Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko
Koroška cesta 46
2000 Maribor, Slovenija

Analiza pomembnosti kompetenc na področju kibernetske varnosti

Projekt Ciljnega raziskovalnega programa CRP 2021 št. V2-2132 »RUKIV - Razvoj programov usposabljanj za kibernetsko varnost«

Poročilo delovnega paketa 2: ANALIZA

Urednik: Muhamed Turkanović

Avtorji dokumenta: Marko Kompara, Lili Nemec Zlatolas, Marko Hölbl, Tatjana Welzer Družovec, Viktor Taneski, Muhamed Turkanović

Maribor, maj 2022

Rezultati, pridobljeni znotraj tega projekta, so bili financirani s strani ARRS in URSIV pod pogodbo št. V2-2132.

Sodelujoče institucije v projektu RUKIV

KRATICA	NAZIV
UM FERI	Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
VIRIS	Viris, varnost in razvoj informacijskih sistemov, d. o. o.

Zagotavljanje kakovosti dokumenta

Zagotavljanje kakovosti dokumenta	Polona Vodopivec, VIRIS

Kazalo

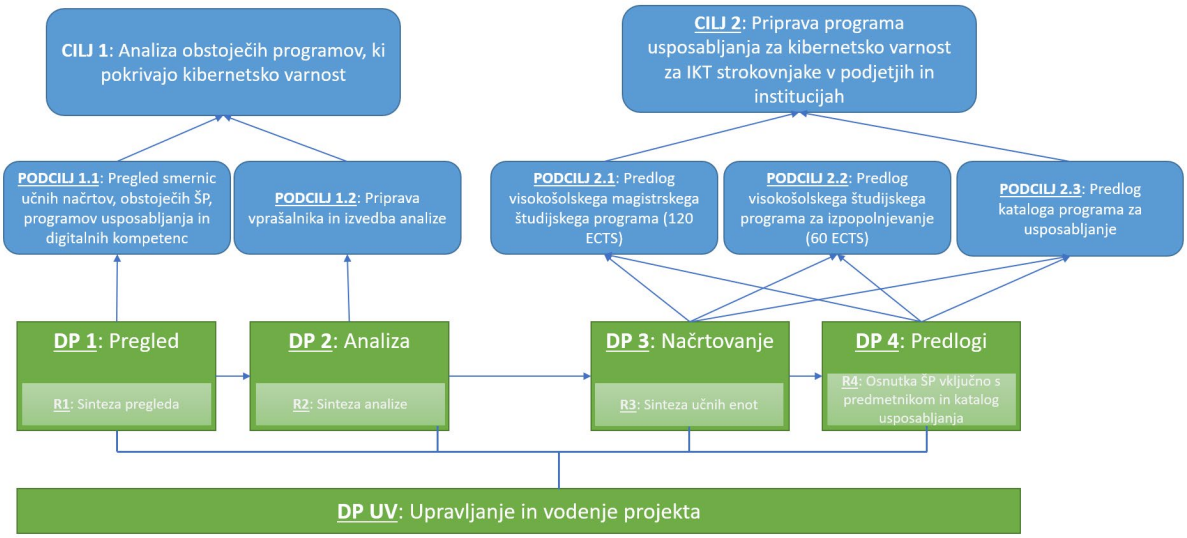
1 Uvod

Delovni paket 2 (DP2) vključuje aktivnosti, ki so potrebna za doseganje drugega podcilja (PODCILJ 1.2) raziskovalnega projekta RUKIV. Natančneje vključuje snovanje vprašalnika, ki temelji na rezultatih DP1. Vprašalnik je namenjen IKT strokovnjakom v podjetjih in institucijah z namenom preverjanja potreb in trenutnega stanja na trgu in tehnološkega razvoja v stroki.

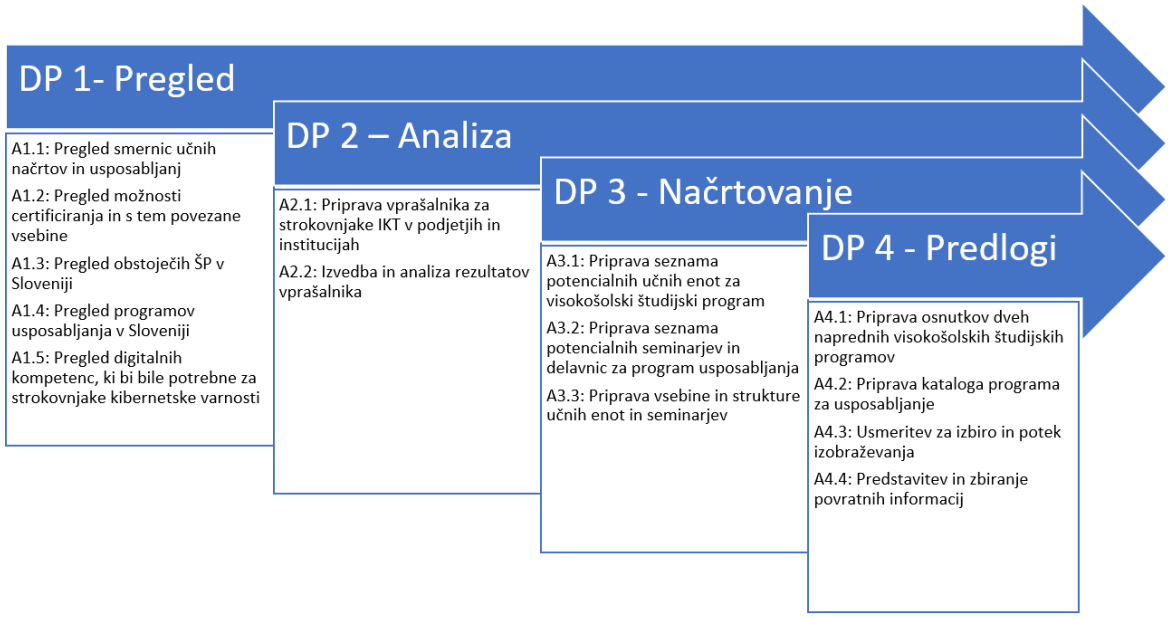
Na osnovi DP1 in R1 smo pripravili vprašalnik, ki je namenjen zaposlenim v podjetjih in/ali javnih institucijah. Cilj vprašalnika je preverjanje in razumevanje trenutnega stanja na slovenskem profesionalnem IKT področju, in sicer iz vidika znanj in veščin oz. kompetenc s področja kibernetske varnosti, potreb po takšnih kompetencah, aktivnostih na področju pridobivanja teh kompetenc, splošnih aktivnostih, ki se navezujejo na področje kibernetske varnosti itn.

Na osnovi pripravljenega vprašalnika smo od zaposlenih v podjetjih in javnih institucijah, ki so posredno ali neposredno povezani s področjem IKT pridobili odgovore o njihovih trenutnih in želenih kapacitetah kadra na področju kibernetske varnosti ter pomembnost posameznih znanj in kompetenc iz področja. Za namen diseminacije vprašalnika smo poleg lastnih komunikacijskih kanalov (npr. spletna stran fakultete in družbena omrežja sodelujočih v projektu po metodi snežne kepe) vključili tudi podporne partnerske organizacije, kot so Digitalno inovacijsko stičišče Slovenije, Digitalno inovacijsko stičišče UM, konzorcij DIGI-SI - Evropsko digitalno inovacijsko stičišče, Sekcijo za kibernetsko varnost GZS in Slovensko društvo INFORMATIKA. Skupno je vprašalnih ustrezno izpolnilo 45 respondentov.

Ta dokument poda nastali vprašalnik, opisuje postopek izvedbe ankete, predstavi postopek analize prejetih odgovorov in njene rezultate.



Slika 1: Delovni paketi, rezultati in podcilji.



Slika 2: Program dela vključno s posameznimi aktivnostmi po delovnih paketih.

2 Analiza pomembnosti kompetenc kibernetske varnosti na podlagi ankete trga

Poleg pregleda pomembnosti znanj iz področja kibernetske varnosti, ki smo ji opravili v visokošolskih izobraževalnih programih in certifikatih (rezultati so bili predstavljeni v DP1) smo želeli preveriti tudi, kako pomembna so posamezna vprašanja za trg dela. V ta namen smo pripravili anketo, ki je bila prosto dostopna vsem organizacijam, ki bi potencialno lahko zaposlovale ljudi s takšnimi znanji in jih vprašali, katera od teh znanj so zanje ključna.

1.1 Priprava in izvajanje ankete

Vprašalnik, ki je bil pripravljen za namen zajemanja mnenja oz. pomembnosti posameznih znanj kibernetske varnosti na trgu dela, je vseboval 22 vprašanj. Prvih osem vprašanj je bilo splošnih o anketirancu in organizaciji, iz katere prihaja, naslednjih pet je bilo o njihovem (trenutnem in bodočem/želenem) kadru na področju kibernetske varnosti, sledilo je osem vprašanj o pomembnosti posameznih kompetenc oz. znanj ter še zadnje odprto vprašanje, kjer so nam lahko anketiranci sporočili, karkoli so želeli o povezani problematiki ali sami anketi. Celoten vprašalnik je v Prilogi na koncu tega dokumenta.

Tako kot v analizi znanj, vključenih v certifikate, in študijske programe je tudi tu bil uporabljen seznam znanj iz Cybersecurity Curricula 2017 [1]. Anketiranci so za vsako od 55 enot znanj podali mnenje o njeni pomembnosti zanje oz. njihovo organizacijo. To so storili na podlagi Likertove lestvice, ki je zajemala pet stopenj od *sploh ni pomembno* (vrednost 1) do *zelo pomembno* (vrednost 5). Anketiranci so za vsako od enot znanja imeli tudi možnost izbrati *Ne morem oceniti*, če so menili, da iz kakršnegakoli razloga ne morejo oceniti pomembnosti posamezne kompetence/znanja.

Anketa je bila oglaševana preko lastnih komunikacijskih kanalov (npr. spletna stran fakultete in družbena omrežja sodelujočih v projektu) ter drugih organizacij, kot so Digitalno inovacijsko stičišče Slovenije, Digitalno inovacijsko stičišče UM, konzorcij DIGI-SI – slovenski EDIH, Sekcija za kibernetsko varnost GZS in Slovensko društvo INFORMATIKA. Anketa je bila aktivna od 9. 2. 2022 do 9. 5. 2022. V tem času je bilo odprtih 358 povezav do ankete. Anketa je bila delno izpolnjena v 62 primerih, vendar smo v končne rezultate vključili samo rezultate zaključenih anket. Rezultatov nedokončanih anket nismo upoštevali, ker so anketiranci vedno imeli možnost zaobiti vprašanje, če nanj niso imeli ali niso želeli podati odgovora. Skupno smo tako analizirali 45 v celoti izpolnjenih vprašalnikov. Stopnja dokončanja ankete glede na število povezav do nje znaša 13 %, kar je znotraj pričakovanih 10-15 % [2] ko gre za zunanje ankete (anketa se ne izvaja znotraj lastne enote/organizacije).

1.2 Podatki o sodelujočih in kibernetskih znanjih na trgu

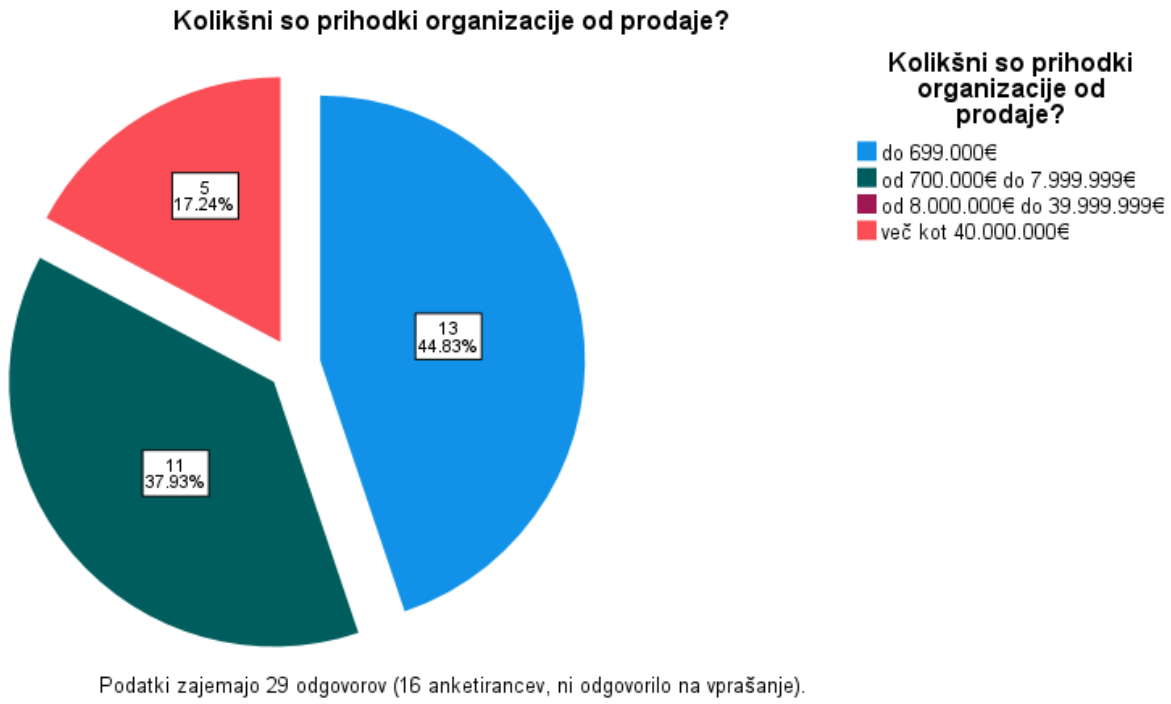
Kot je razvidno iz grafikona 1, je večina anketirancev iz javnega sektorja, ki ni zastopan med drugimi ponujenimi odgovori (46,7 %). Ostali udeleženci so prihajali predvsem iz organizacij, ki ponujajo digitalne storitve in izdelke, zdravstvenega sektorja, varnosti in varovanja, obrambe, telekomunikacij in energetskega sektorja. Velika večina sodelujočih je zaposlenih v organizacijah (glej Grafikon 2), ki pretežno delujejo v osrednji Sloveniji (76,7 %).

[1] https://cybered.acm.org/
[2] https://www.smartsurvey.co.uk/blog/what-is-a-good-survey-response-rate

Grafikon 1: Podatki o sektorju delovanja anketirancev.

Grafikon 2: Kje v Sloveniji so organizacije, iz katerih prihajajo anketiranci.

Po prihodkih sodelujoče organizacije težijo (44,8 %) k nižjim letnim prihodkom (do 700 tisoč evrov), ki jim sledijo organizacije z do 8 milijonov evrov prihodkov od prodaje (37,9 %). Zanimivo v anketi ni sodelovala nobena organizacija z dohodki med 8 in 40 milijonov evrov, medtem ko ima več kot 40 milijonov prihodkov 17,2 % sodelujočih organizacij. Neprofitne organizacije, kot so tudi organizacije javnega sektorja, so lahko to vprašanje preskočile, zato ti podatki zajemajo samo 29 odgovorov.



Grafikon 3: Prihodki organizacij, iz katerih prihajajo anketiranci.

Sodelujoči v anketi so enakomerno prihajali iz vodstvenih kadrov (44,4 %) in IKT tehničnih kadrov (44,4 %). Enakomerno so bili razporejeni tudi glede na velikost organizacij, iz katerih prihajajo, kjer smo kot ločnico med manjšimi in večjimi organizacijami postavili 100 zaposlenih.

Tabela 1: Število in razpored vrst kadrov v večje ali manjše organizacije.

		Število zaposlenih		
		več kot 100	100 ali manj	Skupaj
Kakšna je vaša vloga v organizaciji?	Vodstveni kader	12	8	20
	IKT tehnični kader	12	8	20
	Drugo	3	2	5

Skoraj vsi anketiranci se pri svojem delu srečujejo s kibernetsko varnostjo (glej tabelo 2). Med popolnoma izpolnjenimi anketami je samo ena izjema, ki pa je posledično tudi pri ocenjevanju pomembnosti kompetenc, izbrala možnost *Ne morem oceniti* največkrat od vseh anketirancev, in sicer v 50,9 % ocen.

Tabela 2: Podatki o tem, ali se anketiranci sami srečujejo s kibernetsko varnostjo pri njihovem delu.

Ali se pri svojem delu srečujete s kibernetsko varnostjo?

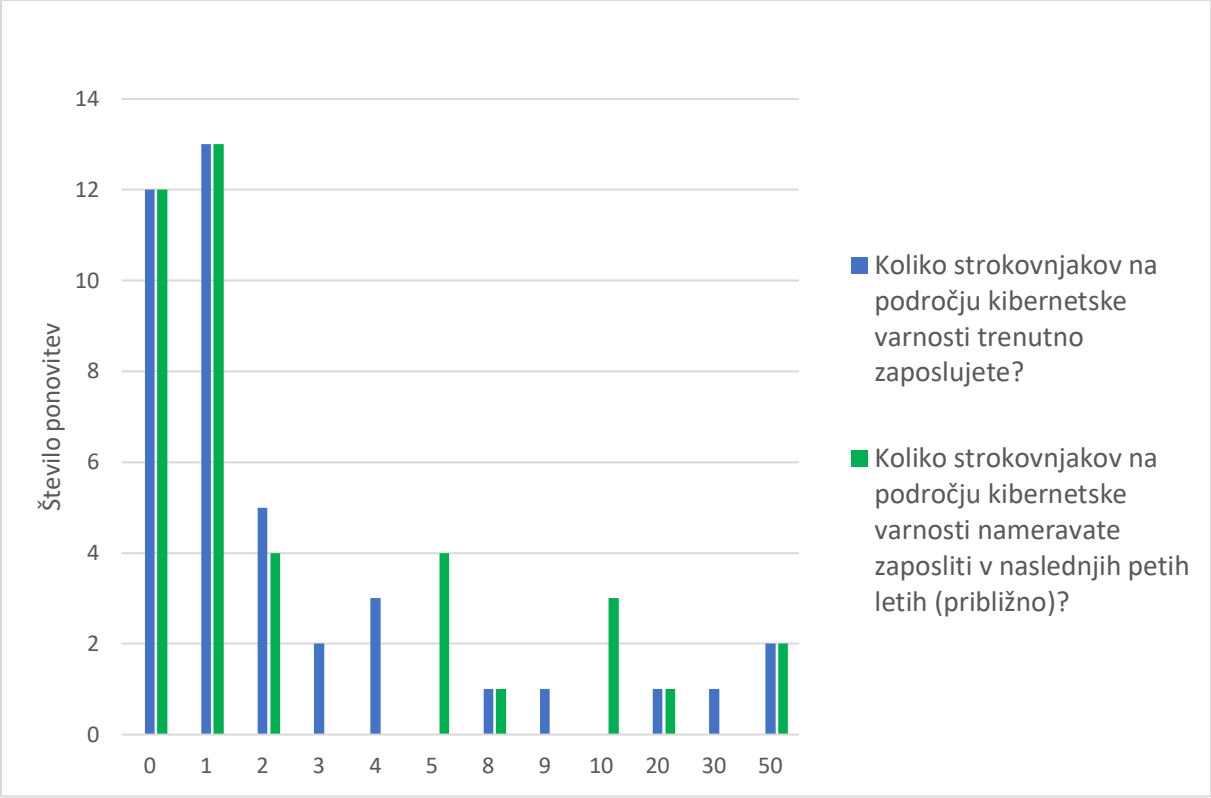
		Število	Odstotek
Odg.	DA	44	97,8
	NE	1	2,2
	Skupaj	45	100,0

V tabeli 3 so zbrani podatki o številu zaposlenih v sodelujočih organizacijah, o številu zaposlenih, ki delujejo na področju kibernetske varnosti in o številu strokovnjakov kibernetske varnosti, ki jih organizacije nameravajo oz. želijo zaposliti v naslednjih petih letih. Vključene organizacije so od velikosti enega zaposlenega do devet tisoč. Povprečna organizacija ima skoraj tisoč sedemsto zaposlenih, čeprav je sodelovalo samo 10 (22,2 %) organizacij, ki imajo več kot tisoč zaposlenih. Večina sodelujočih ima eno zaposleno osebo, ki se ukvarja s kibernetsko varnostjo, na povprečju vseh sodelujočih pa ta številka naraste na 5. Glede na število vseh zaposlenih v sodelujočih organizacijah se s kibernetsko varnostjo ukvarja vsak 365-ti zaposleni v podjetju (tj. 0,27 %). Najbolj zanimive pa so številke o prihodnjih načrtih zaposlovanja kadrov kibernetske varnosti. Želje za naslednjih 5 let so praktično podvojiti trenuten kader na tem področju. Ne samo da so povprečne vrednosti med trenutnim številom zaposlenih na področju kibernetske varnosti in prihodnjih zaposlitvah zelo podobne (Tabela 3), tudi njihove porazdelitve so si neverjetno podobne (glej Grafikon 4). To nam pokaže, da ni želja zgolj ene organizacije, da bo v veliki meri širila svoj kader na tem področju, ampak je ta trend podvajanja kadra prisoten čez praktično vse v anketi sodelujoče organizacije.

Tabela 3: Podatki o zaposlenih v podjetju in kadrih z znanji iz kibernetske varnosti.

		Okvirno število zaposlenih v vaši organizaciji?	Koliko strokovnjakov na področju kibernetske varnosti trenutno zaposlujete?	Koliko strokovnjakov na področju kibernetske varnosti nameravate zaposliti v naslednjih petih letih (približno)?
N	Odgovorilo	45	41	40
	Ni odgovorilo	0	4	5
Aritmetična sredina		1686,67	5,07	4,97
Mediana		135,00	1,00	1,00
Modus		50[a]	1	1
Standardni odklon		3097,279	11,714	11,212
Razpon		8999	50	50
Najmanjša vrednost		1	0	0
Največja vrednost		9000	50	50
Seštevek vseh odgovorov		75900	208	199

a. Obstaja več modusov. Prikazan je najmanjši.

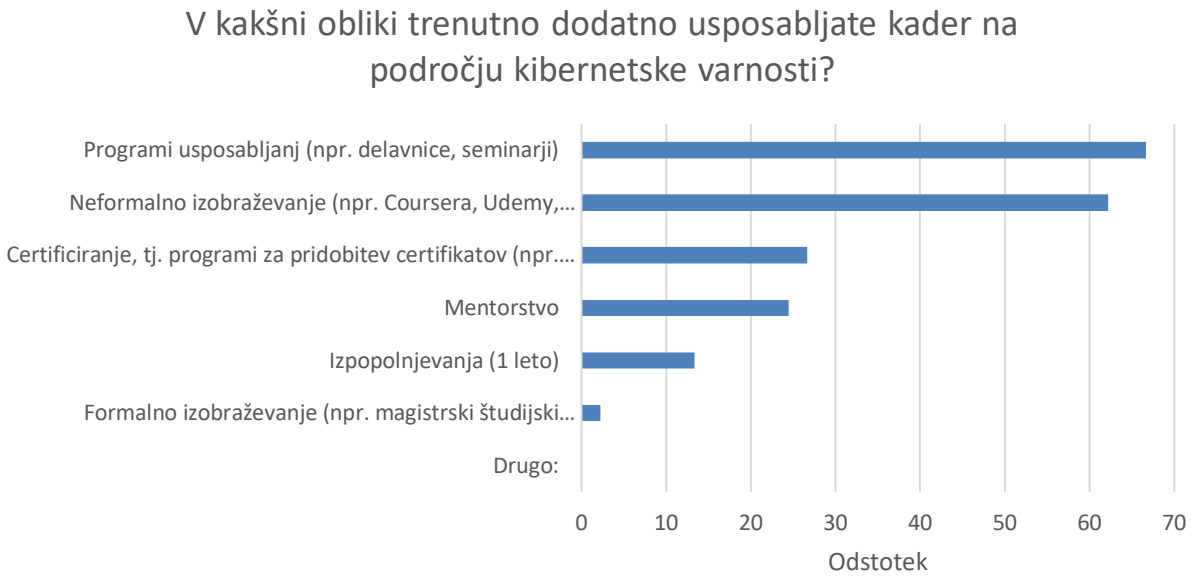


Grafikon 4: Trenutno število zaposlenih v kibernetski varnosti in načrti zaposlovanja.

Čeprav imajo organizacije zelo veliko željo po povečanju števila zaposlenih, ki se ukvarjajo s kibernetsko varnostjo, imajo pri tem očitno zelo velike težave. Anketa je pokazala (Grafikon 5), da imajo v več kot 70 % sodelujočih organizacij velike ali pa zelo velike težave pri pridobivanju novih kadrov na tem področju. Zgolj en anketiranec oz. njihova organizacija pri tem nima težav.

Grafikon 5: Zahtevnost pridobivanja kadra.

V primerjavi oblik usposabljanja na področju kibernetske varnosti, ki jih organizacije trenutno uporabljajo, in oblik, katerih uporabo bi želeli povečati (glej grafikona 6 in 7) so v obeh primerih na prvem mestu različni programi usposabljanja. Certificiranje je trenutno tretja najbolj uporabljena oblika izobraževanja, vendar se uporablja v komaj 25 % sodelujočih organizacij, medtem ko bi v prihodnje več kot 70 % organizacij želelo svoje zaposlene izobraževati na tak način. Poleg certificiranja imajo največji skok formalno izobraževanje, ki se trenutno komajda uporablja, v prihodnosti pa bi ga želelo uporabiti več kot 42 % organizacij. Edina oblika, ki se trenutno uporablja več, kot bi si v organizacijah želeli, je neformalno izobraževanje (npr. Coursera, Udemy, ipd.).



Grafikon 6: Trenutne oblike usposabljanja kadrov na področju kibernetske v organizacijah anketirancev.

Grafikon 7: Želje po usposabljanju kadrov na področju kibernetske varnosti v organizacijah anketirancev.

1.3 Pomembnost kompetenc in znanj iz kibernetske varnosti

Področja znanja so sestavljena iz enot znanja, pomembnost katerih so anketiranci ocenjevali v vprašalniku. Pomembnost posameznih znanj so sodelujoči ocenjevali na lestvici od 1 do 5 (odgovori *Ne morem oceniti* so bili izločeni iz te analize). Na podlagi teh odgovorov smo rezultate združili v ocene za celotna področja znanja, rezultati česar so prikazani v tabeli 4. Razlike v primerjavi s prejšnjimi analizami, ki smo jih izvedli za vsebovanost znanj in kompetenc v učnih vsebinah visokošolskih študijskih programov in v mednarodno priznanih certifikatih so precej obsežne. Pri razlogih za to so zagotovo veliko manjše razlike med ocenami. Če pogledamo povprečne ocene za posamezno področje znanja, opazimo, da je razlika med ocenjeno najpomembnejšim področjem znanja in najmanj pomembnim področjem znanja samo 0,277, kar znaša samo 6,925 %. Te razlike so bile pri prejšnjih oblikah analize pomembnosti znanj veliko bolj izrazite. To nakazuje, da sodelujoči v anketi bili veliko manj kritični do pomembnosti posameznih znanj ali pa so praktično vsa znanja zelo oz. skoraj enako pomembna na trgu dela. Kot bomo videli v nadaljevanju, je ta razlika med posameznimi enotami znanja tudi presenetljivo majhna.

V primerjavi samih rezultatov ankete s prejšnjo analizo visokošolskih študijskih programov in certifikatov je zagotovo največja razlika na področju *Varnosti ljudi*. V prejšnjih analizah je bila varnost ljudi na šestem in sedmem mestu, medtem ko je v tej analizi na prvem mesu. Drugi dve področji, ki sta glede na odgovore s trga dela bolj pomembni, kot sta bili v analizi študijskih programov in certifikatov, sta *Organizacijska varnost* in *Varnost programske opreme*. Področji, ki sta na tem seznamu najbolj zdrsnili, sta bili zanimivo na prvem in drugem ter prvem in tretjem mestu v prejšnjih analizah. Gre za *Varnost podatkov* in *Varnost povezave*. *Varnost komponent* je tako kot tudi v vseh prejšnjih analizah na zadnjem mestu.

Tabela 4: Pomembnost področij znanja glede na anketo trga.

Področje znanja	Ocena (skupaj)	Področje znanja	Ocena (povprečje na enoto)
Organizacijska varnost	40,63	Varnost ljudi	4,684
Varnost podatkov	35,29	Organizacijska varnost	4,546
Varnost povezave	34,62	Varnost programske opreme	4,479
Varnost ljudi	32,58	Varnost podatkov	4,474
Varnost programske opreme	31,07	Družbena varnost	4,473
Varnost sistemov	30,28	Varnost povezave	4,440
Družbena varnost	21,86	Varnost sistemov	4,414
Varnost komponent	17,09	Varnost komponent	4,407

V tabeli 5 so predstavljene povprečne ocene, ki so jih sodelujoči dodelili posameznim enotam znanja (prvi in drugi stolpec) ter vrstni red znanj oz. kompetenc po pomembnosti, kot so bile ugotovljene pri analizi študijskih programov in priznanih mednarodnih certifikatov.

V primerjavi s prejšnjimi metodami analize pomembnosti znanj je razlika med najbolj pomembnimi in najmanj pomembnimi znanji relativno majhna. Najvišje ocenjena enota znanja *Upravljanje identitet* je imela povprečno oceno 4,82, medtem ko je najslabše ocenjena enota *Kriptoanaliza* imela 3,63. Čeprav je tu razlika bolj očitna, kot je bila pri področjih znanja, je najslabše ocenjena enota še vedno visoko nad srednjo vrednostjo 3 (tj. *Niti pomembno niti nepomembno*). Kar ponovno nakazuje, da sodelujoči v anketi niso imeli velikega razkoraka med znanji, ki so zanje pomembna in tistimi, ki niso. Alternativna razlaga bi bila, da je pomembnost vseh znanj enakomerna čez celoten trg dela, kar pa po našem mnenju ni realna predpostavka, zato

kot razlog za tako majhne razlike vidimo predvsem v nekritičnosti sodelujočih oz. odporu do tega, da bi katerokoli znanje označili kot manj pomembno. To mnenje potrjuje tudi modus (tj. najpogosteje izbrana ocena), ki je bil za 46 od 55 enot znanja (83,6 %) najboljša možna ocena 5 (tj. *Zelo pomembno*) in je bil v preostalih devetih primerih 4 (tj. *Pomembno*). Kot primer lahko podamo enoto *Kibernetsko pravo*, ki čeprav ni primarna domena tehničnega osebja in je pomembna za relativno majhno število profilov, ki delujejo na področju kibernetske varnosti ni bila s strani nobenega od sodelujočih ocenjena z nižjo oceno kot 3 (tj. *Niti pomembno niti nepomembno*).

Iz tabele 5 takoj opazimo prevlado vijoličastih enot (tj. *Varnost ljudi*) na vrhu seznama, ki v prejšnjih analizah skoraj ni bila zastopana v zgornji polovici seznama. Zanimivo so se v sam vrh umestila bolj t.i. mehka znanja, kot so *Upravljanje identitet*, *Osveščenost in razumevanje*, *Osebna skladnost s pravili*, ipd. Na splošno tudi izgleda, da so, predvsem v primerjavi z raziskavo pomembnosti v visokošolskih študijskih programih in certifikatih, bolj mehka znanja višje v seznamu in bolj tehnična znanja nižje. To je seveda posplošitev, ampak glede na to, da so anketirani posamezniki prihajali iz vseh vrst organizacij, ki se primarno ne ukvarjajo s kibernetsko varnostjo, je takšen rezultat bilo mogoče pričakovati.

V samem vrhu seznama je tudi veliko modrih enot znanja (tj. *Varnost podatkov*), vendar je nekaj enot iz tega področja uvrščenih veliko nižje v seznamu, kot so bila v prejšnjih raziskavah. Izstopajo predvsem *Kriptografija*, ki je bila v prejšnjih raziskavah izrazito pomembna enota znanja, vendar se je v tej anketi uvrstila šele na 47 mesto ter *Digitalna forenzika* in *Kriptoanaliza*, ki sta bili prejšnjič uvrščeni relativno visoko na seznamu, vendar sta zdaj povsem na koncu seznama. Občuten padec je doživela tudi *Obramba omrežij*, ki je v prejšnjih raziskavah zasedala prvo in drugo mesto, zdaj pa je šele na sedemnajstem.

Tabela 5: Pomembnost enot znanja glede na anketo trga, študijskih programov in certifikatov.

Ocena (Trg)	Enote znanja (Trg)	Enote znanja (Študij - ECTS)	Enote znanja (Certifikati)
4,82	Upravljanje identitet	Kriptografija	Obramba omrežij
4,82	Zasebnost in varnost osebnih podatkov	Obramba omrežij	Nadzor dostopa
4,80	Varnost shranjevanja informacij	Nadzor sistemov	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov
4,73	Varni komunikacijski protokoli	Celovitost in overjanje	Digitalna forenzika
4,73	Zasebnost podatkov	Analiza in testiranje	Upravljanje tveganj
4,71	Osveščenost in razumevanje	Kriptoanaliza	Nadzor sistemov
4,68	Celovitost in overjanje	Zasnova	Kriptografija
4,68	Nadzor dostopa	Kibernetsko pravo	Arhitektura omrežij
4,67	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	Upravljanje tveganj	Varni komunikacijski protokoli
4,66	Uporabna varnost in zasebnost	Kibernetski kriminal	Arhitektura porazdeljenih sistemov
4,65	Omrežne storitve	Arhitektura omrežij	Sistemski dostop

4,64	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	Varnostno upravljanje in politika	Upravljanje identitet
4,64	Varnostno upravljanje in politika	Kibernetska politika	Implementacija omrežij
4,64	Zasebnost	Sistemsko razmišljanje	Celovitost in overjanje
4,61	Nadzor sistemov	Nadzor dostopa	Kibernetsko pravo
4,60	Varnost osebja	Varni komunikacijski protokoli	Varnostno upravljanje in politika
4,59	Obramba omrežij	Temeljna načela	Kibernetski kriminal
4,59	Upravljanje sistemov	Digitalna forenzika	Analitična orodja
4,58	Upravljanje tveganj	Omrežne storitve	Varnost shranjevanja informacij
4,58	Upravljanje sistemov	Načrtovanje kibernetske varnosti	Upravljanje sistemov
4,55	Etika	Zasebnost podatkov	Upravljanje sistemov
4,55	Načrtovanje kibernetske varnosti	Osveščenost in razumevanje	Zasebnost
4,54	Socialni inženiring	Varnost shranjevanja informacij	Arhitektura strojne opreme
4,52	Sistemski dostop	Arhitektura strojne opreme	Varnost osebja
4,50	Temeljna načela	Kibernetska etika	Socialni inženiring
4,50	Kibernetska etika	Tipične arhitekture sistemov	Osveščenost in razumevanje
4,45	Zasnova	Arhitektura porazdeljenih sistemov	Zasebnost podatkov
4,45	Analiza in testiranje	Analitična orodja	Kibernetska politika
4,44	Implementacija	Implementacija	Kibernetska etika
4,44	Implementacija omrežij	Uporabna varnost in zasebnost	Kriptoanaliza
4,42	Testiranje sistemov	Upravljanje identitet	Omrežne storitve
4,40	Testiranje komponent	Implementacija omrežij	Načrtovanje kibernetske varnosti
4,40	Arhitektura omrežij	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	Upravljanje varnostnih programov
4,39	Dokumentiranje	Socialni inženiring	Zasnova komponent
4,39	Družbena in vedenjska zasebnost	Fizični vmesniki in priključki	Implementacija
4,36	Upravljanje varnostnih programov	Zasebnost in varnost osebnih podatkov	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti
4,35	Zasnova komponent	Upravljanje varnostnih programov	Temeljna načela
4,35	Sistemsko razmišljanje	Sistemski dostop	Zasebnost in varnost osebnih podatkov
4,35	Varnostne operacije	Zasnova komponent	Varnostne operacije
4,35	Kibernetski kriminal	Upravljanje sistemov	Analiza in testiranje

4,30	Analitična orodja	Zasebnost	Postavitev in vzdrževanje
4,29	Postavitev in vzdrževanje	Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	Testiranje komponent
4,28	Nabava komponent	Varnostne operacije	Sistemsko razmišljanje
4,27	Arhitektura porazdeljenih sistemov	Upravljanje sistemov	Testiranje sistemov
4,23	Kibernetska politika	Fizični mediji	Tipične arhitekture sistemov
4,17	Arhitektura strojne opreme	Testiranje komponent	Zasnova
4,14	Kriptografija	Družbena in vedenjska zasebnost	Dokumentiranje
4,14	Kibernetsko pravo	Postavitev in vzdrževanje	Etika
4,06	Obratni inženiring komponent	Obratni inženiring komponent	Nabava komponent
4,05	Fizični mediji	Testiranje sistemov	Obratni inženiring komponent
4,05	Fizični vmesniki in priključki	Varnost osebja	Fizični mediji
3,98	Tipične arhitekture sistemov	Etika	Fizični vmesniki in priključki
3,90	Digitalna forenzika	Dokumentiranje	Upokojevanje sistemov
3,81	Upokojevanje sistemov	Nabava komponent	Družbena in vedenjska zasebnost
3,63	Kriptoanaliza	Upokojevanje sistemov	Uporabna varnost in zasebnost

Poleg same pomembnosti enot znanja in kako se te primerjajo z analizo pomembnosti v visokem šolstvu in iskanimi certifikati na področju kibernetske varnosti smo želeli preveriti še, če se morda vidijo kašne razlike v ocenjevanju pomembnosti posameznih znanj glede na to, kakšen kader predstavlja ocenjevalec in glede na velikost organizacije, merjeno v številu zaposlenih. Ti rezultati so predstavljeni v tabeli 6. Organizacije smo kvalificirali kot majhne, če imajo 100 ali manj zaposlenih. Takšnih je bilo v anketi 18 (40 %).

V primerjavi med vodstvenim in IKT tehničnim kadrom lahko opazimo nekaj razlik. Vodstveni kader postavlja večjo težo znanjem iz področja *Organizacijske varnosti* (rdeča polja), medtem ko pri IKT tehničnemu kadru v vrhu seznama prednjačijo področja *Varnosti podatkov* (modra polja). Ta razlika je tudi v neki meri vezana na njihove delovne naloge – vodstveni kader se bolj ukvarja in osredotoča na organizacijo in upravljanje, medtem ko so tehnični kadri bolj osredotočeni na tehnologije in praktično varovanje. V obeh primerih kadrov so znanja iz področja *Varnosti ljudi* (vijoličasta barva) tudi v samem vrhu po pomembnosti. Poleg tega so pri vodstvenih kadrih znanja iz *Družbene varnosti* (turkizna barva) uvrščena višje v primerjavi s tehničnimi kadri, ki pa imajo višje uvrščene izbrane enote znanja iz *Varnosti povezav* (rumena polja) in *Varnosti programske opreme* (zelena polja).

Zelo podoben razkorak lahko vidimo tudi med manjšimi (100 ali manj zaposlenih) in večjimi (več kot 100 zaposlenih) organizacijami. Odgovori, ki smo jih prejeli od manjših podjetij, so bolj poudarili tehnična znanja, podobno kot prej IKT tehnični kader. Tako so bila višje v seznamu znanja iz področja *Varnosti podatkov* (modra polja), *Varnosti programske opreme* (zelena polja) in izbrane enote iz *Varnosti povezav* (rumena polja). Področje *Organizacijske varnosti* (rdeča polja) je tu zelo nizko v primerjavi s povprečnimi odgovori (tabela 5) in presenetljivo, čeprav ne tako nizko na seznamu, je tudi *Varnost ljudi* (vijolična polja). Pri podjetjih z več kot 100 zaposlenimi je

trend pomembnih znanja obraten in veliko bolj podoben tistemu, ki so ga podali vodstveni kadri. Prednjačijo predvsem znanja iz *Varnosti ljudi* (vijolična polja) in *Organizacijske varnosti* (rdeča polja), medtem ko so *Varnost podatkov* (modra polja), *Varnost programske opreme* (zelena polja) in *Varnost povezav* (rumena polja) uvrščena nižje od povprečja. Podoben razpored pomembnosti znanj in kompetenc, kot je razviden iz večjih organizacij, je očiten tudi v organizacijah z največjimi letnimi prihodki (kategorija več kot 40 milijonov evrov letno). Tega seznama nismo uvrstili v tabelo 6, ker smo v raziskavi zajeli samo 5 takšnih organizacij, vendar kot rečeno, je bila razporeditev pomembnosti znanj podobna kot v večjih organizacijah in razporedi vodstvenega kadra, vendar s še veliko bolj izrazitim poudarkom na znanjih iz področja *Organizacijske varnosti* (rdeča polja) in v manjši meri tudi iz *Družbene varnosti* (turkizna barva).

Pokazane podobnosti med kadrom in velikostjo organizacije (po številu zaposlenih ali prihodkih) niso rezultat slabe razporeditve sodelujočih - da bi v anketi sodelovali vodstveni kadri iz večjih organizacij in IKT tehnični kadri iz manjših podjetij (tako kot so se pokazale podobnosti med skupinami), saj je bila v anketi porazdelitev obeh tipov kadrov enaka v obeh velikostih organizacij, kot smo že pokazali v tabeli 1.

Tabela 6: Pomembnost enot znanja glede na profil anketiranca in velikost organizacije.

Vodstveni kader	IKT tehnični kader	Manj kot 100 zaposlenih	Več kot 100 zaposlenih
Upravljanje identitet	Nadzor dostopa	Varnost shranjevanja informacij	Zasebnost in varnost osebnih podatkov
Zasebnost in varnost osebnih podatkov	Zasebnost in varnost osebnih podatkov	Varni komunikacijski protokoli	Upravljanje identitet
Varnost shranjevanja informacij	Varnost shranjevanja informacij	Etika	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov
Varnostno upravljanje in politika	Varni komunikacijski protokoli	Nadzor dostopa	Socialni inženiring
Neprekinjenost, obnova po nesreči in obvladovanje incidentov	Osveščenost in razumevanje	Zasebnost in varnost osebnih podatkov	Osveščenost in razumevanje
Zasebnost	Omrežne storitve	Zasebnost podatkov	Varnostno upravljanje in politika
Načrtovanje kibernetske varnosti	Osebna skladnost s pravili/politiko/ etičnimi normami	Omrežne storitve	Uporabna varnost in zasebnost
Zasebnost podatkov	Upravljanje identitet	Upravljanje identitet	Varnost shranjevanja informacij
Uporabna varnost in zasebnost	Zasebnost podatkov	Celovitost in overjanje	Zasebnost podatkov
Upravljanje sistemov	Celovitost in overjanje	Temeljna načela	Osebna skladnost s pravili/politiko/etični mi normami kibernetske varnosti
Socialni inženiring	Obramba omrežij	Osveščenost in razumevanje	Varnost osebja
Nadzor sistemov	Temeljna načela	Zasebnost	Upravljanje sistemov

Upravljanje tveganj	Neprekinjenost, obnova po nesreči in obvladovanje incidentov	Obramba omrežij	Upravljanje tveganj
Kibernetska etika	Upravljanje sistemov	Zasnova	Sistemski dostop
Varni komunikacijski protokoli	Sistemski dostop	Dokumentiranje	Celovitost in overjanje
Osveščenost in razumevanje	Uporabna varnost in zasebnost	Nadzor sistemov	Načrtovanje kibernetske varnosti
Varnost osebja	Upravljanje sistemov	Implementacija	Varni komunikacijski protokoli
Upravljanje varnostnih programov	Nadzor sistemov	Uporabna varnost in zasebnost	Nadzor sistemov
Upravljanje sistemov	Varnost osebja	Arhitektura omrežij	Upravljanje sistemov
Celovitost in overjanje	Etika	Implementacija omrežij	Zasebnost
Nadzor dostopa	Varnostno upravljanje in politika	Upravljanje sistemov	Omrežne storitve
Etika	Upravljanje tveganj	Osebna skladnost s pravili/politiko/etični mi normami kibernetske varnosti	Nadzor dostopa
Omrežne storitve	Implementacija omrežij	Zasnova komponent	Obramba omrežij
Varnostne operacije	Socialni inženiring	Analiza in testiranje	Varnostne operacije
Implementacija omrežij	Testiranje komponent	Kibernetska etika	Kibernetska etika
Analitična orodja	Načrtovanje kibernetske varnosti	Arhitektura porazdeljenih sistemov	Družbena in vedenjska zasebnost
Sistemski dostop	Zasnova	Testiranje sistemov	Analiza in testiranje
Osebna skladnost s pravili/politiko/ etičnimi normami	Arhitektura omrežij	Varnostno upravljanje in politika	Upravljanje varnostnih programov
Zasnova	Testiranje sistemov	Upravljanje tveganj	Temeljna načela
Analiza in testiranje	Zasebnost	Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov	Implementacija omrežij
Kibernetski kriminal	Analiza in testiranje	Varnost osebja	Testiranje sistemov
Kibernetska politika	Implementacija	Testiranje komponent	Testiranje komponent
Obramba omrežij	Družbena in vedenjska zasebnost	Upravljanje sistemov	Analitična orodja
Implementacija	Sistemsko razmišljanje	Načrtovanje kibernetske varnosti	Implementacija
Arhitektura porazdeljenih sistemov	Dokumentiranje	Sistemsko razmišljanje	Kibernetski kriminal

Arhitektura omrežij	Kriptografija	Postavitev in vzdrževanje	Zasnova
Družbena in vedenjska zasebnost	Kibernetska etika	Kibernetski kriminal	Sistemsko razmišljanje
Temeljna načela	Nabava komponent	Obratni inženiring komponent	Etika
Dokumentiranje	Postavitev in vzdrževanje	Nabava komponent	Arhitektura omrežij
Sistemsko razmišljanje	Zasnova komponent	Kriptografija	Kibernetska politika
Testiranje sistemov	Fizični mediji	Sistemski dostop	Postavitev in vzdrževanje
Zasnova komponent	Digitalna forenzika	Družbena in vedenjska zasebnost	Nabava komponent
Testiranje komponent	Varnostne operacije	Upravljanje varnostnih programov	Zasnova komponent
Arhitektura strojne opreme	Analitična orodja	Kibernetsko pravo	Arhitektura strojne opreme
Postavitev in vzdrževanje	Kibernetski kriminal	Analitična orodja	Dokumentiranje
Kibernetsko pravo	Arhitektura porazdeljenih sistemov	Tipične arhitekture sistemov	Fizični mediji
Tipične arhitekture sistemov	Fizični vmesniki in priključki	Socialni inženiring	Arhitektura porazdeljenih sistemov
Nabava komponent	Arhitektura strojne opreme	Kibernetska politika	Fizični vmesniki in priključki
Fizični vmesniki in priključki	Upravljanje varnostnih programov	Varnostne operacije	Kibernetsko pravo
Obratni inženiring komponent	Kibernetska politika	Digitalna forenzika	Kriptografija
Fizični mediji	Kibernetsko pravo	Arhitektura strojne opreme	Tipične arhitekture sistemov
Kriptografija	Obratni inženiring komponent	Fizični vmesniki in priključki	Obratni inženiring komponent
Upokojevanje sistemov	Kriptoanaliza	Kriptoanaliza	Upokojevanje sistemov
Digitalna forenzika	Tipične arhitekture sistemov	Fizični mediji	Digitalna forenzika
Kriptoanaliza	Upokojevanje sistemov	Upokojevanje sistemov	Kriptoanaliza

3 Zaključek

V raziskavi smo pokazali, kako trg dela ocenjuje pomembnost posameznih znanj in kompetenc iz področja kibernetske varnosti. To smo storili z anketo, v kateri so sodelujoči iz gospodarstva in javnega sektorja podali svoja mnenja o pomembnosti izbranega nabora znanj in kompetenc.

Rezultati so pokazali, da ne obstaja enotna oz. usklajena lestvica, po kateri bi lahko določili pomembnost posameznih znanj. V tej raziskavi so se za trg dela pokazala kot najpomembnejša znanja iz področja varnosti ljudi in organizacijske varnosti, kar pa je v nasprotju s predhodnimi raziskavami, ki smo jih opravili na podlagi vsebin v visokošolskih študijskih programih in mednarodno priznanih certifikatih iz področja kibernetske varnosti. Na kratko bi lahko povzeli, da so bili rezultati iz visokošolskih programov bolj koncentrirani v temeljna znanja in kompetence, s poudarkom na področju varnosti podatkov, medtem ko so rezultati certifikatov nakazovali bolj praktično usmerjenost iz področja varnosti podatkov, ki je še vedno prevladovalo, vendar tudi z veliko večjo vlogo enot znanja organizacijske varnosti in varnosti povezave, usmerjenih v potrebe korporacij. Poleg teh razlik smo v tej raziskavi pokazali, da so velike razlike v pomembnosti posameznih znanj oz. kompetenc odvisne tudi od tega, kakšne vrste kader smo vprašali in iz kako velike organizacije so anketiranci prihajali. Zaključimo lahko, da ne obstaja lestvica pomembnosti znanj, ki bi bila primerna za vse potrebe. Ne glede na to pa lahko na podlagi znanj, ki so se izkazala kot ključna v izobraževalnih programih visokega šolstva, certificiranju in/ali iskanih profilih na trgu dela vzpostavimo nabor najpomembnejših znanj in kompetenc, ki bi koristile večini zaposlenih na področju kibernetske varnosti in bi jih v imenu celovitosti morali pokrivati tudi bodoči izobraževalni programi v Sloveniji.

Na podlagi analize pomembnosti znanj in kompetenc v visokošolskih izobraževalnih programih, mednarodno priznanih certifikatih in trga dela smatramo naslednjih 12 znanj in kompetenc kot splošno najbolj pomembnih na področju kibernetske varnosti (obarvane po področjih v katera spadajo – glej tabelo 4):

- Obramba omrežij
- Nadzor sistemov
- Celovitost in overjanje
- Nadzor dostopa
- Varni komunikacijski protokoli
- Upravljanje tveganj
- Varnostno upravljanje in politika
- Upravljanje identitet
- Varnost shranjevanja informacij
- Neprekinjenost poslovanja, obnova po nesreči in obvladovanje incidentov
- Kriptografija
- Zasebnost in varnost osebnih podatkov

4 Priloga: Anketni obrazec

Potreba po kompetencah s področja kibernetske varnosti

Vprašalnik

Potreba po kompetencah s področja kibernetske varnosti Spoštovani! Kot predstavnike gospodarstva ali javnega sektorja, vas vabimo k sodelovanju v raziskavi projekta RUKIV - Razvoj programov usposabljanj za kibernetsko varnost (ARRS-CRP-2021), ki se osredotoča na trenutne potrebe po znanjih in kompetencah na področju kibernetske varnosti. Cilj raziskave je pridobiti vpogled v potrebne kompetence in znanja na področju kibernetske varnosti v Sloveniji. Rezultati bodo uporabljeni pri razvoju formalnih in neformalnih izobraževanj/usposabljanj za kibernetsko varnost. Sodelovanje v raziskavi je anonimno, reševanje ankete vam bo vzelo približno 10 minut. Vnaprej se vam zahvaljujemo za sodelovanje!

Q1 - Najprej vas prosimo, da odgovorite na nekaj vprašanj o organizaciji, za katerega podajate odgovore.
_____

Q2 - Vaša organizacija je
◯ predstavnik gospodarstva
◯ predstavnik javnega sektorja

Q3 - V katerem sektorju deluje organizacija?
◯ Avdiovizualni in medijski sektor
◯ Kemijski sektor
◯ Obramba
◯ Digitalne storitve in platforme
◯ Energijski sektor
◯ Finančni sektor
◯ Gostinstvo
◯ Javni sektor
◯ Zdravstveni sektor
◯ Proizvodnja in oskrbovalna veriga
◯ Nuklearni sektor
◯ Varnost in varovanje
◯ Vesoljski sektor
◯ Telekomunikacijske infrastrukture
◯ Prevozni sektor
◯ Drugo:

Q4 - Okvirno število zaposlenih v organizaciji: _____

Q5 - Kolikšni so prihodki organizacije od prodaje?
◯ do 699.000€
◯ od 700.000€do 7.999.999€

◯ od 8.000.000€do 39.999.999€
◯ več kot 40.000.000€

Q6 - V kateri statistični regiji deluje organizacija?
◯ Pomurska
◯ Podravska
◯ Koroška
◯ Savinjska
◯ Posavska
◯ Zasavska
◯ Osrednjeslovenska
◯ Jugovzhodna Slovenija
◯ Primorsko-notranjska
◯ Gorenjska
◯ Goriška
◯ Obalno-Kraška

Q7 - Kakšna je vaša vloga v organizaciji?
◯ Vodstveni kader
◯ IKT tehnični kader
◯ Drugo

Q8 - Ali se pri vašem delu srečujete s kibernetsko varnostjo?
◯ DA
◯ NE

Q9 - Koliko strokovnjakov na področju kibernetske varnosti trenutno zaposlujete? _____

Q10 - Koliko strokovnjakov na področju kibernetske varnosti nameravate zaposliti v naslednjih petih letih (približno)? _____

Q11 - Ali imate težave s pridobivanjem kadra na področju kibernetske varnosti?
◯ Niti malo
◯ Malo
◯ Srednje
◯ Veliko
◯ Zelo veliko

Q12 - V kakšni obliki trenutno dodatno usposabljate kader na področju kibernetske varnosti?
Možnih je več odgovorov
☐ Certificiranje, tj. programi za pridobitev certifikatov (npr. CEH)
☐ Programi usposabljanj (npr. delavnice, seminarji)
☐ Izpopolnjevanja (1 leto)
☐ Mentorstvo
☐ Neformalno izobraževanje (npr. Coursera, Udemy, spletni tečaji)
☐ Formalno izobraževanje (npr. magistrski študijski programi)
☐ Drugo:

Q13 - V kakšni obliki bi v prihodnje želeli, da zaposleni pridobivajo dodatna znanja in kompetence na področju kibernetske varnosti?

Možnih je več odgovorov

- ☐ Certificiranje, tj. programi za pridobitev certifikatov (npr. CEH)
- ☐ Programi usposabljanj (npr. delavnice, seminarji)
- ☐ Izpopolnjevanja (1 leto)
- ☐ Mentorstvo
- ☐ Neformalno izobraževanje (npr. Coursera, Udemy, spletni tečaji)
- ☐ Formalno izobraževanje (npr. magistrski študijski programi)
- ☐ Drugo:

Q14 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju varnosti podatkov pri vaši dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VARNOST PODATKOV					
	Sploh ni pomembno	Ni pomembno	Niti pomembno niti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Kriptografija	◯	◯	◯	◯	◯	◯
Digitalna forenzika	◯	◯	◯	◯	◯	◯
Celovitost podatkov in overjanje	◯	◯	◯	◯	◯	◯
Nadzor dostopa	◯	◯	◯	◯	◯	◯
Varni komunikacijski protokoli	◯	◯	◯	◯	◯	◯
Kriptoanaliza	◯	◯	◯	◯	◯	◯
Zasebnost podatkov	◯	◯	◯	◯	◯	◯
Varnost shranjevanja informacij	◯	◯	◯	◯	◯	◯

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Kriptografija: Osnovni in napredni koncepti, zgodovinske šifre, simetrične šifre (zasebni ključ), asimetrične šifre (javni ključ).

- Digitalna forenzika: Pravna vprašanja, orodja za digitalno forenziko, preiskovalni postopek, pridobivanje in ohranjanje dokazov, analiza dokazov, predstavitev rezultatov, preverjanje pristnosti dokazov, poročanje, odzivanje na incidente in ravnanje z njimi, mobilna forenzika.

- Celovitost podatkov in preverjanje pristnosti: Moč avtentikacije, tehnike napadov na gesla, tehnike shranjevanja gesel, integriteta podatkov.

- Nadzor dostopa: Fizična varnost podatkov, logični nadzor dostopa do podatkov, varna zasnova arhitekture, tehnike preprečevanja uhajanja podatkov.

- Varni komunikacijski protokoli: Protokoli aplikacijske in transportne plasti, napadi na TLS, internetna/mrežna plast, protokoli za ohranjanje zasebnosti, plast podatkovnih povezav.

- Kriptoanaliza: Klasični napadi, napadi po stranskih kanalih, napadi na šifre s privatnim ključem, napadi na šifre z javnim ključem, algoritmi za reševanje problema diskretnega loga, napadi na RSA.

- Zasebnost podatkov: Zbiranje, združevanje in razširjanje podatkov ter družbeni mediji.

- Varnost shranjevanja informacij: Šifriranje diskov in datotek, brisanje podatkov, maskiranje podatkov, varnost podatkovnih baz, zakonodaja o varnosti podatkov.

Q15 - Prosimo, da ocenite pomembnost posameznih vidikov znanja s področja varnosti programske opreme pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VARNOST PROGRAMSKE OPREME					
	Sploh ni pomembno	Ni pomembno	Niti pomembno niti nepomembno	Pomembno	Zelo pomembno	Ne morem oceniti
Temeljna načela	○	○	○	○	○	○
Načrtovanje	○	○	○	○	○	○
Implementacija	○	○	○	○	○	○
Analiza in testiranje	○	○	○	○	○	○
Zagon in vzdrževanje	○	○	○	○	○	○
Dokumentacija	○	○	○	○	○	○
Etika	○	○	○	○	○	○

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Temeljna načela: Najmanjši privilegij, privzete varnostne nastavitve, zmanjšanje zaupanja, ekonomičnost mehanizma, zmanjšanje skupnih virov, preprostost, odprta zasnova, plastenje, abstrakcija, modularnost, popolno povezovanje, zasnova za iterativen razvoj.

- Načrtovanje: Izpeljava varnostnih zahtev, specifikacija varnostnih zahtev, življenjski cikel razvoja programske opreme, življenjski cikel razvoja varne programske opreme, programski jeziki.

- Implementacija: Potrjevanje in preverjanje vhodnih podatkov, pravilna uporaba vmesnikov API, uporaba varnostnih funkcij, preverjanje razmerij med časom in stanjem, upravljanje z izjemami in napakami, robustno programiranje, zapiranje struktur in modulov, upoštevanje okolja.

- Analiza in testiranje: Statična in dinamična analiza, testiranje enot, testiranje integracije, testiranje programske opreme.

- Zagon in vzdrževanje: Konfiguriranje, popravljanje in življenjski cikel ranljivosti, preverjanje okolja, DevOps, razgradnja/upokojitev.

- Dokumentacija: Namestitvena dokumentacija, uporabniški vodniki in priročniki, dokumentacija za zagotavljanje pravilnosti, varnostna dokumentacija.

- Etika: Etični, socialni in pravni vidiki razvoja programske opreme, razkritje ranljivosti, kaj, kdaj in zakaj testirati.

Q16 - Prosimo, da ocenite pomembnost posameznih vidikov znanja s področja varnosti komponent pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VARNOST KOMPONENT					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Oblikovanje komponent	◯	◯	◯	◯	◯	◯
Nabava komponent	◯	◯	◯	◯	◯	◯
Testiranje komponent	◯	◯	◯	◯	◯	◯
Povratni inženiring komponent	◯	◯	◯	◯	◯	◯

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Oblikovanje komponent: Načela varnosti komponent, varno načrtovanje komponent, identifikacija komponent, tehnike proti povratnemu inženiringu, preprečevanje napadov po stranskih kanalih, tehnologije proti nepooblaščenim posegom.

- Nabava komponent: Tveganja v dobavni verigi, varnost dobavne verige, preverjanje dobaviteljev.

- Testiranje komponent: Načela testiranja enot, varnostno testiranje.

- Povratni inženiring komponent: Povratni inženiring oblikovanja, povratni inženiring strojne opreme, povratni inženiring programske opreme.

Q17 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju varnosti povezave pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VARNOST POVEZAVE					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Fizični mediji	◯	◯	◯	◯	◯	◯
Fizični vmesniki in priključki	◯	◯	◯	◯	◯	◯
Arhitektura strojne opreme	◯	◯	◯	◯	◯	◯
Arhitektura porazdeljenih sistemov	◯	◯	◯	◯	◯	◯
Omrežna arhitektura	◯	◯	◯	◯	◯	◯
Implementacija omrežij	◯	◯	◯	◯	◯	◯
Omrežne storitve	◯	◯	◯	◯	◯	◯
Obramba omrežja	◯	◯	◯	◯	◯	◯

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Fizični mediji: Prenos v mediju, deljeni mediji in mediji od točke do točke, modeli za deljenje vsebin, običajne tehnologije.

- Fizični vmesniki in priključki: Značilnosti strojne opreme in materiali, standardi, običajni priključki.

- Arhitektura strojne opreme: Standardne arhitekture, standardi strojnih vmesnikov, običajne arhitekture.

- Arhitektura porazdeljenih sistemov: Splošni pojmi, svetovni splet, internet, protokoli in plastenje, visoko zmogljivo računalništvo (superračunalniki), hipervizorji in računalništvo v oblaku, ranljivosti in primeri ranljivosti.

- Omrežna arhitektura: Splošni koncepti, posredovanje, usmerjanje, preklapljanje, novi trendi.

- Implementacija omrežij: Omrežja IEEE 802/ISO, omrežja IETF in TCP/IP, praktična integracija in podporni protokoli, ranljivosti in primeri napadov.

- Omrežne storitve: Pojem storitve, modeli storitev (odjemalec-strežnik, vsak z vsakim), koncepti storitvenih protokolov (IPC, API, IDL), komunikacijske arhitekture (HTTP, SMTP ...), virtualizacija storitev, ranljivosti in primeri napadov.

- Obramba omrežja: Utrjevanje omrežja, implementacija IDS/IPS, implementacija požarnih zidov in VPN-jev, Honeypots, nadzor omrežja, analiza omrežnega prometa, zmanjševanje izpostavljenosti (površina in vektorji napada), nadzor dostopa do omrežja, DMZ, proxy strežniki, razvoj in izvajanje omrežne politike, omrežni napadi (npr. ugrabitev seje, man-in-the-middle), odkrivanje groženj in strojno učenje.

Q18 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju varovanja sistemov pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VAROVANJE SISTEMOV					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Sistemsko razmišljanje	○	○	○	○	○	○
Upravljanje sistema	○	○	○	○	○	○
Sistemski dostop	○	○	○	○	○	○
Nadzor sistema	○	○	○	○	○	○
Upokojitev sistema	○	○	○	○	○	○
Testiranje sistema	○	○	○	○	○	○
Pogoste sistemske arhitekture	○	○	○	○	○	○

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Sistemsko razmišljanje: Kaj je sistem, temeljna načela, celostni pristopi, varnost splošnih sistemov, varnost sistemov za posebne namene, modeli groženj, analiza zahtev, razvoj sistemov za testiranje.

- Upravljanje sistema: Modeli in sestava politik (pravilnikov), uporaba avtomatizacije, popravki in življenjski cikel ranljivosti, delovanje, ustavitev in uničenje, notranje grožnje, dokumentacija, sistemi in postopki.

- Sistemski dostop: Metode avtentikacije, identiteta.

- Nadzor sistema: Nadzor dostopa, avtorizacijski modeli, odkrivanje vdorov, napadi, obramba, revizija, zlonamerna programska oprema, modeli ranljivosti, penetracijsko testiranje, forenzika, obnova, odpornost.

- Upokojitev sistema: Razgradnja, odstranitev.

- Testiranje sistema: Potrjevanje zahtev, potrjevanje sestave komponent, testiranje enot v primerjavi s sistemskim testiranjem, formalno preverjanje sistemov.

- Pogoste sistemske arhitekture: Virtualni stroji, industrijski nadzorni sistemi, internet stvari (IoT), vgrajeni sistemi, mobilni sistemi, avtonomni sistemi, sistemi za splošne namene.

Q19 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju varnosti ljudi pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	VARNOST LJUDI					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Upravljanje identitet	○	○	○	○	○	○
Socialni inženiring	○	○	○	○	○	○
Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti	○	○	○	○	○	○
Ozaveščenost in razumevanje	○	○	○	○	○	○
Družbena in vedenjska zasebnost	○	○	○	○	○	○
Zasebnost in varnost osebnih podatkov	○	○	○	○	○	○
Uporabna varnost in zasebnost	○	○	○	○	○	○

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Upravljanje identitet: Identifikacija in overjanje oseb in naprav, nadzor fizičnih in logičnih sredstev, identiteta kot storitev (IaaS), overitvene storitve tretjih entitet, napadi na nadzor dostopa in ukrepi za njihovo preprečevanje.

- Socialni inženiring: Vrste napadov socialnega inženiringa, psihologija napadov socialnega inženiringa, zavajanje uporabnikov, odkrivanje in preprečevanje napadov socialnega inženiringa.

- Osebna skladnost s pravili/politiko/etičnimi normami kibernetske varnosti: Zloraba sistema in napačno vedenje uporabnikov, uveljavljanje in pravila vedenja, pravilno vedenje v negotovosti.

- Ozaveščenost in razumevanje: Zaznavanje tveganj in komunikacija, kibernetska higiena, izobraževanje uporabnikov o kibernetski varnosti, ozaveščenost o kibernetskih ranljivostih in nevarnostih.

- Družbena in vedenjska zasebnost: Družbene teorije zasebnosti, zasebnost in varnost družbenih medijev.

- Zasebnost in varnost osebnih podatkov: Občutljivi osebni podatki, sledenje osebam in digitalnim odtisom.

- Uporabna varnost in zasebnost: Uporabnost in uporabniška izkušnja, človeški varnostni dejavniki, zavedanje in razumevanje politike, politika zasebnosti, smernice za oblikovanje in posledice.

Q20 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju organizacijske varnosti pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	ORGANIZACIJSKA VARNOST					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Upravljanje tveganj	○	○	○	○	○	○
Varnostno upravljanje in politika	○	○	○	○	○	○
Analitična orodja	○	○	○	○	○	○
Upravljanje sistemov	○	○	○	○	○	○
Načrtovanje kibernetske varnosti	○	○	○	○	○	○
Neprekinjeno poslovanje, obnova po nesreči in obvladovanje incidentov	○	○	○	○	○	○
Upravljanje varnostnih programov	○	○	○	○	○	○
Varnost osebja	○	○	○	○	○	○
Varnostno delovanje	○	○	○	○	○	○

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Upravljanje tveganj: Identifikacija tveganj, ocena in analiza tveganja, notranje grožnje, modeli in metodologije merjenja in vrednotenja tveganj, nadzor tveganj.

- Varnostno upravljanje in politika: Organizacijski kontekst, zasebnost, zakonodaja, etika in skladnost, upravljanje varnosti, komuniciranje na izvršni ravni in ravni upravnega odbora, vodstvena politika.

- Analitična orodja: Merjenje učinkovitosti (metrike), podatkovna analitika, varnostno obveščanje.

- Upravljanje sistemov: Administracija operacijskega sistema, administracija sistema podatkovnih baz, administracija omrežja, administracija oblaka, administracija kibernetsko-fizičnega sistema, utrjevanje sistema, razpoložljivost.

- Načrtovanje kibernetske varnosti: Strateško načrtovanje, operativno in taktično upravljanje.

- Neprekinjeno poslovanje, obnovitev po nesreči in obvladovanje incidentov: Načrtovanje in posodabljanje odzivov na incidente, načrti okrevanja po katastrofi in načrti neprekinjenega poslovanja v primeru nesreče.

- Upravljanje varnostnih programov: Upravljanje projektov in organizacijskih virov, varnostne metrike, zagotavljanje in nadzor kakovosti.

-Varnost osebja: Varnostna ozaveščenost, usposabljanje in izobraževanje, varnostni postopki zaposlovanja, varnostni postopki, prenehanju delovnega razmerja, varnost tretjih enitet, zasebnost osebnih podatkov zaposlenih.

- Varnostno delovanje: Varnostna konvergenca, centri za globalne varnostne operacije.

Q21 - Prosimo, da ocenite pomembnost posameznih vidikov znanja na področju družbene varnosti pri vaših dejavnostih:

Dodatne pojasnitve posameznih vidikov se nahajajo spodaj.

	DRUŽBENA VARNOST					
	Sploh ni pomembno	Ni pomembno	Niti pomembnoniti nepomembno	Pomembno	Zelo pomembno	Ne moremoceniti
Kibernetski kriminal	○	○	○	○	○	○
Kibernetsko pravo	○	○	○	○	○	○
Kibernetska etika	○	○	○	○	○	○
Kibernetska politika	○	○	○	○	○	○
Zasebnost	○	○	○	○	○	○

Dodatne pojasnitve - V kolikor se vam vsaj en aspekt v dodatni pojasnitvi zdi pomemben, smatrajte pri podajanju odgovora kategorijo kot pomembno.

- Kibernetski kriminal: Oblike kibernetskega kriminala, kibernetski terorizem, preiskave kibernetskega kriminala, ekonomija kibernetskega kriminala.

- Kibernetsko pravo: Ustavni temelji kibernetskega prava, intelektualna lastnina, povezana s kibernetsko varnostjo, zakoni o zasebnosti, zakoni o varnosti podatkov, zakoni o računalniških vdorih, digitalni dokazi, digitalne pogodbe, večnacionalne konvencije (sporazumi), zakoni o čezmejni zasebnosti in varnosti podatkov, opredelitev etike, poklicna etika in kodeksi ravnanja, etika in pravičnost/raznovrstnost, etika in pravo, etika avtonomije/robota, etika in konflikt, etični hekerji, etični okvirji in normativne teorije.

- Kibernetska etika: Opredelitev etike, poklicna etika in kodeksi ravnanja, etično hekanje, etika in pravičnost/raznovrstnost, etika v pravu, avtonomija/etika robotov, etični okviri in normativne teorije

- Kibernetska politika: Mednarodna kibernetska politika, domača kibernetska politika, globalni vpliv, politika kibernetske varnosti in nacionalna varnost, nacionalne gospodarske posledice kibernetske varnosti.

- Zasebnost: Opredelitev zasebnosti, pravice do zasebnosti, varovanje zasebnosti, norme zasebnosti in stališča, kršitve zasebnosti, zasebnost v družbah.

Q22 - Bi nam želeli še kaj sporočiti, ste v vprašalniku kaj pogrešali? (npr. znanja in kompetence, ki niso zajete v anketi in so pomembne za vašo organizacijo)

_____