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

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

Rezultat R2

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 Dimenzije doseganja kompetenc

V povezavi z ugotavljanjem informacijsko-varnostne ozaveščenosti je potrebno določiti kaj in kako meriti.

Oblikovali smo tri osnovne dimenzije, ki smo jih želeli meriti znotraj posamezne kompetence:

- **znanje (angl. *knowledge*):** *"kaj posameznik ve"* (generično in specifično znanje, zahtevano za opravljanje dela)
- **namera (angl. *intention*):** *"kaj posameznik namerava"*
- **vedenje (angl. *behaviour*):** "kaj posameznik naredi" (sposobnost uporabljati znanje, spretnosti in vedenja za doseganje pozitivnih rezultatov in doseganje standardov pri opravljanju dela).

Tako je vprašalnik zastavljen v smeri preverjanja več dimenzij vsake posamezne kompetence. Za vsako kompetenco so pripravljena področja, ki mu pripade ustrezno testiranje. Primer spodnja tabela.

Kompetenca: XX	
Dimenzije	**Indikatorji**
znanje	Vprašanje meri dejansko znanje in se ga meri z vprašalnikom, pri čemer se je potrebno izogibati vprašanjem z odgovori pravilno/napačno in vprašanjem z odgovori na Likertovi lestvici. Najprimernejša so vprašanja z odgovori večstranske izbire.
namera	Najprimernejša vprašanja za namero (*intention*) so z odgovori na Likertovi lestvici.
vedenje	Zaradi nujnosti izogibanja samoevalvacije pri preverjanju dejanskega vedenja vprašanja in odgovori niso primerni. Potrebna je neodvisna evalvacija (npr. eksperiment), saj je le tako lahko vedenje objektivno ocenjeno.

2 Stopnje usposobljenosti

-1	**kritična**	Verjetnost resnejšega incidenta ob napadu: **neizogibna**. Posameznik predstavlja kritično nevaren člen v verigi zagotavljanja informacijske varnosti.
0	**neustrezna**	Verjetnost resnejšega incidenta ob napadu: **zelo verjetna**. Posameznik ne dosega minimalnih standardov kompetentnosti na informacijsko-varnostnem področju.
1	**minimalna**	Verjetnost resnejšega incidenta ob napadu: **verjetna**. Posameznik ustreza minimalnim, zadostnim standardom kompetentnosti na informacijsko-varnostnem področju. Razume najosnovnejše koncepte informacijske varnosti, informacijsko-komunikacijske tehnologije lahko varno uporablja v preprostih situacijah, najbolje ob pomoči višje usposobljenega osebja.
2	**ustrezna**	Verjetnost resnejšega incidenta ob napadu: **manj verjetna.** Posameznik ustreza osnovnih standardom kompetentnosti na informacijsko-varnostnem področju. Razume osnovne koncepte informacijske varnosti, informacijsko-komunikacijske tehnologije lahko varno in samostojno uporablja v vsakodnevnih situacijah.
3	**odlična**	Verjetnost resnejšega incidenta ob napadu: **skoraj neverjetna**. Posameznik ustreza najvišjim standardom kompetentnosti na informacijsko-varnostnem področju. Poglobljeno razume koncepte informacijske varnosti in razpolaga z obširnim znanjem, podkrepljenim z ekstenzivnimi izkušnjami s tega področja. Kompetentnost mu omogoča popolnoma samostojno delo. Lahko nudi podporo ostalemu osebju. Sposoben je generalizirati svoja znanja z obstoječih na nove situacije. Predstavlja avtoriteto na informacijsko-varnostnem področju.

3 Načini ocenjevanja kompetenc

Če hočemo ocenjevati stopnje doseganja kompetenc moramo pri tem uporabljati določene metode, v nadaljevanju so našteti poglavitni načini oziroma metode ocenjevanja.

3.1 Vprašalniki

Z vprašalniki prepoznavamo in vrednotimo informalno in neformalno učenje s pomočjo izpitov oziroma v formalnem izobraževanju uveljavljenih metod ocenjevanja.

Vprašalnik je pisen ter je lahko sestavljen iz esejskih vprašanj, vprašanj zaprtega tipa in podobnih pisnih nalog kot je povezovanje, razvrščanje in dopolnjevanje pojmov.

3.1.1 Samoocena

Temelji na posameznikovi samooceni in dokumentiranju njegovih kompetenc in je običajno sopodpisana s strani tretje osebe v potrditev samoocene.

Velja za nezanesljivo, saj je preveč subjektivna, posameznik lahko drugače dojema sebe kot drugi, prav tako lahko pride »privzdignjenih«/»izboljšanih« rezultatov zaradi želje po ustrezanju pogojem.

3.1.2 Test

Prepoznavanje in vrednotenje informalnega in neformalnega učenja s pomočjo izpitov oz. v formalnem izobraževanju uveljavljenih metod ocenjevanja.

3.2 Praktični preizkus

Praktični preizkus pomeni, da je posameznik, da bi ocenili njegove kompetence, postavljen v situacijo, ki izpolnjuje vse kriterije scenarija iz realnega življenja. Na podlagi opazovanja pa se poda ocena o izpolnjevanju kompetence tako, da primerjamo pričakovano in pa dejansko vedenje.

Pri »dokazilih pridobljenih iz dela (ali druge prakse)« kandidat zbere fizična in intelektualna dokazila o učnih izidih, ki se lahko navezujejo na delo, prostovoljne situacije, družinsko ali kakšno drugo okolje. Ta dokazila nato predstavljajo temelje za vrednotenje kompetenc s strani tretje osebe.

3.3 Intervju

Intervju je ustni pogovor z ocenjevanim, podoben je navadnemu vprašalniku, vendar lahko pri intervjuju zaznavamo poleg znanja, tudi posameznikov odnos, namen in vedenje glede posamezne kompetence.

Je bolj podroben/obsežen saj posameznik odgovarja s svojimi besedami, tako pa se lahko zaznava manjše nepravilnosti, jasnost in globino kompetence.

3.4 Poslovne igre

Ljudje se veliko več in lažje naučimo preko igre, ker se ob tem sprostimo, ljudje so tudi ponavadi med delovno rutino sproščeni; v smislu da ne pazijo kako opravljajo svoje delo, saj bi jih lahko nekdo nadzoroval; zato so poslovne igre dober način ocenjevanja dejanskega obnašanja in integritete zaposlenih, ker jih igra zavede v koncentracijo na pravila, ne pa na njihovo integritetno obnašanje. So dobre za ocenjevanje osebnostnih lastnosti.

3.5 360⁰

Ocena po metodi 360° pomeni, da posameznik sam oceni svoje kompetence, ocenijo ga pa tudi drugi. V primeru vodij so to podrejeni, nadrejeni in še kdo na istem nivoju (zato tudi izraz 360°, kar pomeni, da naredimo celoten krog).

4 Razmerja med kompetencami, njihovimi dimenzijami in področji

Za definiranje razmerij med kompetencami, njihovimi dimenzijami in področji moramo sprva definirati razmerja med posameznimi dimenzijami.

Odnos je pomemben pri udejstvovanju **znanja** REZULTAT tega je **namen**, razlika **namena in realnosti** pa je **vedenje.**

Kompetence se lahko z dimenzijami povezujejo tako da so dimenzije tipi kompetenc (vsaka ima samo eno dimenzijo), tako da ima vsaka vse ali pa da ima vsaka kompetenca od enega do štirih dimenzij.

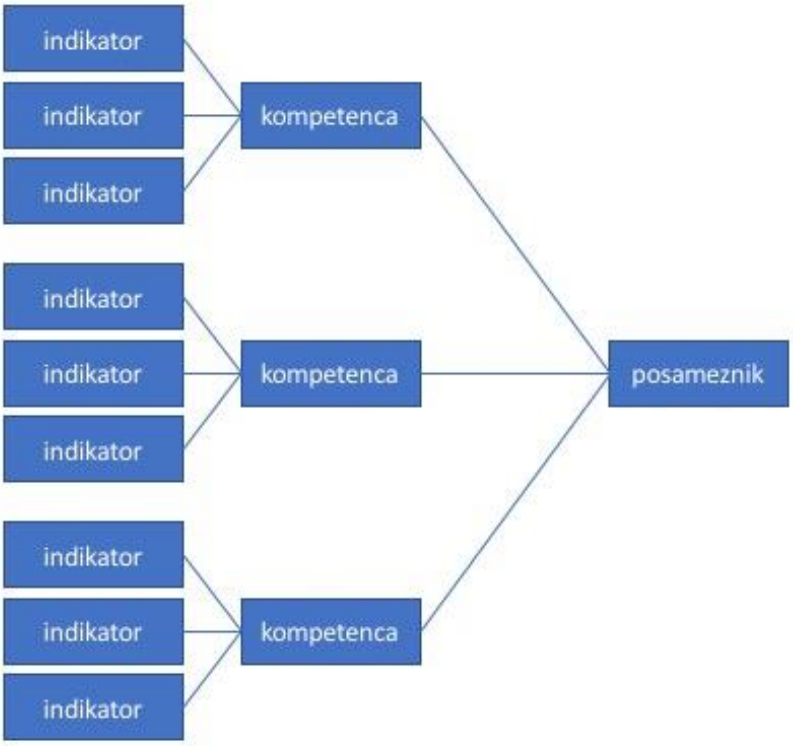
Razmerja so lahko različna in s tem tudi pomembnost posamezne dimenzije, navsezadnje je pomembna le dimenzija vedenja, saj je končni rezultat vseh ostalih; vendar je težko oceniti kje se je "zalomilo", torej v primeru če je bilo vedenje napačno se je lahko zalomilo pri znanju, odnosu, namenu ali vedenju samem, dimenzije so torej pomembne pri izboljševanju kompetenc, saj je le to tako bolj optimizirano.

Poleg tega nima vsaka oseba vseh dimenzij določene kompetence. Študentje na primer imajo veliko znanja, imajo tudi odnos, s prihodom na delovno namesto dobijo namero, vedenje pa pridobivajo z delovanjem na delovnem mestu v nasprotju pa imajo nekateri starejši dobro dimenzijo vedenja, vendar slabo bazo znanja. Tako je lahko določena kompetenca iste osebe ocenjena slabo ali pozitivno glede nato v kateri dimenziji jo merimo.

Vse dimenzije so tako po našem mnenju pomembne, vendar so lahko nekatere bolj kot druge, pri tem moramo upoštevati, kakšno delovno mesto merimo, neko ustaljeno delovno mesto, ki nima dosti razgibanega obsega dela lahko merimo z vedenjem, saj je pri rutinskem delu le to pomembno. Pri zelo razgibanem delu kjer se zaposleni vsak dan sooča z novimi izzivi pa je po našem mnenju pomembna osnova, to je znanje.

Glede na različno vrednost posameznih dimenzij bi lahko posamezni dali različne uteži oziroma koeficient, rezultat določene dimenzije zmnožili, zmnožke vseh pa sešteli, in prek tega dobili celovito oceno usposobljenosti.

Stopnja usposobljenosti je odvisna od "rezultata" dimenzij doseganja kompetenc. Torej sta v odvisnem razmerju. Dimenzije nakazujejo neko stopnjo "uspešnosti" posameznika pri *posamezni kompetenci*, stopnja usposobljenosti pa je "uspešnost" zbira vseh kompetenc za *posameznika kot enoto organizacije*.



5 Tabela vprašanj za posamezno kompetenco

Po analizi načinov ocenjevanja in različnih dimenzij smo se odločili, da ocenjujemo dve glavni dimenziji, to sta znanje in vedenje, v primeru, da vedenja za posamezno kompetenco ni mogoče oceniti se meri njegov najboljši približek to je namera. Znanje bomo merili z vprašalniki zaprtega tipa, povezovanjem in obkroževanjem; namera se bo merila s strinjanjem z določeno izjavo s pomočjo Likertove lestvice, vedenje se lahko meri s preteklim vedenjem še bolje pa je s praktičnim preizkusom.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
1	**Razumevanje zakaj je varovanje informacij pomembno** *To understand why protecting information is important*	-informacije o zaposlenih -informacije o poslovnih procesih -informacije o strankah (kaj/zakaj) -ocena izgube ob zlorabi	Kakšne so lahko neposredne posledice uhajanja informacij o zaposlenih? + infiltracija v sistem s krajo identitete - večja ranljivost za tehnično usmerjene napade + tožba + usmerjeno ribarjenje (angl. spear phishing) + izsiljevanje - izguba strank - vdor brez sledi Kakšne so lahko neposredne posledice uhajanja informacij o strankah? - infiltracija v sistem s krajo identitete - večja ranljivost za tehnično usmerjene napade + usmerjeno ribarjenje (angl. spear phishing) + tožba - izsiljevanje + izguba strank - vdor brez sledi Kakšne so lahko neposredne posledice uhajanja informacij o poslovnih procesih? - infiltracija v sistem s krajo identitete		

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
			+ večja ranljivost za tehnično usmerjene napade + usmerjeno ribarjenje (angl. spear phishing) - tožba + izsiljevanje + izguba strank + vdor brez sledi		

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
2	**Razumevanje informacijsko-varnostnih trendov** *Understanding Information Security trends*	-socialni inženiring ("popravljanje računalnika preko oddaljenega dostopa") -kriptovirus -okužene word datoteke -trojanski konj -programski/računalniški črv -virus	Naštej najbolj popularne vrste informacijsko varnostnih napadov: +socialni inženiring ("popravljanje računalnika preko oddaljenega dostopa") +kriptovirus +okužene word datoteke +trojanski konj +programski/računalniški črv +virus	Redno spremljam nedavne informacijsko varnostne incidente. +sprejemljiva 4-večinoma velja in 5-popolnoma velja.	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
3	**Notranje nevarnosti** *Internal dangers*	-nekompetentni zaposleni -podkupljivi zaposleni -nezadovoljni zaposleni -leni zaposleni	Notranje nevarnosti organizacije so: -dostavljalci hrane v notranjosti organizacije +nekompetentni zaposleni +podkupljivi zaposleni -slaba fizična varnost +nezadovoljni zaposleni +leni zaposleni -slaba notranja informacijska oprema	Preizkuševalec (ki dela v podjetju) je za računalnikom zaposlenega, ki se ga testira, nanj počaka, ob njegovem prihodu oceni reakcijo, ko ga zaloti za računalnikom. -zaposleni ne reagira oziroma ne obvesti o varnostnem incidentu pristojnega, niti ne preveri če je bil računalnik kompromisiran +zaposleni prijavi dejanje ustrezni osebi, ocena je boljša če to naredi nemudoma Zaposlenemu nastavimo keylogger programsko opremo, če se sploh da (test sam po sebi). +če se ne da je ocena najboljša, če je inštalacija uspešna pa ga zazna je ocena pozitivna vendar slaba zaradi dejanske zmožnosti inštalacije -če s programom uspešno pridobimo gesla je kompetenca zaposlenega negativna, še bolj če ne opazi ponovnega pristopa k računalniku za vpogled v sprejete podatke	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
4	**Zunanje grožnje** *External threats*	-napadi preko svetovnega spleta -fizični vdori -osebe, ki se pretvarjajo da so avtoritetne ali neavtoritetne osebe z opravičenim dostopom -naravne in druge nesreče ter ekstremni pojavi	Zunanje grožnje podjetja so lahko: +napadi preko svetovnega spleta -zaposleni, ki z namenom zlonamerne uporabe podatkov, do njih dostopajo od zunaj -zaposleni, ki jim nenamerno uhajajo zaupni podatki +fizični vdori +vse nepoznane osebe podjetju, ki stopajo z njim v komunikacijo -informacijska oprema podjetja zunanjih svetovnih proizvajalcev +naravne in druge nesreče ter ekstremni pojavi	Zunanja oseba se sprehodi podjetju, poizkuša priti čim globlje oziroma bližje informacijskim sredstvom podjetja. +ocenjevani vsi, katere prečka, tisti ki ga ustavi vpraša po avtorizaciji ali še bolje pospremi do varnostnikov ne le receptorja (prijavi dejanje varnostni službi!+++najvišja ocena) je ocenjen pozitivno -vsi tisti, ki ignorirajo zunanjo osebo, malo manj, če jo pospremijo do željene destinacije Zunanji vsiljivec poizkuša v računalnik podjetja priključiti USB napravo/izmakniti informacijsko sredstvo. +lastnik sredstva opazi napravo ++jo prijavi ustrezni osebi +++ takoj ustavi delovanje naprave -lastnik opazi vendar se ne zmeni --ne opazi ---se ne zmeni ob opozorilu na napravo s strani sodelavca	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
5	**Privlačne tarče** *Attractive targets*	-varnostniki z obširnejšim dostopom -direktor in ostali vodilni s povečanim dostopom -ostali zaposleni s povečanim dostopom (informacijski oddelek, čistilke,...) -prenosni pomnilniški mediji -prenosni in stacionarni računalniki -pametni telefoni -tajni podatki/skrivnosti podjetja -podatki o poslovanju -gesla in uporabniška imena	*Trditve z odgovori na Likertovi lestvici.* Računalniški oddelek je bolj izpostavljen spletnim napadom kot oddelek v katerem sem zaposlen. Moj službeni računalnik lahko predstavlja vstopno točko za spletni napad na našo organizacijo.	*Trditve z odgovori na Likertovi lestvici.* S službenim računalnikom se pogosto priključim na domač wifi. S službenim računalnikom se pogosto priključim na javni wifi. Z osebnim računalnikom pogosto obiskujem intranet organizacije od doma. Z osebnim računalnikom pogosto obiskujem intranet organizacije z delovnega mesta.	*Intervju.* Za preverjanje in ugotavljanje dejanskega stanja je v tem primeru najprimernejši pogovor z zaposlenimi (intervjuji), ki vključuje tudi horizontalni nadzor – nadzor nad sodelavci.
6	**Poznavanje vlog v verigi zagotavljanja informacijske varnosti** *Knowledge of cyber security roles*	-oseba, kateri prijavimo IV incident (upravljalec sistema IV) -način predajanja informacij	Na kateri oddelek oz. na katero osebo se je potrebno obrniti v primeru suma informacijsko-varnostnega napada? Odgovor: _____ (zapiše izpraševanec)	*Trditve z odgovori na Likertovi lestvici.* Vloge se lahko zamenjajo s konkretnimi imeni v organizacijah (posamezniki imajo lahko več vlog). 1.a Za informacijsko varnost v celoti poskrbijo specialisti. 1.b Informacijska varnost se me kot zaposlenega ne tiče.	Poznavanje vsake vloge je potrebno preveriti ločeno. 1. Poznavanje lastne vloge se preverja z vsemi ostalimi preizkusi. 2. Poznavanje vloge direktorja informacijske varnosti preverimo tako, da opazujemo, ali in na kakšen način zaposleni posredujejo svoja opažanja (npr. očitne informacijsko-varnostne luknje) v povezavi z njihovim vsakdanjim

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				2.a Če opazim informacijsko-varnostno luknjo pri svojem delu, jo odpravim. 2.b Če opazim informacijsko-varnostno luknjo pri svojem delu, jo sporočim direktorju informacijske varnosti ali njegovi ožji ekipi, da jo odpravijo. 2.c Če opazim informacijsko-varnostno luknjo pri svojem delu, jo sporočim skrbniku incidentov, da jo odpravi. 2.d Če opazim informacijsko-varnostno luknjo pri svojem delu, jo sporočim skrbniku informacijske varnosti, da jo odpravi. 2.e Če opazim informacijsko-varnostno luknjo pri svojem delu, jo sporočim uvajalcu informacijske varnosti, da jo odpravi. 2.f Če opazim informacijsko-varnostno luknjo pri svojem delu, to delim s sodelavci in jo skupaj odpravimo. 3.a Ob okužbi s kripto-virusom ne bi potreboval pomoči ostalih. 3.b Ob okužbi s kripto-virusom bi se najprej obrnil na direktorja informacijske	delom direktorju informacijske varnosti oz. njegovi ekipi. Takih lukenj ne moremo kar podati, saj bi zahtevale spremembo načina dela zaposlenega. Namesto tega lahko z zaposlenim naredimo intervju v zvezi z njegovim vsakdanjim delom, pri katerem smo pozorni na njegova opažanja v zvezi z informacijsko varnostjo. Ko identificiramo njegova opažanja, ga povprašamo o tem, ali in kako je poskušal opažanja posredovati managementu. 3. Poznavanje vloge skrbnika incidentov preverimo z umetnim generiranjem problematične situacije. Na službeni računalnik zaposlenega namestimo navidezno škodljivo programsko opremo (npr. kripto-virus) in opazujemo, ali se bo obrnil na skrbnika incidentov. 4. Poznavanje vloge skrbnika informacijske varnosti preverimo z umetnim generiranjem problematične situacije. Poskrbimo, da službeni računalnik zaposlenemu javi napako, npr. da antivirusni program trenutno ne deluje ali da šifrirane povezave ni bilo mogoče vzpostaviti. Nato opazujemo, ali se bo zaposleni obrnil na skrbnika informacijske varnosti (to vlogo običajno opravljajo sistemski administratorji).

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				varnosti ali njegovi ožji ekipi, da ustrezno ukrepa. 3.c Ob okužbi s kripto-virusom bi se najprej obrnil na skrbnika incidentov, da ustrezno ukrepa. 3.d Ob okužbi s kripto-virusom bi se najprej obrnil na skrbnika informacijske varnosti, da ustrezno ukrepa. 3.e Ob okužbi s kripto-virusom bi se najprej obrnil na uvajalca informacijske varnosti, da ustrezno ukrepa. 3.f Ob okužbi s kripto-virusom bi se najprej obrnil na sodelavce, da skupaj ustrezno ukrepamo. 4.a Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, ne bi potreboval pomoči drugih. 4.b Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na direktorja informacijske varnosti ali njegovi ožji ekipi, da to uredi. 4.c Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na skrbnika incidentov, da to uredi.	5. Poznavanje vloge uvajalca informacijske varnosti preverimo tako, da opazujemo, na koga se zaposleni obrne, ko želi pridobiti več informacij v zvezi z informacijsko varnostjo, npr. če je v dvomih, ali gre za prevaro ali ne.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				4.d Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na skrbnika informacijske varnosti, da to uredi. 4.e Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na uvajalca informacijske varnosti, da to uredi. 4.f Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na sodelavce, da to skupaj uredimo. 5.a Če sem v dvomih, ali je nekaj sporno iz vidika informacijske varnosti, odgovor poiščem na internetu. 5.b Če sem v dvomih, ali je nekaj sporno z vidika informacijske varnosti, se za odgovor obrnem na direktorja informacijske varnosti ali njegovo ožjo ekipo. 5.c Če sem v dvomih, ali je nekaj sporno z vidika informacijske varnosti, se za odgovor obrnem na skrbnika incidentov. 5.d Če sem v dvomih, ali je nekaj sporno z vidika informacijske varnosti, se za	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				odgovor obrnem na skrbnika informacijske varnosti. 5.e Če sem v dvomih, ali je nekaj sporno z vidika informacijske varnosti, se za odgovor obrnem na uvajalca informacijske varnosti. 5.f Če sem v dvomih, ali je nekaj sporno z vidika informacijske varnosti, se obrnem na sodelavce in skupaj pridemo do odgovora.	
	Poznavanje tveganj, ki izhajajo iz dobavne verige, procesov upravljanja in praks *Knowledge of supply chain SCM information systems*	razumevanje meje lastne organizacije -informacijsko-varnostni standardi drugih niso enaki standardom v lastni organizaciji	*Trditve z odgovori na Likertovi lestvici.* Varnostne pomanjkljivosti informacijskega sistema naših dobaviteljev lahko predstavljajo varnostno grožnjo za naš informacijski sistem.	*Trditve z odgovori na Likertovi lestvici.* Varnostno opozorilo v informacijskem sistemu dobaviteljev mi da vedeti, da moram pri delu v tujem informacijskem sistemu delovati previdno. Pojav varnostnega opozorila v informacijskem sistemu dobaviteljev ne potrebuje moje pozornosti, ker ni del naše organizacije. Pojav varnostnega opozorila v informacijskem sistemu dobaviteljev sporočim pristojnim v naši organizaciji.	*Vzpostavitev problematične situacije.* Umetno generiranje problematične situacije: vzpostavitev simuliranega varnostnega opozorila v dobavno-nabavnem informacijskem sistemu. Opazovanje odzivanja pozameznika na simulirano varnostno obvestilo (npr. Ignoriranje, prebiranje, obveščanje zadolženih za informacijske sisteme).

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				Pojav varnostnega opozorila v informacijskem sistemu dobaviteljev javim organizaciji, ki je lastnica informacijskega sistema.	
8	**Sprejemanje etičnih odločitev** *Make ethical choices*	-koruptivnost -osebna integriteta -posredovanje osebnih podatkov znancem	Svoje vstopne podatke za službeni informacijski sistem lahko posredujem: - kateremukoli od mojih nadrejenih - kateremukoli od uslužbencev v našem podjetju - kateremukoli od vzdrževalcev informacijskih sistemov - le določenim osebam iz našega podjetja - le določenim od mojih nadrejenih - le določenim uslužbencem našega podjetja + nič od naštetega	*Trditve z odgovori na Likertovi lestvici.* Zaupne informacije z mojega področja pogosto posredujem svojim nadrejenim. Zaupne informacije z mojega področja včasih posredujem svojim nadrejenim. Zaupne informacije z mojega področja lahko zaupam svojim nadrejenim. Zaupne informacije lahko zaupam le sodelavcem z istega področja.	*Vzpostavitev problematične situacije.* Izpostavitev zaposlenega umetno generirani kritični situaciji. Situacija je lahko vzpostavljena s klicem "zunanjega" tehnika za informacijske tehnologije, ki zaposlenega za neko delo zaupno prosi za svoje uporabniško ime in geslo. Podobno je mogoče preveriti izdajanje uporabniškega imena in gesla neposredno ob testiranju. Zapiše se, če lahko v namene preverjanja kakovosti gesla zapišejo svoje uporabniško ime in geslo ter preverimo odziv.
9	**Pravilna raba informacijsko-varnostnih orodij in naprav** *Correct use of equipment and tools*	-antivirus -USB ključ -remote desktop -VPN -printer -datotečni strežniki -etc.	2. Kaj lahko vsebuje okužen USB ključ in kaj lahko stori vaši napravi? - vsebuje škodljivo programsko opremo in lahko fizično uniči mojo napravo + vsebuje škodljivo programsko opremo in lahko na mojo napravo	Ko mi javi antivirus, da ga je potrebno posodobiti naredim: a)takoj ga posodobim, b) prestavim posodobitev na kasneje in to storim ko imam čas, c) posodobim antivirus po nekaj prejetih obvestilih,	1. PREIZKUS (lažna najava posodobitve antivirusa- koliko časa oseba rabi, da ga posodobi); 2. PREIZKUS (tuj USB ključ in se preveri ali bi ga uporabil na svojem računalniku)-primer že izvedene raziskave https://zakird.com/papers/usb.pdf

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
			namesti zlonamerni program (virus, trojanski konj,...) -USB ključ že s samim vtikanjem ogrozi fizični obstoj naše naprave - vsebuje datoteke tipa HTML, EXE in lahko uničijo našo napravo	d)ignoriram obvestilo ; Kako pogosto uporabljate tuj USB na svojem računalniku? a)nikoli, b)občasno, c)skoraj vedno, d)vedno.	
10	**Odločanje o informacijsko-varnostnih prioritetah** *Decide priorities*	-odzivanje na sistemska varnostna opozorila -upoštevanje politike neglede na okoliščine	V službi ti med urejanjem pomembnih dokumentov na računalniku sodelavec preko Facebooka napiše »gori ti avto«. Kaj boš najprej naredil? - Takoj odhitim preverit svoj avto - Pokličem sodelavca, če je to res - Shranim datoteke na računalniku in odhitim do avta - Zaklenem zaslon in odhitim do avta - Poskrbim za »čisto mizo« in odhitim do avta + Shranim dokumente, zaklenem zaslon, poskrbim za »čisto mizo« in odhitim do avta - Shranim dokumente, poskrbim za »čisto mizo« in odhitim do avta	1. Ko mi računalnik javi sistemsko varnostno opozorilo naredim...?. a)posvetujem se s sodelavci kaj to pomeni in skupaj opravimo zadevo b)sam prepoznam pomembnost obvestila in reagiram brez posveta z drugimi c)sistemska varnostna opozorila ni nujno upoštevati, zato jih včasih prestavim »na kasneje« in se z njimi ukvarjam, ko imam čas d) o sistemsko varnostnem opozorilu obvestim informatike e)odgovor o resnosti sistemsko varnostnega opozorila poiščem na internetu in zadevo rešim sam	1. PREIZKUS (lažno sistemsko varnostno opozorilo-opazuje se reakcije zaposlenih)

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
11	**Varovanje in delo s podatki** *Protecting and Handling Data*	-mehanizmi varovanja podatkov (skrivanje, šifriranje, varnostne kopije) -varnostni kanali za pretakanje podatkov -kaj se zgodi v primeru kraje	1.Katere so vrste ogrožanja varnosti računalniškega sistema, ki ogrožajo tudi varnost podatkov in moramo biti zato na njih pozorni? + Prekinitev-motnja, Prisluškovanje-prestrezanje, sprememba-prikrojitev in ponarejevanje - Prekinitev delovanja, pridobivanje podatkov, spreminjanje podatkov in ponarejanja podatkov - Izklop naprave, spreminjanje naprave, prestrezanje in ponarejanje podatkov - Motnja delovanja, prilagajanje podatkov, dodajanje in prestrezanje	1. V primeru, da bi zaznal, da so podatki na mojem računalniku ogroženi bi se obrnil na: a) neposredno nadrejenega b) vodjo informatikov, c) šefa d) sodelavca na sosednji mizi; e) nobenega, ker podatki na mojem računalniku nikoli niso ogroženi	2. PREIZKUS (Ali znajo uporabljati mehanizme varovanja podatkov-vsaj osnovno)
12	**Poznavanje principov zasebnosti** *Knowledge of Privacy Principles*	-ime in priimek -osebni podatki osebno izkaznice -sorodstvo -zdravstvena kartoteka -zasebnost znotraj podjetja	1. Neznana oseba vas pokliče po telefonu in vas vpraša s kom posluje vaše podjetje ter kdo so vaši poslovni partnerji. Katera izmed možnosti je pravilna? - vse informacije dam, ker se naše podjetje ne ukvarja z nelegalnimi posli. + po telefonu ne dajemo nobenih informacij.	1. Kaj bi storili če bi delodajalec od vas zahteval geslo za mail ? A) ker sem odvisen od službe bi mu ga dal B) gesla nikakor nebi dal C) gesla mu nebi dal, dovolil bi mu pa vpogled v mail, D) geslo bi mu poslal zgolj preko zaščitenega kanala (kriptirano sporočilo).	Na delovnem mestu ne želim da me kdo nadzira - razen če je drugače opredeljeno v pogodbi o delovnem razmerju, svoji pravici o zasebnosti se nebom odpovedal za nobeno ceno. ---> EKSPERIMENT (šef pritisne na delavca - pazi MOBING!)

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
		-zasebnost v razmerju do poslovnih partnerjev	- meni se to ne more zgoditi - nič od naštetega		
13	**Prepoznavanje varnostnih incidentov** *Detect security breaches*	-ponarejene vstopne spletne strani -odzivanje na sistemska varnostna sporočila -socialni inženiring	Kaj od naštetega kaže na okužbo našega računalnika? +delovanje računalnika je upočasnjeno (počasi se opirajo, npr. Word dokumenti, počasi se zaganja brskalnik, počasi se zaganjajo drugi programi, računalnik se ugaša itd.) +ne morete se povezati v internet oz. vaša povezava je zelo počasna + ko se povežete v internet, se v brskalniku odprejo strani, ki jih sploh niste zahtevali + nekatere datoteke so izginile, kot posledica okvare datotečnega sistema +požarni zid in antivirusna zaščita sta deaktivirani - računalnik javlja obstoj škodljive kode - ne morete fizično dostopati do svojega računalnika	2. Kaj bi storili če se vam na ekranu pojavi sistemsko varnostno opozorilo? a)Takoj odreagiram b)odreagiram po dveh opozorilih, c)odreagiram po nekaj zaporednih opozorilih, d)sploh ne odreagiram-ignoriram obvestila.	1. PREIZKUS (Oblikovanje lažne spletne strani in preverimo ali vpišejo notri podatke); 2. PREIZKUS (Lažen varnostni incident in ugotavljamo kakšna je reakcija zaposlenih, ali sploh prepoznajo zadevo kot incident)

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
14	**Poznavanje brezžičnih omrežij in z njimi povezano varnostjo (se prenese na zadnjo kompetenco)** *Understanding Wireless Networks and Security*	-lažne dostopne točke -slabo varovana brezžična omrežja (WEP) -nezavarovana brezžična omrežja	1. Na kaj morate biti pozorni ko se povezujete v brezžično omrežje (WLAN / WIFI) Označite pravilne odgovore: + brezžično omrežje mora biti zaščiteno z geslom (WPA2) + prepričati se moram de gre za zaupanja vredno brezžično omrežje (da ni zlobni dvojček) - na nič. Vsa brezžična omrežja so varna + da če sem povezan v javno brezžično omrežje ne opravljam transakcij - brezžično omrežje mora imeti čim bolj močan signal.	4.a Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, ne bi potreboval pomoči drugih. 4.b Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na direktorja informacijske varnosti ali njegovi ožji ekipi, da to uredi. 4.c Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na skrbnika incidentov, da to uredi. 4.d Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na skrbnika informacijske varnosti, da to uredi. 4.e Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na uvajalca informacijske varnosti, da to uredi. 4.f Če mi računalnik javi, da šifrirane povezave ne more vzpostaviti, bi se takoj obrnil na sodelavce, da to skupaj uredimo.	Svoje brezžično omrežje bom zaščitil z varnostnimi mehanizmi - WPA2 (geslo). Nebom se povezoval v nezaščitena omrežja (omrežja ki so odprta), transakcije bom opravljal zgolj s pomočjo zaščitenih omrežij, če je potrebno nujno opraviti transakcijo bom vzpostavil svojo dostopno točko preko mobilnega omrežja. (EKSPERIMENT ---> vzpostavitev zlobnega dvojčka, spremljanje paketov - recimo z BURPSUITE)
15	**Razumevanje varnosti gesel** *Understanding password security*	-vpliv dostopa preko ugotovljenega gesla -težavnost ugotavljanja različno zapletenih gesel	1. kaj mislite, kje je najbolje shranjevati gesla ? - v za to namenjenih programih - v zvezku + nikjer ni pametno shranjevati gesla - v zvezku in shranjeno v šefovem trezorju.	1. kaj mislite, kaj je najslabši način menjave gesel ? A) To da gesla nikoli ne menjaš B) da zamenjaš zgolj eno črko C) To da ga menjaš vsako leto D) najslabšega načina menjave gesel ni	V prihodnje si več nebom shranjeval gesel v zvezek, sestavil bom nova gesla ki jih bom samo jaz poznal in ki bodo v moji glavi.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				1a gesla nikoli ne menjam 1b ko menjam geslo zamenjam zgolj eno črko 1c geslo menjam vsako leto 1d geslo menjam vsak mesec 1e imam zelo kompleksno geslo zato ga menjam redkeje	
16	**Oblikovanje, uporaba in upravljanje varnih gesel** *Password design, usage and management*	-pogostost menjavanja gesel -upravljanje gesel -skrivanje gesel -vpisovanje gesel (direktno oko ali keylogger) -uporaba več gesel / lastno geslo za vsako storitev -dolžina gesla -uporaba znakov -snovanje lažje pomnljivih	1. Kakšna so varna - unikatna gesla ? + Taka, ki jih je težko uganit in vključujejo črke, številke, znake, itd. - kratka, da si jih je lahko zapomnit - takih gesel ni - gesla, ki vsebujejo zgolj in samo šumnike.	1a uporabljam enotno geslo za vse storitve 1b za skoraj vse storitve uporabljam enotno geslo 1c imam 2 gesli. Za eno polovico uporabljam eno, za drugo pa drugo geslo 1d moja gesla se tudi ponavljajo 1e moja gesla se skoraj ne ponavljajo 1f za vsako storitev uporabljam različno geslo	Za svoje delovanje v organizaciji sestavljam gesla ki so zelo robustna in jih je nemogoče ugotoviti, izogibam se preprostim geslom, uporabljam kompleksna gesla z različnimi znaki in črkami. Skrbim za to, da se moja gesla ne bodo ponavljala. Gesel ne mislim menjati ker se mi do sedaj ni zgodilo še nič slabega.
17	**Razumevanje organizacijske varnostne politike** *Understanding organization's security awareness policy*	-zagotavljanje IV -vpliv IV na celotno podjetje -način varovanja podatkov -način ravnanja s podatki -avtentikacija oseb -vloge in odgovornosti -tajni podatki	Namen uvedbe varnostne politike v organizacijo je: - Spreminjanje navad zaposlenih - Zastraševanje zaposlenih - Preprečevanje izogibanju obveznostim s strani zaposlenih - Imeti pravni akt, na katerega se ob incidentu organizacija lahko sklicuje	Pomembno je, da zaposleni akt varnostne politike preuči ob prihodu v organizacijo. Popolnoma se strinjam-1 2 3 4 5-Popolnoma se ne strinjam Ob vsaki spremembi varnostne politike se zaposleni z njo seznanimo. Popolnoma se strinjam-1 2 3 4 5-Popolnoma se ne strinjam	1. Eksperiment: preverjanje znanja na podlagi različnih testov, ki jih razdelimo članom.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
18	**Organizacijska intelektualna lastnina** *Organizational intelectual property*	-zavedanje lastništva -nedeljenje organizacijske intelektualne lastnine	Kaj vam omogoča zaščita organizacijske intelektualne lastnine? -varno razkritje; -varno uporabo informacijsko-komunikacijske tehnologije; -da ste pravno priznani kot njen lastnik; -da imate dobiček od tržnega izkoriščanja; -preprečiti drugim, da bi jo nepooblaščeno uporabljali.	Kako močno je poskrbljeno za zaščito intelektualne lastnine v vaši organizaciji? Odlično-1 2 3 4 5-Zelo slabo	Kateri so glavni 3je ukrepi s katerimi zagotavljate zaščito intelektualne lastnine v organizaciji?
19	**Varne prakse za delo z elektronsko pošto** *Secure e-mail practices*	-pošiljanje osebnih podatkov po e-mailu -razkrivanje dodatnih podatkov -preverjanje istovetnosti pošiljatelja	Pošiljanje osebnih podatkov po elektronski pošti je povsem varno. DA / NE / ODVISNO KOMU POŠILJAM Pošiljanje elektronskih sporočil na način, da bi bili prejemniki vidni vsem naslovnikom je povsem dopustno. DA / NE / ODVISNO KOMU POŠILJAM	Z dobrim antivirusom sem zavarovan pred posledicami odprtja škodljive elektronske pošte Popolnoma se strinjam-1 2 3 4 5-Popolnoma se ne strinjam	Eksperiment s poskusom kako bi ravnala oseba v primeru, da dobi sumljivo elektronsko sporočilo z neznanim izvorom?
20	**Nepoznani pošiljatelji elektronske pošte in priponke** *Unknown email sources and attachments*	-vir/pošiljatelj -povezave v besedilu -priponke -slovnične napake -generičnost	Zakaj je poznavanje vsiljenih in škodljivih elektronskih sporočil pomembno? ohranjanje podatkov podjetja in preprečevanje vdora v podjetje, zato ker se v priponki nahaja škodljiva programska oprema, zato ker se lahko v sporočilo nahaja nekaj kar nas ne zanima	Ob prejemu sumljive elektronske pošte s priponko neznanega izvora le to odprem, saj lahko le tako sodelavce opozorim na morebitne nevarnosti Popolnoma se strinjam-1 2 3 4 5-Popolnoma se ne strinjam V primeru, da dobim sumljivo elektronsko pošto jo posredujem sodelavcu, saj je pomembno, da se odkrije njen	Vedno ko dobim elektronsko sporočilo, preverim, če elektronski naslov res poznam . DA/NE Kako bi ravnali v primeru, da dobite sumljivo elektronsko sporočilo neznanega izvora?

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
				izvor. Popolnoma se strinjam-1 2 3 4 5-Popolnoma se ne strinjam	
21	**Namestitev in uporaba protivirusnih programov** *Installing and using anti-virus software*	-nameščanje -varnostni pregledi (ob sumu in redni) -karantena -sandbox	Antivirusni programi se uporabljajo z namenom: - preprečevanja izgube podatkov - preprečevanja uporabe uporabnikovih dokumentov - hitrejšega in boljšega delovanja naprave (računalnika) - zaščita pred zlonamernimi kodami Računalniška programska oprema, ki jo namestite na vaš računalnik da ga zaščitimo pred krajo vaših osebnih podatkov ali postavlja zlonamerne programske opreme v računalniku: ANTIVIRUS	Preverim, da računalnik sploh ima antivirusni program. 1 2 3 4 5	Če vidim da program javi napako, se posvetujem z informatikom: DA/NE (preveriti z eksperimentom, če oseba sploh javi da nekaj na računalniku *ne štima*)
22	**Varno brskanje po spletu** *Secure browsing practices*	-https -sumljiva spletna mesta -ne/uporaba občutljivih podatkov -glej zgornje kompetence	Spletno stran prepoznamo za varno če je zgoraj znak: - - - -	Za brskanje po spletu uporabljam povsem nevarna gesla in uporabniška imena: DA/NE	Ob opozorilu spletnega brskalnika da spletna stran ni varna in da je možnost, da se bo naložila škodljiva programska oprema potrdim vstop in nadaljujem: 1 2 3 4 5

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
23	**Identifikacija spletnih groženj** *Identify online threats*	-prenos sumljivih datotek -prenos "programov za prenos" -vnašanje osebnih podatkov -vnašanje bančnih podatkov -strani, ki nudijo "brezplačne" storitve za obogatitev -strani s pornografijo -strani, ki prodajo različne drugače nedostopne izdelke	Katere so najpogostejše spletne grožnje: - Spam - Okužbe - Phishing - Vdor - Kraja podatkov Na katerih spletnih straneh so okužbe najpogostejše: - Spletne strani s pornografijo - Spletne strani z brezplačnimi igrami - Spletne strani ponudnikov dnevnih novic - Spletne strani socialnih omrežij	Če mi spletni brskalnik prikaže, da sem zadel nagrado, kliknem posredujem podatke in čakam na nagrado: DA/NE	Ob prihodu v podjetje preverim varnostno politiko, ter se posvetujem z drugimi, ki so zaposleni v podjetju: 1 2 3 4 5
24	**Varnost mobilnih naprav vključno z BYOD** *Mobile device security including BYOD*	-uporaba kriptiranja -uporaba varnega dostopa do svetovnega spleta -uporaba požarnega zidu in antivirusnih programov -redni antivirusni pregledi -programsko in fizično zaklepanje naprave s kriptiranjem celotnega sistema -razlikovanje med osebno in službeno mobilno napravo	Kateri od ukrepov skrbijo za varnost naše naprave v sistemu: Preden se podjetje odloči za model BYOD mora storiti pomemben napredek na področju: - Izobraževanja zaposlenih - Financ (nakup telefonov, računalnikov, tablic) - Varnostne politike Postopek posega v programsko kodo sistema iPhone OS, s katero omogočimo funkcije, ki jih zaradi določenih razlogov originalna različica ne ponuja, se imenuje: JAILBREAK	Svoje naprave uporabljam tako doma v zasebne in v službi za službene zadeve DA/NE	Strogo ločim zasebno od službenega 1 2 3 4 5

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
26	**Razumevanje politike čiste mize** *Understanding clean desk policy*	-prazna miza -zaklepanje predalov -zaklepanje računalnika -zaklepanje/zapiranje pisarne (če je možno)	1. Kakšen je pomen te politike? a) miza je s tem vedno čista in pospravljena **b) občutljivi podatki so varno shranjeni** c) delo je tako boljše in bolj organizirano 2. Katere nevarnosti se pojavijo če vam neavtorizirana oseba gleda pod prste med uporabo IKT? - Zloraba podatkov, kraja identitete, finančna izguba...	2. Ko odrabim nosilce z občutljivimi podatki jih shranim v: a) predal b) pustim jih na mizi c) odnesem jih domov **d) zaklenem jih v varovan prostor**	3. Eksperiment: preverimo ob koncu delovnika, kako zaposleni poskrbijo za podatke s katerimi delajo.
27	**Gledanje čez ramo** *Shoulder surfing*	-prepoznavanje situacij -vidnost zaslona v odsevnih površinah -vidnost zaslona čez okno -vidnost zaslona izza hrbta -vidnost zaslona preko kamere	1. Kdaj vse lahko pride do prestrezanja podatkov z zaslona? - Ob neugasnjenem zaslonu, ob vidnosti zaslona skozi okno, preko kamere, izza hrbta, v odsevnih površinah. 2. Kako lahko preprečimo prestrezanje podatkov z zaslona? - Pazimo na to, da je zaslon ugasnjen, ko zapuščamo prostor in da je obrnjen stran od vidnega polja neavtorizirane osebe, ki je v bližini.	2. Ob prihodu neavtorizirane osebe v prostor, zaslon vedno ugasnem. 1 2 3 4 5 (nikoli – vedno)	3. Eksperiment: preverimo kako poskrbijo za varovanje podatkov ob prihodu neznane osebe v prostor.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
28	**Brskanje po smeteh** *Dumpster diving*	-sprotno uničevanje zavrženih tajnih podatkov -pravilno ravnanje s smetmi (zaklepanje, po postopku, pazimo da jih kdo ne odnese) -pravilno brisanje elektronskih podatkov	1. Kdo lahko izkoristi podatke najdene v smeteh? a) čistilka b) socialni inženir c) sodelavec **d) vsi našteti** 2. Katere podatke, najdene v smeteh, lahko napadalec izkoristi za napad? - Vsi osebni in organizacijski podatki so lahko pomembni pri pripravi in izvedbi napada 3. Kako se znebimo podatkov na računalniku, da se jih ne more več pridobiti nazaj? a) Datoteko izbrišemo (vržemo v smeti) b) Datoteko trajno izbrišemo c) Za izbris uporabimo program	1. Kaj storiš z dokumenti/podatki, ki jih ne potrebuješ več? (več možnih odgovorov) a) odvržem jih v smeti b) sploh jih ne zavržem **c) preden jih zavržem, uporabim rezalnik papirja** **d) podatke odstranim pri pooblaščenih organizacijah**	3. Eksperiment: ob koncu delovnika preverimo ali ustrezno zavržejo podatke.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
29	**Preprečevanje napadov socialnega inženiringa** *Protecting against social engineering attacks*	-predstavljanje kot dober prijatelj; nekdo z dovoljenim dostopom/avtoriteto -fizični napadi oseb -napadi preko telefona -napadi preko e-pošte -napadi preko socialnih omrežji (pogovori in pritisk množice), -razpoznavni znaki (hitenje, napadalnost, spreminjanje tematike pogovora) -upoštevanje postopkov avtentifikacije	1. Kateri so razpoznavnih znaki, da smo mogoče v interakciji s socialnim inženirjem? (vsaj 5) - Nenapovedanost, Hitenje/nuja; ustrahovanje; hvaljenje s poznanstvi/uporaba avtoritete nadrejenih; nenavadna vprašanja, ki bi se lahko navezovala na informacije o organizacijskih virih; izmikanje učinkoviti avtentikaciji; laskanje in pihanje na ego ob prošnji; napačna poimenovanja; pri pisni interakciji pa tudi slovnične napake	1. Kaj storiš, ko preko maila dobiš elektronsko sporočilo, ki zahteva tvoje osebne podatke? a) svoje podatke vpišem, kjer to zahteva **b) preden vpišem svoje podatke, preverim ali je elektronsko sporočilo verodostojno** c) svojih podatkov nikakor ne vpisujem 2. K vam pristopi oseba, ki ste jo v organizaciji že videli in vas v imenu nadrejenega prosi da mu posredujete varovane informacije. Kaj naredite? a)posredujem informacije b) Preverim identiteto osebe in jo vprašam zakaj se informacije potrebujejo c) Pri nadrejenemu preverim, ali naj se informacije posreduje	3. Eksperiment: izvedemo lažni napad in preverimo kako se odzivajo zaposleni.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
30	**Varna raba socialnih omrežij** *Secure use of social media*	-pomembnost vsakdanjih in za varnost nepomembnih informacij objavljenih na socialnih omrežjih (rudarjenje in analize teh informacij na socialnih omrežjih) -varnostne nastavitve in ukrepi na socialnih omrežjih -katerih informacij ne smemo objavljati na socialnih omrežjih -možno izsiljevanje -zasledovanje -drugo škodovanje	1. Katere podatke se lahko razbere iz digitalnih slik objavljenih na socialnih omrežjih? (več možnih odgovorov) a) Identiteto avtorja slike **b) Datum in čas slike** **c) GPS lokacijo slike** **d) Model in vrsto kamere** e) Vse zgoraj našteto 2. Da na socialnemu omrežju objavljeni podatki izginejo iz interneta je treba: a) Izbrisati objavo b) Izbrisati profil na socialnem omrežju c) Kontaktirati socialno omrežje in jih prositi, da izbrišejo vse podatke o tebi **d) Nič od naštetega**	2. Na delovnem mestu lahko brezskrbno uporabljam socialna omrežja. 1 2 3 4 5 (nikoli – vedno)	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
31	**Kontrola dostopa** *Access control*	-fizični nadzor prostorov z omejenim dostopom (prostori kjer se nahajajo zaupne ali občutljive informacije ali sredstva za dostop do informacijske infrastrukture) -nadzor nad namizjem računalnika	1. Kdo ima dostop do tvojega službenega računalnika? a) Pomočnik b) Sodelavci na istem področju **c) IT uslužbenci** d) Interni vzdrževalci e) S tvoje strani pooblaščene osebe f) Nihče od naštetih 2. V sobo s strežnikom je dovoljeno: a) dostavljavcem b) strankam **c) IT uslužbencem** d) zaposlenim e) internim vzdrževalcem f) vodilnim uslužbencem; Podatki podjetja: -se lahko preventivno hranijo na USB pomnilniku zaposlenega +se ne kopirajo -se lahko povzamejo z zaslonsko sliko -se procesirajo s programi, ki podpirajo urejanja tega tipa podatka	1. Neka oseba želi vstopiti v varovan prostor, kjer so občutljivi podatki. Kaj storiš? a) vprašam jo kdo je, si to zapišem in spustim naprej b) povprašam osebo po osebnem dokumentu in jo spustim naprej **c) preverim ali ima oseba pravico dostopanja do varovanega prostora in identificiram osebo z osebnim dokumentom** 2. Neavtorizirano osebo se lahko spusti v zaščiten prostor, če je prostor pod tehničnim nadzorom a) Da b) Ne	1. Eksperiment: Nastavimo neznano osebo, ki želi priti v varovan prostor in preverimo reakcijo in postopanje zaposlenih.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
32	**Odzivanje na zaznane grožnje** *Responding to perceived threats*	-prekinitev IV napada: fizični/kibernetski -pošta -klic -prisoten storilec -računalnik -konkretne grožnje (če dobiš spam je čisto nekaj drugega kot če hoče nekdo v strežniško sobo)	1. Kateri podatki so nujni pri prijavljanju vsiljenih prenosov? (možnih več odgovorov) a) opis incidenta **b) IP številka/naslov izvora** c) opis škode **d) datum in točen čas dogodka**	1. Na koga bi se obrnili ob varnostnem incidentu? a) na vodjo informacijskega oddelka b) na sodelavca c) na nobenega, saj lahko sam razrešim situacijo Odvisno od organizacije, nekateri zahtevajo, da kontaktiraš neposredno nadrejenega 2. Kaj je prva stvar, ki bi jo naredili, če bi zaznali, da je bila mobilna naprava izgubljena ali ukradena? a) poklicati policijo b) poklicati organizacijo in jih obvestiti o kraji c) poskušati zakleniti in/ali izbrisati podatke na mobilni napravi d) spremenimo gesla, ki smo jih imeli shranjene na napravi e) poskušati geolocirati napravo in jo dobiti nazaj Razen, če je politika organizacije, da se najprej obvesti njih in da ukrepajo oni	3. Eksperiment: Sprožimo lažni preplah in spremljamo odzive zaposlenih.

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
33	**Varnost organizacijske IKT izven delovnega mesta** *Security of organizational ICT outside of the workplace*	-varnost vsega, kar se odnese iz organizacije, to so USB ključi, mobilne naprave, prenosniki, gesla, informacije idr. -prepoznava groženj izven organizacije (kraja, poškodovanje, izguba) -ukrepi za zagotavljanje fizične varnosti IKT (zaklepanje, skrivanje,...) -postopki za ublažitev posledic odtujitve ali izgube IKT (kriptiranje, zaklepanje z geslom)	1. Kateri od naslednjih varnostnih ukrepov pomagajo pri zagotavljanju varnosti IKT izven delovnega mesta? (možnih več odgovorov) **a) napravo imamo vedno pri sebi** b) naredimo varnostno kopijo podatkov, ki jo imamo vedno pri sebi **c) zaklepanje naprave, ko je ne uporabljamo** **d) namestitev alarma na mobilno napravo** e) naprava mora biti vedno na vidnem mestu f) vse zgoraj našteto 2. Katere varnostne ukrepe bi uporabil/a da bi zaščitil/a delovno IKT in informacije izven delovnega mesta? (vsaj 5) - Naprava je vedno pri meni; uporaba ohranjevalnikov zaslona; vklopljeno avtomatično zaklepanje naprave; izdelava varnostne kopije podatkov, ki jo hranimo ločeno od naprave; izogibanje uporabi v javnih prostorih, še posebej v gnečah; uporaba programske opreme za varovanje (npr. alarmi, oddaljeno brisanje naprave), fizično varovanje naprav in nosilcev ko niso pri nas (sef, ključavnice).		

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
			3. Kraja organizacijske IKT napadalcu omogoča dostop do (možnih več odgovorov) a) osebnih podatkov b) vseh gesel, ki jih imamo na napravi c) organizacijske informacijske infrastrukture d) naprav sodelavcev **e) vse zgoraj našteto**		

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
34	**Varne prakse za oddaljeno delo** *Secure practices for working remotely*	-vrste napadov in potencialne posledice pri uporabi oddaljenega dostopa (MitM) -varovanje komunikacijskih kanalov (VPN - SSL, RAS, IPSec; šifriranje) -zavedanje delovne okolice -nevarnosti uporabe lastne IKT za oddaljeno dostopanje do organizacijskih informacijskih sredstev -VPN, šifriranje, zavedanje delovnega prostora, kraja, izguba	1. Napad človeka v sredini (ang. man in the middle) pomeni: (znanje) a) da napadalec poseže v poslane podatke z namenom okužbe naprave b) **da napadalec prisluškuje izmenjavi in spreminja podatke poslane preko oddaljenega dostopa** c) da oseba, ki ji posredujemo informacije za stranke ali predstojnika to znanje izkoristi za napad na organizacijsko IKT 2. Čemu se moramo izogibati za varovanje oddaljenega dostopa? **a) Uporabi v javnih prostorih** **b) Povezovanje na javne dostopne točke, ki imajo znanega lastnika (npr. bari)** c) Rednemu spreminjanju naprave s katero se povežemo na organizacijske strežnike d) Vse zgoraj našteto 3. Kateri varnostni ukrepi so pomembni za zagotavljanje varnosti informacij pri uporabi oddaljenega dostopa? a) Povezovanje na le znane dostopne točke (bi rekel da je razlika med znano in varno dostopno točko) **b) šifriranje podatkov** **c) Robusten sistem avtentikacije** **d) Uporaba naprave s posodobljeno protivirusno zaščito**	Ko se nam mudi, se lahko pozabi na nekatere aspekte varovanja oddaljenega dostopa, kot je na primer uporaba javnih dostopnih točk v interes hitrosti 1 2 3 4 5 (1 nikoli, 5 vedno)	

ŠT	IME	PODROČJA	ZNANJE	NAMERA	VEDENJE
			e) Da preko oddaljenega dostopa ne pošiljamo zelo pomembnih informacij f) Minimalna uporaba tehnologije g) Vse zgoraj našteto		