



Povzetek projekta Po kreativni poti do znanja 2016/2017 za namen objave in predstavitve na spletni strani sklada

1. Polni naslov projekta: IVKZ: Sistem za upravljanje informacijsko-varnostnih kompetenc zaposlenih

- **V katero področje na prvi klasifikacijski ravni KLASIUS-P se uvršča projekt glede na vsebinsko zasnovo** (neustrezno področje izbrišite):

4 - Naravoslovje, matematika in računalništvo

2. V sodelovanju z: (navede se univerza oz. samostojni visokošolski zavod, ki je prijavil projekt in članica, ki je nosilka projekta ter partnerja – podjetja, ki je/sta vključena v projekt)

Univerza v Mariboru Fakulteta za varnostne vede

KOPA računalniški inženiring

3. Besedilo:

- **Opredelite problem, ki se je razreševal tekom izvajanja projekta**

Informacijska varnost postaja vse bolj aktualna tema v dobi, ko so podjetja vedno bolj odvisna od informacijske tehnologije. Za doseganje ustrezne informacijske varnosti so potrebne tako tehnične kot tudi organizacijske rešitve. Kljub temu, da je na trgu na voljo vedno več naprednih tehničnih rešitev za obvladovanje informacijsko-varnostnih tveganj, pa ostajajo šibke točke podjetij predvsem njihovi zaposleni. Namen projekta je bil vzpostavitev sistema za upravljanje informacijsko-varnostnih kompetenc zaposlenih.

Namen projekta je bil najprej nasloviti problem pridobivanja in vzdrževanja pregleda nad dejansko informacijsko-varnostno usposobljenostjo zaposlenih. Ta namen je projekt dosegel z opredelitvijo ključnih informacijsko-varnostnih kompetenc zaposlenih, orodji za njihovo ocenjevanje in ukrepi za njihovo izboljševanje. Na ta način imajo snovalci informacijsko-varnostnega usposabljanja teoretično in praktično oporo, tj. bazo znanja, ki jim omogoča učinkovito planiranje usposabljanja. Poleg tega je bil namen projekta tudi integracija te baze znanja v programsko rešitev v obliki prototipa. Prototip nudi informacijsko podporo snovalcem informacijsko-varnostnega usposabljanja, saj jim omogoča obvladljivo spremljanje tudi v večjih organizacijah, v katerih bi bilo to brez informacijske podpore nemogoče.

- **Opišite potek reševanja problema oz. kratek povzetek projekta**

V okviru projekta je bil najprej narejen pregled relevantnih informacijsko-varnostnih kompetenc, ki omogočajo učinkovito spremljanje kompetenc zaposlenih in načrtovanje njihovega usposabljanja. Za vsako ključno kompetenco so bila pripravljena vzorčna orodja za njihovo ocenjevanje. Za vsako ključno informacijsko-varnostno kompetenco so bili pripravljene tudi vzorčni ukrepi za njihovo izboljšavo, ki omogočajo planiranje izboljševanja informacijsko-varnostnih kompetenc zaposlenih. Na koncu je bil v sodelovanju z Oddelkom za sistemsko integracijo izdelan prototip sistema za upravljanje informacijsko-varnostnih kompetenc zaposlenih, ki omogoča vizualizacijo informacijsko-varnostnih kompetenc v podjetju.

- **Navedite in opišite rezultate projekta ter njihov doprinos k družbeni koristnosti**

Rezultat R1: Seznam ključnih informacijsko-varnostnih kompetenc zaposlenih
Opis ključnih kompetenc in ocena njihove pomembnosti za zagotavljanje informacijske varnosti v podjetju.

Rezultat R2: Nabor vzorčnih orodij za preverjanje oz. oceno ključnih informacijsko-varnostnih kompetenc zaposlenih

Orodja so v različnih oblikah (npr. test, samoocena, klasični vprašalnik), odvisno od specifik posameznih informacijsko-varnostnih kompetenc.

Rezultat R3: Seznam vzorčnih ukrepov za izboljšanje ključnih informacijsko-varnostnih kompetenc zaposlenih

Ukrepi so različne oblike usposabljanja, ki so odvisne od specifik posameznih informacijsko-varnostnih kompetenc.

Rezultat R4: Prototip za vizualizacijo informacijsko-varnostnih kompetenc in njihovih ocen v podjetju
Glavni rezultat projekta je prototip za vizualizacijo informacijsko-varnostnih kompetenc in njihovih ocen v podjetju. Prototip deluje na Kopini HRM platformi.

Neposrednega doprinosa k družbenemu napredku je relativno malo, saj lahko šele z uporabo rezultatov projekta v praksi vplivamo nanj. Rezultati projekta so dovolj dobri za prikaz delovanja sistema za upravljanje informacijsko-varnostnih kompetenc zaposlenih v organizacijah, niso pa še dovolj dobri za dejansko uporabo. To bi namreč zahtevalo bistveno večji časovni vložek. Posreden doprinos rezultatov projekta se pričakuje preko nadgradnje rezultatov projekta iz stani Kope, ki namerava to področje razvijati naprej. S tem, ko bodo svoje produkte ponudili svojim strankam, bodo stranke dobile možnost izboljšave svoje informacijske varnosti, kar pripomore k varnejšem enotnem digitalnem poslovnem okolju (angl. *Single Digital Market*). Tudi ostala podjetja in organizacije, ki bodo dostopala do rezultatov projekta, imajo enako priložnost za prispevek k družbenemu razvoju in napredku.

Doprinos rezultatov projekta k trajnosti rezultatov je v tem, da so rezultati projekta trajni. Predvsem prenos znanj visokošolskih učiteljev je pomembno prispeval k trajnosti rezultatov, saj so na Kopi pokazali kar nekaj zanimanja za nadaljnjo izmenjavo znanj tudi po zaključku projekta, kar potrjuje sklenjen sporazum o sodelovanju. Prenos znanj strokovnjakov iz gospodarstva je imel bistveno manjši učinek, saj so bila ciljna publika študenti, namen pa je bil povsem drugačen kot zagotavljati trajnost rezultatov projekta.

4. Priloge:

- Slikovno gradivo: Priložite vsaj dve sliki npr. sliko končnega produkta, sliko študentov pri delu na projektu, sliko s sestankov ipd. Pri pošiljanju slik bodite pozorni, v kolikor gre za končni produkt, da bo zadoščeno zahtevam glede informiranja in obveščanja (ustrezni logotipi itd.).

Priložene slike so del rezultata R4, ki je z ustreznimi logotipi objavljen na portalu študentskih projektov FVV:

https://psivim.fvv.um.si/moodle/pluginfile.php/118/mod_resource/content/2/R4%20Prototip%20za%20vizualizacijo%20informacijsko-varnostnih%20kompetenc%20in%20njihovih%20ocen%20v%20podjetju.pdf



znam profilov

ajdi

• **VARNOSTNE KOMPETENCE**

Prijava na razpis

Kompetence

Prijavljene osebe



▼ VARNOSTNE KOMPETENCE

▼ Razumevanje

Razumevanje zakaj je varovanje informacij pomembno

Razumevanje informacijsko varnostnih trendov

Poznavanje vlog v verigi zagotavljanja informacijske varnosti

Poznavanje tveganj, ki izhajajo iz dobavne verige, procesov upravljanja in praks

Odločanje o informacijsko-varnostnih prioritetah

Razumevanje varnosti gesel

Razumevanje politike čiste mize

▼ Prepoznavanje

Notranje nevarnosti

Zunanje grožnje

Poznavanje principov zasebnosti

Prepoznavanje varnostnih incidentov

Oblikovanje, uporaba in upravljanje varnih gesel

Identifikacija spletnih groženj

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Utež

Razumevanje	Prepoznavanje	Obnašanje	Tehnologija	Zavedanje
Razumevanje zakaj je varovanje informacij pomembno	Notranje nevarnosti	Nepoznani pošiljatelji elektronske pošte in pripanke	Kontrola dostopa	Privlačne tarče
Razumevanje informacijsko varnostnih trendov	Zunanje grožnje	Varno brskanje po spletu	Razumevanje brezžičnih omrežij in njihove varnosti	Varovanje in delo s podatki
Poznavanje vlog v verigi zagotavljanja informacijske varnosti	Poznavanje principov zasebnosti	Gledanje čez ramo	Varne prakse za delo z elektronsko pošto	Razumevanje organizacijske varnostne politike
Poznavanje tveganj, ki izhajajo iz dobavne verige, procesov upravljanja in praks	Prepoznavanje varnostnih incidentov	Brskanje po smeteh	Namestitvev in uporaba protivirusnih programov	Organizacijska intelektualna lastnina
Odločanje o informacijsko-varnostnih prioritetah	Oblikovanje, uporaba in upravljanje varnih gesel	Odzivanje na zaznane grožnje	Varnost mobilnih naprav vključno z BYOD	Preprečevanje napadov socialnega inženiringa
Razumevanje varnosti gesel	Identifikacija spletnih groženj	Sprejemanje etičnih odločitev	Varnost organizacijske IKT izven delovnega mesta	Varna raba socialnih omrežij
Razumevanje politike čiste mize		Pravilna raba informacijsko-varnostnih orodij in naprav	Varne prakse za oddaljeno delo	