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 vzorčnih ukrepov za izboljšanje ključnih informacijsko-varnostnih kompetenc zaposlenih

Rezultat R3

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

1. Uvod

Upravljanje in izboljševanje ključnih kompetenc zaposlenih je izrednega pomena zaradi potreb na trgu dela, večje zaposljivosti in mobilnosti ter osebnega razvoja in delovanja v sodobni družbi (Pridobivanje temeljnih in poklicnih kompetenc, 2017).Kompetence s področja informacijske varnosti je potrebno, za uspešno in učinkovito delo, konstantno nadgrajevati in dopolnjevati. Kadar zaposleni niso kompetentni ali pa imajo določene kompetence zelo šibke, je lahko ogroženo celotno delovanje organizacije. V takšnih primerih je potrebno poseči po ukrepih, ki bodo izboljšali ali nadgradili kompetentnost zaposlenega. Pri tem je največ poudarka na dodatnem izobraževanju, ki je temeljni pogoj za razvijanje in pridobivanje kompetenc.

Izobraževanje lahko poteka v več oblikah in sicer kot tečaj, seminar, delavnica, kongres, posvet ipd. V teh primerih gre za posredovanje specifičnih znanj in spretnosti, ki jih ljudje potrebujejo pri opravljanju svojih vlog na delovnem mestu. Z učenjem se tako izboljšajo osebni, delovni in organizacijski dosežki (Mlaker, 2010).
Poleg izobraževanja pa prav tako pomembno praktično usposabljanje, kjer se znanja iz teorije prenesejo v prakso.

1. Opis posameznih ukrepov za izboljšanje informacijsko-varnostnih kompetenc

VRSTA UKREPA	OPIS	PREDNOSTI	SLABOSTI
Tečaj	Neformalno izobraževanje, ki pomeni pridobivanje, obnavljanje, razširjanje znanja. Pri tem ne gre za pridobitev določene stopnje izobrazbe oziroma dokazovanje pridobljenega znanja z javno veljavno listino.	• Predstavlja pomembno dopolnitev formalnemu izobraževanju • Posreduje specifična znanja in spretnosti glede na posameznikovo delovno mesto • Intenzivna dopolnitev in osvežitev znanja	• Pomanjkanje posameznikove motivacije za aktivno udeležbo • Prevelika zgoščenost podanega znanja v kratkem času • Različna predznanja udeležencev
Seminar	Skupek organiziranih predavanj z določenega	• Pridobitev dodatnih znanj z	• Pri dolgotrajnih seminarjih, lahko

	področja za dodatno izobraževanje odraslih.	določenega področja	pride do upada koncentracije poslušalcev
Delavnice	Način neformalnega izobraževanja, kjer udeleženci z aktivnim sodelovanjem pridobijo novo, dodatno znanje. Temelj izobraževanja je na praktičnih izkušnjah.	• Izmenjava stališč • Pridobivanje novih znanj • Reševanje konkretnih problemov • Kolektivnost • Neposredna komunikacija	• Pomanjkanje teoretičnega znanja • Nestrokovnost
Praktično usposabljanje	Je proces pridobivanja, razvijanja in izboljšanja tistih sposobnosti, veščin, navad in kompetenc zaposlenih, ki jim bodo omogočile večjo učinkovitost in s tem doseganje ciljev podjetja. Gre za usposabljanje, pridobivanje spretnosti za konkretno delo na konkretnem delovnem mestu.	• Dodatni trening tistih znanj, sposobnosti in navad, ki so potrebna za opravljanje določenega dela v okviru celote neke dejavnosti-vlaganje v implicitno znanje • Lahko se pridobi potrdilo o usposobljenosti	• Časovna omejitev • Nezainteresiranost udeležencev
Preizkusni testi - »preverjanje znanja«	Preizkusni testi so sestavljeni iz ključnih vprašanj, na katera je ponujeno več možnih odgovorov, uporabnik pa mora izbrati pravilnega. Na koncu reševanja testa se pojavijo rezultati testa, vključno s preglednico nepravilnih odgovorov ter navedbo in razlago pravilnih odgovorov.	• Preverjanje posameznikovega teoretičnega znanja • Zajemanje širokega spektra znanja	• Neustreznost zastavljenih vprašanj • Merjenje znanja samo v teoriji in ne praksi • Individualnost
Delovni sestanki	Najbolj pogosta oblika sestankov, ki imajo na dnevnem redu tekoča vprašanja in naloge in naloge o katerih se razpravlja in sklepa. Pomeni določeno fazo v procesu, kjer lahko analiziramo in predebatiramo že opravljeno delo in načrtujemo nadaljnje aktivnosti.	• Neposredno medsebojno obveščanje • Vzpostavitev medsebojnega stika in sodelovanja • Možnost takojšnjih povratnih informacij	• Neustreznost vodenja delovnega sestanka • Premoč vodje • Nezainteresiranost udeleženih • Časovna omejitev

2. Tabela ukrepov za izboljšanje posamezne informacijsko-varnostne kompetence

V spodnjo tabelo smo razvrstili ukrepe za izboljševanje posameznih kompetenc s področja informacijske varnosti.

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.*
- Izobraževanja s področja varovanja informacij (pokriva več kompetenc) - Analiza tveganj-priprava ukrepov za zmanjševanje tveganj in nadzor njihove uporabe - Jasno začrtana varnostna politika, s katero morajo biti seznanjeni vsi zaposleni; varovanje informacij izhaja iz ciljev organizacije		
2. Razumevanje informacijsko-varnostnih trendov	*Understanding information security trends*	*Ažurnost na področju različnih vrst napadov, s poudarkom na poznavanju trenutnih trendov in njihovega gibanja.*
- Preverjanje znanja zaposlenih s praktičnimi mesečnimi preizkusnimi testi - Predstavitev aktualnih raziskav (predavanja)		
3.Notranje nevarnosti	*Internal dangers*	*Zavedanje obstoja možnosti sabotaž in napadov s strani zaposlenih, pozornost na neavtoriziran dostop sodelavcev, povzročanje izpostavljenosti zaradi človeških napak.*
- Izobraževanje o obstoju in lastnostih notranjih nevarnosti, o razlogih za nastanek in o preprečevanju notranjih napadov - Notranja skupina za nadzor (neodvisni posamezniki), ki skrbi za upoštevanje oz. zagotavljanje varnostne politike - Revizija informacijskih sistemov		
4.Zunanje grožnje	*External threats*	*Zavedanje obstoja in prepoznavanje potencialnih nevarnosti, posledic zunanjih napadov ter nezgod na informacijsko infrastrukturo organizacije. Vključujejo tako načrtovane napade s strani posameznikov in/ali organizacij na eni strani ali npr. elementarne nesreče v*

		obliki višje sile na drugi strani.
- Izobraževanje o različnih vrstah zunanjih nevarnosti, njihovih lastnostih, možnimi posledicami in prepoznavnih znakih - Sistem pravočasnega alarmiranja (na koga se obrniti) in razreševanja problema - Postopki za zagotavljanje varnosti (lastne) delovne IKT pri naravnih nesrečah (npr. poplavah, ognju)		
5.Privlačne tarče	*Attractive targets*	*Zavedanje kateri deli informacijske infrastrukture in subjekti znotraj organizacije so najbolj privlačne ali najbolj ranljive tarče.*
- Izobraževanja s področja ranljivosti in izpostavljenosti različnih delov informacijske infrastrukture in privlačnost le-teh za napadalce - 2x letno delavnice ali seminarji na temo ranljivosti informacijske strukture		
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 – Chiefinformationsecurityofficer.«*
- Ozaveščanje o znanju ter odgovornosti ostalih zaposlenih (plakati o funkcijah posameznika) - Delovni sestanki (predstavitev mesečnih poročil posameznih »sektorjev«)		
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.*
- Izobraževanje o tveganjih, ki izhajajo iz dobavne verige in medorganizacijskih povezav - Plakati, ki zaposlenih v organizaciji prikazujejo tveganja, ki izhajajo iz vsakodnevnega poslovanja		
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.*
- Preverjanje znanja – primeri etičnih dilem (na koncu prikaz rešitev) - Prepoznavanje in uresničevanje potencialov zaposlenih (povezanost) - Organiziranje etičnih treningov-etični managerji oz. vodje prenašajo znanja na podrejene - Sistem nagrajevanja		
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.
- Izobraževanje na področju pravilne rabe organizacijske IKT in varnostnih orodij za zagotovitev zaželenih rezultatov		
10. Odločanje o infromacijsko-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.*
- Sprejem pravilnikov in pravilnih postopanj ob obdelavi podatkov (prioritete)		
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*
- Praktično in teoretično izobraževanje na temo hrambe podatkov (kako, na kakšen način in kje jih hraniti)		
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.*
- Izobraževanje in opozarjanje na pomembnost zasebnosti, tako za posameznike (zaposlene in stranke) kakor tudi za celotno organizacijo - Oblikovanje brošure na temo zasebnosti		
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.*
- Usposabljanje skupaj z informatiki v podjetju, delo z njimi (ti predstavijo svoj vidik dela, in povedo na koga se je potrebno obrniti če zaposleni naleti na težavo)		

14. Razumevanje brezžičnih omrežij in njihove varnosti	*Understanding Wireless Network sand 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.*
- Izobraževanje in praktični prikaz s strani informatikov, kako se razlikujejo zlonamerne ali klonirane dostopne točke in točke ki so varne, uporaba protivirusnih programov. - Izobraževanje o lastnostih dostopnih točk in brezžičnih omrežij (npr. varnostni algoritmi, šifriranje)		
15. Razumevanje varnosti gesel	*Understanding password security*	*Od zaposlenega se pričakuje razumevanje pomembnosti in zavedanja posledic šibkih gesel.*
- Prikaz kaj se lahko zgodi, če gesla niso dovolj močna (plakati, delavnice) - Izobraževanje na področju hranjena 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.*
- Izobraževanje na temo varovanja in oblikovanja robustnih gesel		
17. Razumevanje organizacijske varnostne politike	*Understanding organization's security awareness policy*	*Podrobno razumevanje in spoštovanje varnostne politike organizacije.*
- Preučitev varnostne politike ob prihodu osebe v organizacijo (osnovna dejstva) - Ustvariti dokument na katerem bodo pomembne točke o zagotavljanju varnosti podjetja		
18. Organizacijska intelektualna lastnina	*Organizational Intelectual property*	*Razumevanje da so dokumenti intelektualna lastnina in last organizacije.*
- Izobraževanje s področja intelektualne lastnine in pomembnosti varovanja le-te za organizacijo		
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 (prettygoodprivacy).
- Program praktičnega usposabljanja za prepoznavanje identifikacijskih znakov nelegitimne elektronske pošte - Vzpostavitev in spremljanje sistema internega ažuriranja in opozarjanja na potencialne nevarnost		
20. Nepoznani pošiljatelji elektronske pošte in priponk	*Unknown e-mail 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.*
- Program praktičnega usposabljanja za preverjanje izvora elektronskih sporočil in zagotavljanje varnosti prenesenih priponk		
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.*
- Program praktičnega usposabljanja za pravilno rabo in analiziranja podatkov antivirusnih programov		
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.*
- Izobraževanje o pomenu rednega posodabljanja programske opreme - Delavnica na temo analiziranja informacij, ki jih brskalniki ponudijo in uporabe njihovih varnostnih mehanizmov		
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.*
- Program praktičnega usposabljanja za prepoznavanje znakov spletnih nevarnosti in metod preverjanja varnosti prenosov in 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.
- Program izobraževanja o ranljivostih, ki jih v organizacijo vnesejo lastne naprave in dobrih praks za zmanjševanje ranljivosti na tem področju (vključno z uporabo zunanjega omrežja)		
25. Razumevanje politike "čiste mize"	*Understanding the »clean desk policy«*	*Doslednost in sposobnost sledenja navodilom. Uporaba postopkov za zagotavljanje fizične varnosti delovnega območja.*
- Program izobraževanja in opominjanja na pomembnost čistih miz v organizaciji		
26. "Gledanje čez ramo"	*Shoulder surfing*	*Preprečevanje fizičnega prestrezanja informacij, predvsem z zaslona, ki ga zaposleni v tistem trenutku uporablja.*
- Izobraževanje zaposlenih o nevarnosti gledanja čez ramo (na zaslon ali pod prste) in dobrih praksah za preprečevanje le-tega		
27. "Brskanje po smeteh''	*Dumpster diving*	*Zavedanje pomembnosti zaupnosti in integritete tudi tistih dokumentov, ki so bili zavrženi. Preprečevanje prestrezanja informacij zavrženih listin.*
- Izobraževanje zaposlenih o možni zlorabi informacij iz zavrženih listin - Izobraževanje o pravilnem uničevanju elektronskih in fizičnih informacij		
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.*
- Izobraževanje zaposlenih o pojavu in poteku socialnega inženiringa - Program praktičnega usposabljanja za preprečevanja socialnega inženiringa na podlagi prikaza že izvedenih napadov		
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 kibernetskiprostor. Informacije, ki se vanj injicirajo se znotraj mega-sistema 'kibernetske divjine' razpršijo in izgubijo.*
- Izobraževanje zaposlenih o možnosti zlorabe prostovoljno objavljenih podatkov - Delavnica na temo varne rabe socialnih omrežij in varnostnih mehanizmih, vključno z informiranjem o podatkih, ki so neprostovoljno pripeti na objave		

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*
- Izobraževanje zaposlenih o varnostnih implikacijah neavtoriziranega dostopa - Program za zagotavljanje aktivne kontrole dostopa - Usposabljanje zaposlenih za varno rabo tehnologije varovanja dostopa		
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.*
- Izobraževanje zaposlenih o organizacijskem postopku za odzivanje na varnostne incidente - Program praktičnega usposabljanja zaposlenih za prepoznavo in hitro odzivanje ob incidentih		
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.*
- Izobraževanje o varnostnih posledicah izgube naprave - Učenje najboljših praks za zagotavljanje zaščite delovne IKT izven organizacijskih prostorov - Praktično usposabljanje zaposlenih za pravilno uporabo varnostnih rešitev na tem področju (gps lokatorji, alarmi, programi za zaklepanje in brisanje IKT, fizično varovanje,..)		
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. VirtualPrivateNetwork –VPN povezava.*
- Izobraževanje o varnostnih aspektih oddaljenega dostopa. - Program praktičnega usposabljanja za varno rokovanje z napravo v primeru oddaljenega dostopa		

3. Viri in literatura

Mlaker, D. (2010). *Vloga dejavnikov, ki vplivajo na razvoj kompetenc: primer podjetja* (Diplomsko delo). Ljubljana: Fakulteta za družbene vede.

Pridobivanje temeljnih in poklicnih kompetenc. (2017). Pridobljeno dne, 22.5.2017 na http://www.cdi-univerzum.si/pridobivanje-temeljnih-in-poklicnih-kompetenc/