Javni štipendijski, razvojni, invalidski in preživninski sklad Republike Slovenije

EVROPSKA UNIJA
EVROPSKI SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE, ZNANOST IN ŠPORT

Univerza v Mariboru
Fakulteta za varnostne vede

KOPA

Po kreativni poti do znanja 2016/2017

IVKZ: Sistem za upravljanje informacijsko-varnostnih kompetenc zaposlenih

Seznam ključnih informacijsko-varnostnih kompetenc zaposlenih

Rezultat R1

Študenti:
Žan Babič
Damjan Fujs
Gašper Gruden
Nejc Hribernik
Sara Kandolf
Ema Kobal
Anže Mihelič
Petra Žiberna

Pedagoški mentorji:
Simon Vrhovec
Blaž Markelj
Tomaž Hovelja

Delovni mentor:
Domen Ocepek

Ljubljana, julij 2017

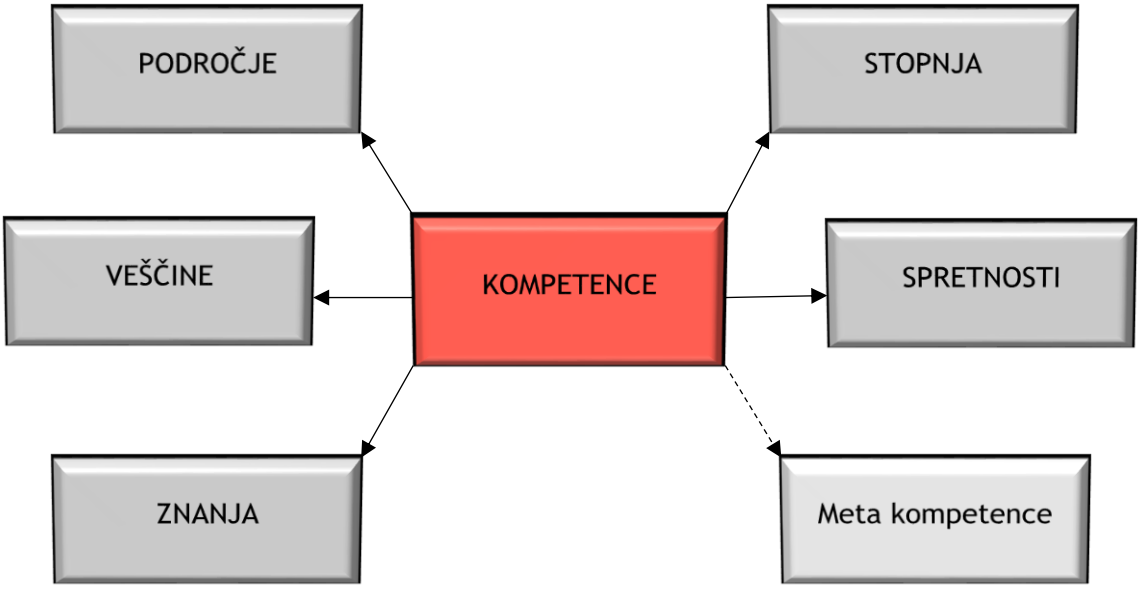
KAZALO

1. DEFINICIJA KOMPETENC

Boyatzis definira kompetenco "kot notranjo značilnost posameznika, ki je vzročno povezana z nadpovprečno storilnostjo na delovnem mestu, njeni konstitutivni deli pa so: motivacija, sposobnosti, samopodoba, znanja in veščine ter socialne vloge posameznika". V slovarjih sta pri izrazu kompetenca in sorodnih izrazih dva različna pojma: – kompetenten v smislu pooblaščen, pristojen in – kompetenten v smislu zmožen, sposoben, primeren, zadosten, merodajen, ki temeljito pozna in obvlada določeno področje, usposobljen. Ko se na kadrovskem področju pogovarjamo o kompetencah, mislimo na zmožnosti zaposlenih za opravljanje dela v najširšem smislu.

Kompetence so opisi znanj, spretnosti, veščin in vedenja posameznika, ki mu omogočajo, da uspešno in učinkovito opravlja svoje delo, lahko pa ga pri tem tudi zavirajo. Poleg zmogljivosti (sposobnosti, spretnosti in znanj) zajema pojem kompetenc tudi motiviranost za neko nalogo, osebni stil in relacijo do koncepta samega sebe. Tako se pojem kompetence neposredno povezuje z dejavniki učinkovitosti ter uspešnosti pri delu (Roblek, 2008).

Pojem kompetenca je eden pogosteje uporabljenih terminov med kadrovskimi strokovnjaki, nikakor pa ni omejen zgolj na kadrovanje, temveč se ga opazuje in uporablja v mnogih znanstvenih disciplinah. V prispevku bomo skušali skozi različne konceptualne zorne kote osvetliti definicijo kompetenc in kompetentnosti ter pojem predstaviti v luči zagotavljanja informacijske varnosti znotraj podjetij, kjer zaposleni predstavljajo najšibkejši člen med varnostjo in ne-varnostjo pogosto zaupnih informacij. Prispevek tako predstavlja korak v smeri iskanja jasne, celovite, enoznačne in natančne definicije kompetenc, tako v strokovnem kot tudi kulturnem kontekstu.



2. SEZNAM SPLOŠNIH INFORMACIJSKO VARNOSTNIH KOMPETENC

Izdelali smo seznam s 33 splošnimi informacijsko varnostnimi kompetencami, ki prikazuje slovenske in angleške različice. Večina kompetenc je bila definirana v angleškem jeziku, zato se nam je zdelo smotrno da se ohrani izvirnik ter doda slovensko različico. Večina kompetenc se nanaša na zaposlene, ki bi morali dosegati vsaj nek delež teh kompetenc pri zagotavljanju informacijske varnosti.

SPLOŠNE IV KOMPETENCE SLO -ANG			KRATEK OPIS KOMPETENCE
1	**Razumevanje zakaj je varovanje informacij pomembno**	*To understand why protecting information is important*	*Zavedanje pomembnosti dostopnosti, integritete in zaupnosti informacij za delovanje organizacije in s tem pomembnosti varovanja informacij.*
2	**Razumevanje informacijsko-varnostnih trendov**	*Understanding information security trends*	*Ažurnost na področju različnih vrst napadov, s poudarkov na poznavanju trenutnih trendov in njihovega gibanja.*
3	**Notranje nevarnosti**	*Internal dangers*	*Zavedanje obstoja možnosti sabotaž in napadov s strani zaposlenih, pozornost na neavtoriziran dostop sodelavcev, povzročanje izpostavljenosti zaradi človeških napak.*
4	**Zunanje grožnje**	*External threats*	*Zavedanje obstoja in prepoznavanje potencialnih nevarnosti, posledic zunanjih napadov ter nezgod na informacijsko infrastrukturo organizacije. Tu mislimo tako na načrtovane napade s strani posameznikov in/ali organizacij na eni strani ali npr. elementarnih nesreč v obliki višje sile na drugi strani.*

5	**Privlačne tarče**	*Attractive targets*	*Zavedanje kateri deli informacijske infrastrukture in subjekti znotraj organizacije so najbolj privlačne ali najbolj ranljive tarče.*
6	**Poznavanje vlog v verigi zagotavljanja informacijske varnosti**	*Knowledge of cyber security roles*	*Razumevanje lastne vloge in vlog ostalih v organizaciji v povezavi z informacijsko varnostjo. Primer: »CISO – Chief information security officer.«*
7	**Poznavanje tveganj, ki izhajajo iz dobavne verige, procesov upravljanja in praks**	*Knowledge of supply chain SCM information systems*	*Poznavanje procesov upravljanja ter dobrih praks poslovanja pripomore k zmanjševanju izgube informacijskega premoženja. Mislimo tudi na varovanje informacij, ki jih dobimo od drugih delov sistema ki so vpeti v dobavno verigo.*
8	**Sprejemanje etičnih odločitev**	*Make ethical choices*	*Etične odločitve slehernega zaposlenega so premo sorazmerno povezane z zagotavljanjem katerekoli varnosti. Razumevanje pomembnosti etičnih odločitev in poznavanje resnosti posledic neetičnih odločitev ki pogosto vodijo do groženj informacijski varnosti.*
9	**Pravilna raba informacijsko-varnostnih orodij in naprav**	*Correct use of equipment and tools.*	*Poznavanje in uporaba primerne opreme in metod varovanja informacij je ključnega pomena za preprečevanje varnostnih tveganj in soočanje z grožnjami in morebitnimi že nastalimi težavami. K pravilni rabi prištevamo tudi dejstvo, da ne uporabljamo piratskih kopij, ker lahko predstavljajo varnostno tveganje. Zaposlene je tudi potrebno poučit o pravilni in varni rabi USB ključev.*

10	**Odločanje o informacijsko-varnostnih prioritetah**	*Decide priorities*	*Smiselno določanje prioritet (tj. razvrščanje po pomembnosti) je pomembno pri hitrem in učinkovitem odločanju o varnostnem postopanju, ki izhajajo iz vsakodnevnih rutin in nepazljivosti.*
11	**Varovanje in delo s podatki**	*Protecting and Handling Data*	*Znanje o varnostnih rešitvah in postopkih za varovanje in pravilno manipulacijo z informacijami. Zavedanje pomembnosti varnostnega kopiranja, uporabe varnostnih kopij in njihove manipulacije za zagotavljanje varnosti, zaupnosti, dostopnosti in integritete informacij.*
12	**Poznavanje principov zasebnosti**	*Knowledge of Privacy Principles*	*Osnovno poznavanje pomembnosti zasebnosti kot ene bolj poudarjenih človekovih pravic v informacijski dobi. Vedeti moramo, da so informacije strank ali poslovnih partnerjev njihove in je zato treba z njimi delati še toliko bolj previdno. Te informacije so bile podjetju zaupane in varovati jih mora vsakdo, ki je v podjetju zaposlen.*
13	**Prepoznavanje varnostnih incidentov**	*Detect security breaches*	*Izvrševanje ustreznega nadzora nad informacijskimi delovnimi sredstvi in zaznavanje kakršnihkoli sprememb. Pomembna lastnost te kompetence je, da znaš ugotoviti ali je prišlo do varnostnega incidenta.*
14	**Razumevanje brezžičnih omrežij in njihove varnosti**	*Understanding Wireless Networks and Security*	*Osnovno znanje o delovanju brezžičnih omrežij, s poudarkom na varnostnih grožnjah, ki izhajajo iz tovrstnih omrežij kot npr. vrste zaščite, šifriranja, saj se še vedno uporabljajo šifriranja, ki niso več varna. Pomembno je poznavanje odprtih omrežij, razlikovanje med WEP in WPA,*

			prepoznavanje zlobnih dvojčkov, da se ne povezuješ v nezaščitena omrežja in da znaš prepoznati HTTPS povezave.
15	**Razumevanje varnosti gesel**	*Understanding password security*	*Od zaposlenega se na eni strani pričakuje razumevanje pomembnosti in zavedanja posledic šibkih gesel.*
16	**Oblikovanje, uporaba in upravljanje varnih gesel**	*Password design, usage and management*	*Od zaposlenih se pričakuje znanje kako sestaviti visoko kvalitetno robustno geslo in kako varnost gesla vzdrževati. Pomembno je tudi, da se zaposleni zavedajo, da je pisanje gesel na listke eno izmed tveganj pri zagotavljanju informacijske varnosti.*
17	**Razumevanje organizacijske varnostne politike**	*Understanding organization's security awareness policy*	*Podrobno razumevanje in spoštovanje varnostne politike organizacije.*
18	**Organizacijska intelektualna lastnina**	*Organizational intelectual property*	*Razumevanje da so dokumenti intelektualna lastnina in last organizacije.*
19	**Varne prakse za delo z elektronsko pošto**	*Secure e-mail practices*	*Osnovno poznavanje delovanja elektronskega sporočanja, ki ni nujno omejeno samo ne elektronsko pošto in postopkov za varno uporabo aplikacij za elektronsko sporočanje in za manipulacijo z elektronskimi sporočili. Zavedati se je potrebno, da se dokumentov ne pošilja po elektronski pošti, ker je e-pošta brez dodatnih varnostnih vzvodov nezaščiten kanal. Za te namene se uporablja orodje PGP (pretty good privacy).*
20	**Nepoznani pošiljatelji elektronske pošte in priponke**	*Unknown email sources and attachments*	*Zavedanje ranljivosti in resnosti posledic pri ne-varni rabi elektronske pošte. Pozornost in upoštevanje predpisanih postopkov pri odpiranju elektronskih sporočil in priponk iz neznanih ali nenavadnih virov.*

21	**Namestitev in uporaba protivirusnih programov**	*Installing and using anti-virus software*	*Namestitev in pravilna uporaba antivirusnega programa, s poudarkom na rednem in sprotnem skeniranju prenešenih informacij.*
22	**Varno brskanje po spletu**	*Secure browsing practices*	*Poznavanje najosnovnejših groženj, ki izhajajo iz uporabe interneta in delovanje v skladu s tem znanjem. Pomembno je, da zaposleni znajo uporabljati varni brskalnik (npr. Firefox) in da uporabljajo oz. prepoznajo HTTPS povezavo.*
23	**Identifikacija spletnih groženj**	*Identify online threats*	*Sposobnost pravilne identifikacije spletnih groženj, ki lahko ogrozijo informacijsko premoženje. Zaposleni morajo vedeti, kaj narediti, če so preusmerjeni oz. so se znašli na sumljivi spletni strani.*
24	**Varnost mobilnih naprav vključno z BYOD**	*Mobile device security including BYOD*	*Zavedanje potencialnih nevarnosti, ki jih predstavljajo naprave v osebni lasti, ki jih zaposleni v službene ali zasebne namene s seboj prinesejo na delovno mesto. Gre za pravilno uporaba zasebne IKT v poslovne namene ali obratno.*
25	**Razumevanje politike čiste mize**	*Understanding »clean desk policy«*	*Doslednost in sposobnost sledenja navodilom. Uporaba postopkov za zagotavljanje fizične varnosti delovnega območja.*
26	**Gledanje čez ramo**	*Shoulder surfing*	*Preprečevanje fizičnega prestrezanja informacij, predvsem z zaslona, ki ga zaposleni v tistem trenutku uporablja.*
27	**Brskanje po smeteh**	*Dumpster diving*	*Zavedanje pomembnosti zaupnosti in integritete tudi tistih dokumentov, ki so bili zavrženi. Preprečevanje prestrezanja informacij zavrženih listin.*
28	**Preprečevanje napadov socialnega inženiringa**	*Protecting against social engineering attacks*	*Spoštovanje pravil izdajanja občutljivih podatkov, prijava*

			nenapovedanih zahtev za informacije ali storitve nadrejenemu. Zmožnost da posamezni zaposleni ne podlega socialnim pritiskom.
29	**Varna raba socialnih omrežij**	*Secure use of social media*	*Varna raba socialnih omrežij v smislu zagotavljanja zasebnosti in zavedanja koncepta zobne paste; pasta, ki je enkrat iztisnjena jo je težko zlit nazaj. Podobno je s podatki. Varna raba socialnih omrežij v smislu zagotavljanja zasebnosti in zavedanja posebnosti kibernetskega prostora v smislu injiciranja informacij v kibernetski prostor. Informacije, ki se vanj injicirajo se znotraj mega-sistema 'kibernetske divjine' razpršijo in izgubijo.*
30	**Kontrola dostopa**	*Access control*	*Nadzor obiskovalcev in fizičnega dostopa neavtoriziranih oseb, ne glede na to kdo so – prijave nenavadnih dogodkov in izpraševanje neznanih oseb.*
31	**Odzivanje na zaznane grožnje**	*Responding to perceived threats*	*Odzivanje na zaznane grožnje je ključnega pomena za obvladovanje nastale škode. hiter in takojšen odziv zmanjšuje nastale stroške in izgubo informacijskega premoženja. Razumevanje pomembnosti in poznavanje predpisanih postopkov v primeru varnostnih incidentov. Med drugim gre za znanje o tem koga o tem obvestiti in kako v teh situacijah postopati.*
32	**Varnost organizacijske IKT izven delovnega mesta**	*Security of organizational ICT outside of the workplace*	*Razumevanje nepomembnosti prostorske komponente kibernetskega prostora in s tem zagotavljanje tako fizične, kakor tudi tehnološke varnosti delovne IKT tudi ko se zaposleni ne nahaja neposredno na delovnem mestu.*

33	**Varne prakse za oddaljeno delo**	*Secure practices for working remotely*	*Upoštevanje mehanizmov varne rabe oddaljenega dostopa, zagotavljanje zasebnosti ter varovanja informacij. Uporaba varnih – kriptiranih povezav. Zaposleni bi naj vedeli, da lahko vzpostavijo omrežni tunel oz. ti. Virtual Private Network – VPN povezava.*

Tabela 1 Seznam splošnih IV kompetenc. Rdeča polja so posamezne kompetence. Dodani so tudi kratki opisi kompetenc za lažjo interpretacijo.

3. SPECIFIČNE KOMPETENCE

Delovno specifične kompetence-Aktivnosti v določeni delovni vlogi. Potrebne so, da lahko uspešno opravimo določeno delovno nalogo. Nanašajo se na podobna delovna mesta in so le-tem skupna. **Organizacijsko specifične kompetence -** kompetence, ki niso odvisne od vloge, ki jo ima posameznik v organizaciji. Povezane so z uspešnostjo posameznika v organizaciji kot celoti in se lahko po njej prenašajo.

Primer specifičnih kompetenc:

Kompetenca [SL]	**Kompetenca [EN)**
Načrtovanje in razvoj informacijskih sistemov	Planning in Information Systems Development

Razumevanje zakonov in drugih predpisov v zvezi z informacijsko varnostjo	Understanding of laws and regulations on information security
Razumevanje standardov in meril v zvezi z informacijsko varnostjo	Understanding of standards and criteria related to information security
Znanje o nasprotnih taktikah, tehnikah in postopkih	Knowledgeof common adversary tactics, techniques and procedures
Znanje o informacijski tehnologiji varnostnih načel in metod (požarni zid, šifriranje,...)	Knowledgeof information technology (IT) security principles and methods (e.g., firewalls,demilitarized zones, encryption)
Znanje o zlonamerni programski opremi	Knowledge od malware analysis concepts
Znanje o zaznavanju vdorov in tehnike za odkrivanje gostiteljev in omrežnih vdorov preko tehnologije za zaznavanje vdorov	Knowledge of intrusion detection methodologies and techniques for detecting host- andnetwork-based intrusions via intrusion detection technologies
Znanje kriptografije	Knowledge of cryptography
Poznavanje metodologiji šifriranja	Knowledge of encryption methodologies
Poznavanje mrežnega prometa (prenos, kontrolni protokoli in internetni protokoli) in imenih storitev	*Knowledge of how traffic flows across the network (i.e. transmission and encapsulation) (DNS- domain name system)*
Znanje o sistemih in uporabi varnostnih groženj in ranljivosti (mobilna koda, postopkovni jezik, zlonamerna koda, bufferoverflow, cross-site scripting,..)	*Knowledge of system and application security threats and vulnerabilities (e.g., bufferoverflow, mobile code, cross-site scripting,..)*