KATALOG ZNANJA

1. IME PREDMETA

VARNOST RAČUNALNIŠKIH OMREŽIJ IN SISTEMOV

2. SPLOŠNI CILJI

Splošni cilji predmeta so:

- predstaviti pomen varnosti računalniških omrežij v podjetjih;
- predstaviti zgodovinski razvoj varnosti omrežij;
- naučiti o tveganjih ob uporabi omrežij (npr. izguba podatkov, vdori, zmanjšanje zmogljivosti, i. d.);
- naučiti za strokovno izražanje;
- usposobiti za razreševanje težav, kritično mišljenje, analitično razmišljanje, sprejemanja odločitev, učinkovite komunikacije ter digitalno pismenost;
- naučiti za načrtovanje in določanje prioritet, samoupravljanje, samostojno učenje ter samorefleksijo;
- usposobiti za projektno vodenje.

Specifično strokovno usmerjeni cilji so:

- poznati temeljne principe varnosti računalniških omrežij ter primere dobrih praks;
- obvladati delovanje omrežnih naprav (npr. usmerjevalniki, stikala, i. d.) ter pojme kot so na primer požarni zid, zgoščevalna funkcija MD5, sloj varnih vtičnic SSL, VPN, AES, SHA, RSA, DES, 3DES in druge;
- poznati kriptografijo z javnim ali zasebnih ključem;
- poznati vrste napadov na omrežja (npr. phishing, napadi DNS, SQL-vrinjanje, Denial of Service – DoS, Man-In-the-Middle, i. d.);
- ukrepati s protiukrepi za izboljšavo varnosti računalniških omrežij (npr. računalništvo v oblaku, sistemi PaaS, IaaS, i. d.);
- administrirati varnostne sisteme omrežnih naprav;
- implementirati varnostne ukrepe za omrežja v podjetjih;
- implementirati nastavitve za omrežne naprava in okolja računalniških omrežij;
- izvajati varnostne preglede, izboljšave ter popravila in iskanje tveganj.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu študenti poleg generičnih pridobijo naslednje kompetence:

1. nadzorovanje varnostnih procesov za zaščito na različnih operacijskih sistemih;
2. analiziranje standardov, protokolov ter temeljnih principov varnosti računalniških omrežij;

3. izdelovanje varnih računalniških omrežij za rabo v podjetjih;
4. konfiguriranje varnostnih ukrepov za računalniška omrežja v podjetjih;
5. izvajanje analiz ter pregledov na omrežjih z uporabo testnega načrta.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
1. Nadzorovanje varnostnih procesov za zaščito na različnih operacijskih sistemih	
● opiše računalniški sistem kot nabor procesov in objektov ter našteje pristope in stopnje zaščite; ● definira pomen zaščite domen (npr. uporabniki, procesi, procedure, i. d.); ● razčleni pravice do dostopa in definira različne načine organizacije zaščite (npr. hierarhične, matrike dostopa, i. d.); ● ovrednoti problematiko vdorov v sisteme ter razlikuje med napadi na operacijske sisteme, programsko opremo in omrežja.	● izdela zaščito za razne objekte v različnih sistemih s pomočjo sistemske programske opreme različnih operacijskih sistemov (npr. Windows Server, Linux, i. d.). ● prepozna grožnje ter ustrezne ukrepe (npr. za trojanske konje, hrošče, viruse, i. d.); ● namesti in uporabi programsko opremo za zaščito in odpravljanje nevarnosti (npr. požarni zid, protivirusna programska oprema, nadzor pred vdori, anti-spyware, i. d.).
2. Analiziranje standardov, protokolov ter temeljnih principov varnosti računalniških omrežij	
● opiše zgodovinski razvoj varnosti računalniških omrežij (ustanovitev Skupine za odziv v nuji – CERT); ● utemelji vrste varnostnih naprav za omrežja; ● analizira pogosta ter napredna tveganja pri varnosti omrežij (npr. zlonamerna programska oprema, ranljivosti na omrežjih, vdori, i. d.); ● razčleni naprave ter postopke za varnost računalniških omrežij (varnostno ogrodje, avtentikacija, avtorizacija); ● ovrednoti ter razčleni varnostne protokole (npr. MD5, SSL, VPN, AES, SHA-1/2, RSA, DES, 3DES, IPSec, DNS, DHCP, HTTP, HTTPs, FTP, FTPs, POP3, SMTP, IMAP, i. d.); ● ovrednoti različne vrste kriptografije za računalniška omrežja (npr. javni, zasebni	● izdela preglednico v kateri izpostavi razlike med glavnimi varnostnimi protokoli za omrežja; ● izdela predstavitev o pomenu varnosti računalniških omrežij v podjetjih.

ključi Caesar Cipher, Vigenere, Hash, i. d.).	
3. Izdelovanje varnih računalniških omrežij za rabo v podjetjih	
● opiše glavne pomisleke o praktičnem namenu računalniških omrežij ter scenarije za njihovo uporabo; ● analizira zahteve za strojno ter programsko opremo za določeno; ● ovrednoti namen in zahteve varnih omrežij za vnaprej določen scenarij.	● izdela načrt varnega omrežja za vnaprej določen scenarij ter namen uporabe ter ga realizira; ● izdela skripte/datoteke/slike zaslona varnostnih nastavitev za omrežja, ter predstavi komentarje;
4. Konfiguriranje varnostnih ukrepov za računalniška omrežja v podjetjih	
● razčleni različne varnostne nastavite za računalniška omrežja; ● definira vlogo požarnih zidov, usmerjevalnikov, stikal, prehodov, varnostnega prenosnega sloja SSL, protokola http in FTP ter nosilce varnostnih kopij; ● analizira pomen pojma kakovosti storitve (Quality of Service – QoS) ter kako je povezan z varnostnimi nastavitvami računalniških omrežij. ● ovrednoti različne vrste kriptografije za varna omrežja.	● implementira nastavitve nadzor omrežne varnosti za vnaprej določen scenarij.
5. Izvajanje analiz ter pregledov na omrežjih z uporabo testnega načrta	
● opiše postopek izvedbe testiranja omrežnih naprav (npr. požarni zid, strežniki, krmilniki domene, strežniki za e-pošto, usmerjevalniki, stikala ter prehodi, i. d.); ● analizira podatke, primerja dejanske rezultate s pričakovanimi; ● ovrednoti načrt, izdelavo ter implementacijo nastavitev za testiranje omrežja.	● izdela načrt pregledovanja omrežnih naprav, ● izvede postopek celostnega testiranja računalniškega omrežja; ● izdela dokumentacijo testiranja računalniškega omrežja ter poda priporočila za izboljšavo varnosti v podjetju.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 60 ur (30 ur predavanj, 30 ur seminarskih vaj).
Število ur samostojnega dela študenta: 150 (študij literature, delo s programsko in strojno opremo, delo z besedilom in preglednicami, priprava pisne dokumentacije, …).