DIGITAL INNOVATION HUB SLOVENIA

ANALIZA POTREB MALIH IN SREDNJIH PODJETIJ NA PODROČJU KIBERNETSKE VARNOSTI

NOVEMBER 2024

ZADHAJMO DIGITALNO!

info@dihslovenia.si
https://dihslovenia.si

Kazalo vsebine

Kazalo slik

Kazalo tabel

POVEZETEK

Analiza ocenjuje stanje in potrebe slovenskih malih in srednjih podjetij (MSP) na področju kibernetske varnosti (KV). Namen analize je prepoznati ključne izzive in oblikovati konkretna priporočila za krepitev kibernetske odpornosti MSP-jev, s posebnim poudarkom na uvedbi kaskadnega financiranja, izboljšanju kompetenc in razvoju učinkovitega podpornega okolja.

MSP-ji se soočajo s pomanjkanjem znanja, časa in finančnih virov, kar omejuje njihovo sposobnost obrambe pred kibernetskimi grožnjami. Zaradi teh omejitev podjetja pogosto zaostajajo za večjimi organizacijami, kar je privedlo do potrebe po poenostavljenih finančnih mehanizmih, kot so vavčerji. Večina podjetij je ocenila, da so vavčerji učinkovito izpolnili njihove potrebe po kibernetski varnosti, kar poudarja potrebo po nadaljevanju tovrstne podpore.

Analiza digitalne zrelosti, ki jo izvaja DIH Slovenije, razkriva, da le manjši del MSP-jev izvaja kibernetske strategije, kar pomeni, da so naložbe v digitalizacijo in varnost še vedno omejene. Pomembna ugotovitev je, da se večina MSP-jev zanaša na zunanje izvajalce za IT storitve in da je le majhen delež podjetij digitalizacijo vključil kot strateški del poslovanja.

Slovenija ima dobro razvito mrežo ponudnikov kibernetskih storitev, vendar je potreben večji poudarek na praktičnih usposabljanjih in povezovanju z izobraževalnimi ustanovami za razvoj specifičnih veščin, kot je socialni inženiring. Povezovanje s tujimi institucijami bi prav tako pripomoglo k razvoju inovacij in boljšemu usklajevanju potreb trga.

Kaskadno financiranje se je izkazalo za ključno orodje, ki lahko MSP-jem zagotovi hitrejši in lažji dostop do finančnih virov. Prilagoditev razpisov po vzoru evropskih praks s krajšimi cikli in enostavnimi postopki prijave je nujna, da podjetja uspešno izkoristijo sredstva za projekte, ki izboljšujejo njihovo kibernetsko varnost.

Vzpostavitev osrednjega Nacionalnega kompetenčnega centra (NCC) je ključnega pomena za povezovanje različnih deležnikov in zagotavljanje trajnostne podpore podjetjem. NCC mora imeti jasno opredeljene naloge in pristojnosti ter spodbujati uporabo umetne inteligence in digitalnih peskovnikov za varno testiranje rešitev. Le s celostnim pristopom bo mogoče zagotoviti konkurenčnost in varnost slovenskih MSP-jev na globalnem trgu.

1. UVOD

URSIV je za potrebe delovanja nacionalnega kompetenčnega centra za kibernetsko varnost (NCC-SI) s pomočjo DIH Slovenije pripravil analizo stanja in potreb po storitvah kibernetske varnosti. Za potrebe analize smo izvedli delavnico – fokusno skupino, kamor smo povabili majhna in srednja podjetja (MSP), strokovnjake s področja kibernetske varnosti, podporna okolja ter ostale strokovnjake, ki se ukvarjajo s kibernetsko varnostjo na drugih področjih.

MSP se pogosto srečujejo s pomanjkanjem virov kot so znanje, čas in finančni viri in s tem zaostajajo za velikimi podjetji. Iz tega razloga so mnoge države vzpostavile podporna okolja, ki MSP pomagajo pri premagovanju ovir na poti do celostne in varne digitalne preobrazbe. Da bi vzpostavili prave podporne mehanizme, je nujno prepoznati potrebe na trgu in tudi oceniti zrelost podjetij, da bodo znali implementirati ponujene ukrepe ter da bodo le ti narejeni na način, ki bo MSP koristil in služil pravim namenom.

DIH Slovenije je pripravil presek stanja in potreb MSP iz obstoječih lastnih in javno dostopnih virov. DIH Slovenije je stanje malih in srednjih podjetij na področju kibernetske varnosti redno spremljal

od leta 2019 dalje, zaradi facilitiranja vavčerjev za kibernetsko varnost, ki so podjetjem omogočali pridobitev subvencij za izvedbo vdornih in varnostnih testiranj ter izobraževanju zaposlenih. DIH Slovenije je med MSP izvedel raziskavo o ustreznosti vavčerjev.

Drugi vir informacij o odnosu MSP do kibernetske varnosti, je merjenje digitalne zrelosti, kjer je pokazatelj pripravljenosti na zahteve in nevarnosti digitalnega okolja in poslovanja, hkrati pa merjenje digitalne zrelosti pripomore h identifikaciji potreb MSP, ki jih je potrebno obravnavati na širšem nivoju.
Pridobljene podatke smo preverili tudi v bazi Statističnega urada Republike Slovenije (SURS), kjer sicer nismo našli neposrednih odgovorov na vprašanja glede potreb MSP po storitvah, ki bi jim pomagale k boljši kibernetski varnosti, poročila SURS se namreč osredotočajo na varno rabo informacijske tehnologije fizičnih oseb.

Poleg tega se DIH Slovenije srečuje s problematiko kibernetske varnosti pri malih in srednjih podjetjih v projektu EDIH DIGI-SI, kjer za podjetja s partnerji organiziramo dogodke demistifikacije tehnologij. Poleg MSP so obiskovalci teh dogodkov tudi deležniki javne uprave in drugih inštitucij, kjer se pojavljajo enake glavne potrebe kot pri MSP: dvig kompetenc zaposlenih, potrebe po testiranju obstoječih sistemov ter prihajajoče poročanje po zakonu o informacijski varnosti.

Po pogovorih s koordinatorji Sekcije za kibernetsko varnost kjer se prvotno združujejo predvsem ponudniki rešitev na tem področju, pa tudi podjetja, ki se zavedajo pomena kibernetske varnosti in se s članstvom želijo opredeliti do prihajajočih zakonodaj ter z obiskovanjem dogodkov povečati svoje kompetence na tem področju.

Iniciativa Ženske v kibernetski varnosti želi povečati vključenost žensk na področju, s tem povečati bazen delovne sile in hkrati navdušiti mlada dekleta in ženske za poklice v kibernetski varnosti.

Projekt Cyberhubs naslavlja pomanjkanje strokovnjakov kibernetske varnosti v Evropi z razvojem učinkovite in sodelovalne vseevropske mreže inkubatorjev veščin kibernetske varnosti.
Univerza v Mariboru je vključena tudi v mrežo Cyber Security for Europe, ki združuje več projektov, CyberSec4Europe, ki oblikuje, testira in demonstrira vodstvene strukture za bodočo Evropsko mrežo kompetenc v kibernetski varnosti. (glej: https://cybersec4europe.eu/our-community/)

Evropska Unija podpira 22 projektov vezanih na kibernetsko varnost v 18ih državah, za kar je namenila skupno 10,9 milijonov EUR.

Cilj tega poročila je prepoznati ključne potrebe MSP-jev in oblikovati konkretna priporočila za izboljšanje kibernetske varnosti, s posebnim poudarkom na kaskadnem financiranju, izboljšanju kompetenc in vzpostavitvi učinkovitega podpornega okolja. Na ta način bomo pomagali MSP-jem, da postanejo bolj odporni na kibernetske grožnje ter uspešnejši v digitalnem okolju.

2. PRESEK TRENUTNEGA STANJA IN POTREB MSP NA PODROČJU KV

2.1. Evalvacija vavčerja za kibernetsko varnost

Na vprašalnik s področja kibernetske varnosti je odgovorilo **53 podjetij**, ki je v letih 2019-23 pridobilo vavčer za kibernetsko varnost. Vavčer je vseboval storitve sistemskega varnostnega pregleda s sofinanciranjem do 60% oziroma skupno vrednostjo do največ 5.000 EUR ter vdorno (penetracijsko) testiranje prav tako do 60% oziroma skupne vrednosti 9.999,99 EUR.

Na podlagi vzorca 53 podjetij, ki je rešilo evalvacijski vprašalnik za področje kibernetske varnosti se **velika večina (98,1%) strinja**, da je vavčer **izpolnjeval njihove potrebe** vezane na področje kibernetske varnosti.

56,6% podjetij, ki so izpolnila vprašalnik je navedlo, da so zaradi izvedbe aktivnosti v okviru vavčerja za kibernetsko varnost **zaznali pozitivne spremembe v poslovanju**, 43,4 % navaja, da pozitivnih sprememb niso zaznali.

Podjetja navajajo, da po zaključku aktivnosti zaznavajo naslednje pozitivne spremembe v poslovanju:

- Zaposleni so bolj previdni pri uporabi digitalnih medijev.
- Sprememba miselnosti zaposlenih.
- Manjša možnost vdora.
- Večjo zavedanje o kibernetskih pasteh.
- Večja varnost poslovanja.
- Odpravljanje odkritih težav.
- Izvedba določenih ukrepov za povečanje kibernetske varnosti.

Večina podjetij (**75,5%**) meni, da po končanem projektu konkurenco na področju kibernetske varnosti **dohajajo** oziroma so z njo na **enakovrednem položaju**. 17% podjetij meni, da so na področju kibernetske varnosti nekaj korakov pred konkurenco, zgolj 7,5% pa jih meni, da konkurence kljub izvedenim aktivnostim še vedno ne dohaja.

Večina (**73,6%**) podjetij, ki je izpolnilo vprašalnik je menilo, da je **vrednost sofinanciranja** aktivnosti na področju kibernetske varnosti **zadostna**, manjšina (26,4%) meni, da je vrednost sofinanciranja prenizka.

Dobra polovica podjetij (**52,8%**) pravi, da je v namen gospodarne rabe sredstev pred izborom zunanjega izvajalca **kontaktirala tudi druge ponudnike**, slaba polovica (47,2%) pravi, da proti-ponudb ni zbrala. Med podjetji, ki so pred izborom zunanjega izvajalca zbirale proti-ponudbe jih je 57,1% zbrala 3 ali več, 32,1% je zbrala 2 ponudbi, 10,7% pa 1.
Med 53 podjetji, ki so izpolnila vprašalnik jih 69,8% meni, da je cena, ki jo je postavil zunanji izvajalec primerna, 17% jih meni, da je cena previsoka, 13,2% jih meni, da je cena prilagojena maksimalni vrednosti vavčerja.

67,9% podjetij, ki je pridobilo vavčer za kibernetsko varnost pravi, da je z izvedbo aktivnosti čakalo do pridobitve vavčerja, 32,1% podjetij na vavčer ni čakalo, pač pa je bil na razpolago ravno v obdobju, ko so načrtovali izvedbo aktivnosti na področju kibernetske varnosti.

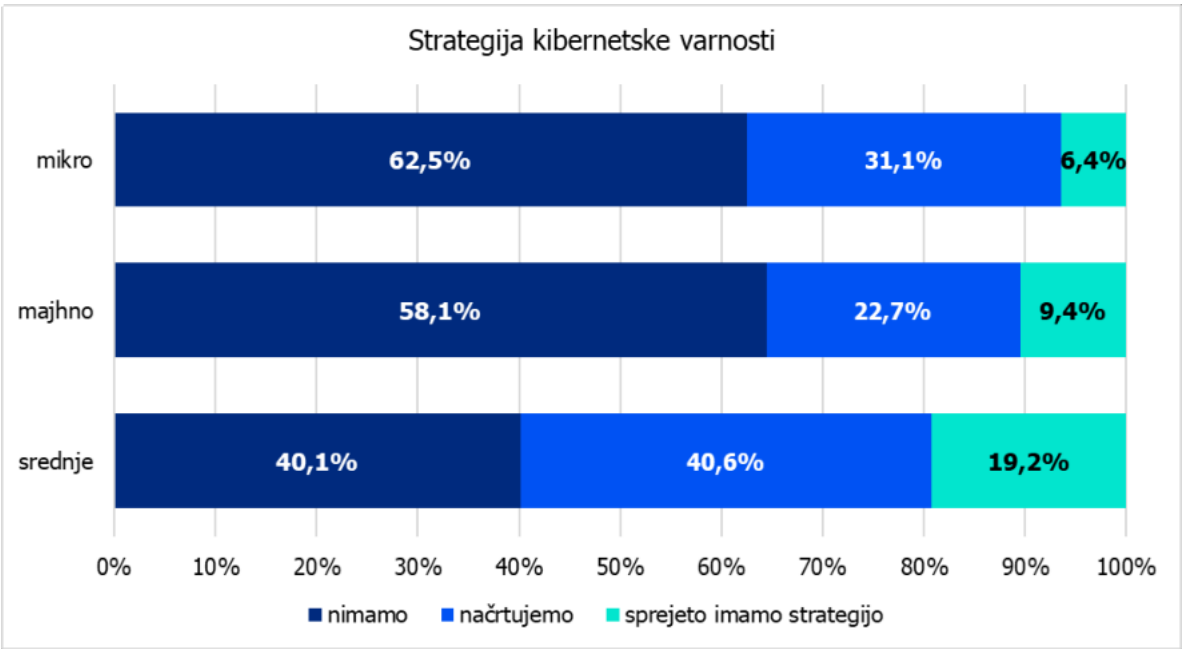
56,6% podjetij pravi, da brez vavčerja sistemskega varnostnega pregleda oziroma penetracijskega testa ne bi izvedlo, manj 43,4% pravi, da bi aktivnosti izvedli ne glede na vavčer.

Velika večina podjetij (92,5%) pravi, da zaradi rezultatov izvedenih testiranj nadaljujejo z vlaganji na področju kibernetske varnosti, le 7,5% pa pravi, da so z vlaganji na področju kibernetske varnosti zaključili.

2.2. OCENA DIGITALNE ZRELOSTI

DIH Slovenije spremlja digitalno zrelost podjetij od leta 2021 dalje. V tem času se je samo-ocenilo več kot **1200 MSP**, oziroma skupno **več kot 1500 vseh organizacij**. Glede kibernetske varnosti smo neposredno merili predvsem izdelavo strategije za kibernetsko varnost s strani MSP. Strategijo

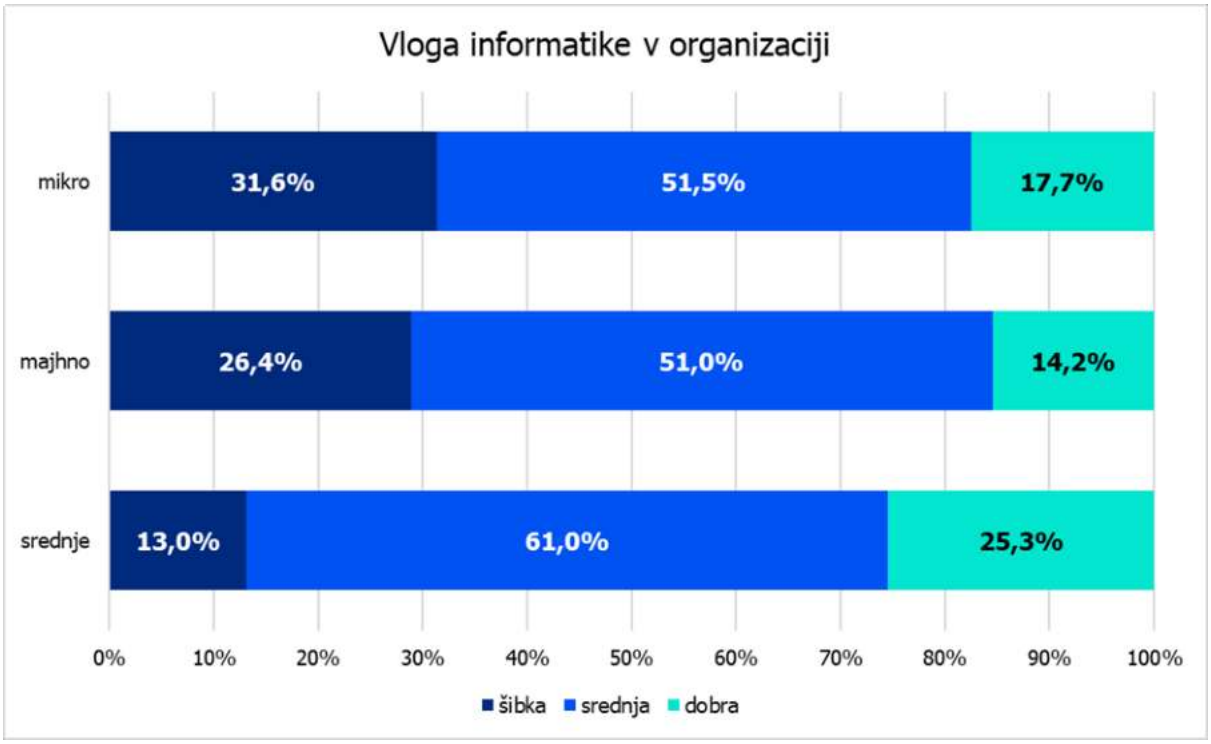
za kibernetsko varnost (Slika 1) ima 6% mikro, 9% malih in 19% srednje velikih podjetij. Medtem ko kar **40% srednje velikih podjetij, 58% malih in 62% mikro podjetij** poroča, da **strategije kibernetske varnosti nimajo**. Preostali delež MSP pa načrtuje sprejem strategije kibernetske varnosti.



Slika 1: Stanje izdelave strategije za KV med slovenskimi MSP-ji

Nadalje so MSP preko vprašalnika odgovarjali o vlogi informatike v podjetju, kjer v podjetjih vseh velikosti prevladuje najemanje zunanjih strokovnjakov - outsourcing (srednja 41,21%, mala 62,63% in mikro 65,72%), sledi kombinacija zunanjih in notranjih sodelavcev za IT (srednja 26,32%, mala 18,48% in mikro 13,2%), v preostalih primerih pa za IT skrbijo le notranji sodelavci. Večina podjetij namerava v naslednjih 12. do 18. mesecih vlagati v informatiko toliko kolikor bo potrebno, da zadostijo zakonodajnim zahtevam delu na daljavo (34% srednje velikih, 48% malih in skoraj polovico mikro podjetij). Za prilagajanje zahtevam trga namerava investirati v informatiko 38% srednje velikih, 30% malih in 26% mikro podjetij. Investicije v informatiko ima kot del strategije vključenih 26% srednje velikih, 17% malih in 17% mikro podjetij.

Iz tega smo ocenili, da podjetja v **celotno informatiko** v podjetju, kamor štejejo tudi kibernetsko varnost, še vedno **vlagajo** v majhni meri, saj skupna ocena kaže, da kot strateško pomemben del poslovanja šteje le **četrtina srednjih podjetij**, **14% malih** in **slabih 18% mikro podjetij**. Srednjo vrednost ocene pomembnosti dosega približno polovica podjetij, medtem ko se zaskrbljujoče število, skoraj **četrtina v vseh primerih**, **vloge informatike** in vseh ostalih dejavnikov sploh **ne zaveda** (Slika 2).



Slika 2: Vloga informatike v slovenskih MSP-jih

2.3. DESI INDEX – Digitalno desetletje 2024

V poročilu kompozitnega indeksa DESI, oziroma od leta 2023 dalje Digitalno desetletje, lahko primerjamo Slovenijo glede na EU povprečje ali na druge države članice.

Glede digitalnih kompetenc, kjer lahko za posameznike predvidevamo, da imajo v primeru, da se zavedajo kibernetskih nevarnosti in imajo vsaj osnovne veščine kibernetske varnosti, smo gledali kazalnik »Above basic digital skills«, kjer je Slovenija precej pod povprečjem Evropske Unije (EU). Povprečje **EU je namreč leta 2021 predstavljalo 26,46% posameznikov** z nadpovprečnimi digitalnimi veščinami, medtem ko je 2021 takšnih **v Sloveniji bilo 19,72%**, v letu 2023 pa se je razkorak še bolj povečal: **povprečje EU je 27,32% posameznikov**, v **Sloveniji** pa je takšnih zgolj **18,88%**.

V preteklih letih je Slovenija prednjačila po kazalniku **IKT strokovnjaki** (ICT specialists), ki je bilo leta 2022 še enako povprečju EU, 4,5% vseh posameznikov v aktivnem življenjskem obdobju, leta 2023 pa je povprečje EU zraslo na 4,8%, v Sloveniji pa **padlo na 3,8%.**

Prav tako je v letu 2023 močno pod povprečje EU **padlo število MSP-jev** z več kot 10 zaposlenimi v kazalniku **Spletna prodaja MSP-jev** (SMEs selling online) in sicer iz 19,3% na **17%**.

Prav tako padec kaže kazalnik **MSP z vsaj osnovno stopnjo digitalne intenzivnosti** (SME with at least a basic level of digital intensity), ki je iz EU povprečja leta 2021 55,2% vseh podjetij nad 10 zaposlenih v letu 2023 **padel na 50,4%**, povprečje pa je zraslo na 57,7% na evropskem nivoju. Po drugi strani pa Slovenija **prednjači po uporabi tehnologij umetne inteligence v podjetjih** in **e-računih**.

Vse to pomeni, da morajo slovenska podjetja **več vlagati v digitalizacijo** in posledično še toliko **bolj v kibernetsko varnost**, če želijo ostati **konkurenčna trgu EU**.

2.4. SURS

Slovenski statistični urad spremlja kazalnik: »Število podjetij, ki uporabljajo varnostne ukrepe ali postopke pri uporabi IKT v podjetju, po velikostnem razredu, Slovenija, večletno«. Podatki SURS izključujejo mikro podjetja, ki imajo manj kot 10 zaposlenih. Za potrebe analize smo pretvorili razrede števila zaposlenih, da rezultati sovpadajo s smernicami[1] določanja velikosti podjetij. Pri tem smo zanemarili letne prihodke.

SURS razredi	Analiza razredi
10 ali več zaposlenih	Malo podjetje
10-49 zaposlenih	Malo podjetje
50-249 zaposlenih	Srednje podjetje

Tabela 1: Razredi MSP-jev po metodologiji SURS

SURS podatkov o mikro podjetjih ne zbira, izločili smo tudi podjetja z več kot 250 zaposlenimi, ker ne spadajo v klasifikacijo MSP. Podatki se nanašajo se na leti 2022 in 2024, Zbirajo se podatki o varnostnih ukrepih:

1 Podjetja, ki uporabljajo katerega od varnostnih ukrepov ali postopkov
1.1 Avtentikacija z močnim geslom, tj. geslom z določeno minimalno dolžino, ki vsebuje številke in posebne znake ter se ga redno spreminja
1.2 Avtentikacija z biometričnimi metodami, npr. s prstnim odtisom, glasom, obrazom
1.3 Avtentikacija, ki je kombinacija vsaj dveh avtentikacijskih mehanizmov, npr. uporabniškega gesla in enkratnega gesla ali biometrične metode
1.4 Enkripcija podatkov, dokumentov ali e-pošte
1.5 Hranjenje kopij podatkov na drugi lokaciji ali v oblaku
1.6 Kontrola dostopa do omrežja (upravljanje pravic uporabnikov v omrežju podjetja)
1.7 Navidezno zasebno omrežje (VPN – prek javnega omrežja razširi zasebno omrežje za varno izmenjavo podatkov)
1.8 Varnostni nadzorni sistem IKT, ki omogoča odkrivanje sumljivih aktivnosti v sistemih IKT in podjetje opozori nanje, npr. sistemi za zaznavanje/preprečevanje vdorov
1.9 Hranjenje dnevnikov aktivnosti za izvedbo analize po morebitnem varnostnem incidentu (revizijska sled)
1.10 Ocena tveganja IKT, tj. periodično presojanje verjetnosti in posledic morebitnih varnostnih incidentov, povezanih z uporabo IKT
1.11 Testiranje varnosti pri uporabi IKT, npr. izvajanje penetracijskih testov, testiranje varnostnih opozorilnih sistemov, pregledovanje varnostnih ukrepov, testiranje sistemov za izvajanje varnostnih kopij
1.12 Varnostni nadzorni sistem IKT, ki omogoča odkrivanje sumljivih aktivnosti, npr. sistemi za zaznavanje ali preprečevanje vdorov, ki spremljajo obnašanje uporabnikov, naprav, omrežni promet
2 Podjetja, ki uporabljajo vsaj 3 varnostne ukrepe ali postopke

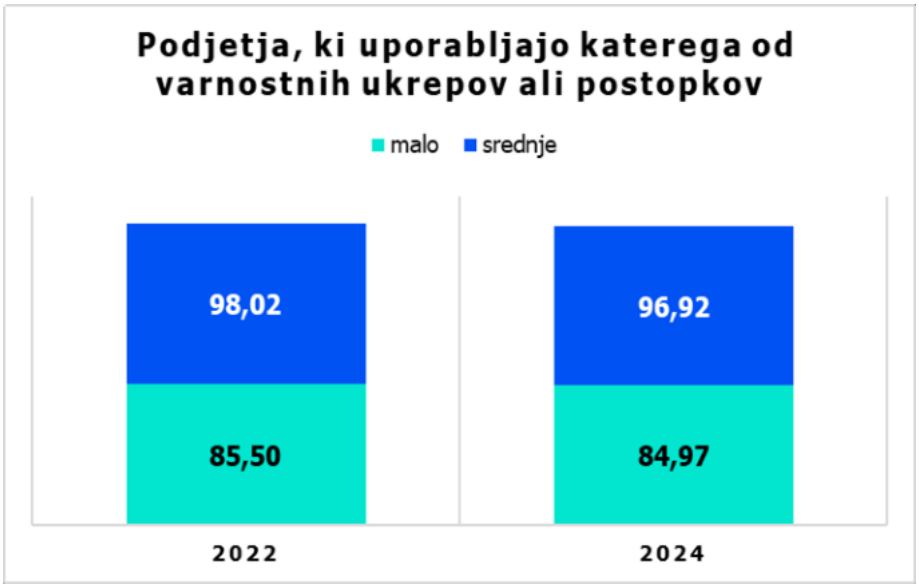
[1] file:///C:/Users/Katja/Downloads/sme_definition_user_guide_sl.pdf

3 Podjetja, ki uporabljajo vsaj 5 varnostne ukrepe ali postopke
4 Podjetja, ki uporabljajo vsaj 7 varnostne ukrepe ali postopke
5 Podjetja, ki imajo sklenjeno zavarovanje kibernetske zaščite za poravnavo stroškov varnostnih incidentov, povezanih z IKT
6 Podjetja, v katerih izvajajo aktivnosti, povezane z varno uporabo IKT zaposleni v podjetju ali zunanji izvajalci
6.1 Podjetja, v katerih izvajajo aktivnosti, povezane z varno uporabo IKT zaposleni v podjetju (tudi zaposleni v matičnem ali povezanih podjetjih)
6.2 Podjetja, v katerih izvajajo aktivnosti, povezane z varno uporabo IKT zunanji izvajalci

Tabela 2: Klasifikacija varnostnih ukrepov med slovenskimi MSP-ji

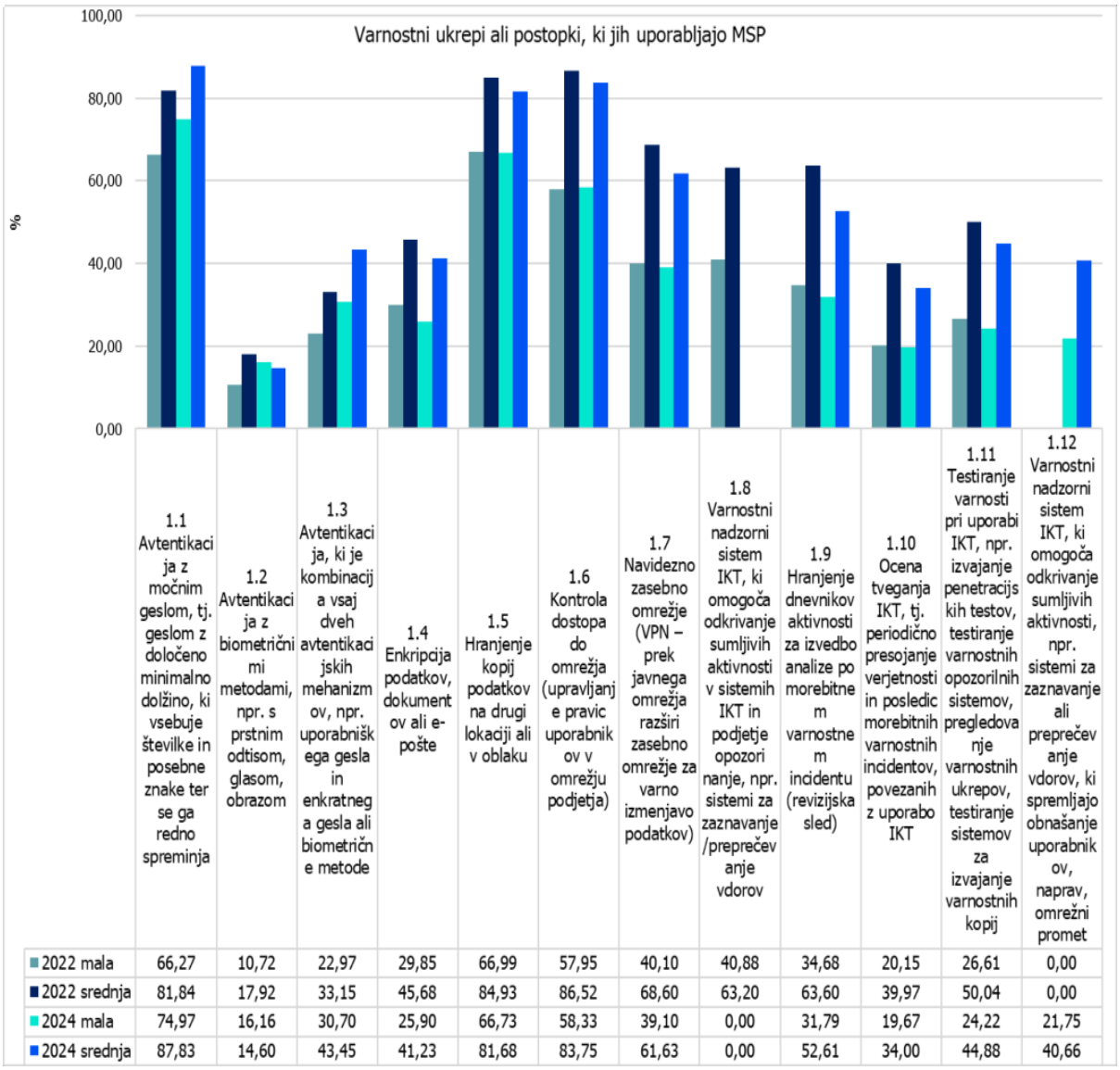
Analiza izvoza podatkov nam kaže spremembe po letih, da je letu 2022 je na vprašalnik odgovorilo 16031 podjetij, v letu 2024 pa 17558 podjetij.

Med podjetji, ki so odgovorila na vprašalnik v letih 2022 in 2024, je v letu 2022 98,02% srednjih podjetij uporabljalo katerega izmed varnostnih ukrepov ali postopkov, pri malih je ta odstotek 85,5%, v letu 2024 pa se je pri obeh kategorijah odstotek nižal: varnostne ukrepe uporablja 96,92 srednjih in 84,97 malih.



Slika 3: Uporaba katerega od varnostnih ukrepov ali postopkov med slovenskimi MSP-ji

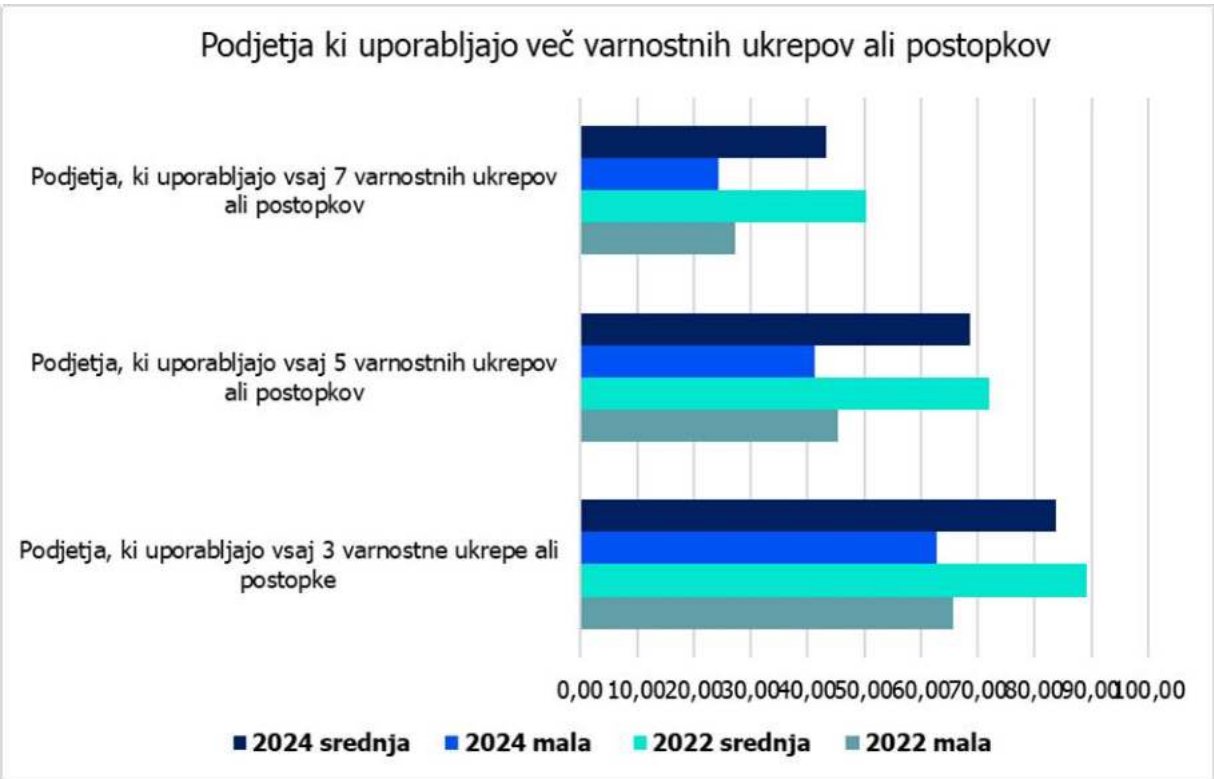
Slika 4 kaže varnostne ukrepe ali postopke po kategorijah. Glede na preglednico **največ podjetij uporablja avtentikacijo z močnim geslom**, temu sledi kontrola dostopa do omrežja, hranjenje kopij podatkov na drugi lokaciji ali v oblaku in hranjenje dnevnikov aktivnosti za izvedbo analize po morebitnem varnostnem incidentu. Sledijo navidezna zasebna omrežja VPN, kombinacija avtentikacijskih mehanizmov testiranje varnosti pri uporabi IKT, medtem ko se le redka podjetja odločajo za oceno tveganja IKT in varnostne nadzorne sisteme IKT.



	1.1 Avtentikacija z močnim geslom, tj. geslom z določeno minimalno dolžino, ki vsebuje številke in posebne znake ter se ga redno spreminja	1.2 Avtentikacija z biometričnimi metodami, npr. s prstnim odtisom, glasom, obrazom	1.3 Avtentikacija, ki je kombinacija vsaj dveh avtentikacijskih mehanizmov, npr. uporabniškega gesla in enkratnega gesla ali biometrične metode	1.4 Enkripcija podatkov, dokumentov ali e-pošte	1.5 Hranjenje kopij podatkov na drugi lokaciji ali v oblaku	1.6 Kontrola dostopa do omrežja (upravljanje pravic uporabnikov v omrežju podjetja)	1.7 Navidezno zasebno omrežje (VPN – prek javnega omrežja razširi zasebno omrežje za varno izmenjavo podatkov)	1.8 Varnostni nadzorni sistem IKT, ki omogoča odkrivanje sumljivih aktivnosti v sistemih IKT in podjetje opozori nanje, npr. sistemi za zaznavanje/preprečevanje vdorov	1.9 Hranjenje dnevnikov aktivnosti za izvedbo analize po morebitnem varnostnem incidentu (revizijska sled)	1.10 Ocena tveganja IKT, tj. periodično presojanje verjetnosti in posledic morebitnih varnostnih incidentov, povezanih z uporabo IKT	1.11 Testiranje varnosti pri uporabi IKT, npr. izvajanje penetracijskih testov, testiranje varnostnih opozorilnih sistemov, pregledovanje varnostnih ukrepov, testiranje sistemov za izvajanje varnostnih kopij	1.12 Varnostni nadzorni sistem IKT, ki omogoča odkrivanje sumljivih aktivnosti, npr. sistemi za zaznavanje ali preprečevanje vdorov, ki spremljajo obnašanje uporabnikov, naprav, omrežni promet
2022 mala	66,27	10,72	22,97	29,85	66,99	57,95	40,10	40,88	34,68	20,15	26,61	0,00
2022 srednja	81,84	17,92	33,15	45,68	84,93	86,52	68,60	63,20	63,60	39,97	50,04	0,00
2024 mala	74,97	16,16	30,70	25,90	66,73	58,33	39,10	0,00	31,79	19,67	24,22	21,75
2024 srednja	87,83	14,60	43,45	41,23	81,68	83,75	61,63	0,00	52,61	34,00	44,88	40,66

Slika 4: Uporaba varnostnih ukrepov ali postopkov po kategorijah med slovenskimi MSP-ji

Največ podjetij, ki je uporabljajo vsaj 7 varnostnih ukrepov ali postopkov je bilo med srednjimi podjetji v letu 2022, sledijo srednja v letu 2024, mala v letu 2024, kjer se kaže trend rasti. Največja uporaba je treh varnostnih ukrepov ali postopkov med srednjimi podjetji v letu 2022, 89% respondentov, v letu 2024 je ta odstotek padel na 84% (Slika 5).



Slika 5: Podjetja, ki uporabljajo 7 ali več varnostnih ukrepov ali postopkov

Za leto 2024 podatki o kazalnikih o zunanjih izvajalcih, zavarovanjih in aktivnostih, povezanih z varno rabo interneta, ni na voljo, kar pa smo pridobili v preteklih navedenih raziskavah v tem dokumentu.

Če povežemo s prejšnjimi poročili, lahko vidimo, da se še vedno skoraj četrtina MSP sploh ne zaveda pomena digitalizacije in kibernetske varnosti, da se je močno pokazal upad digitalnih veščin in digitalizacije poslovanja na splošno, kar močno sovpada s prenehanjem sofinanciranja digitalizacije MSP in izgube digitalizacije kot strateške državne in politične prioritete.

3. STROKOVNJAKI, IZVAJALCI STORITEV ZA KIBERNETSKO VARNOST

Slovenija ima razvit trg kibernetskih storitev, ki je zasnovan na bogati mreži ponudnikov, prilagojeni potrebam malih in srednjih podjetij (MSP-jev). Digitalno inovacijsko stičišče Slovenije (DIHS) vzdržuje katalog izvajalcev, ki vključuje 33 podjetij, specializiranih za kibernetsko varnost. Izvajalci so se v katalog vpisali ali posodobili svoje podatke v letu 2022, ko so bila še na voljo sredstva za vavčer kibernetske varnosti. Prek teh vavčerjev so MSP-ji pridobili sofinanciranje za izvajanje vdornega testa, varnostnega pregleda ter izobraževanje zaposlenih, vključno s simulacijami vdora (socialni inženiring).

Katalog DIHS se redno posodablja za vsak posamezen razpis vavčerjev, kar omogoča izvajalcem, da prilagodijo svoje podatke, se pridružijo katalogu ali pa se iz njega izbrišejo. Ta dinamična posodobitev zagotavlja aktualnost in relevantnost informacij za MSP-je.

3.1. Sekcija za kiberetsko varnost (SeKV)

Poleg kataloga DIHS ima pomembno vlogo tudi Sekcija za kibernetsko varnost (SeKV), ki deluje pod okriljem Gospodarske zbornice Slovenije (GZS). SeKV vključuje 51 članov, med katerimi so ponudniki kibernetskih rešitev, univerze, fakultete ter uporabniki kibernetskih storitev. Vendar niso vsi člani neposredni izvajalci storitev za podjetja, saj sekcija vključuje tudi izobraževalne in raziskovalne institucije.
Strokovnjaki za kibernetsko varnost iz SeKV so v večini vpisani tudi v katalog izvajalcev DIHS, kar omogoča sinergijo med člani in izvajalci. Članstvo v SeKV nudi uporabnikom možnost, da se osredotočijo na svojo osnovno dejavnost, medtem ko se vprašanja kibernetske varnosti rešujejo s pomočjo ekspertne skupnosti. Ponudnikom kibernetskih rešitev pa članstvo omogoča razvoj in vpliv na trg, sodelovanje pri oblikovanju politik ter lažji nastop na globalnem trgu.
Z uresničevanjem Programa dela SeKV se povezujejo gospodarstvo, javni sektor, državne institucije in posamezni strokovnjaki, kar spodbuja skupni razvoj kibernetskih varnostnih zmogljivosti in digitalni napredek slovenskega gospodarstva.

3.2. Povpraševanje MSP-jev

Trenutna povpraševanja MSP-jev nakazujejo na visoko potrebo po naslednjih storitvah:

- **Penetracijski testi in varnostni pregledi:** Osnovne storitve, ki zagotavljajo pregled nad kibernetskimi tveganji.
- **Napredni sistemi za zaznavanje groženj (EDR, SIEM):** Rešitve, ki MSP-jem omogočajo sprotno zaznavanje in odzivanje na incidente.
- **Skladnost z zakonodajo:** Storitve za zagotavljanje skladnosti z GDPR, NIS in ISO standardi.
- **Izobraževanja in ozaveščanje:** Povečanje pripravljenosti zaposlenih prek izobraževalnih programov.
- **Svetovanje in varnostna arhitektura:** Uvajanje najboljših praks za zaščito kritične infrastrukture.

Te ugotovitve izhajajo iz individualnih pogovorov s strokovnjaki iz kataloga DIHS in člani SeKV, ki so nam pomagali bolje razumeti aktualne potrebe in izzive, s katerimi se MSP-ji soočajo. Strokovnjaki so izpostavili, da so te storitve ključne za učinkovito zaščito podjetij pred kibernetskimi grožnjami in za zagotavljanje skladnosti s hitro spreminjajočimi se regulativnimi zahtevami.

4. DELAVNICA - VSEBINSKE USMERITEV ZA PRIHODNJE SHEME FINANCIRANJA

Z namenom razumevanja potreb MSP-jev na področju KV, smo izvedli delavnico **s fokusno skupino**, preko katere smo prišli do **vsebinskih usmeritev za prihodnje sheme financiranja** v okviru Nacionalnega kompetenčnega centra za kibernetsko varnost (NCC).

Za namene izvedbe delavnice je bil oblikovan **seznam** podjetij iz različnih sektorjev ter ključnih deležnikov, vključno s predstavniki akademskih in strokovnih institucij ter izvajalci kibernetskih storitev, da zagotovimo raznolikost perspektiv in kakovost prispevkov. Na delavnico je bilo povabljenih 30 organizacij. Na vabilo se je odzvalo **20 organizacij** in se nanjo tudi prijavilo. Delavnico smo izvedli 8.11.2024 preko spletne aplikacije ZOOM. Na sami delavnice je sodelovalo **14 organizacij** (v to številko partnerske organizacije in DIHS niso upoštevane). Z delavnico smo pričeli ob 9.00 in je trajala do 11.20.

Vsebina delavnice je bila razdeljena na **6 področij**:
- PODPORA NCC ZA MSP
- KOMPETENCE IN RAZVOJ TALENTOV
- PODROČJA DELOVANJA NCC
- VIDNOST IN PREPOZNAVNOST NCC
- FINANČNE POTREBE IN STRUKTURA FINANCIRANJA
- STRATEŠKE IN OPREATIVNE POTREBE

Skupaj je bilo pripravljenih XX vprašanj. Vprašanja so bila bodisi odprtega tipa ali zaprtega tipa, pri čemer smo kot glasovalno orodje uporabili **Mentimeter**, ki je odgovore organizacij beležila. Celotno poročilo delavnice z vprašanji in odgovori udeležencev je v Prilogi 1.

MSP-ji imajo **močno potrebo po enostavnih in dostopnih finančnih mehanizmih**, kot so vavčerji, ki bi jim omogočili lažji dostop do ključnih kibernetskih storitev. Kljub temu veliko podjetij še vedno ni ustrezno pripravljenih na okrevanje po morebitnih kibernetskih napadih, kar kaže na **nujnost nadaljnjega ozaveščanja** in **pomoči** pri oblikovanju načrtov za obvladovanje incidentov. Poleg tega bi lahko večji poudarek na **interaktivnih oblikah izobraževanja**, kot so simulacije, vaje in certificiranja, pomembno prispeval k večji pripravljenosti podjetij. Za učinkovito dvigovanje kibernetske varnostne kulture je potrebna **strategija**, ki cilja tako na vodilne kadre kot na zaposlene, da bi se znanje in varnostna praksa v celoti prenesla v poslovno okolje.

Pomembno je zagotoviti **sofinanciranje praktičnih izobraževalnih programov**, kot so delavnice, poletne šole in simulacije, da bi povečali kompetence na področju kibernetske varnosti. Poleg tega je ključnega pomena **razvoj krajših in specializiranih usposabljanj**, ki se prilagajajo specifičnim potrebam podjetij in vključujejo praktične veščine za neprekinjeno poslovanje. Sodelovanje z izobraževalnimi ustanovami, kot so univerze in fakultete, bi omogočilo oblikovanje ustreznih kurikulumov ter podprlo štipendije za bodoče strokovnjake. Dostopnost do mednarodnih certifikatov bi bilo smiselno povečati z delnim sofinanciranjem, kar bi prispevalo k boljši usposobljenosti kadrov na tem hitro razvijajočem se področju.

NCC bi moral spodbujati **razvoj programov za praktično usposabljanje**, ki mladim strokovnjakom omogočajo pridobivanje izkušenj, ne glede na formalno izobrazbo. Posebno pozornost bi morali nameniti sofinanciranju specifičnih kompetenc, kot je **socialni inženiring**, da bi podjetja lahko razvijala veščine, ki so ključne za zaščito pred sodobnimi grožnjami. **Povezovanje z univerzami, srednjimi šolami in podjetji** bi omogočilo učinkovitejše usklajevanje izobraževanja s tržnimi potrebami, kar bi zagotovilo večjo pripravljenost delovne sile. Prav tako bi bilo koristno **podpirati podjetja pri razvijanju različnih kadrovskih profilov** za kibernetsko varnost, z vključevanjem tako tehničnih kot analitičnih znanj.

Za **povečanje prepoznavnosti NCC** je ključno izkoristiti **digitalne medije** in **družbena omrežja**. Širjenje ozaveščenosti bi se lahko okrepilo z uporabo infografik in sodelovanjem z vplivneži za večji doseg. **Redna organizacija dogodkov**, konferenc in delavnic ostaja bistvena, a hkrati je pomembno **raziskati možnost strateških partnerstev**, ki bi zagotovila širši vpliv. **Ustanovitev informacijske platforme** za deljenje podatkov o kibernetskih grožnjah bi izboljšala odzivnost podjetij in omogočila dostop do ključnih informacij, vključno s primerjalnimi analizami po regijah in panogah. Poleg tega bi NCC-SI moral **ustvarjati sinergije z že obstoječimi programi kibernetske varnosti**, da bi učinkoviteje uporabil razpoložljive vire in povečal vpliv svojih aktivnosti.

Za povečanje privlačnosti domačih razpisov za MSP bi bilo potrebno **zmanjšati stopnjo zahtevane lastne udeležbe**, po možnosti **na največ 15%**, saj višji prispevki odvračajo podjetja, še posebej ob primerjavi s konkurenčnimi evropskimi financiranji. Pomembna bi bila tudi

prilagoditev modelov kaskadnega financiranja, tako da bi se razpisi zasnovali po evropskem vzoru z **bolj fleksibilnimi in krajšimi cikli**, kar bi omogočilo hitrejši dostop do sredstev za že pripravljene projekte. Dovoljevanje MSP-jem, da **povežejo financiranje z obstoječimi projekti**, bi optimiziralo uporabo razpoložljivih sredstev in povečalo učinkovitost izvedbe. Potrebna bi bila tudi raziskava o sprostitvi ali **prilagoditvi omejitev sofinanciranja v slovenski zakonodaji**, saj je trenutna **zgornja meja (50%) za številna podjetja previsoka**.

Vzpostavitev osrednjega kompetenčnega centra (NCC) mora temeljiti **na jasno opredeljenih nalogah**, kot so povezovanje akademske sfere in podjetij za spodbujanje raziskav in razvoja ter krepitev inovacijskega okolja s sodelovanjem s tujimi institucijami. Ključnega pomena je, da NCC **jasno definira svoje pristojnosti** in **odgovornosti,** da bi se izognil zmedi in podvajanju, hkrati pa ohranja **pregled nad obstoječimi iniciativami**, kot so SRIPI in Cyberhubs. Pomembno bi bilo preučiti **možnosti za vzpostavitev digitalnih peskovnikov za varno testiranje rešitev**, pri čemer bi lahko nadgradili že obstoječe platforme. Poleg tega je potrebno raziskati vlogo umetne inteligence pri odkrivanju in preprečevanju kibernetskih groženj ter spodbujati projekte, ki se osredotočajo na te tehnologije. Podpreti bi bilo treba tudi uvedbo osnovnih vsebin o kibernetski varnosti v šolske programe in organizirati dogodke, ki bi pritegnili mlade in spodbujali zanimanje za to področje.

5. ZAKLJUČEK

Slovenska mala in srednja podjetja (MSP) se soočajo s številnimi izzivi na področju kibernetske varnosti, kar zahteva večplastno podporo in strateške usmeritve. Pregled trenutnega stanja in potreb MSP-jev razkriva, da kljub naraščajočemu zavedanju o pomembnosti kibernetske varnosti številna podjetja še vedno nimajo vzpostavljenih osnovnih varnostnih mehanizmov. Finančne in kadrovske omejitve otežujejo vzpostavitev dolgoročnih strategij in pripravljenosti na kibernetske grožnje, kar poudarja nujnost enostavnih in dostopnih finančnih mehanizmov. Vavčerji so se v tem kontekstu izkazali kot učinkovit način spodbujanja podjetij k investiranju v varnostne rešitve.

Analiza je pokazala, da potreba po kaskadnem financiranju ostaja izjemno pomembna za MSP-je. Kaskadno financiranje, ki ga bo izvajal tudi Nacionalni kompetenčni center za kibernetsko varnost, mora biti oblikovano na način, ki MSP-jem omogoča hiter in fleksibilen dostop do sredstev. Pomembno je, da se razpisi prilagodijo potrebam podjetij s krajšimi cikli in poenostavljenimi postopki prijave, ki bodo podjetjem omogočali, da hitro realizirajo projekte in se učinkovito zaščitijo pred nenehno spreminjajočimi se kibernetskimi grožnjami. Povezovanje s tujimi praksami na področju kaskadnega financiranja bi prav tako lahko prispevalo k razvoju inovativnih in trajnostnih rešitev.

Poleg tega je poudarjen pomen vzpostavitve osrednjega NCC, ki bo deloval kot ključni povezovalni člen med akademsko sfero, industrijo in državnimi institucijami. S tem se bo okrepila inovacijska podpora, izboljšalo povezovanje na področju raziskav in razvoja ter zagotovila večja varnostna pripravljenost. Uvedba digitalnih peskovnikov za varno testiranje rešitev in raziskave na področju umetne inteligence za odkrivanje groženj bosta dodatno pripomogla k dvigu kibernetske odpornosti.

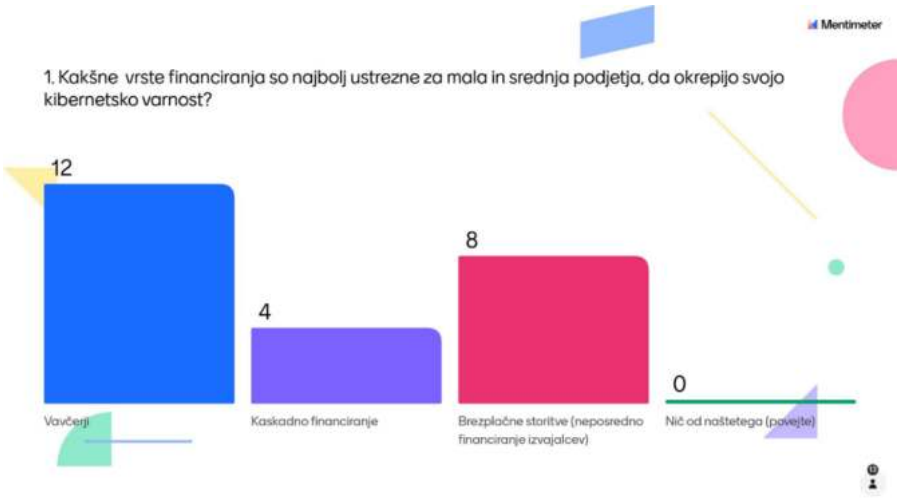
Zato je usklajeno prizadevanje za učinkovito kaskadno financiranje in strateško oblikovanje razpisov ključnega pomena za prihodnji uspeh MSP-jev. Le z jasno opredeljenimi nalogami, dobro zastavljenimi finančnimi mehanizmi in povezovanjem različnih deležnikov bomo lahko zagotovili zaščito slovenskih podjetij in omogočili njihovo konkurenčnost na globalnem trgu.

6. Priloga 1 – Poročilo delavnice Vsebinskih usmeritev za prihodnje sheme financiranja v okviru Nacionalnega kompetenčnega centra za kibernetsko varnost

Strokovna delavnica - Vsebinskih usmeritev za prihodnje sheme financiranja v okviru Nacionalnega kompetenčnega centra za kibernetsko varnost, 8.11.2024

1. PODPORA NCC ZA MSP

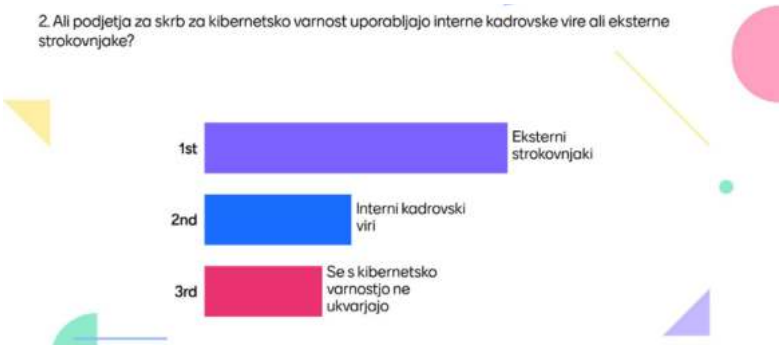
Na podlagi prikazanih rezultatov, kjer smo analizirali vprašanja o potrebnih vrstah financiranja za mala in srednja podjetja (MSP) na področju kibernetske varnosti, je ugotovljeno naslednje:



Rezultati

1. **Vavčerji**: Največji delež odgovorov (12) nakazuje, da so MSP-ji najbolj naklonjeni podpori v obliki vavčerjev. To kaže na pomembnost preprostih in hitro dostopnih finančnih mehanizmov za izboljšanje kibernetske varnosti.
2. **Kaskadno financiranje**: Manjši delež (4) se je odločil za kaskadno financiranje. Ta vrsta financiranja je očitno manj priljubljena ali manj poznana med MSP-ji, kar lahko kaže na potrebo po dodatnem ozaveščanju o možnostih, ki jih nudi.
3. **Brezplačne storitve (neposredno financiranje izvajalcev)**: Z 8 odgovori se kaže precejšnja potreba po brezplačnih storitvah, ki bi MSP-jem omogočile izboljšanje kibernetske varnosti brez neposrednih stroškov.
4. **Nič od naštetega**: Ni bilo odgovorov, ki bi nakazovali na potrebo po alternativnih vrstah financiranja ali storitev, kar kaže na zadovoljstvo s predlaganimi možnostmi.

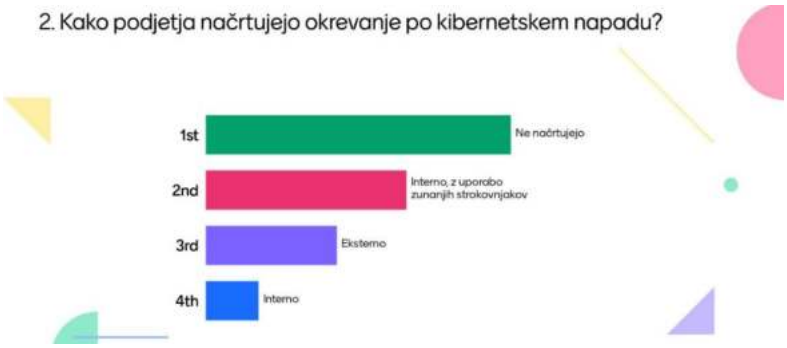
Na podlagi prikazanih rezultatov, kjer smo analizirali, katere vire podjetja uporabljajo za skrb za kibernetsko varnost, je ugotovljeno naslednje:



Rezultati

5. **Eksterni strokovnjaki:** Največji delež podjetij (prvo mesto) se odloča za uporabo zunanjih strokovnjakov za zagotavljanje kibernetske varnosti. To kaže na potrebo po specializiranih znanjih, ki jih MSP-ji pogosto nimajo interno.
6. **Interni kadrovski viri:** Drugo mesto pripada podjetjem, ki se zanašajo na lastne kadre. Ta skupina podjetij ima morda osnovne zmožnosti, a je lahko omejena pri obvladovanju kompleksnejših kibernetskih groženj.
7. **Podjetja, ki se ne ukvarjajo s kibernetsko varnostjo:** Na tretjem mestu so podjetja, ki kibernetski varnosti ne posvečajo pozornosti, kar predstavlja znatno tveganje in priložnost za ozaveščanje ter razvoj podpornih ukrepov.

Na podlagi rezultatov vprašanja o načrtovanju okrevanja po kibernetskem napadu ugotavljamo:



Rezultati

1. **Podjetja, ki ne načrtujejo**: Največ podjetij je odgovorilo, da nimajo načrtov za okrevanje po kibernetskem napadu, kar je skrb vzbujajoče in kaže na potrebo po večji ozaveščenosti in pripravi strategij za nepredvidene incidente.
2. **Interno z uporabo zunanjih strokovnjakov**: Na drugem mestu so podjetja, ki se zanašajo na notranje ekipe v kombinaciji z zunanjo strokovno podporo. To kaže na hibridni pristop k upravljanju incidentov.
3. **Eksterno**: Tretja možnost je popolno zanašanje na zunanje izvajalce, kar je pogosto pri podjetjih, ki nimajo zadostnih virov ali znanja za samostojno upravljanje okrevanja.

4. **Interno**: Na četrtem mestu so podjetja, ki imajo lastne interne načrte za okrevanje, kar kaže na manjšo pripravljenost in notranje kapacitete za spopadanje z incidenti.

Na podlagi rezultatov vprašanja o deležu letnega prometa, ki se nameni za IT, ugotavljamo:

Rezultati

1. **Ne vem**: Največ anketirancev je odgovorilo, da ne vedo, kolikšen delež prometa se namenja za IT. To kaže na pomanjkanje preglednosti ali ozaveščenosti glede vlaganj v IT, kar lahko vpliva na strateško načrtovanje in odločanje.
2. **Manj kot 1% letnega prometa**: Na drugem mestu so podjetja, ki vlagajo manj kot 1% svojega prometa v IT. To nakazuje na zelo nizke investicije, kar lahko ogroža dolgoročno kibernetsko odpornost.
3. **Med 1% in 5%**: Tretja kategorija vključuje podjetja, ki namenjajo med 1% in 5% prometa za IT. Ti anketiranci že vlagajo v IT, a še vedno morda ne dovolj za celovito zaščito in modernizacijo sistemov.
4. **Več kot 5%**: Le majhen delež podjetij namenja več kot 5% prometa za IT, kar pomeni, da je intenzivno vlaganje v informacijske tehnologije še vedno redkost.

Na podlagi rezultatov o ustreznih tipih izobraževanj o kibernetski varnosti (KV) za MSP ugotavljamo:

Rezultati

1. **Simulacije in vaje**: Največji delež (10 odgovorov) je naklonjen simulacijam in praktičnim vajam. To poudarja potrebo po interaktivnih in realističnih treningih, ki MSP-jem omogočajo, da se učinkovito pripravijo na resnične kibernetske incidente.
2. **Strokovna izobraževanja in pridobivanje certifikatov**: Devet odgovorov kaže na pomembnost strukturiranega učenja in certifikacij za poglobljeno znanje o KV. To je ključno za podjetja, ki želijo vzpostaviti zanesljivo varnostno kulturo.
3. **Ozaveščanje skozi predavanja in obisk dogodkov**: Osem udeležencev meni, da so ozaveščevalne aktivnosti prek predavanj in dogodkov pomembne za širjenje osnovnega znanja o kibernetski varnosti.
4. **Nič od naštetega**: Le en odgovor je nakazal potrebo po alternativnih metodah, kar pomeni, da večina podpira že obstoječe možnosti.

Analiza odgovorov na odprta vprašanja iz delavnice

1. Vprašanje: Kje sedaj velika podjetja orjejo ledino in bodo MSP sledili?

- **Ines Vlahovič**: Izpostavila je, da se kaskadna financiranja pogosto uporabljajo pri velikih in srednjih podjetjih zaradi obsežne papirologije, višje stopnje financiranja in kadrovskih omejitev. Za mala podjetja pa so bolj primerni vavčerji, saj so enostavnejši in manj zahtevni.
- **Ugotovitev**: Mala podjetja imajo pogosto težave s kompleksnostjo prijav na večje projekte, kar zahteva prilagojene finančne mehanizme, kot so vavčerji.

2. Vprašanje: Ozaveščanje – kako doseči MSP-je?

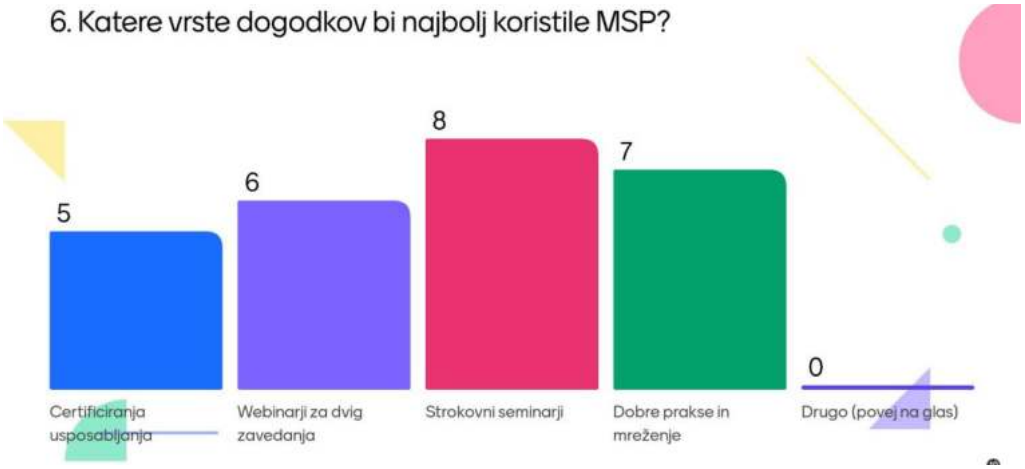
- **Žiga Epicoro**: MSP-ji pogosto ne razmišljajo o kibernetski varnosti in je ne smatrajo kot pomembno. Priporoča, da jih motiviramo z vavčerji ali brezplačnimi izobraževanji. Izpostavi pomen certifikacije, ki bi MSP-jem lahko predstavljala konkurenčno prednost, podobno bonitetni oceni.
- **Nina Hojnik**: Poudarila je, da je pomembna pomoč pri sestavljanju poročil, kar MSP-jem olajša upravljanje s kibernetskimi ukrepi.

- **Jože**: Omenil je potrebo po certifikacijskih organih, auditorjih in izobraževalnih storitvah. Udeleženci iz kritične infrastrukture se bolj zavedajo, kaj bodo inšpektorji preverjali, kar jih bolj motivira k ukrepom.
- **Katja**: Pojasnila je, da je cilj delavnice zajeti širok spekter, saj gre za splošni pregled potreb MSP-jev in kritične infrastrukture na več nivojih.
- **Katarina**: Izpostavila je dolgoročni cilj povezovanja izobraževalnih ustanov in industrije. Poudarila je potrebo po začetku pogovorov med deležniki in pridobivanju sredstev za ključne projekte.
- **Mojca Gea**: Predlagala je, da je treba ukrepe naslavljati na direktorje, medtem ko naj drugi del ukrepov ciljano naslavlja zaposlene.

Potrebna sofinanciranja za kibernetsko varnost na področju proizvodnih sistemov in kritičnih infrastruktur

- **Izobraževanja**: Največ odgovorov (7) kaže na potrebo po sofinanciranju usposabljanj, kar poudarja pomembnost izobraževanja zaposlenih.
- **Certificiranje in skladnost s standardi**: Z 5 odgovori se je izkazala tudi potreba po sredstvih za zagotavljanje skladnosti in pridobitev certifikatov.
- **Programska oprema**: Trije odgovori nakazujejo potrebo po financiranju varnostnih orodij.
- **Sistemi**: Le en odgovor je nakazal potrebo po financiranju celostnih sistemskih rešitev.

Vrste dogodkov, ki bi najbolj koristile MSP-jem



- **Strokovni seminarji**: Največ odgovorov (8) kaže, da MSP-ji potrebujejo seminarje, ki ponujajo poglobljeno razumevanje in izmenjavo znanja.
- **Dobre prakse in mreženje**: Sledi potreba po dogodkih za izmenjavo dobrih praks in povezovanje (7 odgovorov), kar je ključno za izmenjavo izkušenj.
- **Webinarji za dvig zavedanja**: Z 6 odgovori webinarji ostajajo pomembno orodje za izobraževanje.
- **Certifikacijska usposabljanja**: S 5 odgovori je izpostavljena tudi potreba po formalnih izobraževanjih z možnostjo pridobitve certifikatov.

Skupna ugotovitev in priporočila

Potreba po poenostavljenih finančnih podporah: MSP-ji potrebujejo dostopne in manj zapletene finančne mehanizme, kot so vavčerji.

Izboljšanje pripravljenosti na kibernetske incidente: Veliko MSP-jev ni pripravljenih na okrevanje po napadu, zato je treba vlagati v ozaveščanje in pomoč pri pripravi načrtov za obvladovanje incidentov.

Spodbujanje interaktivnih izobraževanj: Večji poudarek na simulacijah, vajah in certificiranju bi lahko izboljšal pripravljenost MSP-jev.

Osredotočanje na ključne deležnike: Potrebna je dvojna strategija, ki nagovarja tako direktorje kot zaposlene, da bi se celostno dvignila varnostna kultura.

2. KOMPETENCE IN RAZVOJ TALENTOV

Vprašanje: Ali poznate program Kibertalent? Kako lahko postane učinkovito orodje za vzgojo prihodnjih KV strokovnjakov?

- **Organizacija delavnic in priprav na tekmovanja (6 odgovorov)**: Udeleženci menijo, da so delavnice in tekmovanja koristne za praktično izobraževanje in motivacijo mladih.
- **Kontinuirano izobraževanje mladih (6 odgovorov)**: Podobno število odgovorov poudarja pomen nenehnega izobraževanja, ki bi mlade usmerjalo v področje kibernetske varnosti.
- **Vplivništvo med vrstniki (2 odgovora)**: Ta pristop je bil redkeje omenjen, a je vseeno zanimiv za dvig zanimanja med mladimi.
- **Organizacija mednarodnih izmenjav (3 odgovori)**: Mednarodne izmenjave so prav tako prepoznane kot pomembne za širitev znanja in izkušenj.

Vprašanje: Katere vrste izobraževanj za mlade in osebe, ki menjavajo karierno pot, bi bile najbolj smiselne za sofinanciranje s strani NCC?

- **Dvigovanje zavedanja in navduševanje (7 odgovorov)**: To vključuje spodbujanje zanimanja za kibernetsko varnost preko programov, kot je Kibertalent.
- **Simulacije in vaje (7 odgovorov)**: Interaktivne vaje so ključne za pripravo na realne situacije, kar je zelo cenjeno.

- **Izobraževanje skozi igro (6 odgovorov)**: Ta oblika učenja je zanimiva in spodbuja ustvarjalnost ter učinkovito pomnjenje.
- **Strokovna usposabljanja za odzivanje na incidente (4 odgovori)**: Pomembno za izboljšanje operativnih znanj, čeprav je bilo to redkeje omenjeno.

Interpretacija odprtih vprašanj

Poznavanje drugih programov za razvoj talentov v kibernetski varnosti

- Obstajajo izobraževalni programi, ki pa so pogosto plačljivi in zato manj dostopni širši publiki. Udeleženci so izpostavili, da so poletne šole in podobni programi zelo koristni za mlade, saj jim omogočajo vpogled v področje kibernetske varnosti.
- Univerze in fakultete igrajo ključno vlogo pri oblikovanju prihodnjih kibernetskih strokovnjakov. Pomembno je tudi vzpostaviti štipendije za podporo študentom, ki se odločajo za izredne študije.
- Izpostavljena je bila potreba po bolj segmentiranih izobraževalnih programih, ki bi zajemali specifične vidike informacijske varnosti. Trenutni kurikulum ne vključuje vseh potrebnih vsebin, kot so orodja za zagotavljanje neprekinjenega poslovanja.

Pristopi za spodbujanje in razvoj talentov

- Potrebno je spodbuditi večje število srednješolcev, da se prijavijo na kibernetsko-varnostne programe, ter jih navdušiti z raznolikimi in zanimivimi vsebinami.
- Pristopi za sofinanciranje naj vključujejo tudi podporo mednarodnim certifikatom, da bi se povečala usposobljenost mladih strokovnjakov. Krajša in ciljno usmerjena usposabljanja so prav tako ključna, saj trenutno na trgu manjka praktičnih in krajših programov za kibernetsko varnost.

Priporočila

Sofinanciranje izobraževalnih programov: Poudariti je treba pomen sofinanciranja praktičnih delavnic, poletnih šol, in simulacij za dvig kompetenc v kibernetski varnosti.

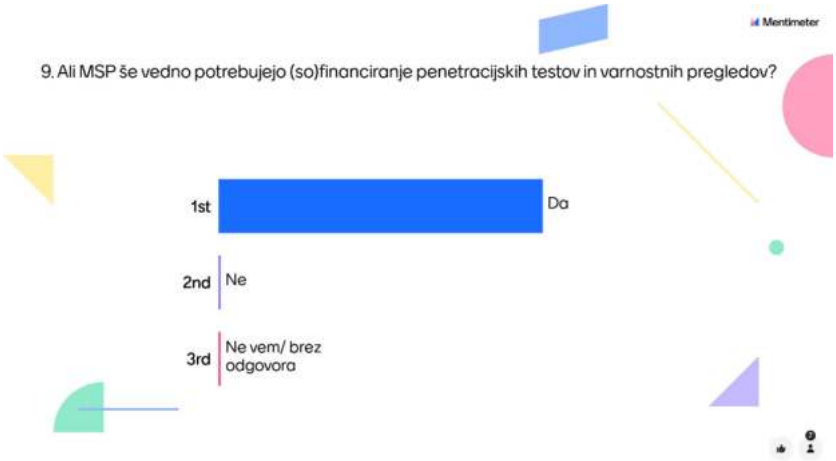
Razvoj krajših in ciljanih izobraževanj: Pomembno je razviti kratka in specializirana usposabljanja, ki odgovarjajo na specifične potrebe podjetij, vključno s praktičnimi veščinami za neprekinjeno poslovanje.

Povezovanje z izobraževalnimi ustanovami: Sodelovanje z univerzami in fakultetami za vzpostavitev ustreznega kurikuluma ter podpora pri pridobivanju štipendij za študente, ki želijo vstopiti na področje kibernetske varnosti.

Povečanje dostopnosti certifikatov: Spodbujanje pridobivanja mednarodnih certifikatov z delnim sofinanciranjem je ključno za izboljšanje usposobljenosti strokovnjakov.

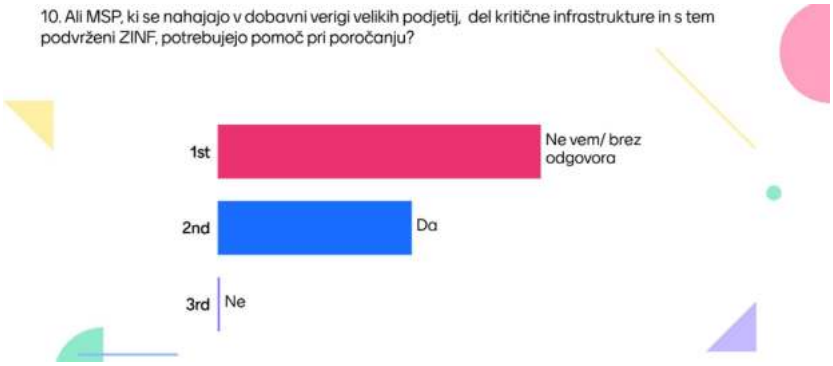
3. PODROČJA DELOVANJA NCC

Vprašanje: Ali MSP, ki se nahajajo v dobavni verigi velikih podjetij, del kritične infrastrukture in s tem podvrženi ZINF (Zakon o informacijski varnosti), potrebujejo pomoč pri poročanju?



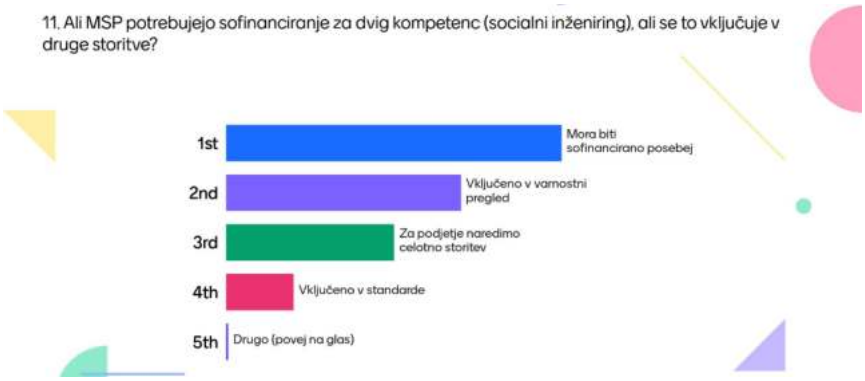
1. **Ne vem / brez odgovora**: Večina udeležencev se ni opredelila ali ni vedela, ali MSP-ji potrebujejo pomoč pri poročanju. To kaže na pomanjkanje ozaveščenosti ali nepoznavanje specifik poročanja, ki ga zahteva ZINF.
2. **Da**: Drugi najpogostejši odgovor je bil pritrdilen. Nekateri MSP-ji, vključeni v dobavne verige kritičnih podjetij, očitno prepoznavajo potrebo po dodatni podpori pri izpolnjevanju zakonskih zahtev.

Vprašanje: Ali MSP, ki se nahajajo v dobavni verigi velikih podjetij, del kritične infrastrukture in s tem podvrženi ZINF (Zakon o informacijski varnosti), potrebujejo pomoč pri poročanju?



1. Ne vem / brez odgovora: Večina udeležencev se ni opredelila ali ni vedela, ali MSP-ji potrebujejo pomoč pri poročanju. To kaže na pomanjkanje ozaveščenosti ali nepoznavanje specifik poročanja, ki ga zahteva ZINF.
2. Da: Drugi najpogostejši odgovor je bil pritrdilen. Nekateri MSP-ji, vključeni v dobavne verige kritičnih podjetij, očitno prepoznavajo potrebo po dodatni podpori pri izpolnjevanju zakonskih zahtev.

Vprašanje: Ali MSP potrebujejo sofinanciranje za dvig kompetenc (socialni inženiring), ali se to vključuje v druge storitve?



1. **Sofinanciranje za dvig kompetenc (socialni inženiring)**
    - **Mora biti sofinancirano posebej**: Obstaja jasna potreba po posebnem sofinanciranju, saj podjetja prepoznavajo socialni inženiring kot specifično področje, ki zahteva usmerjena izobraževanja.
    - **Vključeno v varnostni pregled**: Nekateri anketiranci predlagajo, da bi lahko to kompetenco vključili kot del širših varnostnih pregledov.
    - **Celostne storitve**: MSP-ji bi lahko imeli korist od celostnih rešitev, ki pokrivajo različne aspekte kibernetske varnosti.
    - **Standardi**: Predlog za vključitev teh kompetenc v obstoječe standarde kaže na potrebo po integraciji z že obstoječimi varnostnimi praksami.
2. **Dodatna opažanja o potrebah po kadrih za kibernetsko varnost**
    - **Raznolikost kadrov**: Izpostavljena je potreba po različnih profilih kadrov za interno varnost, analitiko, razvoj produktov ter izvajanje izobraževanj. Telekomunikacijski sektor potrebuje tako visoko izobražene kot tudi kadre, ki se učijo skozi prakso.
    - **Praktično usposabljanje**: Omenjeno je, da se veliko strokovnjakov izoblikuje skozi praktično delo in izkušnje, ne nujno z visokošolskimi diplomami. To še posebej velja za analitike, ki se kalijo z dejanskimi delovnimi izkušnjami.

Priporočila

Razvoj programov za praktično usposabljanje: NCC bi moral razmisliti o vzpostavitvi programov, ki omogočajo mladim strokovnjakom, da se kalijo na praktičen način, ne glede na formalno izobrazbo.

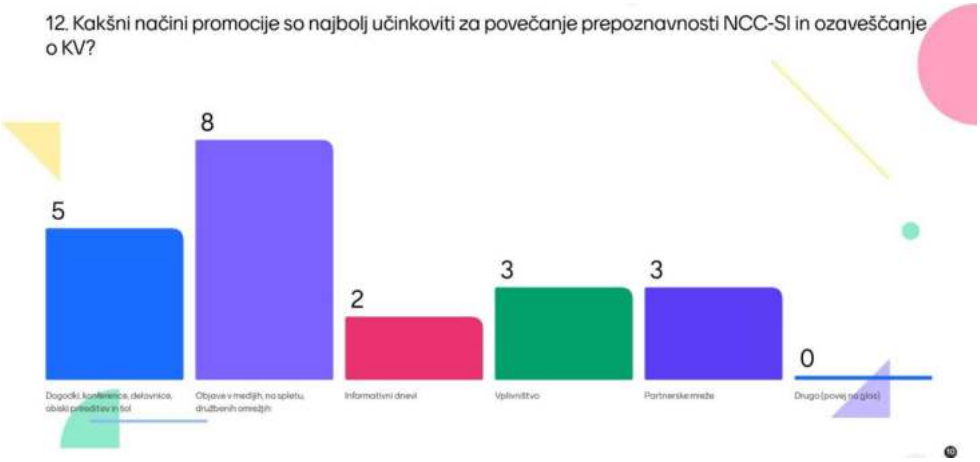
Sofinanciranje specifičnih kompetenc: Posebno sofinanciranje za področja, kot je socialni inženiring, bi pripomoglo k razvoju specifičnih veščin, ki jih podjetja potrebujejo.

Povezovanje z izobraževalnimi ustanovami: Sodelovanje z univerzami, srednjimi šolami in podjetji bi omogočilo boljše usklajevanje med izobraževanjem in potrebami trga.

Razvijanje kadrovskih profilov: Podjetjem bi bilo smiselno ponuditi podporo pri razvoju različnih kadrovskih profilov za kibernetsko varnost, kar vključuje tako tehnične kot analitične veščine.

4. VIDNOST IN PREPOZNAVNOST NCC

Kakšni načini promocije so najbolj učinkoviti za povečanje prepoznavnosti NCC-SI in ozaveščanje o kibernetski varnosti?



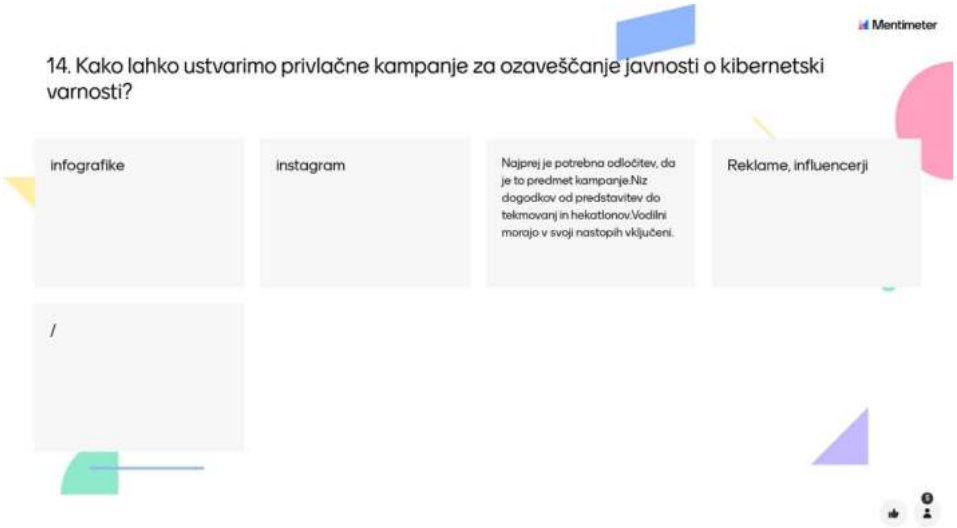
- **Objave v medijih, na spletu in družbenih omrežjih (8 odgovorov)**: Največji poudarek je na digitalnih objavah, kar kaže na pomen uporabe sodobnih komunikacijskih kanalov za dosego širšega občinstva.
- **Dogodki, konference, delavnice (5 odgovorov)**: Fizične aktivnosti, kot so delavnice in obiski šol, so prav tako zelo cenjene, saj omogočajo neposreden stik in globlje razumevanje teme.
- **Partnerstva in vplivništvo (3 odgovori vsak)**: Vključevanje vplivnežev in partnerskih mrež bi lahko dodatno pripomoglo k širjenju sporočil o kibernetski varnosti.
- **Informativni dnevi (2 odgovora)**: Informativni dogodki so nekoliko manj izpostavljeni, vendar ostajajo koristni za ozaveščanje specifičnih ciljih skupin.

Ali menite, da bi bila koristna vzpostavitev platforme za deljenje informacij o kibernetskih grožnjah?

- **Da (večina odgovorov)**: Prevladujoče mnenje je, da bi platforma za deljenje informacij o grožnjah izboljšala odzivnost in pripravljenost podjetij na kibernetske incidente.
- **Dodatna opažanja**: Platforma bi omogočila hitro obveščanje o novih grožnjah in incidentih. Udeleženci so omenili potrebo po poročanju groženj NCC-ju, ki bi nato te informacije delil

naprej. Izpostavljen je tudi pomen primerjalnih analiz (benchmarking) za podjetja, da razumejo, kje stojijo v primerjavi z drugimi.

Kako ustvariti privlačne kampanje za ozaveščanje o kibernetski varnosti?



- **Infografike, Instagram, reklame in influencerji**: Vizualna in moderna komunikacijska orodja so izpostavljena kot učinkovita sredstva za angažiranje občinstva.
- **Sodelovanje s projekti in kampanjami**: Predlagana je povezava z obstoječimi projekti, kot je "Varni v pisarni", da bi se dosegla večja sinergija in razširila ozaveščenost.

Priporočila

Izkoristek digitalnih medijev: Osredotočite se na digitalne objave in družbena omrežja za širjenje ozaveščenosti, pri čemer uporabite infografike in vplivneže za večji doseg.

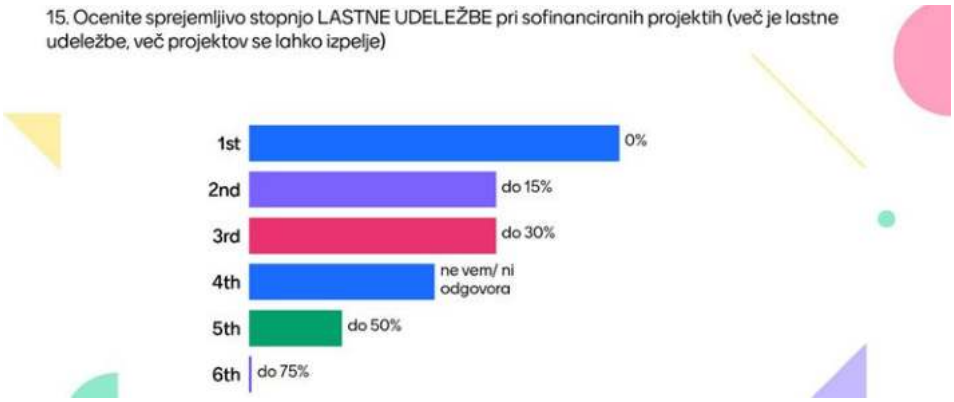
Organizacija dogodkov in partnerstev: Redna organizacija dogodkov, konferenc in delavnic ostaja ključna, vendar bi NCC moral raziskati tudi možnost strateških partnerstev za širši vpliv.

Vzpostavitev informacijske platforme: Ustanovitev platforme za deljenje informacij o kibernetskih grožnjah bi izboljšala odzivnost in omogočila podjetjem dostop do ključnih informacij. Upoštevati je treba, da bi bile pomembne tudi primerjalne analize po regijah in panogah.

Povezovanje z obstoječimi programi: NCC-SI bi moral ustvarjati sinergije z obstoječimi programi kibernetske varnosti za večji vpliv in bolj učinkovito uporabo virov.

5. FINANČNE POTREBE IN STRUKTURA FINANCIRANJA

Vprašanje: Ocenite sprejemljivo stopnjo lastne udeležbe pri sofinanciranih projektih (večja kot je lastna udeležba, več projektov se lahko izpelje)



1. **Do 15% (večina odgovorov)**: Udeleženci menijo, da je maksimalna stopnja lastne udeležbe pri financiranju, ki jo lahko podjetja sprejmejo, 15%. Višja stopnja udeležbe bi povzročila nižjo pripravljenost MSP-jev za sodelovanje v projektih.
2. **Do 30% in do 50%**: Nekateri so še pripravljeni na sofinanciranje do 30%, vendar je sprejemljivost hitro upadajoča. Le malo jih podpira sofinanciranje do 50%.
3. **Dodatni komentarji**:
    - **Povečanje lastne udeležbe odvrača MSP-je**: Izpostavljeno je, da se podjetja, ki morajo prispevati večji delež, redkeje prijavljajo na razpise. Konkurenčnejši pogoji financiranja v EU (100% sofinanciranje) še dodatno zmanjšujejo zanimanje za domače razpise.
    - **Kaskadno financiranje**: Predlagano je, da bi morali domače razpise prilagoditi evropskim praksam, z bolj odprtimi razpisi in krajšimi cikli financiranja (pol leta do eno leto), kar bi olajšalo dostop podjetjem z že pripravljenimi projekti.

Priporočila

Zmanjšanje stopnje lastne udeležbe: Da bi povečali privlačnost domačih razpisov za MSP-je, bi bilo smiselno zmanjšati zahtevano lastno udeležbo na največ 15%, kjer je to mogoče. Večje stopnje prispevkov odvračajo podjetja, zlasti zaradi konkurenčnih financiranj v EU.

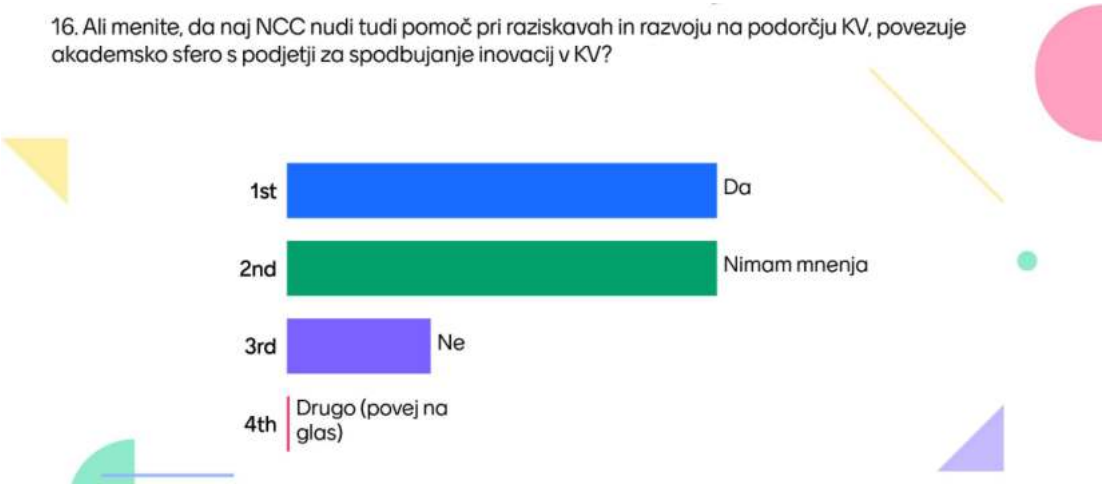
Prilagoditev modelov kaskadnega financiranja: Slediti evropskemu modelu odprtih razpisov z bolj fleksibilnimi in krajšimi cikli, da bi podjetja lahko lažje prijavila že pripravljene projekte in hitreje dostopala do sredstev.

Spodbujanje sinergij z obstoječimi projekti: Dovoliti MSP-jem povezovanje financiranja z obstoječimi projekti, da bi povečali uporabo razpoložljivih sredstev in optimizirali izvedbo več projektov.

Raziskava zakonodajnih omejitev: Ugotoviti, ali bi bilo mogoče sprostiti ali prilagoditi omejitve sofinanciranja v slovenski zakonodaji, saj se trenutna zgornja meja (50%) izkaže za previsoko za številna podjetja.

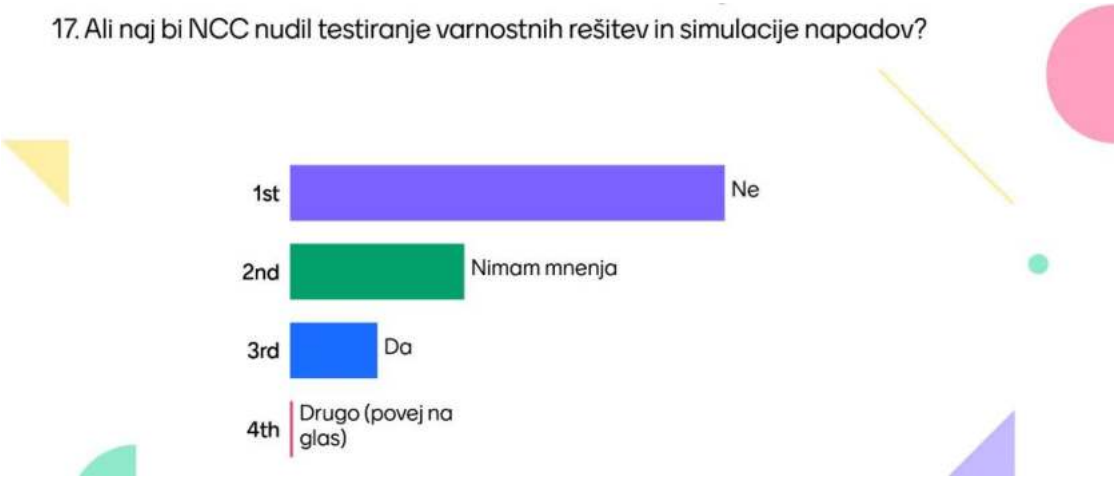
6. STRATEŠKE IN OPREATIVNE POTREBE

Vprašanje: Ali naj NCC nudi pomoč pri raziskavah in razvoju na področju KV ter povezuje akademsko sfero s podjetji za spodbujanje inovacij?



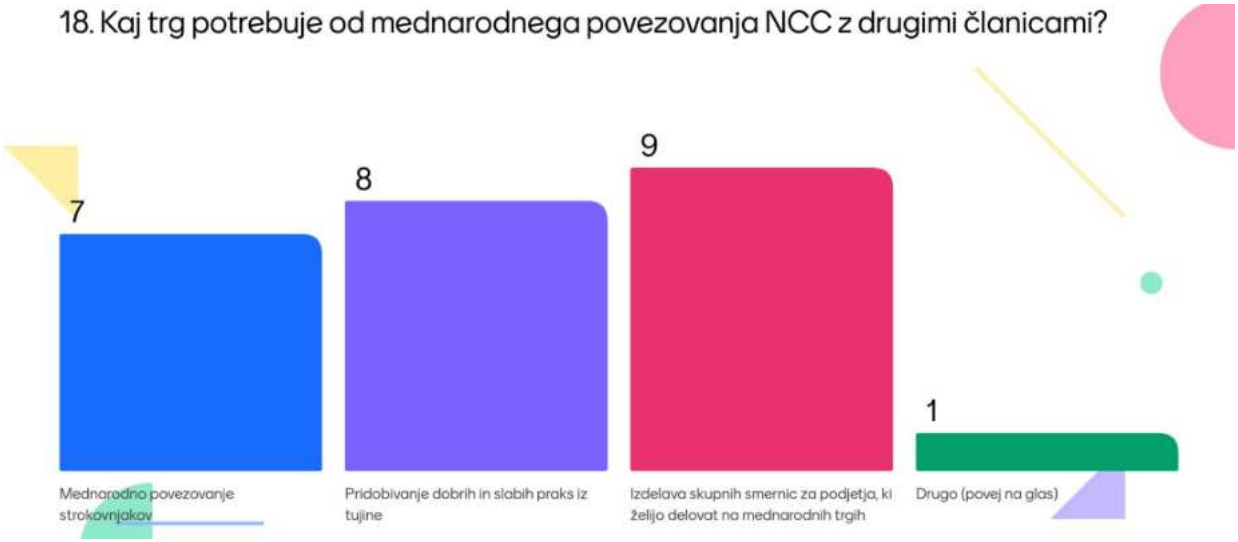
- **Večina udeležencev (Da)**: Izpostavljena je potreba po vzpostavitvi kompetenčnega centra, ki bi učinkovito povezoval raziskovalne ustanove s podjetji in spodbujal inovacije na področju kibernetske varnosti. Pomembna je tudi sinhronizacija sodelovanja s pristojnimi državnimi organi.
- **Kritika in predlogi**: Udeleženci so poudarili pomen vzpostavitve jasnih struktur za raziskave in razvoj ter strateškega povezovanja, da bi se izognili podvajanju in neučinkovitosti.

Vprašanje: Ali naj NCC nudi testiranje varnostnih rešitev in simulacije napadov?



- **Prevladujoče mnenje (Ne)**: Večina je menila, da to ne bi smela biti primarna naloga NCC. Vendar pa so bili izraženi pomisleki glede jasnosti nalog in pristojnosti, saj je pomembno, da je definicija aktivnosti NCC jasna in javno dostopna.
- **Poudarek na jasnosti**: Udeleženci so opozorili, da je pomembno, da NCC definira, kaj se bo izvajalo in da se naloge ne podvajajo s že obstoječimi iniciativami.

Vprašanje: Kaj trg potrebuje od mednarodnega povezovanja NCC z drugimi članicami?



- **Izdelava skupnih smernic (9 odgovorov)**: Najbolj izpostavljeno je bilo oblikovanje skupnih smernic za podjetja, ki želijo delovati na mednarodnih trgih, kar bi omogočilo boljše razumevanje in skladnost s standardi.
- **Pridobivanje dobrih in slabih praks (8 odgovorov)**: Udeleženci so poudarili potrebo po izmenjavi praks iz tujine, kar bi koristilo izboljšanju kibernetske varnosti doma.
- **Mednarodno povezovanje strokovnjakov (7 odgovorov)**: Povezovanje s tujimi strokovnjaki bi bilo koristno za krepitev znanja in zmogljivosti na področju kibernetske varnosti.

Dodatne ugotovitve iz diskusije

- **Razvoj infrastrukture**: Obstaja potreba po vzpostavitvi trajnostne infrastrukture, kot so digitalni peskovniki, ki bi omogočili varno testiranje in razvoj novih rešitev. Vprašanje ostaja, ali uporabiti že obstoječe platforme ali razviti nove.
- **Področje umetne inteligence (UI)**: Udeleženci so izpostavili pomen raziskovanja priložnosti, ki jih UI ponuja pri odkrivanju in preprečevanju kibernetskih groženj.
- **Potreba po osnovni izobrazbi o KV**: Udeleženci so poudarili, da v splošni populaciji primanjkuje znanja o kibernetski varnosti, zato bi bilo smiselno, da se vsebine o KV uvedejo že v osnovnošolske programe.

Priporočila

Vzpostavitev osrednjega kompetenčnega centra: NCC bi moral imeti jasno opredeljene naloge, vključno s povezovanjem akademske sfere in podjetij za spodbujanje raziskav in razvoja. Povezovanje s tujimi institucijami bi prav tako okrepilo inovacijsko okolje.

Jasna opredelitev pristojnosti: Da bi se izognili zmedi in podvajanju, je ključno, da NCC jasno definira svoje naloge in odgovornosti. To vključuje pregled nad obstoječimi pobudami, kot so SRIPI in Cyberhubs.

Razvoj digitalnih peskovnikov: Preučiti možnost vzpostavitve digitalnih peskovnikov za varno testiranje rešitev. Če je mogoče, uporabiti že obstoječe platforme in jih nadgraditi.

Spodbujanje uporabe umetne inteligence: Raziskati načine, kako lahko UI pripomore k izboljšanju odkrivanja in preprečevanja kibernetskih groženj, ter spodbuditi projekte, ki se osredotočajo na te tehnologije.

Izobraževanje o kibernetski varnosti: Podpreti uvedbo osnovnih vsebin o KV v šolske programe in organizirati dogodke, ki pritegnejo mlade.