MI 2021/2022

1. Detektirajte sigurnost te navedite i opišite temeljne zahtjeve.

Sigurnost je kontinuirani proces čijim provođenjem se osigurava određeno stanje (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim zahtjevima. Kada su oni ispunjeni onda kažemo da je sustav siguran, u suprotnom kažemo da se desio incident tj. da je narušena sigurnost.

Temeljni zahtjevi su: Tajnost/Povjerljivost (zaštita tajnih informacija od napada), Cjelovitost/Integritet (zaštita od neovlaštenih izmjena), Raspoloživost (zaštita od uskraćivanja dostupnosti informacija ovlaštenim korisnicima)

2. Navedite podjelu kontrola u grupe te za svaku grupu navedite nekoliko konkretnih primjera kontrole.

Fizičke: kamere, zaštitari, blindirana vrata,

Tehničke: kriptografija, vatrozidi, sustavi za detekciju napada,

Administrativne kontrole: politike, pravilnici, različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašat, kako uređaji moraju biti podešen…

3. Navedite organizacijske faktore koji utječu na sigurnost informacijskog sustava.

Organizacijski faktori: Nedostatak budžeta, Kratki rokovi, Nedostatak podrške menadžmenta, Nedostatak odgovarajuće procjene rizika, Nepostojanje sigurnosnih procedura

4. Zašto su sistematski i operativni zapisi bitni te što sve treba učiniti kako bi bili sigurni i upotrebljivi?

Jer omogućavaju rekonstrukciju događaja i detekciju neočekivanih događaja. Nužno je držati ih na zasebnom mjestu radi prevencije neovlaštenih izmjena. CISO definira način upravljanja sistemskih i operativnim zapisima: vrši nadzor, te u manjim organizacijama moguće analizira logove te traži očitovanja. Današnji trend je da tvrtke sigurnost nadziru u Sigurnosno operativnim centrima (SOC), koji kontinuirano prate poboljšavaju sigurnosno stanje i sprečavaju, detektiraju sve sigurnosne incidente.

5. Koji je temeljni alat koji CISO koristi za svoj rad i zašto (što mu omogućava)?

Upravljanje rizicima (proces propisan internim aktima). Omogućava da se odrede rizici kojima je izložena organizacija. Tu spadaju procjena rizika, mogućnost prioritizacije rizika, te na temelju toga odluka pristupanja identificiranim rizicima (da li će se prihvatiti, ovladati ili prenijeti na treću stranu, no konačnu riječ u toj odluci ima uprava organizacije).

6. Korisnik *adminbp* kreirao je bazu podataka *nastavabp* u sustav PostgreSQL te je u navedenoj bazi kreirao sljedeće tablice: *student* i *ispit* (s nekim atributima). Korisnik *adminbp* ukinuo je korisniku PUBLIC dozvolu spajanja na bazu podataka *nastavabp* i sve dozvole za shemu public u *nastavabp*, a zatim je kreirao korisnika *novak*. Napiši naredbe kojima će *adminbp* omogućiti korisniku *novak* sljedeće:

a) Spajanje na bazu *nastava* i korištenje sheme public i *nastavabp:*
   GRANT CONNECT ON DATABASE nastavabp TO novak;
   GRANT USAGE ON SCHEMA public TO novak;
   GRANT USAGE ON SCHEMA public TO novak;
b) Pregled svih podataka u tablici *student* osim adrese, s tim da *novak* može dodjeljivati tu dozvolu ostalim korisnicima:
   GRANT SELECT(matBr, ime, prez, pbr) ON student TO novak WITH GRANT OPTION;
c) Pregled, unos, izmjenu i brisanje svih podataka u tablici *ispit:*
   GRANT SELECT, INSERT, UPDATE, DELETE ON ispit TO novak;
d) Izmjenu svih podataka u tablici *student*, ali samo za one n-torke koje se odnose na studente iz Zadra (poštanski broj = 2300):
   CREATE VIEW zadrani AS
      SELECT * FROM student WHERE pbr = 2300 WITH CHECK OPTION;
   GRANT UPDATE on zadrani TO novak;
e) Korištenje već kreirane uloge *nastavnik:*
   GRANT nastavnik TO novak;

7. Model Bell-la Padula (BLP) spada u koje upravljanje pristupom?:

a) diskrecijsko upravljanje pristupom,
b) mandatno upravljanje pristupom,
c) upravljanje pristupom temeljeno na ulogama

8. Što sadrži tipični zapis datoteke za pamćenje rada korisnika (auditing)?

SQL naredba koja se izvršava, mjesto s kojeg je upućen zahtjev (terminal, IP adresa računala), identifikator korisnika koji je pokrenuo operaciju, datum i vrijeme operacije, n-torke, atributi na koje se zahtjev odnosi, stara vrijednost n-torke, nova vrijednost n-torke

9. Što omogućuju pohranjene procedure u provođenju sigurnosne politike, a da se to ne može riješiti samo dozvolama nad tablicama i nad virtualnim tablicama? Napišite naredbu kojom će se korisniku *novak* omogućiti korištenje procedure *izracunaj*.

Omogućuje zaštitu podataka od neovlaštene uporabe na razini funkcija.

GRANT EXECUTE ON izracunaj TO novak

10. Objasnite princip strong-star-property kod mandatne politike pristupa u bazama podataka.
Korisnik može pisati isključivo na svojoj razini, nije moguće pisati u objekte koje mogu pročitati subjekti s nižom razinom - spriječeno propuštanje informacija.