PITANJA ZA ZSIS

1. **Definiraj sigurnost te opiši temeljne zahtjeve**

   Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima. Tri temeljna zahtjeva su: tajnost – pristup podacima moraju imati samo autorizirane osobe, cjelovitost – očuvanje integriteta podataka i raspoloživost – podaci moraju stalno biti dostupni, a kako dodatni mogu se navesti i autentičnost i neporecivost.

2. **Navedi kategorije zaštite te za svaku navedi nekoliko konkretnih primjera.**

   Kategorije zaštite se mogu podijeliti u 3 grupe:
   a. fizičke kontrole – nadzorne kamere, zaštitari,..
   b. tehničke kontrole – vatrozid, antivirus,..
   c. administrativne kontrole – politike, pravilnici, procedure,..

3. **Što sve spada u organizacijske faktore sigurnosti?**

   U organizacijske faktore spadaju: nedostatak budžeta, kratki rokovi, nedostatak podrške menadžmenta, nedostatak odgovarajuće procjene rizike, nepostojanje sigurnosnih procedura…

4. **Zašto su sistemski i operativni zapisi bitni za sigurnost informacijskog sustava te što sve treba osigurati da bi oni bili sigurni i upotrebljivi?**

   Takvi zapisi su bitni jer omogućavaju rekonstrukciju i detekciju anomalija događaja, a nužno ih je držati na zasebnom mjestu kako bi se zaštitili od neovlaštenih izmjena i satovi zapisa moraju biti usklađeni kako bi se rekonstrukcija mogla pravilno odraditi.

5. **Koji je temeljni alat kojeg koristi CISO i zašto (što mu on omogućuje)?**

   Temeljni alat CISO-a je upravljanje rizicima što uključuje procjenu i prioritizaciju rizika te na temelju prioriteta odlučiti daljnje postupanje s rizicima. Upravljanje rizicima omogućava da se odrede rizici kojima je izložena organizacija.

6. **Korisnik bpadmin kreirao je bazu podataka nastavabp te u njoj tablice student (matBr, ime, prezime, pbr, adresa) i ispit (…). Svima je ukinuo dozvolu za spajanje na bazu te je korisniku PUBLIC ukinuo sve dozvole za shemu public. Napiši naredbe kojima će adminbp korisniku novak omogućiti:**
   a. **spajanje na nastavabp bazu te korištenje sheme public**

      GRANT CONNECT ON DATABASE nasavabp TO admindb;
      GRANT USAGE ON SCHEMA public TO admindb;
   b. **pregled svih podataka u tablici student osim adrese, uz mogućnost dodjele te dozvole drugim korisnicima**

      GRANT SELECT(metBr, ime, prezime, pbr) ON student TO admindb WITH GRANT OPTION;

   c. **pregled, unos, izmjenu te brisanje podataka u tablici ispit**

      GRANT SELECT, INSERT, UPDATE, DELETE ON ispit TO admindb;

   d. **izmjenu podataka u tablici student, ali samo za one studente koji su iz Zadra (poštanski broj im je 23 000)**

      CREATE VIEW studentiZadar AS
        SELECT * FROM student WHERE pbr = 23000
          WITH CHECK OPTION;
      GRANT UPDATE ON studentiZadar TO admindb;

   e. **korištenje već definirane uloge nastavnik**

      GRANT nastavnik to admindb;

7. **Bell – La Padula model pripada…**
   a. diskrecijskom upravljanju pristupom
   b. mandatnom upravljanju pristupom
   c. upravljanju pristupom baziranom na ulogama

8. **Kako izgleda tipičan zapis audit trail datoteke?**

Audit trail treba sadržavati podatke o tome koji događaj se dogodio, tko ga je proizveo i vrijeme događanja.

9. **Što omogućuju pohranjene procedure, a da nije moguće odraditi s dozvolama nad tablicama i virtualnim tablicama? Napiši naredbu kojom se korisniku novak dodjeljuje dozvola izvođenja procedure izračunaj.**

Pohranjene procedure omogućavaju zaštitu podataka od neovlaštene uporabe na razini funkcija. Korisniku se dodijeli dozvola za obavljanje procedure, a time je precizno određen način na koji se obavljaju operacije nad podacima, za razliku od davanja dozvola za UPDATE i INSERT.

10. Objasni strong-star-property u mandatnoj politici pristupa u bazama podataka

Korištenjem strong-star-property korisnik ne može čitati ni pisati po objektima koji imaju ili veću ili manju razinu sigurnosti već isključivo na svojoj sigurnosnoj razini.

11. Definirajte pojam sigurnosti

Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima.

12. Navedite i vrlo kratko opišite tri temeljna zahtjeva sigurnosti.

Tri temeljna zahtjeva su:

tajnost – pristup podacima moraju imati samo autorizirane osobe,

cjelovitost – očuvanje integriteta podataka i

raspoloživost – podaci moraju stalno biti dostupni za pristup

13. Što je prijetnja i ranjivost

Prijetnja i ranjivost su dva preduvjeta potrebna za nastanak incidenta. Prijetnja je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu. Ranjivost je pogreška ili slabost u sustavu koja se može iskoristiti za narušavanje sigurnosti.

14. Navedite svrhu voditelja sigurnosti (CISO-a)

CISO nadzire i koordinira aktivnosti vezane uz sigurnost, inicira primjenu dobrih praksi vezanih uz sigurnost i ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

15. Ukratko objasnite što je sigurnosni zahtjev a što slučaj zloporabe te kako se modeliraju

Sigurnosni zahtjevi su nefunkcionalni zahtjevi sustava vezani uz sigurnost, primjer takvih zahtjeva su zahtjevi za kontrolom pristupa, zahtjevi za enkripcijom i sl. Slučajevi zloporabe uključuju neautoriziran dohvat i izmjenu podataka te uskraćivanje usluge. Modeliraju se nekim od procesa poput SQUARE, TRIAD, UML grafovima, use casevima i sl.

16. Navesti koja je svrha voditelja sigurnosti (CISO) u organizacijama.

CISO nadzire i koordinira aktivnosti vezane uz sigurnost, inicira primjenu dobrih praksi vezanih uz sigurnost i ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

17. Koji je temeljni akt na kojemu se temelji sigurnost organizacije te što je njegova svrha?

Politika sigurnosti informacijskog sustava, krovni dokument koji definira što za informacijski sustav znači da je siguran.

18. Zašto je potrebno nadzirati rad voditelja sigurnosti te tko obavlja tu zadaću?

Potrebno je nadzirati CISO-a zbog sprječavanja potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja i zbog poboljšanja njegovog rada.

19. Objasnite osnovne postavke BLP modela (Bell- La Padula Security Model) i ilustrirajte primjerom.

BLP model se temelji na dva načela koja osiguravaju tajnost:

Simple property – subjekt može čitati iz onih objekata kojima je njegova klasa pristupa dominantna i

star-property – subjektu može pisati u objekt samo ako je njegova klasa pristupa dominantna.

20. Objasnite što je sigurnosna politika.

Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti.

21. Objasnite razliku između otvorene i zatvorene politike upravljanja pristupom.

Kod otvorene politike generalno je pristup podacima dozvoljen, no pristup je uskraćen za podatke za koje postoje dodatne zabrane. Kod zatvorene politike pristup podacima je dozvoljen ukoliko korisnik ima pozitivnu dozvolu.

22. Objasnite:

a. Što je sigurnost programske podrške?

Sigurnost je kontinuirani proces čijim se provođenjem osigurava određeno stanje sustava koje je definirano zahtjevima.

b. Što je sigurna programska podrška?

Za podršku možemo reći da je sigurna kada su svi sigurnosni zahtjevi ispunjeni.

c. Kada je sigurnost softverski problem?

Sigurnost postaje softverski problem radi prevencije iznimki u slučaju da dođe do pogrešaka u projektiranju, razvoju, ugradnji, nadogradnji ili održavanju aplikacije.

d. Čime se bavi softverska sigurnost?

Softverska sigurnost se bavi softverom i osigurava da pri napadu nastavlja ispravno raditi.

23. Opišite diskrecijsko i mandatno upravljanje pristupom u bazama podataka.

Diskrecijsko upravljanje pristupom je način ograničavanja pristupa objektima na temelju identiteta i/ili grupa kojoj oni pripadaju. Mandatno upravljanje je sigurnosna politika na razini sustava koja određuje tko ima pravo pristupa, a na vlasnik objekta.

24. Za svaku od navedenih faza sigurnog životnog ciklusa navedite ključne prakse:

a. **Zahtjevi**
   Definiranje sigurnosnih zahtjeva, procjena rizika
b. **Dizajn**
   Modeliranje prijetnji, analiza površine napada
c. **Implementacija**
   Statička analiza
d. **Verifikacija**
   Dinamička analiza, fuzz testiranje
e. **Objava**
   Plan odgovora na incidente, finalni pregled