KATALOG ZNANJA

1. IME PREDMETA

KIBERNETSKA VARNOST IN ETIČNI HEKING

2. CILJI PREDMETA

Splošni cilji predmeta so:

- razvijati sposobnost za uporabo informacijske tehnologije pri delu;
- ozavestiti pomeni spremljanja novosti na področju kibernetske varnosti;
- razvijati sposobnosti za skupinsko delo;
- razvijati sposobnost sprejemanja odločitev;
- upoštevati zakonske in panožne zahteve za zaščito občutljivih informacij in ohraniti zaupanje strank.

Specifično strokovno usmerjeni cilji so:

- razumeti uporabo triade (CIA) (zmogljivost, celovitost, razpoložljivost);
- zagotoviti varno shranjevanje, nadzorovati dostop in preprečiti nepooblaščeno obdelavo, prenos ali brisanje podatkov;
- izobraziti uporabnike o najboljših varnostnih praksah in morebitnih grožnjah za izboljšanje njihove ozaveščenosti in budnosti;
- zaščititi omrežja in računalniško strojno opremo pred krajami, grožnjami ali razkritjem občutljivih podatkov;
- izvajati ukrepe za zaustavitev nepooblaščenega dostopa;
- prepoznati in oceniti varnostna tveganja;
- integracija varnostnih praks in kontrolnikov za preprečevanje ranljivosti.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu si študenti poleg generičnih pridobijo naslednje kompetence:

1. ohranjanje točnosti in zanesljivosti podatkov in sistemov, zaščita pred nepooblaščenimi spremembami ali nedovoljenimi posegi;
2. poznavanje in uvajanje penetracijskega testiranja;
3. poznavanje tehnik hekerskega napada;
4. načrtovanje in uvajanje varnosti v računalniških sistemih;
5. poznavanje in analiziranje etičnih in pravnih posledic informacijskih sistemov.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
Študent:	Študent:
1. Ohranjanje točnosti in zanesljivosti podatkov in sistemov, zaščita pred nepooblaščenimi spremembami ali nedovoljenimi posegi	
• razloži pojme zaupnost, celovitost in razpoložljivost in njihovo povezljivost; • razlikuje različne vrste incidentov; • razloži namen zaščite občutljivih podatkov;	• zbira podatke (npr. imena omrežij in domen, poštni strežnik) za boljše razumevanje delovanja ciljnih sistemov in njihovih morebitnih ranljivosti;

• pojasni pomen standardov, zakonov in varnostnih politik; • pojasni lastnosti in potek asimetričnega in simetričnega šifriranja ter ročnega šifriranja, podpisovanja, dešifriranja in preverjanja podatkov; • navede varnostne prakse za preprečevanje nepooblaščenega dostopa do kritičnih sistemov in podatkov; • pojasni pomen ozaveščenosti o informacijski varnosti ter uveljavljanja pravilnikov in standardov; • opredeli zaščitne ukrepe, ki bi jih bilo treba vzpostaviti za obravnavanje groženj in tveganj.	• pregleda kodo aplikacije, da oceni, kako program deluje med izvajanjem; • odkrije in popravi ranljivosti pri izvajanju kode; • konfigurira nastavitve WAF in druge varnostne rešitve aplikacij za odpravljanje ranljivosti in zaščito pred prihodnjimi napadi; • uporabi socialni inženiring; • meri zmožnost organizacije, da takoj uporabi varnostne popravke za ranljivosti sistemov in programske opreme; • spremlja omrežni promet; • zaščiti omrežje pred morebitnimi grožnjami, zlonamerno programsko opremo in napadi z lažnim predstavljanjem; • prepreči kršitve varstva podatkov.
2. Poznavanje in uvajanje penetracijskega testiranja	
• opiše prepoznavanje tveganj s penetracijskim preskušanjem; • razišče, kako so strukturirani penetracijski preskusi; • opiše vrste (test črne škatle, bele škatle ali sive škatle) in stopnjo preskušanja; • razloži preskušanje ranljivosti omrežij.	• poišče pomanjkljivosti in ranljivosti s penetracijskim preskušanjem; • zaznava varnostne vrzeli v pravilnikih in procesih; • izvaja simulirane lažne predstavitve; • preveri veljavnost varnostnih kontrolnikov in pravilnikov; • simulira scenarij napada in preizkusi zmogljivosti odziva na incidente; • meri čas, potreben za zaznavanje kibernetskega incidenta od trenutka, ko se zgodi; • meri čas, potreben za odziv na kibernetski incident in njegovo zajezitev, ko je ta odkrit.
3. Poznavanje tehnik hekerskega napada	
• navede področja, kjer bi bili lahko občutljivi podatki ogroženi v primeru kibernetskega napada; • opiše tehnike izkoriščanja ranljivosti; • razloži vdor v omrežje prek vrat in pojasni protiukrepe za zaščito naprav ali omrežij v primeru vdora; • opiše preverjanje identitete uporabnikov in naprav; • navede najpogostejše napake in ranljivosti sistemov.	• izdela načrt za izgradnjo virtualnega hekerskega okolja in ga izvede; • izkoristi vbrizgavanje SQL za iskanje baz podatkov, preglednic in občutljivih podatkov, kot so uporabniška imena, gesla; • odkrije odprta vrata, nameščene storitve in ranljivosti v računalniških sistemih; • izvede pogoje za učenje, vdiranje, preskušanje in zaščito spletnih aplikacij pred obstoječimi in nastajajočimi varnostnimi grožnjami.
4. Načrtovanje in uvajanje varnosti v računalniških sistemih	
• razloži stalni razvoj računalniških sistemov z izboljšanimi metodami šifriranja, trajno šifriranje z obstoječimi metodami; • pojasni oceno tveganja; • razloži pomen varnostne politike in vsebino dokumenta varnostne politike; • opiše neprekinjeno poslovanje in zmogljivosti vnovične vzpostavitve po katastrofi;	• s primerno metodologijo izvede oceno tveganja za fizično in informacijsko varnost sistemov na praktičnem primeru podjetja; • izdela dokument varnostne politike organizacije ter uporabi potrebne programske in strojne metode za njeno izvajanje;

• pojasni omejevanje dostopa do informacij v podjetju; • razloži mehanizme preverjanja pristnosti uporabnikov in nadzora dostopa; • opiše varno uvedbo storitev v oblaku in hkrati učinkovito upravlja podatke v okolju oblaka.	• z uporabo varnostnih protokolov, šifriranjem in nadzorom dostopa zagotovi zaupnost in celovitost podatkov; • na različnih operacijskih sistemih izvaja napredne varnostne ukrepe, kot so sistemi za zaznavanje in preprečevanje vdorov, požarni zidovi, protivirusna programska oprema in varni protokoli; • zagotavlja neprekinjeno poslovanje z izvajanjem načrtov za neprekinjeno poslovanje in obnovo po nesreči; • izvaja proaktivno odkrivanje groženj, uporabo napredne analitike, strojnega učenja in umetne inteligence za prepoznavanje skritih groženj in ranljivosti.
5. Poznavanje in analiziranje etičnih in pravnih posledic informacijskih sistemov	
• razloži koncepte pričakovane zasebnosti uporabnika (Privacy by design); • pojasni etični kodeks in njegove prednosti ter pomanjkljivosti; • opiše pomen etike informacijskih sistemov; • opiše postopke odločanja, ki so v etičnih okvirih; • opiše ključne etične vidike v predstavljenih tehnologijah; • opiše ključne lastnosti etičnega hekerja; • pojasni sistem za upravljanje informacijske varnosti v poslovnem subjektu; • opredeli mednarodne standarde na področju varnosti informacijskih sistemov.	• obnovi sistem po delovanju kibernetskega napada za zagotovitev neprekinjenega poslovanja in pripravi poročilo o napadu.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 72 ur (24 ur predavanj, 48 ur laboratorijske vaje).

Število ur samostojnega dela: 78 ur (30 ur študij literature, 8 ur vaj, 40 ur projektna naloga).