabo povezani v mreži.

Povezavo VPN z zunanjimi sodelavci in za delo od doma ali na drugih lokacijah, ki je bila po napadu zaprta kar tri mesece, smo bistveno bolje zavarovali pred napadom. Ob vseh ukrepih, ki smo jih izpeljali, smo prepričani, da smo najbolj varni, kolikor je trenutno pač mogoče.

»Najbolj nas je bilo strah izgube podatkov. Zamudili bi roke, na katere smo pri projektih pogodbeno vezani.«

Kako so zaposleni doživljali napad? Kakšna je bila njihova psihološka reakcija?

Bili so nekako prestrašeni, podobno kot v času epidemije. Le da je bilo še huje.

Zakaj huje?

Ker so med epidemijo lahko delali in se denimo prek interneta povezali s svetom. Po kibernetskem napadu pa naša skupina v službi ni mogla niti na internet. Bili smo zaprti in brez stika.

»Moje prvo sporočilo je, da nihče ni varen. Popolne varnosti ni. Kibernetski napad lahko prizadene vsakogar. Toda varnost je mogoče izboljšati.«

Kako ste kot direktor napad doživljali vi?

Imeli smo krizno skupino znotraj skupine, kjer smo sproti izmenjevali informacije, kaj se je dogajalo, kako potekajo pogajanja, kaj se odpira, kaj se zapira, kaj smo ugotovili v zvezi z napadom ... Vsi smo delovali zelo trezno in ciljno, da razrešimo situacijo.

Kakšen je po napadu vaš pogled na kibernetsko varnost kot investicijo?

Dejstvo je, da je poslovni model napadalcev imeti več in več posla. Nujno je torej, da smo previdni in pazljivi. Ocenjujem, da se celoten strošek zdaj giblje med 5 in 10 odstotki prometa, ampak to ni le kibernetska varnost.

Kaj bi svetovali podjetnikom, ki še vedno menijo, da se njim to ne more zgoditi?

Povedal bi jim, da se to hitro lahko zgodi vsakomur. Vsak zase mora zato izračunati, kaj bi pomenilo, če ne bi mogel delati od enega do treh mesecev, če bi izgubil vse podatke in zamudil pogodbene roke. Potem lahko hitro izračuna, koliko je smiselno vložiti v kibernetsko varnost. Tako preprosto je to.

NOVO: Aktualni razpisi na našem portalu

EVROPSKI MILIJONI ZA KIBERNETSKO VARNOST: RAZPISI 2026–2027

- Kako lahko slovenska podjetja izkoristijo evropske razpise kot vzvod za močnejšo rast, tudi globalno?
- Ali imate jasno strategijo, kako povezati razvoj, regulativo (NIS2) in financiranje?
- Ste pripravljeni sodelovati v mednarodnih konzorcijih, kjer nastajajo prebojne tehnologije?

Aleksandra Godec

V naslednjih dveh letih bo Evropska unija razdelila več sto milijonov evrov za razvoj kibernetske varnosti, umetne inteligence (UI) in obrambnih tehnologij. V ospredju niso več le velike korporacije, temveč tudi manjša inovativna podjetja. Del tega denarja je namenjen tudi slovenskim podjetjem. A le tistim, ki bodo znala pravočasno prepoznati priložnost in se nanjo pripraviti.

Programi, kot sta Digitalna Evropa in Obzorje Evropa, niso več le okvirne priložnosti, temveč konkretni finančni mehanizmi z jasnimi roki, pogoji in proračuni.

Med aktualnimi so razpisi za krepitev kibernetskih zmogljivosti MSP, uvajanje rešitev UI in razvoj naprednih varnostnih tehnologij, kjer so na voljo večdesetmilijonski proračuni.

Hkrati se odpirajo nacionalne priložnosti, kot so razpisi Javne agencije za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije (ARIS) za razvojno-raziskovalne projekte.

A. Program Digitalna Evropa (DIGITAL): za prenos rešitev v prakso

Program Digitalna Evropa je namenjen uvedbi tehnologij v dejansko uporabo in ne financira osnovnih raziskav, temveč konkretno implementacijo in testiranje.

Ključni prihajajoči razpisi s tega področja so naslednji:

1. Krepitev kibernetskih zmogljivosti evropskih MSP z uporabo rešitev UI (DIGITAL 2.2)

Namenjen je MSP-jem za uvajanje praktičnih rešitev UI (npr. SaaS), ki avtomatizirajo varnostne procese.

Predvidena višina subvencioniranja: cca. 20 milijonov evrov
Rok za prijavo: 3. kvartal 2026
Povezava Tiko Pro:

2. Krepitev kibernetskih zmogljivosti EU skladno z zakonodajo (DIGITAL 2.14)

Namenjen je pomoči organizacijam pri prilagajanju na nove standarde, kot je Direktiva o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2).

Predvidena višina subvencioniranja: cca. 32 milijonov EUR
Rok za prijavo: 1. kvartal 2027
Povezava Tiko Pro:

3. Dvojna raba tehnologij (DIGITAL 2.16)

Na voljo je za podjetja, katerih tehnologije (UI, kibernetika) so uporabne tako v civilne kot v obrambne namene.

Predvidena višina subvencioniranja: 10 milijonov evrov
Rok za prijavo: 3. kvartal 2026
Povezava Tiko Pro:

B. Obzorje Evropa (Horizon Europe): za vizionarje in razvojnike

Nacionalni koordinacijski center za kibernetsko varnost (NCC-SI), ki deluje v okviru Urada Vlade Republike Slovenije za informacijsko varnost (URSIV), je nacionalna kontaktna točka Republike Slovenije v evropski mreži centrov za kibernetsko varnost.

Kot pravijo, je razpis namenjen za razvoj inovativnih rešitev in orodij na področju varnosti strojne in programske opreme, UI ter kriptografije.

»Ta program financira razvoj popolnoma novih metod in tehnologij, ki še niso v celoti zrele za vstop na trg. Projekti pa se izvajajo v mednarodnih konzorcijih,« dodajajo na Tiko Pro.

Upravičenci: raziskovalne organizacije, univerze, podjetja in druge inovativne entitete.

Cilj je sofinanciranje projektov na treh ključnih področjih:

V ospredju razpisov niso več le velike korporacije, temveč tudi manjša inovativna podjetja.

- ★ Varnost programske in strojne opreme (20 mio evrov): varne arhitekture čipov, varnost v dobavnih verigah, pristopi »security-by--design« (»varnost od začetka«) ter UI in formalna varnostna testiranja.
- ★ Odpornost UI – SecureAI (21,2 mio evrov): obramba modelov UI pred napadi (zastrupitev podatkov, stranska vrata), detekcija anomalij in tehnologije za varovanje zasebnosti.
- ★ Napredna kriptografija (15 mio evrov): postkvantne kriptografske rešitve (tudi za zaščito digitalnih denarnic) in orodja za formalno verifikacijo ob prehodu na postkvantno dobo.

Višina sredstev: 56,2 milijona evrov

1. Razpisi z rokom 15. september 2026:

1. **Pristopi in orodja za varnost v razvoju programske in strojne opreme** (HORIZON-CL3-2026-02-CS-ECCC-01):
   Povezava Tiko Pro:
2. **Krepitev varnosti, zasebnosti in robustnosti sistemov UI** (HORIZON-CL3-2026-02-CS-ECCC-02):
   Povezava Tiko Pro:
3. **Napredne kriptografske rešitve in varne implementacije** (HORIZON-CL3-2026-02-CS-ECCC-03):
   Povezava Tiko Pro:

1 mrd €
je na voljo za financiranje vrhunske obrambne inovacije z namenom povečanja tehnološke neodvisnosti EU.

2. Razpisi z rokom 15. september 2027:

1. **Umetna inteligenca za uporabo v kibernetski varnosti** (HORIZON-CL3-2027-02-CS-ECCC-01):
   Povezava Tiko Pro:
2. **Varen računalniški kontinuum (IoT, Edge, Cloud, Data Spaces)** (HORIZON-CL3-2027-02-CS-ECCC-02):
   Povezava Tiko Pro:
3. **Varne implementacije postkvantne kriptografije, kriptoanaliza in digitalno zaupanje v postkvantnem obdobju** (HORIZON-CL3-2027-02-CS-ECCC-03):
   Povezava Tiko Pro:
4. **Novi kriptografski primitivi in protokoli za funkcionalnosti prihodnjih hibridnih in kvantnih omrežij** (HORIZON-CL3-2027-02-CS-ECCC-04):
   Povezava Tiko Pro:

C. Evropski obrambni sklad (EDF): priložnost leta z milijardnim proračunom

Gre za Evropski obrambni sklad (EDF), ki financira vrhunske obrambne inovacije z namenom povečati tehnološko neodvisnost EU.

Višina financiranja: skupni proračun za leto 2026 znaša skoraj milijardo evrov.
Rok za prijavo: 29. september 2026
Sklad pokriva širok spekter področij:

- ★ Razvojni projekti: od prihodnjih tankovskih sistemov in polavtonomnih plovil do vesoljskih tehnologij in lovcev nove generacije.
- ★ Raziskovalni projekti: pametni senzorji, avtonomno dolivanje goriva v zraku in uporaba UI za vojaško odločanje.
- ★ Spodbude za MSP (EUDIS): več kot 60 milijonov evrov je rezerviranih posebej za mala in srednja podjetja ter prebojne tehnologije.

Č. Javni razpis – spodbude za raziskovalno-razvojne projekte 2026/1 (JR RRI 2026/1)

Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije (ARIS) je objavila razpis za sofinanciranje projektov, ki razvijajo nove izdelke in storitve z visoko dodano vrednostjo, med drugim tudi s področja IKT in kibernetske varnosti.

»Razpis je namenjen podjetjem, ki želijo svoje delujoče prototipe dokončno pripraviti za komercializacijo in vstop na trg,« še sporočajo z ARIS-a (NCC-SI).

Upravičenci so podjetja vseh velikosti (samostojno ali v konzorciju do 3 partnerjev). Javni zavodi niso upravičeni prijavitelji.

Višina financiranja: 100.000–300.000 evrov na projekt (do 60 odstotkov)
Rok za prijavo: 13. Junij 2026 do 14. ure
Povezava ARIS:

D. Nov razpis – Evropski kompetenčni center za kibernetsko varnost

Razpis Cyber-10 v okviru programa Digital Europe je usmerjen v krepitev Cyber Hubov po vsej EU. »S tem ukrepom Evropski kompetenčni center za kibernetsko varnost (European Cybersecurity Competence Centre – ECCC) prispeva k izvajanju Akta o kibernetski solidarnosti (Cyber Solidarity Act), ki predvideva vzpostavitev mreže kibernetskih vozlišč kot dela Evropskega sistema za kibernetsko opozarjanje,« pojasnjujejo na ARIS-u (NCC-SI).

Višina financiranja: 4 milijone EUR
Rok za prijavo: 28. Junij 2026
Povezava ARIS:

32 mio €
je namenjenih za pomoč organizacijam pri prilagajanju na nove standarde, kot je direktiva NIS2.

Grafika Spotnet

KDO OBVLADUJE SLOVENSKA VARNOSTNA PODJETJA?

- Kako močan je že Sintal in z njim Robert Pistotnik?
- Kdo izstopa na področju kontrole pristopa v podjetja in organizacije?
- Kaj počne Dat-Con, da tako hitro raste?

Goran Novković

Več kot 20 let je minilo, odkar sem zadnjič urejal posebno prilogo o varnostnih podjetjih. Od takrat se je spremenilo marsikaj, ne pa ravno vse. Med drugim na lestvici največjih podjetij z licencami za fizično in tehnično varovanje še vedno kraljuje Sintal, ki izvira iz lastništva družine Pistotnik, že leta pa je glavni igralec v tej družbi Robert Pistotnik.

1. Edini na lestvici največjih podjetniških skupin – Pistotnik

Na lestvici prvih 50 podjetij z licencami za različna področja varovanja je namreč kar 12 odstotkov ali natančneje šest Sintalovih podjetij. Vključno z najmočnejšim, krovnim Sintalom na vrhu lestvice, ki dosega skoraj 40 milijonov evrov prodaje.

Skupno vsa Sintalova podjetja konsolidirano presegajo 53 milijonov evrov prodaje, kar je skoraj dvakrat več kot najmočnejše proizvodno podjetje

Skupno vsa Sintalova podjetja konsolidirano presegajo 53 milijonov evrov prodaje. To je skoraj dvakrat več kot najmočnejše proizvodno podjetje Dat-Con na 3. mestu lestvice.

Dat-Con na 3. mestu lestvice. Nič čudnega, da se prav Robert Pistotnik, skupaj z Lidijo Pilko, kot edini s področja varovanja uvršča med največje slovenske podjetniške skupine.

Prav tako je najvišje med največjimi podjetji v lasti podjetnikov – za to panogo na visokem 131. mestu. Ti dve lestvici že tradicionalno objavljamo vsakič v februarski izdaji Podjetne Slovenije.

2. Drugi močan igralec – Strmljan

Prav tako ni presenečenje Aktiva varovanje na 2. mestu lestvice. Tudi to podjetje je že desetletja znano kot močan igralec na slovenskem trgu varovanja. Tudi v tej družbi ima Robert Pistotnik z Lidijo Pilko, prek svoje firme, skoraj petinski delež, kar še krepi njegovo moč na tem trgu. Večinski lastnik pa je prek svoje firme MS Holding Mihael Strmljan.

Njegova skupina ima v lasti kar nekaj varnostnih podjetij: poleg Aktive varovanja v Sloveniji še Varnost Maribor in Protect Infro, v Srbiji pa Aktivo varnost in Aktivo varovanje. V ta sklop podjetij pa sodijo še znana podjetja na drugih področjih: Aktiva čiščenje in Čistoča v Sloveniji, Aktiva Čišćenje na Hrvaškem, celo proizvajalec sokov Presad in drugi.

A varovanje se zdi najmočnejša panoga, saj je že Aktiva varovanje po prodaji močnejša od sicer bolj znane Aktive čiščenja.

Podobno znan kot Sintal in Aktiva varovanje je na 4. mestu Tenzor iz Ptuja, podjetje za tehnično varovanje. Stari znanec iz te panoge je v lasti Alberta Beneta ter Mirana in Miha Senčarja. Miran Senčar je sicer znan tudi kot župan Ptuja v mandatu 2014–2018.

Med pravimi proizvodnimi in visokotehnološkimi podjetji s področja varovanja je na vrhu Dat-Con s Polzele, ki je od leta 2020 do leta 2024 skoraj potrojilo prodajo.

3. Naj varnostna proizvodnja: Dat-Con

Med pravimi proizvodnimi in visokotehnološkimi podjetji s področja varovanja je na vrhu Dat-Con iz Polzele, ki je od leta 2020 do leta 2024 skoraj potrojilo prodajo. Nekdaj podjetje v lasti družine Plaskan ima zdaj že nekaj časa savdskega večinskega lastnika Khalid Fahad Alboayz Holding Group. Stane in Domen Plaskan pa imata še vedno 30-odstoten delež.

Podjetje je med drugim tehnološko močno na področju antidronske obrambe, mobilnih nadzornih sistemov, prenosnih sistemov za opazovanje, obalnih varnostnih sistemov in obalnega nadzora, sistemov za zgodnje odkrivanje požarov, različnih kamer, programske opreme in tako naprej.

Sodeč po rasti in lastniški sestavi se utegne zgoditi, da bo v prihodnjih letih še veliko višje na lestvici največjih podjetij z varnostnimi licencami v Sloveniji.

4. Špica International med petimi v špici

Na naši tokratni lestvici so tudi mnoga podjetja, ki se ne ukvarjajo samo s fizičnim ali tehničnim varovanjem, imajo pa licence za nekatera področja varovanja. V zadnjih letih se je denimo veliko pisalo o evidentiranju delovnega časa, to pa je povezano s kontrolo pristopa v podjetja in druge organizacije oziroma ustanove.

Špica International v večinski lasti Toneta Stanovnika (skupaj s šestimi drugimi partnerji) je med temi podjetji uvrščena najvišje. Na naši lestvici je na visokem 5. mestu.

Pri tem pa je treba opozoriti, da vsi prihodki takšnih podjetij ne izvirajo nujno s področja takšnega ali drugačnega varovanja. Ne glede na to je znano, da je Špica International na omenjenem področju postala zelo močna – ne samo v Sloveniji, temveč tudi širše v regiji.

5. Drugi stari znanci z lestvice

Poleg omenjenih je še nekaj drugih starih znancev na naši tokratni lestvici. Zarja elektronika, Prosignal, FIT, GVS, Valina varovanje, Sinet, Janez, Parks 1, Varnost Vič, Rival – VTS so že dolga leta na tem trgu. Mnogo med njimi je novodobnih podjetij, ki so nastala po letu 1991. A to ne pomeni, da ta trg ni konsolidiran; konsolidiral se je že pred 20 do 30 leti.

Seveda pa je vedno prostor za nove, hitro rastoče igralce. Ne toliko na področju fizičnega, ampak predvsem na področju visokotehnološkega tehničnega varovanja. Prav omenjeni Dat-Con je dokaz za to.

6. Kje je priložnost za nove igralce?

Dat-Con pa ni edini, ki s pridom izkorišča hiter tehnološki razvoj. Poleg njega ter omenjenih Tenzorja in Špice International je še kar nekaj podobnih že blizu vrha lestvice.

Takšna podjetja so denimo: podjetje za tehnično varovanje A koda plus Gregorja Bana, Četrta pot večinskega lastnika Borisa Šolarja in še petih partnerjev (sistemi za kontrolo pristopa in varovanje prostorov so sicer je del njihove dejavnosti) in tudi Elektrina, ki je bila nekoč posredno v lasti Joca Pečečnika, zdaj pa je že nekaj časa v tuji lasti.

Morda je hitro rastoče še kakšno podjetje na mejnem področju varovanja. Na naši lestvici so namreč podjetja, ki imajo vsaj eno od različnih uradnih licenc za varovanje. Obenem pa smo z nje izločili tista med njimi, ki na internetni prvi strani ne omenjajo te dejavnosti. Nekatera podjetja v Sloveniji imajo namreč takšno licenco zgolj zaradi varovanja lastnega podjetja. Tako smo dobili bolj čisto in bolj realno lestvico top podjetij za varovanje.

Varovanje se zdi najmočnejša panoga v skupini Mihaela Strmljana, saj je že Aktiva varovanje po prodaji močnejša od sicer bolj znane Aktive čiščenja.

TOP 50 PODJETIJ, POVEZANIH Z VAROVANJEM

Uvrst.	Podjetje	Prodaja 2024 (v €)
1.	Sintal	39.848.193
2.	Aktiva varovanje	34.227.062
3.	Dat - Con	28.187.321
4.	Tenzor	15.690.636
5.	Špica International	13.822.553
6.	A Koda Plus	12.189.275
7.	Konica Minolta Slovenija	10.803.254
8.	Zarja elektronika	10.276.074
9.	Prosignal	9.403.171
10.	Četrta pot	8.968.597
11.	Elektrina	8.550.688
12.	Elektro Ugovšek	8.320.835
13.	FIT	8.203.241
14.	GVS	7.894.720
15.	Varovanje Galekom	7.806.949
16.	Aktiva Inpod	7.115.241
17.	Sintal Celje	6.543.986
18.	Sintal Maribor	6.217.957
19.	Valina varovanje	5.508.102
20.	Sinet	5.260.200
21.	Janez	4.428.660
22.	Nova panorama	4.310.932
23.	Alarm automatika	4.111.470
24.	Urmet	3.599.156
25.	Sintal Fiva	3.570.020

Uvrst.	Podjetje	Prodaja 2024 (v €)
26.	Protect Infra	3.562.025
27.	Parks 1	3.400.049
28.	Sintal Obala	3.277.566
29.	G4S	3.248.459
30.	PKE Electronics	3.151.137
31.	SSO	2.966.684
32.	Varnost Vič	2.886.757
33.	Team7	2.776.009
34.	Rival – VTS	2.711.041
35.	Klemm Varovanje	2.703.937
36.	Org. Tend	2.681.746
37.	HSI	2.680.419
38.	911 VRS	2.543.741
39.	GVS varovanje	2.435.432
40.	Sintal IPO	2.317.446
41.	Suprima, AZV	2.127.326
42.	Vargas-Al	1.934.803
43.	Indic	1.873.427
44.	Gymco Security	1.829.779
45.	Dolenjska-Rival varovanje	1.785.607
46.	Invarst	1.784.141
47.	BbBR Security	1.732.606
48.	IBS Varovanje	1.724.230
49.	Vezave	1.723.857
50.	VTZ	1.570.702

Vir podatkov: AJPES, statistična baza letnih poročil, preiskani računovodski izkazi, letna in revidirana letna poročila za leto 2024 (javno objavljena do 3. 1. 2026)
Kriterij razvrščanja: čisti prihodki od prodaje 2024
Opomba: podjetja na lestvici imajo vsaj eno od različnih licenc za varovanje; podjetja z licenco, ki na internetni prvi strani ne omenjajo te dejavnosti, smo izločili.

Grafika: Spotnet

NOV POJAV PRI KLASIČNIH NAPADIH NA PODJETJA – KOMBINIRANI NAPADI!

- Kako kriminalne skupine kombinirajo fizične in digitalne metode?
- Kako tatovi danes opazujejo podjetja, preden udarijo?
- Zakaj bo v prihodnje več kriminala, a manj fizičnih napadov?

Almira Sakalić

V času, ko je pozornost javnosti usmerjena v kibernetske grožnje in napade s pomočjo umetne inteligence, se v tišini dogaja nekaj drugega. Fizični napadi na podjetja v Sloveniji se prilagajajo, postajajo bolj ciljno usmerjeni in tehnološko dovršeni. Klasična kriminaliteta proti podjetjem ne usiha, ampak raste. In postaja drugačna. Bolj načrtovana. Bolj premišljena.

Kot opozarjata slovenska Policija in Branko Slak, predsednik Zbornice za razvoj slovenskega zasebnega varovanja, klasična premoženjska kriminaliteta danes zahteva strateški odziv vodstva podjetij, saj storilci niso več le priložnostni neznanci, temveč dobro pripravljene skupine.

1. Visoka rast kriminalitete v petih letih

Podatki Policije za obdobje med letoma 2021 in 2025 razkrivajo zaskrbljujoč trend. Če smo leta 2021 beležili 13.583 kaznivih dejanj na škodo pravnih oseb, se je ta številka do leta 2025 povzpela na 20.618 primerov. Gre za več kot 50-odstoten porast kriminalitete v petih letih. Največji delež k tej številki prispevajo tatvine, ki so s 6.422 primerov narasle na več kot 11.200 letno. Sledijo jim velike tatvine oziroma vlomi, ki vztrajno rastejo in so presegli mejo 2.600 primerov na leto.

Posebno pozornost zbuja tudi področje ponarejanja denarja, kjer se je število primerov v obravnavanem obdobju več kot podvojilo, ter zlorabe položaja in poslovne goljufije. Ali povedano drugače, v zadnjih dveh letih je bilo v Sloveniji ugotovljenih več kot 1.500 primerov, ko je nekdo znotraj podjetja izkoristil svoj položaj.

2. Kdo je glavna tarča?

Najpogosteje so na udaru podjetja z visoko koncentracijo likvidnega premoženja, gotovine ali hitro unovčljivega blaga. Iz statistike in operativnega spremljanja izstopajo predvsem trgovina in maloprodaja, logistični centri ter skladišča.

V urbanih in logističnih središčih so tarča predvsem podjetja z visoko vrednostjo tehničnega in trošarinskega blaga, ki na črnem trgu praktično takoj postane denar. Policija opozarja, da so tarča tudi infrastrukturni objekti, kjer poškodovanje tuje stvari (več kot 1.500 primerov letno) povzroča ogromne posredne stroške zaradi izpada delovnih procesov.

3. Fenomen kombiniranih napadov

Če so v preteklosti prevladovali spontani vlomi, danes trendi kažejo na nevarno povečanje načrtovanih akcij. Branko Slak pojasnjuje: »Storilci danes pogosto predhodno opazujejo objekt, preučujejo delovni čas, navade zaposlenih in celo dostavne poti. Iščejo varnostne rutine, ki jih zaposleni izvajajo avtomatično in brez razmišljanja.«

Pojavlja se tudi fenomen kombiniranih napadov. Storilci zlorabijo javno dostopne informacije na spletu, da se lažje infiltrirajo v objekt pod pretvezo dostave ali servisa. Namesto da bi vdrli skozi najbolje zavarovana vrata, poiščejo »najšibkejši člen« v organizaciji. Pogosto je to receptor ali zaposleni v skladišču, ki v trenutku stresa ali gneče opusti varnostni protokol.

4. Zaposleni so lahko rešitev ali problem

Zaposleni so prva bojna linija obrambe, a hkrati tudi največja potencialna ranljivost. Policija poudarja, da se podjetja premalo zavedajo notranjih tveganj. Statistično pomemben delež škodnih dogodkov namreč izvaja ali omogoča »notranji faktor« – lahko gre za kraje, neupravičeno posredovanje informacij zunanjim storilcem ali zlorabo pooblastil. Zloraba položaja ali zaupanja pri gospodarski dejavnosti se je v zadnjem letu ustalila pri visokih 760 primerih.

Storilci danes pogosto predhodno opazujejo objekt, preučujejo delovni čas, navade zaposlenih in celo dostavne poti.«
Branko Slak

Hkrati so zaposleni pogosto žrtve manipulacij. Napadalci računajo na človeško prijaznost in ustrežljivost. »Napadalec ne potrebuje lomilke, če ga zaposleni sam spusti skozi vrata, ker mu verjame, da je prišel popravit tiskalnik,« ponazarja Slak.

Ključno je torej graditi kulturo varnosti, kjer preverjanje identitete obiskovalcev ni razumljeno kot nezaupanje, temveč kot standarden varnostni postopek.

5. Zakaj kamere niso dovolj?

Najpogostejša napaka je prepričanje, da so kamere same po sebi dovolj, opozarja Slak: »V praksi podjetja pogosto zanemarijo osnove: nadzor dostopa, osvetlitev okolice, mehansko zaščito vhodov, redne varnostne preglede, upravljanje ključev in kartic ter usposabljanje zaposlenih.« Alarmni sistem obstaja, ni pa odzivnega protokola; kamere snemajo, nihče pa ne spremlja dogajanja ali redno preverja posnetkov.

»Učinkovita zaščita je vedno sistem, ne posamezna naprava,« poudarja Slak. Policija z istega zornega kota svetuje: »Ključno je uvajanje integriranih varnostnih sistemov, ki vključujejo videonadzor, alarmne sisteme in nadzor dostopa, ter dosledno upravljanje vstopov in gibanja oseb znotraj objektov.« Pomembno je tudi omejevanje dostopa glede na pooblastila ter nadzor nad zaposlenimi in zunanjimi izvajalci.

Kriminalci pogosto poiščejo najšibkejši člen v organizaciji. Pogosto je to receptor ali zaposleni v skladišču, ki v trenutku stresa ali gneče opusti varnostni protokol.

V urbanih in logističnih središčih so tarča predvsem podjetja z visoko vrednostjo tehničnega in trošarinskega blaga, ki na črnem trgu praktično takoj postane denar.

6. Prihodnost: kako pomaga tehnologija?

Kljub vsemu zgoraj naštetemu je tehnologija danes močnejše orodje za varovanje kot kadarkoli prej. Slak opisuje dogajanje na terenu: »Pametne kamere prepoznajo gibanje v prepovedanem območju, nenavadno zadrževanje oseb, puščene predmete ali gibanje zunaj delovnega časa. Senzorji zaznajo odpiranje vrat, lom stekla, vibracije ali prisotnost v varovanem območju.«

Umetna inteligenca (UI) pomaga zmanjševati lažne alarme in varnostnim službam izpostavlja resnične incidente, njene naloge navaja Slak.

Ključna moč tehnologije danes ni posnetek dogodka – to smo imeli že pred petnajstimi leti. Pomembno je zgodnje opozorilo, da se lahko ukrepa še pred nastankom škode, poglavitna prednost teh sistemov pa je hitrost. Varnostna služba dobi opozorilo, še preden nastane dejanska škoda.

»Napadalec ne potrebuje lomilke, če ga zaposleni sam spusti skozi vrata, ker mu verjame, da je prišel popravit tiskalnik.«
Branko Slak

7. V prihodnosti več kriminala, a manj klasičnih ropov

Napoved policije temelji na podatkih zadnjih petih let: »V prihodnje je pričakovati počasno nadaljnjo rast kaznivih dejanj zoper premoženje na škodo podjetij. Hkrati je mogoče predvideti, da se bo nadaljevalo delo kriminalnih skupin, ki bodo vse pogosteje izvajale ciljno usmerjene napade na specifične sektorje, kot so trgovina, logistika in podjetja z visoko vrednostjo sredstev.«

Dobra novica v tej zgodbi pa je, da ropi kot klasično kaznivo dejanje pojenjajo. Policija pojasnjuje: »Pri določenih oblikah kaznivih dejanj, zlasti ropih, je mogoče pričakovati rahel upad – razmere v družbi se spreminjajo in na srečo klasičnih oboroženih ropov bank in drugih finančnih institucij skoraj ni več.«

8. Ključni poudarki za podjetnike:

- ★ **Integriran pristop:** Ne zanašajte se le na videonadzor. Povežite ga z alarmnimi sistemi, mehansko zaščito in strogim nadzorom dostopa.
- ★ **Varnostna kultura:** Redno usposabljajte zaposlene za prepoznavanje socialnega inženiringa in manipulacij. Zaposleni morajo vedeti, kako ravnati ob incidentu.
- ★ **Nadzor notranjih tveganj:** Dosledno omejite dostope do občutljivih delov podjetja (skladišča, blagajne, strežniki) glede na področja dela.
- ★ **Sodelovanje s strokovnjaki:** Redno izvajajte varnostne preglede in sodelujte s policijo ter licenciranimi varnostnimi službami.
- ★ **Strateška naložba:** Varnosti ne obravnavajte kot strošek, temveč kot naložbo v stabilnost poslovanja.

Grafika: Spotnet

KAKO V PODJETJIH ZAŠČITITE SVOJ DENAR V DOBI UI PREVAR IN GLOBALNIH TVEGANJ?

- Ena transakcija, milijonska škoda: kje podjetja delajo največjo napako?
- Katera sodobna tveganja danes najbolj ogrožajo finance podjetij?
- Kako se učinkovito zaščititi pred novo generacijo prevar, ki jih poganja umetna inteligenca?

Vida Petrovčič

Največje finančne katastrofe se v slovenskih podjetjih ne začnejo z zrušenimi strežniki, temveč z eno samo nepreverjeno transakcijo, rutinsko spremembo podatkov dobavitelja ali slepim poslušanjem navodil.

Najnaprednejši požarni zidovi in programska oprema ne morejo preprečiti, da bi zaposleni pod vplivom socialnega inženiringa ali zvočnega klona (deepfake) sam prostovoljno nakazal sredstva na tuji račun. V takšnem okolju človeški nadzor pogosto ne zadostuje brez dodatnih avtomatiziranih kontrol.

V zadnjih letih se je narava teh napak bistveno spremenila – od klasičnih prevar do visoko avtomatiziranih napadov, ki jih poganja umetna inteligenca (UI).

A. Notranja tveganja: prevare, ki jih poganja UI

Največja sprememba v zadnjih letih ni geopolitična, temveč tehnološka. Razvoj UI je bistveno spremenil naravo finančnih prevar. Klasične »direktorske prevare« prek e-pošte nadomeščajo napadi z uporabo zvočnih klonov in lažnih videoklicev (deepfake). Kriminalci lahko danes prepričljivo oponašajo glas direktorja ali ustvarijo videoklic, ki deluje povsem avtentično.

Ob tem dodatno tveganje predstavljajo takojšnja plačila, denimo takojšnja bančna plačila v evroobmočju (SEPA Instant), ki bistveno skrajšajo čas za preverjanje in reakcijo. V takšnem okolju človeški nadzor pogosto ni več dovolj hiter.

Čeprav tehnologija postaja vse naprednejša, ključna ranljivost ostaja človek. Podjetja, ki bodo uspešna, ne bodo tista z največ orodji, temveč tista z najboljšimi procesi odločanja.

B. Ključni ukrepi, kako zaščititi denar v praksi

Za učinkovito zaščito ni dovolj le tehnologija. Potrebna je jasna struktura odločanja, nadzora in odgovornosti. Zbrali smo sodobne in v prihodnost usmerjene nasvete za optimalno zaščito:

1. Finančni model ničelnega zaupanja (ang. zero trust)

Koncept ničelnega zaupanja ni več rezerviran samo za IT sisteme in kibernetsko varnost, temveč postaja zlati standard v financah.

Kaj ničelno zaupanje pomeni v praksi? Organizacija po privzetem stanju ne zaupa nobeni zahtevi za plačilo ali spremembi podatkov – niti če ta na videz prihaja od dolgoletnega dobavitelja, finančnega direktorja ali celo člana uprave.

Ukrep. Vsaka sprememba bančnega računa (IBAN) dobavitelja ali zahteva po izrednem nakazilu mora biti preverjena prek ločenega kanala (če zahteva pride po e-pošti, se preveri s klicem na vnaprej znano, uradno telefonsko številko partnerja – in ne tisto v podpisu e-sporočila).

2. Priprava na prevare UI

Klasične »direktorske prevare« (CEO fraud) prek e-pošte se pospešeno umikajo prevaram z uporabo UI. Kriminalci danes rutinsko klonirajo glasove direktorjev ali celo ustvarjajo lažne videoklice v realnem času (deepfakes), da odobrijo nujna izplačila.

Ukrep. Vzpostavitev tako imenovanih varnostnih besed (safewords) ali internih PIN kod za vodstveno ekipo. Če direktor po telefonu ali videoklicu zahteva nujno in tajno nakazilo, mora finančnik zahtevati varnostno besedo. Če je ne dobi, transakcije ne sme izvesti.

Največje finančne katastrofe v slovenskih podjetjih se ne začnejo z zrušenimi strežniki, temveč z eno samo nepreverjeno transakcijo.

3. Vedenjska analitika in avtomatizirano zaznavanje anomalij

Ker se plačila danes izvajajo v nekaj sekundah (SEPA Instant), človeško oko težko pravočasno zazna vse sumljive vzorce.

Ukrep. Podjetja in banke v svoje celovito upravljanje virov podjetja (Enterprise Resource Planning, ERP) in računovodske sisteme vse pogosteje integrirajo orodja UI (tehnologije, namenjene upravljanju skladnosti z zakonodajo in regulativo, RegTech), ki se naučijo »normalnega« finančnega vedenja podjetja.

Sistem samodejno zadrži in opozori na transakcijo, če se ta izvaja ob neobičajni uri, če znesek rahlo odstopa od povprečja, značilnega za tega dobavitelja, ali če gre za transakcijo v državo, s katero podjetje sicer ne posluje.

4. Kontinuiran nadzor partnerjev

Preverjanje poslovnih partnerjev (Know Your Business – KYB) zgolj na začetku sodelovanja ni več dovolj. Lastništvo podjetij in seznami posameznih sankcij se hitro spreminjajo.

Ukrep. Uporaba rešitev za stalen (avtomatiziran) nadzor bonitete, lastniških struktur in politične izpostavljenosti dobaviteljev in strank. S tem se podjetje izogne tveganju neskladnosti (compliance), blokadi lastnih računov zaradi sumov pranja denarja ali poslovanju s slamnatimi podjetji.

5. Strateška razpršitev in skrbna ocena

Podjetja se pri plemenitenju presežnih sredstev pogosto obračajo na nove fintech platforme, kripto ekosisteme ali alternativne posojilne platforme.

Ukrep. Pred prenosom sredstev na nove, pogosto tuje platforme, je nujna stroga skrbna ocena (due diligence). Podjetje mora preveriti, ali je platforma regulirana s strani uveljavljene centralne banke oziroma regulatorja in ali za sredstva velja jamstvena shema.

Sredstev (ali likvidnosti) podjetje nikoli ne sme kopičiti pri enem samem alternativnem ponudniku.

C. Operativni protokol: kako ustaviti prevaro v realnem času

Ker tehnologija sama ne more zanesljivo prepoznati deepfake napadov, mora zaščita temeljiti na jasnih procesih.

Če zaposleni v financah prejme nujen klic, glasovno sporočilo ali celo videoklic direktorja, ki zahteva takojšnje (in pogosto »tajno«) nakazilo, mora slediti naslednjemu protokolu:

1. Uvedba »varne besede« (protokol »safeword«)

Vodstvena ekipa in računovodstvo se vnaprej dogovorita za tajno besedo ali kratko frazo, ki se redno menja (na primer vsako četrtletje). Če direktor po telefonu zahteva izredno nakazilo, mora zaposleni vprašati za varno besedo. Brez nje se transakcija ne sme izvesti, ne glede na pritiske.

2. Pravilo »Prekini in pokliči nazaj« (Hang-up & Call-back)

Če zahteva pride s sumljive številke ali po nenavadni poti (na primer prek WhatsAppa namesto uradnega telefona), mora zaposleni klic takoj prekiniti. Nato mora sam poklicati direktorja nazaj na njegovo znano, uradno telefonsko številko.

3. Validacija prek drugega kanala (preverjanje »out-of-band«)

Vsako zahtevo, ki pride po enem kanalu, je treba potrditi po drugem. Če navodilo za plačilo pride prek e-pošte, se potrditev izvede po telefonu. Če pride po telefonu, se pošlje kratko sporočilo na interni sistem podjetja za potrditev.

4. Odstranitev »kazni za preverjanje«

Največji zaveznik prevarantov je strah zaposlenih pred avtoriteto (»Če ne nakažem takoj, bo direktor jezen«). Podjetje mora uvesti kulturo, kjer je zaposleni nagrajen, če prekine klic vodstva z namenom varnostnega preverjanja. Obenem pa nikoli ne sme biti kaznovan za zamudo pri izvedbi nakazila zaradi varnostnih protokolov.

Prava varnost se ne začne pri tehnologiji, temveč pri procesih.

Najnaprednejši požarni zidovi ne morejo preprečiti, da bi zaposleni pod vplivom socialnega inženiringa sam nakazal sredstva na tuji račun.

D. Zunanja tveganja: pritisk okolja na finančno stabilnost

Poleg notranjih procesov so podjetja izpostavljena tudi širšim globalnim tveganjem. Kot poudarja Mojca Piškurič, regijska direktorica za upravljanje tveganj za Coface CER regijo (= Srednja in Vzhodna Evropa), finančno stabilnost podjetij danes najbolj ogrožajo naslednja zunanja tveganja:

- motnje v dobavnih verigah in ohlajanje gospodarstva,
- geopolitična trenja in vojne, ki vplivajo na energente, transport in proizvodnjo,
- tarifne politike in premiki proizvodnje (friend-shoring in near-shoring),
- povišanje stroškov transporta,
- inflacija,
- omejitve pri dostopu do ključnih surovin,
- nepredvidljive sankcije in regulatorni ukrepi.

Globalizacija se spreminja in nastajajo novi gospodarski bloki, to pa vpliva na stabilnost evropskega gospodarstva, opozarja Piškuričeva.

E. Kako se lahko podjetja obvarujejo pred zunanjimi tveganji?

Odgovor na zunanja tveganja je predvsem v prilagodljivosti. Glavni ukrepi po mnenju Mojce Piškurič in Klemna Tomca vključujejo:

- diverzifikacijo dobaviteljev, partnerjev, naložb in trgov,
- diverzifikacijo delovne sile in kompetenc,
- zmanjšanje odvisnosti od posameznih platform ali virov prihodkov,
- zgodnje prepoznavanje sprememb v vedenju strank in konkurence ter
- redno stresno testiranje poslovanja.

Ukradena sredstva se po izvedeni transakciji skoraj takoj razpršijo prek mreže mednarodnih denarnih mul.

Grafika: Spotnet

KORPORATIVNE PREVARE V SLOVENIJI: TUDI MILIJONSKA OŠKODOVANJA

- Kdaj ste nazadnje preverili, kdo v vašem podjetju lahko odobri plačilo?
- Bi opazili, če bi nekdo spremenil bančni račun vašega dobavitelja?
- Ste prepričani, da največja finančna grožnja prihaja od zunaj, in ne od znotraj?

Vida Petrovčič

Največje finančne izgube se pogosto zgodijo daleč stran od hekerskih vdorov – znotraj vsakodnevnih poslovnih procesov. Na to opozarjajo strokovnjaki za finančno varnost, Združenje bank Slovenije (ZBS) in Sektor za gospodarsko kriminaliteto pri MNZ.

Sodobne grožnje financam podjetij izvirajo iz zlorabe človeškega zaupanja, pomanjkljivih notranjih finančnih kontrol, manipulacije klasičnih poslovnih tokov in tveganj, ki jih prinašajo nove, pogosto premalo regulirane finančne platforme. Digitalizacija je tveganja sicer razširila, ni pa spremenila njihovega bistva: najšibkejši člen ostaja človek.

Prava finančna varnost podjetja je zato v svojem jedru vprašanje obvladovanja človeškega faktorja, strogih revizijskih procesov in neprepustnih procedur odobravanja transakcij.

A. Tradicionalna in nova tveganja: ista logika, novi kanali

Podjetja se danes soočajo z bistveno širšim naborom finančnih tveganj kot v preteklosti, ugotavljajo na Združenju bank Slovenije (ZBS). Tveganja se pojavljajo tako na tradicionalnih kot na novih, digitalnih finančnih platformah.

Na eni strani ostajajo klasična tveganja, kot so likvidnostni pritiski, spremembe obrestnih mer, valutna nihanja in kreditna tveganja v dobavnih verigah.

Na drugi strani v ospredje vse bolj stopajo sodobne grožnje, povezane z digitalizacijo – predvsem kibernetski napadi, zlorabe plačilnih sistemov, prevare ter tveganja, povezana z uporabo novih tehnologij in platform – pa tudi tveganja, povezana z geopolitičnimi razmerami, kot so vojne, sankcije, trgovinski konflikti in nestabilnost na globalnih trgih.

Ključna sprememba ni v tem, da so tveganja nova, temveč v tem, da so hitrejša, bolj prikrita in pogosto videti povsem legitimna.

Podjetja morajo zato dandanes zaščito svojega premoženja razumeti bistveno širše, kot je zgolj klasično zavarovanje. Ključno sporočilo za podjetja je, da finančna varnost ni produkt, ampak sistem. To pa pomeni boljše razumevanje izpostavljenosti, uvedbo procesnih varovalk, aktivno sodelovanje s finančnimi partnerji in stalno prilagajanje spremembam.

B. 5 korakov do varnosti

1. Prepoznajte tveganja
Vzpostavite popoln pregled nad denarnimi tokovi, terjatvami, dobavitelji in digitalnimi sredstvi. Brez tega zaščita ni mogoča.

2. Okrepite upravljanje likvidnosti
Analizirajte vpliv globalnih sprememb (energija, dobavne verige, povpraševanje) na poslovanje.

3. Razpršite tveganja
Ne zanašajte se na en vir financiranja, en trg ali enega ključnega partnerja.

4. Nadgradite zaščito pred sodobnimi grožnjami
Kibernetska varnost in preprečevanje prevar morata vključevati tehnologijo in ljudi. Redno usposabljanje je nujno.

5. Prilagajajte se spremembam
Podjetja, ki se hitro prilagajajo, so dolgoročno stabilnejša in varnejša. Okrepite upravljanje likvidnosti in analize učinkov sprememb globalnih razmer (učinke na cene energije, dobavne verige in povpraševanje) na svoje poslovanje in likvidnost ter razpršite tveganja.

Vir: ZBS

Največje finančne izgube se pogosto ne zgodijo zaradi hekerskih vdorov, temveč precej bolj neopazno – znotraj vsakodnevnih poslovnih procesov.

C. Največje grožnje prihajajo iz poslovnih procesov

Največje finančne grožnje danes ne izvirajo iz IT oddelka, temveč iz poslovnih procesov. Najpogostejši scenariji so naslednji:

1. Direktorske prevare in manipulacija plačilnih procesov (socialni inženiring)
Kriminalci ne napadajo strežnikov, temveč ljudi. S psihološkim pritiskom, ponarejenimi listinami ali lažnimi navodili zaposlene v financah prepričajo, da nakažejo sredstva na tuje račune ali spremenijo bančne podatke dolgoletnih dobaviteljev. Napad je usmerjen neposredno v poslovni proces.

2. Investicijske prevare in zlorabe novih finančnih platform
Podjetja v iskanju višjih donosov za presežna likvidnostna sredstva vstopajo na nove »fintech« platforme, neregulirane trge ali posojilne sheme (crowdlending), kjer ni ustreznih jamstvenih shem ali strogega nadzora centralnih bank. Sredstva so tu izpostavljena popolni izgubi zaradi sistemskih zlorab platform samih.

3. Notranje prevare in poneverbe
Ena najstarejših, a še vedno najbolj uničujočih groženj. Pomanjkanje striktnega ločevanja dolžnosti (segregation of duties) in mehanizma »štirih oči« zaposlenim omogoča prirejanje bilanc, fiktivna izplačila, kreiranje lažnih dobaviteljev ali neupravičeno rabo podjetniških kreditnih linij.

4. Tveganja neskladnosti in pranje denarja
S poslovanjem prek alternativnih platform in globalnih verig se podjetja (včasih nevede) vpletejo v sumljive finančne tokove. Blokade računov s strani bank zaradi sumov pranja denarja ali drakonske kazni regulatorjev lahko čez noč ustavijo likvidnost podjetja.

Finančno izčrpavanje podjetij je danes redko videti kot spektakularen napad. Pogosteje gre za tihe, postopne odlive, skrite v legitimnih procesih.

Iz policijskih podatkov izhaja, da je gospodarska kriminaliteta vse bolj mednarodna in organizirana, sredstva pa se po transakciji hitro razpršijo prek mreže posrednikov, kar otežuje njihovo povrnitev.

Slovenska policija in ZBS redno beležita primere korporativnih prevar, kjer posamezna oškodovanja podjetij dosegajo več sto tisoč ali celo milijone evrov. Ukradena sredstva se po izvedeni transakciji skoraj takoj razpršijo prek mreže mednarodnih denarnih mul.

Č. Kako vzpostaviti neprepusten sistem?

Čeprav podjetja pogosto iščejo zunanje grožnje, praksa kaže, da ima velik del tveganj svoj izvor znotraj organizacije. ZBS v sklopu rednih preventivnih kampanj poudarja, da je najboljša obramba pred finančnim izčrpavanjem podjetja kritična presoja zaposlenih in strogo, večnivojsko preverjanje vseh zahtevkov za spremembe transakcijskih računov. Ključne varovalke so naslednje:

1. Striktno ločevanje dolžnosti

Gre za temeljno varnostno pravilo. Ista oseba ne sme imeti pooblastila za vnos novega dobavitelja v sistem in hkrati za potrjevanje plačil temu dobavitelju. Procesna ločitev teh nalog drastično zmanjša možnost manipulacij.

2. Načelo štirih oči

Vsaka izhodna transakcija nad določenim zneskom ali sprememba ključnih finančnih podatkov (na primer TRR dobavitelja) mora iti skozi sito dveh neodvisnih oseb. Avtomatizacija tega pravila v računovodskih in bančnih sistemih preprečuje samovoljno odtekanje sredstev.

3. Politika obveznih dopustov in rotacija nalog

Številne dolgoletne in skrbno prikrite poneverbe se razkrijejo šele, ko mora zaposleni oditi na daljši strnjen dopust (na primer za vsaj 14 dni), njegove vsakodnevne naloge pa začasno prevzame sodelavec.

4. Neodvisne in nenapovedane revizije

Redni letni pregledi pogosto niso dovolj, saj se je nanje mogoče pripraviti. Občasno in nenapovedano revidiranje naključnih vzorcev finančnih tokov – bodisi s strani zunanjih strokovnjakov bodisi neodvisne notranje kontrole – deluje kot izjemno močan preventivni mehanizem.

5. Vzpostavitev varnih kanalov za prijavo (whistleblowing)

Statistično gledano se največ notranjih prevar ne odkrije z vgrajenimi kontrolami, temveč prek namigov sodelavcev. Podjetja morajo ustvariti varno okolje in sistem, ki omogoča anonimno in zaščiteno prijavo sumov nepravilnosti.

D. Ključno sporočilo za vodstva

Največja napaka podjetij je prepričanje, da je varnost vprašanje zaupanja. Ni. Katera so tri pravila za večjo finančno varnost podjetij?

1. Zaupanje ni kontrolni mehanizem.

Največje finančne izgube se v praksi ne zgodijo zaradi pomanjkljive tehnologije, temveč zaradi slepega zaupanja. Ker so ljudje najpogostejša tarča manipulacij, mora organizacija iz kulture absolutnega zaupanja preiti v kulturo »zaupaj, a preverjaj« – tako pri lastnih zaposlenih kot pri dolgoletnih zunanjih partnerjih.

2. Varnost mora biti sistemska, ne osebna.

Če je finančna stabilnost vašega podjetja odvisna od ene same »nepogrešljive« osebe v financah ali računovodstvu, je vaše podjetje v visoki nevarnosti. Pravilo štirih oči in strogo ločevanje dolžnosti morata biti vgrajena v same temelje poslovanja in procese odobravanja, ne glede na velikost podjetja.

3. Nove platforme zahtevajo staro previdnost.

Hitri donosi na nereguliranih alternativnih finančnih platformah ali poslovanje prek nepreverjenih mednarodnih posrednikov so pogosto past. Pred vstopom v vsak nov finančni ekosistem je nujna stroga presoja tveganj, saj izguba sredstev na tovrstnih platformah običajno ni krita z državnimi ali bančnimi jamstvi.

Grafika: Spotnet

POŠKODBE PRI DELU: STAREJŠA DELOVNA SILA PRINAŠA NOVA TVEGANJA

- Kako se danes spreminjajo poškodbe pri delu v primerjavi s preteklostjo?
- Kako staranje delovne sile vpliva na tveganja pri delu?
- Katera tveganja pri delu danes najbolj naraščajo?

Marija Mica Kotnik

Pod vplivom staranja delovne sile ter tudi digitalizacije in avtomatizacije se spreminja narava poškodb. Zdaj ni več vprašanje, kako preprečiti nezgode, ampak kako zaščititi vse bolj raznoliko in starajočo se delovno populacijo.

Poškodbe pri delu v Sloveniji ostajajo pomemben izziv. V letu 2024 je bilo prijavljenih več kot 14.000 nezgod, od tega okoli 16 smrtnih in več kot 900 težjih poškodb. Kljub napredku varnostnih ukrepov se njihovo število ne zmanjšuje bistveno, temveč niha.

A. Trendi: Poškodbe so drugačne

Slovenija se hitro stara. Leta 2024 je bilo že približno 22 odstotkov prebivalcev starejših od 65 let, kaže raziskava Statističnega urada Republike Slovenije (SURS). Povprečna starost prebivalstva narašča, hkrati pa se povečuje tudi delež starejših v delovno aktivni populaciji. Približno tretjina delovno aktivnih je starih od 50 do 64 let, kažejo podatki ministrstva za delo, družino, socialne zadeve in enake možnosti.

Raziskave v članku Pojavnost, dejavniki tveganja in izidi nefatalnih delovnih poškodb pri starejših delavcih – Pregled raziskav iz obdobja 2010–2019 – kažejo, da starejši delavci praviloma utrpijo manj nezgod kot mlajši, vendar so njihove poškodbe navadno hujše, okrevanje pa daljše.

V takšnih razmerah se nujno spreminjajo tudi tveganja pri delu, opozarja direktorica podjetja CPV in strokovnjakinja za tveganja pri delu Sara Mlakar: »Poškodbe pri delu se v prihodnje ne bodo nujno zmanjševale, ampak se bodo predvsem spreminjale po svoji naravi, kar kaže tudi trend v Sloveniji.«

Tehnologija, digitalizacija in avtomatizacija sicer zmanjšujejo nekatere klasične fizične poškodbe, zlasti v industriji in gradbeništvu. Lahko pa pričakujemo porast poškodb zaradi nenadnih obremenitev, kognitivne preobremenjenosti ter novih oblik sodelovanja med človekom in strojem, pojasnjuje Sara Mlakar.

Ob tem posebej izpostavlja starejše delavce: »Z leti se zmanjšujejo fizične sposobnosti, podaljšuje čas okrevanja in povečuje verjetnost hujših posledic ob nezgodah.« To pomeni, da staranje delovne sile ne vpliva le na število poškodb, ampak predvsem na njihovo resnost.

> **Začelo se bo povečevati število poškodb zaradi novih tehnologij, kot je interakcija človek–mehanizacija–roboti.«**
> Dani Mirnik

B. Nova tveganja: več nevidnih poškodb

Kot ocenjuje asistent dr. med. Dani Mirnik iz Centra za medicino dela na Zavodu za varstvo pri delu, se bodo trendi na področju poškodb pri delu v prihodnjih letih jasno preoblikovali.

V prihodnje bodo bolj izpostavljene različne skupine delavcev iz različnih razlogov. Mlajši delavci bodo bolj ogroženi predvsem zaradi pomanjkanja izkušenj, zlasti pri delu z novimi tehnologijami, medtem ko bodo starejši delavci bolj izpostavljeni zaradi zmanjšanih fizičnih sposobnosti, daljšega okrevanja in večje verjetnosti hujših posledic ob nezgodah, našteva Mirnik.

Povečano tveganje se kaže tudi v posameznih dejavnostih. V zdravstvu, socialni oskrbi in storitvenih dejavnostih pričakujemo največji porast

Starejši delavci praviloma utrpijo manj nezgod kot mlajši, vendar so njihove poškodbe večinoma hujše, okrevanje pa daljše.

poškodb, predvsem zaradi staranja prebivalstva in večjega števila ljudi, ki potrebujejo oskrbo, navaja Mirnik: »To se kaže v več nezgodah pri premeščanju pacientov, več je zdrsov in padcev ter tudi več primerov napadov ali ugrizov.«

Dodatno tveganje predstavljajo tudi dolge izmene in hibridne oblike dela, ki povečujejo utrujenost in s tem verjetnost za nastanek nezgod. Toda po drugi strani Mirnik opozarja, da se bo hkrati začelo povečevati število poškodb zaradi novih tehnologij, kot je interakcija človek–mehanizacija–roboti.

Povečevalo pa se bo tudi število ponavljajočih se poškodb in poškodb, povezanih s psihosocialnimi obremenitvami. V ospredje prihajajo mišično-skeletne težave, preobremenjenost in posledice dolgotrajnega dela pod pritiskom.

Staranje delovne sile bo vplivalo predvsem na resnost poškodb in podaljšalo čas okrevanja, opozarja Mirnik: »Poškodbe bodo zato pogosteje imele hujše posledice, tudi če jih bo morda absolutno manj.« S starostjo se namreč zmanjšujejo predvsem fizične in senzorične sposobnosti, kaže raziskava EU-OSHA. To pa povečuje tveganja pri fizično zahtevnih delih in zahteva prilagoditve delovnega okolja.

V proizvodnji in montažnih delih se z avtomatizacijo zmanjšujejo klasične poškodbe, a rastejo mišično-skeletne poškodbe in psihofizične obremenitve pri nadzoru strojev, dodaja Mirnik.

C. Kako poskrbeti za varnost?

Evropska agencija za varnost in zdravje pri delu (EU-OSHA) opozarja, da postaja upravljanje varnosti v kontekstu starajoče se delovne sile ena ključnih prioritet sodobnih delovnih okolij. Kot pravi Sara Mlakar, bo ključen celosten pristop k varnosti in zdravju pri delu. Ta ne vključuje le fizičnih tveganj, temveč tudi psihosocialne obremenitve in organizacijo dela.

Z leti se zmanjšujejo fizične sposobnosti, podaljšuje čas okrevanja in povečuje verjetnost hujših posledic ob nezgodah.«
Sara Mlakar

Po besedah sogovornikov bo preprečevanje poškodb pri delu v prihodnje zahtevalo bolj ciljno usmerjen in celosten pristop. Med ključnimi ukrepi izpostavljajo natančnejše ocenjevanje tveganj, tudi z uporabo digitalnih orodij, ki omogočajo boljše prepoznavanje nevarnosti v delovnem procesu.

Pomembno vlogo bodo imele tudi obvezne ergonomske ocene delovnih mest, saj se vse več poškodb pojavlja kot posledica dolgotrajnih obremenitev in ponavljajočih se gibov. Nujno bo tudi ustrezno usposabljanje zaposlenih za delo z novimi tehnologijami, vključno z umetno inteligenco (UI) in robotiko.

D. Klasične poškodbe ostajajo, a počasi upadajo

V Sloveniji se po podatkih Nacionalnega inštituta za javno zdravje (NIJZ) število prijavljenih poškodb pri delu v obdobju od leta 2014 do 2024 ne zmanjšuje, temveč opazno niha. Poškodbe prednjačijo v panogah kmetijstva, predelovalne dejavnosti, gradbeništva ter prometa in skladiščenja.

Največ poškodb je po Mirnikovih ugotovitvah še vedno zabeleženih v gradbeništvu in težki industriji, kjer je tveganje za poškodbe visoko.

Prevladujejo klasične mehanske poškodbe:

- padci z višine,
- udarci,
- zmečkanine.

Te poškodbe bodo ostale prisotne, napoveduje sogovornik, a hkrati dodaja, da se bo pogostnost teh poškodb zmanjševala zaradi boljših zaščitnih sistemov, izboljšane mehanizacije in robotizacije ter eksoskeletonov.

E. Najpogostejši vzroki za nezgode pri delu

- nepoučenost delavcev o nevarnostih pri delu,
- slaba organizacija dela in neurejenost delovišča,
- neposreden nadzor in pomanjkljivo vodenje pri nevarnejših opravilih,
- neustrezno delovno okolje ter delovna oprema brez zaščit ali varoval,
- nepazljivost in podcenjevanje nevarnosti,
- neupoštevanje predpisanih navodil in znakov za nevarnosti,
- improviziranje, kljub dolgoletnim izkušnjam, ter neizkušenost novih delavcev,
- pomanjkljiva uporaba ali pa neuporaba osebne varovalne opreme.

(Vir: IRSD)

Grafika: Spotnet

NOVE POKLICNE BOLEZNI SO POVEZANE Z – ZELENIM PREHODOM

- Katere poklicne bolezni prihajajo zaradi sprememb v ekonomiji?
- Kako občutno se je povečalo število primerov izgorelosti?
- Katera poklicna obolenja povzroča – hibridno delo?

Marija Mica Kotnik

Struktura poklicnih bolezni se hitro spreminja. Klasične bolezni počasi upadajo, po drugi strani pa naraščajo nove. Prinašajo jih sodobna tveganja, povezana predvsem z nanomateriali, zelenim prehodom in močnimi psihosocialnimi obremenitvami.

V Sloveniji priznavamo le okoli 25 do 50 poklicnih bolezni na leto. Nekateri strokovnjaki sicer ocenjujejo, da bi jih moralo biti med 800 in 1.000 – to pa bi pomenilo, da jih podcenjujemo tudi do 400-kratno.

Ta razkorak kaže na pomanjkljivo odkrivanje in prepoznavanje povezave med delom in zdravstvenimi težavami. Toda še bolj zanimivo je, da se nove poklicne bolezni pojavljajo zaradi nove ekonomije.

1. Novi vzroki za poklicne bolezni: recikliranje, biomasa …

Specialist medicine dela as. dr. Dani Mirnik iz Centra za medicino dela na Zavodu za varstvo pri delu opozarja, da bosta napredek industrializacije in zeleni prehod prinesla nove izpostavljenosti, in sicer:

- ★ kemikalijam pri recikliranju,
- ★ raznim respiratornim težavam pri delu z biomaso in
- ★ težavam pri izdelovanju ter predelavi baterij.

V storitvenih dejavnostih pa bodo v ospredje stopile duševne in vedenjske motnje, predvsem izgorelost, anksioznost in depresija.

Glavni vzroki so večji psihosocialni pritiski, informacijska preobremenitev, pomanjkanje socialnih stikov pri hibridnem delu ter slaba ergonomija delovnih mest, ki vodi v porast mišično-skeletnih težav.

Pri tem moramo poudariti, da nobena od zgoraj naštetih duševnih in vedenjskih motenj še vedno ni priznana kot poklicna bolezen. Spadajo med bolezni, ki so povezane z delom, vendar brez pravnih posledic poklicne bolezni.

Po podatkih Nacionalnega inštituta za javno zdravje (NIJZ) za leto 2024 so duševne in vedenjske motnje na četrtem mestu med vzroki za bolniški stalež in predstavljajo vse večji delež izgubljenih delovnih dni.

Število primerov izgorelosti se je od leta 2014, ko so jih zabeležili 108, močno povečalo, in sicer na 1.810 v letu 2024/25, navaja NIJZ. Število izgubljenih dni je s 5.000 na leto naraslo na skoraj 97.000. Bolniške za izgorelost v povprečju namreč trajajo 53,4 dni.

Na ministrstvu za delo so sicer že pred časom pojasnili, da je izgorelost težko objektivno dokazati in da bi uvrstitev med poklicne bolezni zahtevala stroge kriterije, kar pa je pri tej vrsti motnje zelo zahtevno.

Nova tveganja: kemikalije pri recikliranju, respiratorne težave pri delu z biomaso in težave pri izdelovanju in predelavi baterij.

V Sloveniji priznavamo le okoli 25 do 50 poklicnih bolezni na leto. Strokovnjaki ocenjujejo, da je teh primerov med 800 in 1.000.

2. V ZDA bistveno več izgorelosti kot v EU

Po podatkih Mednarodne organizacije za delo (ILO) in Svetovne zdravstvene organizacije (WHO) delo vsako leto povzroči približno 2,9 milijona smrti po vsem svetu, od tega kar 89 odstotkov zaradi z delom povezanih bolezni (ne nesreč).

Psihosocialni dejavniki tveganja (dolge delovne ure, visok pritisk, pomanjkanje nadzora, mobing) so odgovorni za več kot 840.000 smrti letno zaradi srčno-žilnih bolezni in duševnih motenj ter za izgubo skoraj 45 milijonov let zdravega življenja.

V Evropski uniji (EU) kar 29 odstotkov delavcev poroča o stresu, depresiji ali anksioznosti, ki so jih povzročili ali poslabšali delovni pogoji, navaja poročilo Poklicna varnost in zdravje 2025: Klimatske spremembe na delu, ki ga pripravlja Evropska agencija za varnost in zdravje pri delu (EU-OSHA).

V ZDA celo polovica zaposlenih poroča o zmerni do hudi izgorelosti, depresiji ali anksioznosti, kaže raziskava o duševnem zdravju na delovnem mestu, ki so jo naredili pri organizaciji za duševno zdravje zaposlenih Mind Share Partners. Najbolj so izpostavljeni zdravstveni delavci, učitelji, negovalci in mlajše generacije.

A vzroki poklicnih bolezni ne bodo več klasične fizikalne in kemijske nevarnosti, temveč psihosocialna tveganja in spreminjajoče se delovno okolje, napovedujejo tuji strokovnjaki. EU-OSHA in ILO poudarjata, da so največji izzivi digitalizacija, hibridno delo, zeleni prehod in podnebne spremembe (ekstremna vročina, izpostavljenost novim snovem).

V Evropski uniji 29 % delavcev poroča o stresu, depresiji ali anksioznosti, ki so jih povzročili ali poslabšali delovni pogoji. V ZDA o tem poroča polovica.

3. Število klasičnih bolezni bo upadalo

Dani Mirnik dodaja, da bodo v industriji, rudarstvu in gradbeništvu še vedno prevladovale klasične poklicne bolezni:

1. poklicna naglušnost zaradi hrupa,
2. silikoza,
3. azbestoza,
4. kostno-mišične bolezni zaradi vibracij in težkih bremen, ki bodo še vedno prisotne zaradi dolge latence.

Število klasičnih poklicnih bolezni bo verjetno z leti sicer upadlo, pričakujemo pa lahko porast novih poklicnih bolezni oziroma z delom povezanih bolezni tako v industrijah kot v storitvenih dejavnostih, dodaja Mirnik.

10 PRAKTIČNIH NASVETOV ZA ZAŠČITO ZAPOSLENIH

1. Redna ocena tveganj na delovnem mestu.
2. Zagotavljanje ergonomsko prilagojenih delovnih mest.
3. Kontinuirana izobraževanja o varnem delu, vključno z grajenjem kompetenc.
4. Promocija dobrega duševnega zdravja in obvladovanje stresa.
5. Pravilna uporaba zaščitne opreme, kjer je to potrebno.
6. Spodbujanje odprte komunikacije med zaposlenimi in vodstvom.
7. Zagotavljanje možnosti za odmore in regeneracijo.
8. Uvedba fleksibilnega delovnega časa.
9. Redni zdravstveni pregledi.
10. Spodbujanje redne telesne dejavnosti.

Število izgubljenih dni zaradi izgorelosti na leto je s 5.000 leta 2014 naraslo na skoraj 97.000 (2024/25).

CWS WORKWEAR

NAJEM DELOVNIH OBLAČIL KOT PODPORA PRI IZPOLNJEVANJU INVALIDSKIH KVOT

Podjetja z več kot 20 zaposlenimi imajo po veljavni zakonodaji obveznost zaposlovanja invalidov v določenem deležu, ne glede na dejavnost.

Če tega deleža ne dosežejo, morajo za vsako manjkajoče delovno mesto plačevati prispevek v ustrezni državni sklad, namenjen spodbujanju zaposlovanja invalidov. Ti stroški se lahko hitro povečajo, saj že pri dveh manjkajočih zaposlenih predstavljajo skoraj 25.000 € letno.

Ena izmed zakonsko predvidenih možnosti je nadomestno izpolnjevanje kvot preko sodelovanja z invalidskimi podjetji. V podjetju CWS Workwear IP d.o.o. to obveznost nadgrajujemo v praktično poslovno rešitev: celovit sistem najema in vzdrževanja delovnih oblačil, ki podjetjem prinaša konkretno operativno vrednost.

Storitev ni omejena le na podjetja, ki uveljavljajo kvote. Namenjena je širokemu spektru naročnikov iz različnih panog in velikosti, od proizvodnje do farmacije. Cenovni model je enoten za vse uporabnike, ne glede na morebitne olajšave, ki izhajajo iz invalidske zakonodaje.

Celostni pristop k upravljanju delovnih oblačil

Model najema delovnih oblačil je v številnih evropskih državah že uveljavljen standard, v Sloveniji pa še vedno predstavlja sodoben pristop k upravljanju delovnih oblačil. Gre za sistem, ki združuje logistiko, higieno in stroškovno predvidljivost ter hkrati zagotavlja urejen in profesionalen videz zaposlenih.

V okviru storitve najema delovnih oblačil pri CWS Workwear je vključeno naslednje:

- ★ strokovno svetovanje in prilagoditev oblačil posameznikom,
- ★ možnost personalizacije (barve, logotipi, imena, kroji),
- ★ redno organizirano zbiranje umazanih in dostava opranih oblačil,
- ★ industrijsko pranje v certificiranih pralnih obratih,
- ★ popravila in vzdrževanje poškodovanih kosov,
- ★ zamenjava obrabljenih oblačil,
- ★ digitalno sledenje kosom z oznakami in RFID tehnologijo.

Storitveni model temelji na mesečnem naročilu, ki ostaja stabilno in pregledno, brez dodatnih ali skritih stroškov. To podjetjem omogoča boljšo organizacijo, manj administrativnega dela in večji nadzor nad procesi.

Vzdrževanje zaščitnih lastnosti tekstila

Pri delovnih oblačilih je ključnega pomena, da po uporabi in čiščenju ohranijo svoje zaščitne funkcije. Da bi vam to lahko zagotovili, se v naših certificiranih pralnicah uporabljajo specializirani postopki čiščenja, prilagojeni različnim materialom in zahtevam posameznih industrij.

To je posebej pomembno v okoljih, kjer zaposleni uporabljajo zaščitno opremo ali so izpostavljeni toploti, kemikalijam, iskram, ali biološkim dejavnikom. Pravilno vzdrževanje podaljšuje življenjsko dobo tekstila in zagotavlja skladnost z varnostnimi ter higienskimi standardi.

Rešitve za različne industrije

Storitev je primerna za številne dejavnosti, od lažje industrije, za katere ponujamo splošna delovna oblačila, do zahtevnih proizvodnih in storitvenih okolij, za katera so na voljo specializirana zaščitna oblačila. Med uporabniki so podjetja iz kovinske, živilske in farmacevtske industrije, zdravstva, gradbeništva, gostinstva in logistike. Sistem omogoča prilagoditev oblačil specifičnim delovnim pogojem ter hkrati prispeva k enotni in urejeni podobi podjetja.

Profesionalna obdelava tekstila za institucije

Poleg delovnih oblačil izvajamo tudi storitve profesionalnega čiščenja in obdelave ravnega perila za bolnišnice, hotele in druge ustanove. V ta namen deluje specializiran pralni obrat v Škofji Loki, kjer zagotavljamo visoko raven higiene in standardizirane postopke obdelave tekstila.

Grafika: Spotnet

BI VAŠE PODJETJE PREŽIVELO PRAVO NESREČO?

V IGRI SO LAHKO MILIJONI EVROV.

- Kje so najpogostejše napake, ki lahko podražijo ali celo onemogočijo uspešno reševanje v podjetjih?
- Ali veste, da boste morali do oktobra zamenjati gasilne pene, ki vsebujejo PFAS snovi?
- Ali z vsako dograditvijo proizvodnje poskrbite za primerne spremembe v načrtu za reševanje?

Almira Sakalić

Zaščita in reševanje v sodobnem industrijskem okolju že dolgo nista več le vprašanje gasilnega aparata na hodniku. Postajata visokotehnološka disciplina, ki za varno in uspešno obvladovanje izrednih dogodkov zahteva tesno sodelovanje med gospodarstvom in interventnimi službami.

Kot poudarjajo na Upravi RS za zaščito in reševanje (URSZR) ter na Gasilski zvezi Slovenije (GZS), največja nevarnost ni pomanjkanje predpisov, temveč razkorak med papirnatimi načrti in dejansko pripravljenostjo na terenu.

A. Koliko stane industrijska nesreča?

Škoda pri industrijskih nesrečah v Sloveniji je zelo različna. Manjši in srednji požari v podjetjih po podatkih Policije in zavarovalnic običajno povzročijo škodo med 50.000 in 300.000 evrov. Resnejši dogodki (večji požari, eksplozije ali nesreče z nevarnimi snovmi) hitro presežejo milijon evrov neposredne materialne škode.

Ko k temu prištejemo izpad proizvodnje, izgubo naročil, dodatne stroške sanacije in škodo pri ugledu, se končni znesek pogosto podvoji ali celo potroji. Primer eksplozije v Melaminu Kočevje leta 2022 kaže, da lahko skupna škoda pri resnih industrijskih nesrečah doseže več deset milijonov evrov.

Po podatkih Evropske agencije za varnost in zdravje pri delu (EU-OSHA) delovne nesreče in poklicne bolezni Evropo letno stanejo kar 476 milijard evrov oziroma 3,3 odstotka BDP.

Evropske države v povprečju vlagajo relativno malo v preventivne ukrepe proti naravnim in tehnološkim nesrečam (pogosto pod 0,2 odstotka BDP na ravni države), kažejo podatki Svetovne banke in Evropske komisije. Pri tem Slovenija zaostaja za državami z močnejšo industrijsko varnostno kulturo, kot sta Avstrija in Nemčija.

B. Kaj morajo podjetja storiti pred prihodom reševalcev?

Zaščita in reševanje nista zgolj zakonska obveza, temveč ključni del strategije neprekinjenega poslovanja. Podjetje, ki vlaga v varnostno kulturo, ne varuje le svojih strojev in prostorov, temveč predvsem svoje najdragocenejše premoženje – svoje ljudi. Kako se lahko bolje pripravite?

Ključni koraki so:

1. Ažurna dokumentacija:
En izvod požarnega načrta mora biti vročen gasilski enoti, ki opravlja javno službo na vašem območju. Gasilci lahko predlagajo dopolnitve, če ocenijo, da je načrt pomanjkljiv.

2. Proste poti in dostopi:
Evakuacijske poti, dovozi in delovne površine za intervencijska vozila morajo biti v vsakem trenutku prehodni, prosti in pravilno označeni. Dostop do gasilne opreme ne sme biti blokiran s skladiščenim materialom.

3. Vaje evakuacije:
»Organizacije spodbujamo, naj vaje evakuacije izvedejo vsaj enkrat letno,« svetujejo na URSZR. Le tako zaposleni razvijejo avtomatizem, ki v stresu prepreči paniko.

4. Sodelovanje z lokalno gasilsko enoto:
Skupni ogledi objekta in vaje so najučinkovitejši način, da reševalci spoznajo specifike vaših tehnoloških procesov še pred nesrečo.

Manjši in srednji požari v podjetjih po podatkih Policije in zavarovalnic običajno povzročijo škodo med 50.000 in 300.000 evrov. Resnejši dogodki presežejo milijon evrov škode.

5. Digitalna pripravljenost:
Uporaba sodobnih orodij (termovizija, droni) povečuje varnost reševalcev in učinkovitost reševanja premoženja.

6. Priprava na prepoved v letu 2026:
Pravočasno začnite načrtovati zamenjavo gasilnih pen, ki vsebujejo PFAS, saj bo njihova uporaba po oktobru 2026 prepovedana.

7. Pripravljeni zaposleni:
Ob intervenciji morajo biti vaši zaposleni pripravljeni takoj usmeriti reševalce in jim podati ključne informacije o nevarnostih v objektu.

C. Kje so najpogostejše vrzeli?

Izkušnje s terena kažejo, da največ težav ne nastane zaradi pomanjkanja predpisov, temveč zaradi razkoraka med formalnimi zahtevami in realnostjo. Gasilska zveza Slovenije opozarja na:

- ★ **Neskladje med dokumentacijo in dejanskim stanjem:** Dograditve ali spremembe v proizvodnji, ki niso vnesene v načrte.
- ★ **Pomanjkljivo označevanje:** Neustrezno označene nevarne snovi ali poti.
- ★ **Pomanjkanje komunikacije:** Podjetja pogosto izpolnijo le formalne obveznosti, zanemarijo pa preventivne oglede objektov skupaj z lokalnimi gasilci.

Č. Tehnološki preboji v gasilstvu

Tako kot se digitalizira industrija, se posodablja tudi oprema reševalcev. Danes oprema postaja ergonomska, robustna in digitalno podprta, to pa bistveno prispeva k varnosti gasilcev v zahtevnih razmerah:

- ★ **Sodobni izolirni dihalni aparati:** Omogočajo stalno spremljanje porabe zraka in fiziološkega stanja gasilca.
- ★ **Termovizijske kamere:** Danes so nepogrešljivo orodje pri orientaciji in odkrivanju skritih žarišč, zlasti v kompleksnih industrijskih objektih.
- ★ **Brezpilotni letalniki (droni):** Omogočajo hiter pregled večjih območij in podporo pri taktičnih odločitvah z varne razdalje.

Slovenija pri preventivnih ukrepih v podjetjih zaostaja za državami z močnejšo industrijsko varnostno kulturo, kot sta Avstrija in Nemčija.

Tudi usposabljanje prostovoljnih in poklicnih gasilcev prehaja v hibridni model. Klasične praktične vaje se združujejo z e-učenjem, spletnimi seminarji in virtualnimi vadbenimi okolji, kar omogoča simulacijo najzahtevnejših scenarijev brez dejanskega tveganja.

D. Prelomno leto 2026: Konec pen s PFAS

Ena največjih tehničnih sprememb v bližnji prihodnosti je povezana z okoljsko zakonodajo. Evropska komisija je sprejela Uredbo (EU) 2025/188, ki močno vpliva na uporabo gasilnih pen po vsej EU. Po 23. oktobru 2026 bodo morale vse enote in podjetja opustiti pene, ki vsebujejo PFAS (per- in polifluoroalkilne snovi).

Te snovi, ki jih pogosto imenujemo tudi večne kemikalije, so bile doslej zelo priljubljene v gasilnih penah, ker odlično dušijo plamene, nastale zaradi vnetljivih tekočin, kot so bencin, olja in topila. Vendar so izjemno obstojne v okolju, kopičijo se v živih organizmih in so potencialno škodljive za zdravje ljudi.

Podjetja bodo morala:

- pregledati obstoječe zaloge gasilnih aparatov in sistemov,
- postopoma zamenjati pene z okolju prijaznejšimi alternativami,
- preveriti združljivost nove pene z obstoječo opremo (gasilniki, fiksni sistemi).

To je pomembna sprememba, ki zahteva pravočasno načrtovanje, saj lahko neustrezna zamenjava vpliva na učinkovitost gašenja.

Skupni ogledi objekta in vaje z lokalno enoto gasilcev so najučinkovitejši način, da reševalci spoznajo specifike vaših tehnoloških procesov še pred nesrečo.

E. Zakonodajni okvir kot stalnica, ki zahteva doslednost podjetij

Naloge gospodarskih družb na področju varstva pred naravnimi in drugimi nesrečami so sicer jasno določene v Zakonu o varstvu pred naravnimi in drugimi nesrečami (ZVNDN) ter Zakonu o varstvu pred požarom (ZVPoZ). Čeprav se temeljna zakonodaja v zadnjih letih ni drastično spreminjala, ostajajo obveznosti podjetij obsežne in ključne za varnost, navajajo na URSZR.

Podjetja morajo, odvisno od svoje dejavnosti in velikosti, zagotoviti:

- **Izdelavo načrtov zaščite in reševanja:** To velja predvsem za obrate, ki uporabljajo nevarne snovi (skladno z direktivo SEVESO), jedrske snovi ali upravljajo velike infrastrukturne sisteme.
- **Oceno požarne ogroženosti:** Na podlagi te se določi požarni red, za bolj ogrožene objekte pa tudi požarni načrti in načrti evakuacije.
- **Usposabljanje zaposlenih:** Delodajalec mora poskrbeti, da je vsak zaposleni (redno ali občasno) usposobljen za varstvo pred požarom.

»PODJETJA POZIVAM, NAJ OPRAVIJO PRESOJO POTRESNE OGROŽENOSTI

- Kaj najbolj skrbi Srečka Šestana, legendo slovenske Civilne zaščite?
- Zakaj meni, da podjetja podcenjujejo nevarnosti, ki jih lahko ogrozijo?
- Ali veste, da je drone mogoče uporabljati tudi ob karavanški burji?

Goran Novković
Foto: Barbara Reya

»Obstaja področje, ki me strašno skrbi in bi moralo začeti skrbeti še mnoge druge. To je odpornost proti potresu.«

Srečko Šestan je že 30 let v Civilni zaščiti in 14. leto njen poveljnik. V Sloveniji je postal že prava legenda – obraz, ki nas s svojo prijaznostjo prek TV zaslonov hkrati obvešča in pomirja ob vsaki večji nesreči. S kakovostjo slovenske zaščite in reševanja je zato odlično seznanjen.

Kje se je v zadnjih letih najbolj spremenila vloga civilne zaščite v družbi?

Največje spremembe so se zgodile v času migracijskega vala in epidemije. Zakaj? Ker to nista bili klasični nesreči. Na takšne dogodke se v Civilni zaščiti nismo pripravljali, niti zanje nismo imeli primerne opreme.

Toda javili smo se prostovoljno. Sam sem v obeh primerih pisal tudi sklepe za vlado, da nam je naložila delo, ki smo ga potem opravljali.

Kaj pa ste počeli v času epidemije in migrantskega vala?

V času epidemije smo delili zaščitna sredstva, razvažali cepiva in podobno. Lotevali smo se torej nalog, ki jih ni opravljal nihče drug.

V času migrantskega vala pa smo skrbeli za nastanitev migrantov, ki jih je bilo izjemno veliko. Skrbeli smo za kar nekaj nastanitvenih centrov, pa tudi za prehrano ljudi. Nabava hrane je bila poseben izziv zaradi potrebnega certifikata halal.

Vrniva se k naravnim nesrečam: ali so res pogostejše in hujše kot v preteklosti ali pa smo o tem le bolje medijsko obveščeni in imamo zato občutek, da jih je veliko več?

Rekel bi, da drži oboje. Drži, da smo bolje obveščeni, tudi zaradi družbenih medijev, res pa so se tudi značilnosti dogodkov spremenile. To velja zlasti za ekstremne dogodke.

Ko so v Agenciji RS za okolje (ARSO) pred kratkim napovedali veter na severu Slovenije, so mi povedali, da v njihovi karieri tam še ni bil predviden tako neugoden veter, celo do hitrosti 140 kilometrov na uro, kar se je na koncu tudi zgodilo.

Podobno je bilo ob poplavah leta 2023, poplavah v Železnikih leta 2007 in pozneje tudi v Poljanski dolini leta 2014. To so lokalni ekstremni dogodki. Na žalost nas čakajo tudi v prihodnosti.

Kako podnebne spremembe vplivajo na posledice naravnih nesreč?

Zaradi njih se takšni dogodki zgodijo zelo hitro, v kratkem času. To velja tako za ogromno količino padavin kot za močne sunke vetra, ki lahko hkrati spremljajo nalive. V preteklosti tako ekstremnih pojavov ni bilo toliko.

»70.000 je operativnih članov, ki jih lahko pošljemo na vsako nesrečo.«

Potresa ni mogoče napovedati. Število žrtev in škodo lahko zmanjšamo s potresno odporno gradnjo. Naše stavbe izpred 50 let in več pa niso grajene tako. Takšnih stavb je preveč.«

Mi smo se sicer na to pripravljali že od leta 2004. Takrat smo v Civilni zaščiti razpisali raziskovalno nalogo. Zanimivo, njena nosilka je bila Lučka Kajfež Bogataj, ki je bila takrat na Biotehniški fakulteti. Želeli smo vedeti, kako bodo klimatske spremembe vplivale na naše delo in kako naj se nanje pripravimo.

Smo v Sloveniji dovolj pripravljeni na ekstremne vremenske dogodke?

V zadnjih letih smo že bolje pripravljeni, kot smo bili. Tudi zato, ker imamo veliko sodobne opreme. Ta je bila sofinancirana iz evropskih sredstev. Obstaja pa področje, ki me strašno skrbi in bi moralo začeti skrbeti še mnoge druge. To je odpornost proti potresu.

Potresa ni mogoče napovedati. Število žrtev in škodo lahko zmanjšamo le s potresno odporno gradnjo. Pred 50 in več leti pa naše stavbe niso bile grajene tako in teh je danes preveč. Dokler jih ne bomo sanirali, bo to grožnja. Če se pojavi močan potres, bomo imeli veliko škode.

Gre za stavbe, zgrajene od druge svetovne vojne do skopskega potresa leta 1963. Potem je bila gradnja malo boljša. Stavbe, ki so zgrajene po letu 2008, pa bi morale biti potresno odporne.

Na državni ravni smo že usposobili enoto Civilne zaščite, ki upravlja drone.«

Kako pa nove tehnologije vplivajo oziroma spreminjajo delo reševalnih služb?

Umetne inteligence še ne uporabljamo, verjamem pa, da jo nekoč bomo. Zelo koristni pa so droni. Sam sem bil na začetku do njih zelo skeptičen, ker se na žalost uporabljajo v vojnah. A na našem področju je njihova uporaba zdaj nujna. Uporabljali smo ga tudi ob zadnji karavanški burji.

Ga ne odpihne močan veter?

Ne, bil je malo težji. Z njim smo v Žirovnici pregledali vse strehe in posneli vse objekte. Ob določanju koordinat nam je to v veliko pomoč, tako pri organizaciji pomoči kot pri oceni škode, pa tudi pri hitrosti našega dela.

Dron veliko uporabljamo tudi, ko iščemo ljudi ali pa živali, ki denimo pobegnejo s pašnika. Na državni ravni smo že usposobili enoto Civilne zaščite, ki upravlja drone, imajo jih tudi gasilske enote in podobno.

Katera tehnološka inovacija na področju zaščite vas je najbolj navdušila?

Pred 20 leti smo imeli program Kras. V okviru razvojnega projekta smo opremljali gasilce na območju 21 občin submediteranskega dela Slovenije. Takrat smo ob pomoči partnerskih ustanov razvili tovornjake za gašenje požarov v naravi. Šlo je predvsem za njihovo nadgradnjo.

S čim ste jih nadgradili?

S pogonom na vsa kolesa in z visokotlačnimi črpalkami z manjšimi rezervoarji vode. Ta voda je zelo učinkovita, ker jo z visokim tlakom spršimo v meglo, tako pa pogasimo velike površine. Cevi so tanjše in dolge tudi 200 metrov, kar je zelo uporabno. Nadgradili pa smo še nekatere druge zadeve.

Katere so najpogostejše napake podjetij pri preventivi?

V industriji sem bil zaposlen 16 let, in to v takšni, ki je bila požarno zelo ogrožena. Glede na svoje izkušnje bi rekel, da v podjetjih kar precej podcenjujejo nevarnosti.

Spomnimo se primera Kemis. V tem primeru je neka ustanova v dokumentu celo navedla, da podjetje zunaj svojega območja ne ogroža ničesar. Toda videli smo, kaj se je zgodilo.

V Sloveniji se v podjetjih še vedno premalo zavedajo, kaj vse se lahko zgodi – češ, nam se kaj takšnega ne more zgoditi. Takšna miselnost ni dobra.

Treba je biti realen ter pošten do sebe in do okolice. Pripraviti je treba oceno ogroženosti in načrte, ki takšnim ocenam sledijo, potem pa lahko bolj mirno spijo vsi – tako v podjetju kot v njegovi občini.

Glede na svoje izkušnje bi rekel, da v podjetjih kar precej podcenjujejo nevarnosti.«

Kako pa so podjetja pripravljena na kombinirane grožnje, denimo na naravne nesreče in kibernetske napade?

Podjetja so, kljub omenjeni miselnosti, bolje pripravljena na naravne nesreče kot na druge grožnje, denimo hibridne ali kibernetske. Tudi zato, ker v primeru naravnih nesreč sistem deluje že več desetletij. Takšne sisteme bo treba vzpostaviti tudi, ko gre za druge grožnje.

Katere vrste tveganj bodo najbolj kritične v prihodnje? Iste ali nove?

Ne bo se veliko spremenilo, razen pri kibernetskih grožnjah, ki niso naravne nesreče. Bi pa opozoril na potresne grožnje, tudi v gospodarstvu. Nekatere firme bi morale dobro preveriti, v kakšnih objektih delujejo.

Prostovoljci gredo nad požar, poplavo ali kam drugam pomagat s kavča, od doma, iz službe. S tem nimajo nobenih težav.«

Gradbeni inštitut ZRMK in Zavod za gradbeništvo izvajata presoje potresne varnosti, strošek pa ni pretirano visok. Tako podjetja lahko pridejo do ocene, v kakšni stavbi delajo. Vse pozivam, naj opravijo to presojo.

Katero prvo varnostno pravilo bi uvedli, če bi en dan vodili podjetje?

Najprej bi pogledal, ali ima opravljeno oceno ogroženosti, tudi z vidika verižnih nesreč. To je zelo pomembno. Obstajajo podjetja, ki so nenehno ogrožena, recimo poplavno. Ukrepi morda ne bi bili poceni, a še vedno bistveno cenejši od posledic.

Katera situacija na terenu je bila za vas najbolj nenavadna?

Ob velikih nesrečah je v Sloveniji izjemno veliko ljudi, ki bi radi pomagali. To pa lahko povzroča organizacijske izzive. Tako je bilo ob poplavah v Železnikih; takrat smo morali celo zapreti območje. Nismo jih mogli razporediti zaradi značilnosti območja, ozke doline. Podobno se je ponovilo pri velikih poplavah leta 2023.

Ko namreč nekoga sprejmemo, da nam pomaga, pa četudi samo z lopato, zanj prevzamemo odgovornost, zato moramo biti pri tem zelo previdni. Če pridejo prostovoljci, jim moramo razdeliti naloge, ki niso nevarne, takšne situacije pa so lahko zelo nerodne. Tudi ob velikih poplavah smo morali nekatera območja zato zapreti. Seveda pa smo hvaležni vsakomur, ki želi pomagati.

Ob velikih poplavah leta 2023 smo čez vikend naredili celo aplikacijo za ponudbe prostovoljstva, vendar nismo imeli časa, da bi to aplikacijo bolj uspešno uporabljali, ker je nismo mogli promovirati prej in je ljudje niso dovolj poznali.

Drugi fenomen v Sloveniji je prostovoljstvo v različnih organizacijah, društvih, enotah, ki so temelj našega sistema.

Kdo je med temi največji?

Med njimi so daleč največja organizacija gasilci. So pa še druge: gorski reševalci, jamarji, kinologi … Druga največja organizacija je Rdeči križ. Gasilska zveza ima več kot 170 tisoč članov. Njenih operativnih članov, ki jih lahko pošljemo na vsako nesrečo, je 45 tisoč, v celotnem sistemu pa okrog 70 tisoč.

Katera pa je bila najpomembnejša lekcija, ki ste se jo naučili v svoji karieri?

Uporaba zdrave kmečke pameti. Poleg tega je v primeru nesreč treba izkazati iskrenost, odgovornost in umirjenost. V Civilni zaščiti ne gre za poveljevanje, čeprav imam naziv poveljnik, ampak gre za dogovarjanje, za koordinacijo.

Zavedati se je treba, da delamo pretežno s prostovoljci. Prostovoljci gredo nad požar, poplavo ali kam drugam pomagat s kavča, od doma, iz službe. S tem nimajo nobenih težav.

KOMPAS telekomunikacije

INTEGRACIJA RADIJSKIH OMREŽIJ

NAČRTOVANJE IN OBLIKOVANJE

VZDRŽEVANJE RADIJSKE OPREME

REŠITVE NA KLJUČ

L3HARRIS™
FAST. FORWARD.

SITRAC
DISPEČERSKI CENTER SITRAC VOICE

MOTOROLA SOLUTIONS
PLATINUM RESELLER

MOTOTRBO

KONTAKT

01/530 51 10 mail@kompas-telekom.com
01/530 58 32 prodaja@kompas-telekom.com

www.kompas-telekom.com

KOMPAS TELEKOMUNIKACIJE d.o.o.
Pot k sejmišču 30, Ljubljana, 1231 LJUBLJANA-ČRNUČE