Naučite se prepoznati, preprečiti in odzvati se na sodobne kibernetske grožnje.

SRIP GoDigital

zit SeKV

CyberHub Slovenia

Akademija kibernetske varnosti

Brezplačna akademija kibernetske varnosti v obsegu 4 tečajev v izvedbi Fakultete za elektrotehniko, računalništvo in informatiko (UM FERI) in z možnostjo pridobitve mikrodokazila.

Trajanje : med 14. 10. 2024 in 22. 11. 2024

Sofinancira Evropska unija
Financira Evropska unija NextGenerationEU
Sofinancira program Evropske unije Erasmus+

Akademija kibernetske varnosti

Zakaj akademija kibernetske varnosti

V današnjem digitaliziranem svetu je kibernetska varnost postala ključnega pomena. V poslovnem svetu predstavlja kibernetska varnost strošek, ki je lahko upravičen le, če preprečuje še višje stroške, ki bi nastali brez teh vlaganj. Zaradi predpisnih zahtev, potencialne izgube ugleda organizacije in komercializacije napadov, je razmerje med stroški in koristjo kibernetske varnosti strmo narastlo v prid uporabe učinkovite zaščite in sodelovanja IKT strokovnjakov s področja kibernetske varnosti. Eurobarometer poroča, da 45 % podjetij navaja **težave pri iskanju osebja** z ustreznimi znanji kot enega glavnih izzivov s področja kibernetske varnosti.

Potrebe po strokovnjakih s kompetencami na področju kibernetske varnosti strmo naraščajo tako pri vseh organizacijah, kot tudi pri ponudnikih in proizvajalcih rešitev in storitev informacijske tehnologije. Vsak košček digitalnih rešitev in storitev mora biti načrtovan in narejen z mislijo na kibernetsko varnost. Izobraževalni sistem in trg dela ne sledita naraščajočim potrebam po kibernetski varnosti, zato je izrednega pomena čim prej nasloviti naraščajočo vrzel. EU in tudi države članice pripravljajo različne ukrepe in programe za vse življenjsko učenje, ki bodo zaposlenim omogočili tako posodabljanje znanja, kot tudi prekvalifikacije.

Fakulteta za elektrotehniko, računalništvo in informatiko, Univerze v Mariboru (UM FERI) sodeluje v projektu Razvoj prožnih učnih pristopov z mikrodokazili za digitalno in zeleno preobrazbo izobraževanja za prehod v Družbo 5.0 (RPUP), ki je med drugim namenjen razvoju Slovenskega okolja za uporabo mikrodokazil. **Mikrodokazilo** (ang. Micro-credential) pomeni zapis učnih izidov, ki jih je posameznik dosegel z učenjem manjšega obsega. Ta omogočajo posameznikom pridobivanje znanj, spretnosti in kompetenc, ki jih potrebujejo v razvijajočem se trgu dela in družbi. Takšne oblike izobraževanj močno podpira tudi EU in se intenzivno uvajajo v evropski izobraževalni prostor kot nova oblika dopolnjevanja znanja.

UM FERI, CyberHub Slovenija, SRIP GoDigital in Združenje za informatiko in telekomunikacije s Sekcijo za kibernetsko varnost vas vabimo da se udeležite **Akademije kibernetske varnosti**, ki je sestavljena iz štirih tečajev, s katerimi boste pridobili znanja in potencialno tudi mikrodokazila (ko bo v Sloveniji vzpostavljen sistem) iz izbranih področij kibernetske varnosti.

Ne zamudite te edinstvene priložnosti
Vabimo vas, da izkoristite to **priložnost** in se nam pridružite na izobraževanjih na katerih boste imeli priložnost razširiti svoje znanje in veščine iz kibernetske varnosti. Več o vsebini posameznih tečajev akademije si lahko preberete v nadaljevanju.

Vsebina akademije kibernetske varnosti

Izobraževanja, vključena v akademijo kibernetske varnosti, pokrivajo različna področja kibernetske varnosti. **Spletna varnost in vdorno testiranje** sta v veliki meri dve strani istega kovanca, kjer se ena stran ukvarja z oblikami varovanja, medtem ko druga izkorišča prisotne ranljivosti oz. pomanjkljivosti (predvidoma za namene izboljšanja varnosti). **Tehnologija veriženja blokov v kontekstu upravljanja** digitalnih identitet je v zadnjih nekaj letih dozorela do mere, da njena uporaba ni več samo najnovejša moda in je večji poudarek na njeni uporabnosti. Vsebina enega od tečajev bo podrobno predstavila decentralizirane tehnologije in s tem povezano področje digitalnih identitet. **Digitalna forenzika** ni znanost, s katero bi se srečevali pogosto, vendar predstavlja zanimivo in še kako potrebno področje kibernetske varnosti. Čeprav jo povezujemo s kriminalističnimi preiskavami, je njena najboljša lastnost pridobivanje po nesreči izbrisanih ali uničenih podatkov prav v vsaki organizaciji. **Upravljanje informacijske varnosti** je zahtevna in kompleksna naloga, ki jo morajo naslavljati vse (večje) organizacije. Izobraževanje bo predstavilo osnovne problematike in naslovilo pristope upravljanja za zagotovitev smiselnega varovanja zaupnosti, celovitosti in dostopnosti sredstev organizacije pred potencialnimi grožnjami.

Potek akademije kibernetske varnosti

Akademija je sestavljena iz štirih tečajev, od katerih vsak pokriva svoje področje. Predavanja iz vsebine tečajev potekajo v živo v Ljubljani (GZS), medtem ko se druge obveznosti (vaje, preverjanje znanja) večinoma opravljajo na daljavo. Vsak od štirih tečajev bo organiziran na podoben način:

- **predavanja**: 1 do 2 dni (odvisno od tečaja) in se izvajajo v živo;
- **vaje:** 1 dan in se izvajajo (odvisno od tečaja) v živo, na daljavo ali asinhrono (tj. video)
- **samostojno delo:** 2 do 4 dni (odvisno od tečaja), kjer imajo udeleženci čas opraviti obvezne vaje in se pripraviti na preverjanje znanja
- **preverjanje znanja:** na daljavo in vedno na zadnji dan tečaja.

Akademijo izvajamo v okviru projekta razvoja slovenskega okolja za uporabo mikrodokazil zato so vsi elementi učnega programa za udeležence obvezni.

Akademijo kibernetske varnosti sestavljajo 4 tečaji

Izobraževanja bodo potekala po naslednjem urniku:

TEČAJ 1: Spletna varnost in vdorno testiranje	**14. 10. 2024 do 23. 10. 2024**
TEČAJ 2: Identifikacija, overjanje in avtorizacija	**4. 11. 2024 do 8. 11. 2024**
TEČAJ 3: Digitalna forenzika	**11. 11. 2024 do 15. 11. 2024**
TEČAJ 4: Upravljanje informacijske varnosti	**18. 11. 2024 do 22. 11. 2024**

Pogoji udeležbe

- Udeležiti se je mogoče poljubnega nabora tečajev, vendar se v primeru prevelikega števila prijav daje prednost tistim, ki izberejo več izobraževanj.
- Za zagotovitev pogojev, ki so potrebni za kakovostno izvedbo tečajev, je število udeležencev omejeno na maksimalno 15.
- Potrebno predznanje je opredeljeno v okviru opisa tečajev.

Lokacija akademije kibernetske varnosti

Izobraževanja bodo potekala na GZS, Dimičeva 13, Ljubljana v dvorani F – medetaža.

Potrdilo o pridobljenem znanju

Udeleženci, ki bodo uspešno zaključili (udeležba na predavanjih, vaje, izpit) akademijo kibernetske varnosti, bodo za opravljene tečaje pridobili **kreditne točke** (ECTS) ter potrdilo Fakultete za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, o uspešnem zaključku posameznega kratkega izobraževanja. Omenjeno potrdilo bo možno pretvoriti v mikrodokazilo, ko bodo ta dokončno uveljavljena na ravni države oziroma EU.

Kotizacija

Izvedba kratkih izobraževanj, ki so vključena v akademijo kibernetske varnosti, potekajo v sklopu NOO projekta Razvoj prožnih učnih pristopov z mikrodokazili za digitalno in zeleno preobrazbo izobraževanja za prehod v Družbo 5.0 in je brezplačna. Akademijo kibernetske varnosti bomo predvidoma ponovno izvedli v 2025. Če vas zanima udeležba, prosimo pošljite interes na mateja.baebler@gzs.si.

Rok za prijavo je 15. 09. 2024.

Neudeležbo na posameznem tečaju bomo zaračunali s 150 € + DDV.

TEČAJ 1: Spletna varnost in vdorno testiranje

Predavatelj: izr. prof. dr. Muhamed Turkanović (UM FERI), izr. prof. dr. Marko Hölbl (UM FERI) in Milan Gabor (Viris)
Datum: 14. 10. 2024 do 23. 10. 2024
Kreditne točke: 2 ECTS

Kratek opis:
V okviru tečaja bodo udeleženci spoznali področje spletne varnosti in vdornega (penetracijskega) testiranja.
Predstavljena bodo načela etičnega hekanja ter s tem povezane faze etičnega hekanja, procesi, orodja in ogrodja za izvedbo le tega. Fokus bo vdorno testiranje povezano s spletnimi aplikacijami, pri čemer pa bo predstavljeno tudi izvidništvo, skeniranje omrežja, sistemsko vdiranje, itn.

V drugem delu bodo predstavljena načela spletne varnosti z vidika odjemalca, strežnika in komunikacijske povezave. Kot eden ključnih vidikov spletne varnosti bo obravnavan spletni varnostni model in njegovi gradniki (SOP, CSP, SRI, CORS), ki zagotavlja varnost na strani odjemalca. Prav tako bo predstavljen strežniški del spletne varnosti preko seznama najbolj pogostih ranljivosti (OWASP Top 10). Pri tem bodo obravnavane omenjene ranljivosti in kako se pred njimi zaščititi. Del tečaja bo tudi namenjen mehanizmom varovanja komunikacijske povezave med strežnikom in odjemalcev, kar je mogoče s pomočjo varnostnega protokola HTTPS in ustreznega upravljanja sej.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili/nadgradili znanja s področja celovite spletne varnosti in vdornega testiranja, ki predstavljata dopolnjujoči se temi kibernetske varnosti.

Želena predznanja in oprema:.
- Priporočljivo osnovno poznavanje tehnologij, ki jih bomo uporabljali: HTML, CSS, JavaScript, SQL ipd
- Osnovno znanje računalniških omrežij
- Osnovno znanje programiranja
- Na dan vaj bodo udeleženci potrebovali tudi lastne prenosnike

Po zaključku izobraževanja bo udeleženec sposoben:
- razumeti mehanizme, metode in protokole za zaščito spletih aplikacij, spletni varnosti model in varovanje komunikacijske povezave
- razumeti tipično spletno infrastrukturo in načine napadov
- opisati faze etičnega hekanja
- opisati etične in pravne posledice etičnega hekanja
- načrtovati vdorni test
- opisati orodja namenjenega vdornemu testiranju in njihove glavne zmogljivosti

Urnik izobraževanja

Dan	Vsebina	Datum	Predviden obseg	Lokacija	Predavatelj
1. dan	Predavanja	14. 10. 2024	6 šolskih ur	GZS	izr. prof. dr. Muhamed Turkanović (UM FERI), in Milan Gabor (Viris)
2. dan	Predavanja	15. 10. 2024	6 šolskih ur	GZS	izr. prof. dr. Marko Hölbl (UM FERI)
3. dan	Vaje	16. 10. 2024	8 šolskih ur	GZS	dr. Viktor Taneski (UM FERI)
4. –7. dan	Samostojno delo	17. – 22. 10. 2024		/	
8. dan	Izvedba pisnega preverjanja znanja	23. 10. 2024	2 šolski uri	Na daljavo	

TEČAJ 2: Identifikacija, overjanje in avtorizacija

Predavatelj: izr. prof. dr. Muhamed Turkanović (UM FERI)
Datum: 4. 11. 2024 do 8. 11. 2024
Kreditne točke: 1 ECTS

Kratek opis:
Izobraževanje bo zajemalo osrednje koncepte identifikacije, overjanja in avtorizacije (ang. Identification, authentication and authorization – IAA), pri čemer bomo začeli z uvodom v IAA, ključnimi koncepti in terminologijo. Raziskali bomo modele digitalnih identitet, vključno s silosnimi, centraliziranimi, federativnimi in decentraliziranimi pristopi, ter primere uporabe posameznih modelov. Nadaljevali bomo z metodami identifikacije in overjanja, kot so gesla, PIN kode, žetoni, pametne kartice, biometrija, ter overjanje na nivoju mobilnih in spletnih rešitev.
V okviru infrastrukture bomo pokrili infrastrukturo javnih ključev, X.509 certifikate, kvalificirana in nekvalificirana digitalna potrdila ter ponudnike digitalnih identitet, kot so federativno poslovni ali Google in Microsoft. V implementaciji overjanja bomo raziskali protokole in standarde, kot so OAuth2.0, OpenID Connect in SAML, ter upravljanje sej s pomočjo JWT žetonov. Poudarek bo tudi na več faktorskem overjanju z uporabo WebAuthn in FIDO2/U2F. Avtorizacijo in nadzor dostopa bomo obravnavali skozi ogrodja RBAC in ABAC ter implementacijo v sodobnih IT arhitekturah, vključno z mikrostoritvami in spletnimi storitvami. V zadnjem delu izobraževanja se bomo posvetili praktičnim aplikacijam in prihajajočim tehnologijam, kot so decentralizirane in samo-upravljane identitete, podprte z verigami blokov, ter digitalne denarnice in uredbe, kot je eIDAS 2.0.

To izobraževanje bo udeležencem omogočilo celovit vpogled v identifikacijo, overjanje in avtorizacijo, ter jih opremilo s praktičnimi znanji za učinkovito upravljanje digitalnih identitet in izboljšanje kibernetske varnosti.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili/nadgradili znanja za potrebe »full stack« razvijalca spletnih aplikacij, kjer bodo razvili zaledne komponente interaktivne spletne aplikacije na poljubno izbrani problemski domeni.

Želena predznanja:
- Osnovno razumevanje tehnologij svetovnega spleta (npr. HTTP, HTML, CSS)
- Poznavanje sistemov za nadzor verzij (npr. git) in platform (npr. GitHub)
- Poznavanje vsaj enega objektno usmerjenega programskega jezika (priporočljivo JavaScript)
- Osnovno poznavanje okolij/orodij, ki jih bomo uporabljali: Node.js, MongoDB, Docker, Visual Studio Code

Po zaključku izobraževanja bo udeleženec sposoben:
- razumeti koncepte digitalne identitete, overjanja in avtorizacije
- razpravljati o prednostih in slabostih različnih metod overjanja
- razumeti, kako izbrati najprimernejšo metodo overjanja,
- opisati in primerno uporabiti tehnologije za upravljanje identitet ter zagotavljanje overjanja
- izvajati in upravljati varno overjanje z uporabo protokolov in standardov, kot so OAuth2.0, OpenID Connect, SAML, ter upravljati seje s pomočjo JWT žetonov

Urnik izobraževanja

Dan	Vsebina	Datum	Predviden obseg	Lokacija	Predavatelj
1. dan	Predavanja	4. 11. 2024	8 šolskih ur	GZS	izr. prof. dr. Muhamed Turkanović (UM FERI)
2. dan	Vaje	5. 11. 2024	6 šolski uri	Na daljavo	Asistenti Vid Keršič, dr. Viktor Taneski (UM FERI)
3. in 4. dan	Samostojno delo	6. – 7. 11. 2024		/	
5. dan	Izvedba pisnega preverjanja znanja	8. 11. 2024	1 šolska ura	Na daljavo	

TEČAJ 3: Digitalna forenzika

Predavatelj: izr. prof. dr. Marko Hölbl
Datum: 11. 11. 2024 do 15. 11. 2024
Kreditne točke: 1 ECTS

Kratek opis:
Obravnavali bomo pojem in načela digitalne forenzike ter predstavili postopek forenzične analize. Pogledali si bomo metodologijo preiskave in s tem povezan pojem skrbniške verige, postopek zbiranja digitalnih dokazov ter poročanje in dokumentacijo, ki sta pomemben sestavni del digitalne forenzike. Obravnavali bomo tudi orodja in tehnike, ki se uporabljajo v postopku, kot so forenzično ustrezen zajem podatkov, časovni podatki in obnovitev izbrisanih podatkov. Prav tako bomo na kratko podali povezano tehnično ozadje, kot so datotečni sistemi in specifične pomnilniške naprave. Za zaključek bomo digitalno forenziko pogledali skozi prizmo različnih okolij, ki vključujejo forenziko brskalnikov, omrežij in elektronske pošte.

Izobraževanje je namenjeno posameznikom, ki bi radi pridobili znanja o digitalni forenzika, njenem tehničnem ozadju in uporabi.

Želena predznanja:
- Osnovno poznavanje informacijske varnosti
- Osnovno poznavanje računalniških sistemov (npr. operacijski sistemi)
- Osnovno poznavanje računalniških omrežij;
- Osnovno poznavanje programiranja

Po zaključku izobraževanja bo udeleženec sposoben:
- opisati postopek zbiranja digitalnih dokazov in njihovo analizo
- aplicirati načela zbiranja dokazov
- uporabiti orodja in tehnike za analizo digitalnih dokazov
- prepoznati in ovrednotiti ključne tehnike forenzične analize
- kritično ovrednotiti forenzične dokaze

Urnik izobraževanja

Dan	Vsebina	Datum	Predviden obseg	Lokacija	Predavatelj
1. dan	Predavanja	11. 11. 2024	6 šolskih ur	GZS	izr. prof. dr. Marko Hölbl (UM FERI)
2. dan	Vaje – asinhrone vsebine (video s predstavitvijo orodja in naloge)	12. 11. 2024	4 šolske ure	Na daljavo	doc. dr. Marko Kompara (UM FERI)
3. in 4. dan	Samostojno delo	13. – 14. 11. 2024		/	
5. dan	Izvedba pisnega preverjanja znanja	15. 11. 2024	1 šolska ura	Na daljavo	izr. prof. dr. Marko Hölbl (UM FERI)

TEČAJ 4: Upravljanje informacijske varnosti

Predavatelj: doc. dr. Lili Nemec Zlatolas in doc. dr. Marko Kompara
Datum: 18. 11. 2024 do 22. 11. 2024
Kreditne točke: 1 ECTS

Kratek opis:
Tečaj upravljanja informacijske varnosti je osnovan na podlagi in vključuje vsebine, potrebne za ISACA certifikat CISM (Certified Information Security Manager). V skladu s tem je tudi tečaj razdeljen na štiri področja:

- Vodenje informacijske varnosti: organizacijska kultura, strukture, vloge in odgovornosti, strategija informacijske varnosti, ogrodja in standardi upravljanja informacij, metode pregleda informacijske varnosti…
- Upravljanje tveganj informacijske varnosti: ogrodja za obvladovanje/upravljanje tveganj, ocena, vrednotenje tveganj, odziv na informacijska tveganja, spremljanje, poročanje in sporočanje o tveganjih…
- Program informacijske varnosti: razvoj programa informacijske varnosti in sredstva/viri, standardi in ogrodja IV, metrike programa, varnostne kontrole…
- Upravljanje incidentov: upravljanje incidentov in načrti odzivanja nanje, obvladovanje incidentov, obveščanje, odpravljanje, obnova in pregled incidenta, vpliv na poslovanje in neprekinjeno delovanje, načrtovanje obnovitve po nesreči…

Izobraževanje je namenjeno posameznikom, ki bi se radi naučili ali nadgradili znanja o upravljanju informacijske varnosti. Posebej je primerno za tiste, ki delujejo ali bi želeli delati na delovnih mestih, ki usmerjajo informacijsko varnost v podjetjih (vodja informacijske varnosti, vodja informatike, CISO ipd.). Izobraževanje je tudi dobra začetna točka za tiste, ki razmišljajo o certificiranju CISM.

Želena predznanja:

- Osnovno poznavanje konceptov informacijske varnosti

Po zaključku izobraževanja bo udeleženec sposoben:

- prepoznati standarde, ogrodja in zahteve za upravljanje informacijske varnosti
- razpravljati o prednostih in pomanjkljivostih skladnosti z varnostnimi zahtevami
- oblikovati strateški varnostni načrt in varnostno politiko
- razumeti običajna tveganja in kontrole na področju informacijske varnosti
- razumeti kompleksnost upravljanja ljudi, procesov in tehnologije za doseganje informacijske varnosti
- prepoznati osnovne ekonomske zahteve in zahteve po virih, ki so potrebni za doseganje ciljev organizacije na področju informacijske varnosti

Urnik izobraževanja

Dan	Vsebina	Datum	Predviden obseg	Lokacija	Predavatelj
1. dan	Predavanja	18. 11. 2024	6 šolskih ur	GZS	doc. dr. Lili Nemec Zlatolas (UM FERI), doc. dr. Marko Kompara (UM FERI)
2. dan	Predavanja in vaje	19. 11. 2024	4 šolske ure	Na daljavo	doc. dr. Lili Nemec Zlatolas (UM FERI)
3. in 4. dan	Samostojno delo	20. – 21. 11 2024		/	
5. dan	Izvedba pisnega preverjanja znanja	22. 11. 2024	1 šolska ura	Na daljavo	doc. dr. Lili Nemec Zlatolas (UM FERI)

O projektu RPUP

Projekt *Razvoj prožnih učnih pristopov z mikrodokazili za digitalno in zeleno preobrazbo izobraževanja za prehod v Družbo 5.0*, oziroma na kratko RPUP je financiran v okviru Načrta za okrevanje in odpornost (NOO), ki je namenjen pridobivanju znanj in veščin, potrebnih za spodbujanje trajnostnega razvoja, med drugim tudi z vključevanjem okolijskih in podnebnih vprašanj v visokošolsko izobraževanje, ki ob hkratni uporabi digitalnih tehnologij kot dodatnih omogočevalcev zelenega prehoda pospešuje trajnostno ravnanje pri razvoju in uporabi digitalnih rešitev.

Projekt RPUP primarno naslavlja področja STE(A)M, ki je izkazano kot prioritetno področje Evropske unije in Slovenije. Osredotočajo se na področja elektrotehnike, računalništva in informatike, telekomunikacij, podatkovne znanosti, kibernetske varnosti, ter visokozmogljivega in visokopropustnega računalništva. Navedena področja so ključna za doseganje digitalne in ter zelene preobrazbe ob prehodu v Družbo 5.0.

Osrednji cilj projekta je približati osnovna in aktualna ekspertna tehnična znanja znotraj in zunaj izobraževalnega sistema ter ponuditi izobraževanja v oblikah, ki bodo omogočale različne fleksibilne poti za pridobitev mikrodokazil. To vključuje možnosti prilagajanja vsebin in struktur posameznih učnih enot in izobraževanj za pridobivanje mikrodokazil identificiranim ciljnim skupinam, različnim ravnem znanja in nasloviti izziv neenake zastopanosti spolov, ter s tem omogočiti učinkovitejši, sodobnejši in kakovostnejši prenos znanja. Osrednja teza, ki jo želimo v sklopu projekta nasloviti, je da lahko v visokošolski izobraževalni prostor, kot je FERI in UM, vpeljemo nove pristope (npr. krajša izobraževanja za pridobitev mikrodokazila, asinhrona izvedba itn.), ki bodo deležnikom, ki primarno niso redni študenti, omogočili pridobivanje potrebnih znanj in kompetenc, s katerimi bodo lahko aktivno prispevali k digitalnemu in zelenemu prehodu. Več informacij o NOO projektih na univerzi, o projektu RPUP in izobraževanjih iz drugih področij, ki nastajajo v okviru projekta lahko najdete na naslednjih povezavah:

- Pilotni projekti NOO
- Projekt RPUP
- Krajša izobraževanja UM FERI

O SRIP GoDigital

Strateško razvojno inovacijsko partnerstvo SRIP GoDigital predstavlja nov razvojni korak za krepitev IKT panoge in možnost boljše podpore ZIT članom na področju razvoja inovativnih digitalnih storitev in produktov. Naše poslanstvo je osredotočenje raziskovalnih in inovacijskih kapacitet ter vlaganj za razvoj in trženje zahtevnejših, celovitih in integriranih digitalinih storitev in izdelkov/rešitev v dialogu s člani in oblikovalci politik. Ena od ključnih aktivnosti je krepitev naprednih kompetenc IKT strokovnjakov in razvoj sistema vse življenjskega učenja in mikrodokazil s ciljem ustrezno opremiti že zaposlene v slovenskem gospodarstvu z novimi znanji in veščinami. Mikrodokazila bodo omogočila fleksibilno in ciljno usmerjeno pridobivanje kompetenc, kar bo pripomoglo k večji prilagodljivosti in konkurenčnosti delovne sile.

O Sekciji za kibernetsko varnost pri združenju za informatiko in telekomunikacije

V okviru Združenja za informatiko in telekomunikacije pri GZS deluje Sekcija za kibernetsko varnost (SeKV), ki se osredotoča na združevanje in usklajevanje interesov uporabnikov in ponudnikov kibernetskih varnostnih rešitev. Poslanstvo SeKV je z aktivnim sodelovanjem z vsemi deležniki kibernetske varnosti spodbuditi razvoj kibernetskih zmogljivosti slovenskih podjetij ponudnikov in uporabnikov storitev ter prispevati k celostnem razvoju kibernetske varnosti v RS.

O CyberHub Slovenija

V okviru projekta CyberHub nastaja slovensko stičišče za krepitev kompetenc na področju kibernetske varnosti. Zasnovano je kot strateška platforma za povezovanje strokovnjakov s področja kibernetske varnosti, strokovnih združenj in pobud, ponudnikov rešitev in storitev na področju kibernetske varnosti, predstavnikov uporabnikov rešitev, institucij znanja ter oblikovalcev politik. V okviru projekta se bo izvedla analiza stanja in potreb po strokovnjakih na področju kibernetske varnosti ter njihovih veščinah in kompetencah. Med ostalim bomo na podlagi teh analiz v okviru stičišča oblikovali tudi projektno nacionalno strategijo za izboljšanje stanja kibernetske varnosti v Sloveniji ter organizirali različne aktivnosti za ozaveščanje.