

Tematska delavnica za ravnatelje KIBERNETSKA VARNOST, NUJA VSAKDANA.

Kdaj: **sreda, 12. maj 2021**

Kako: na daljavo, z uporabo aplikacije **Zoom**

Izvajalec: **dr. Blaž Markelj, Fakulteta za varnostne vede, Univerza v Mariboru**

Za koga: za **ravnatelje in strokovne delavce, ki se ukvarjajo s tem področjem**

VSEBINA DELAVNICE

Varnost predstavlja temelj človekovega delovanja. To kot družba v teh časih dojemamo še toliko bolj. Delovanje osnovnih, človeku popolnoma vsakdanjih in rutinskih del, se je v celoti prestavilo iz fizičnega v kibernetiski prostor. Zagotavljanje varnosti pa ni več samo podobno tistemu, ko preprosto zaklenemo vrata sobe, stanovanja ali hiše, ampak je treba za zagotavljanje zasebnosti in nedotakljivosti posameznika poznati in vedeti bistveno več o informacijsko-komunikacijski tehnologiji, grožnjah, ki delujejo v kibernetiskem prostoru, in o tem, kako se pred njimi zaščititi. Celotna komunikacija v šolstvu in visokem šolstvu v času epidemije poteka v kibernetiskem prostoru. To predstavlja enormno količino podatkov, ki tako ali drugače opredeljujejo posameznika, ki je v to komunikacijo vključen. Vsaka naprava, s katero se posameznik priključi v kibernetiski prostor in v komunikacijo, ne predstavlja zgolj enega kanala komunikacije, ampak lahko več. Če ponazorimo s primerom: organizacija je imela eno pisarno, danes v primeru dela od doma pa ima organizacija toliko dislociranih pisarn, kot je v nekem trenutku zaposlenih, ki se priključilo v kibernetiski prostor in med seboj komunicirajo. Zagotavljanje kibernetiske varnosti mora potekati na vseh nivojih. Osnovna podlaga za zagotavljanje kibernetiske varnosti je znanje o delovanju tehnologije, o tem, kje obstajajo grožnje in kako se pred njimi zavarovati. Predvsem pa je treba ugotoviti, kateri podatki so za posameznika pomembni in kako jih zavarovati. Ni rečeno, da bo podatek, ki je odtujen oziroma objavljen v kibernetiskem prostoru danes, zaznamoval posameznika takoj, to se lahko zgodi šele čez nekaj let. Ljudje težko ponotranjimo grožnje, ki jih ne vidimo in so lokacijsko težko določljive, čas njihove uresničitve pa je nedoločljiv. Govorimo o grožnjah, ki na posameznika pretijo v kibernetiskem prostoru. Zato je posamezniku težko razumeti tveganja, ki obstajajo ob uporabi tehnologije in podatkov. Še težje pa je razumeti potrebne investicije, ki jih morata posameznik in organizacija vložiti, da zmanjšata stopnjo tveganja uresničitve teh groženj. Investicije niso nujno finančne narave, govorimo lahko tudi o izobraževanjih, vpeljavi politik, ki urejajo področje informacijske varnosti v organizaciji, itn. Pomembno je poznati tudi scenarije, kako ravnati v primeru uresničitve katere od kibernetiskih groženj, na koga se lahko v slovenskem prostoru obrnemo, kaj lahko naredimo kot posameznik in zakaj se je bolje obrniti na ustrezne inštitucije.

POTEK DELAVNICE

Delavnica bo potekala od 9. do 13. ure.

PRIJAVA IN UDELEŽBA

Prijava na delavnico preko **KATIS-a do ponedeljka, 10. maja 2021.**

Udeležba je brezplačna.

Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega socialnega sklada, projekt Krepitev kompetenc strokovnih delavcev na področju vodenja inovativnega vzgojno-izobraževalnega zavoda v obdobju od 2018 do 2022.