Ishod 1 (12 bod, 30 min)

1. **(1,5) Objasnite što su tri aspekta sigurnosti (CIA)? Objasnite 2 najvažnija načina napada na dostupnost?**

Povjerljivost – zaštita podataka od neovlaštenog pristupa

Integritet – zaštita podataka od izmjena

Dostupnost – osiguravanje da su podaci dostupni ovlaštenim korisnicima

Dva najvažnija napada na dostupnost su: Ransomware i DDoS.

2. **(1) Što je sigurnosni rizik? Zašto je procjena rizika važna?**

Mogućnost da prijetnja iskoristi ranjivost, te potencijalno ošteti podatke/informacije . Procjena rizika je važna jer pomaže u otkrivanju i prioritetiziranju prijetnji kako bi se smanjile štete.

3. **(2) Kratko objasnite korake u procjeni rizika? Što je rezultat procjene rizika?**

Identifikacija prijetnji i ranjivosti > Procjena utjecaja i vjerojatnosti >Određivanje rizika >

Predlaganje mjera za smanjenje rizika

Rezultat je popis i procjena rizika s prijedlozima kontrole.

4. **(2) Što su kontrole? Kakve vrste načina djelovanja postoje? Zašto je potrebno postići balans u definiranju kontrola?**

Kontrole su mjere za smanjenje rizika.
Vrste: preventivna, detektivna i korektivna.
Balans je potreban kako bi se trošila optimalna količina resursa na zaštitu.

5. **(1) Objasnite utjecaj Paretovog načela na izbor sigurnosnih kontrola. Pojasnite navedeno na Australskom kontrolnom okviru.**

Paretovo načelo kaže da 20% kontrola može riješiti 80% problema.
Australski kontrolni okvir primjenjuje ovo načelo fokusirajući se na najvažnije kontrole za smanjenje rizika. (Patch Aplications, Operating System, ...)

6. **(1) Koje su prednosti i nedostaci kvalitativne procjene rizika?**

Prednosti kvalitativne procjene: jednostavna i brza.
Nedostaci: subjektivna je i manje precizna od kvantitativne procjene.

7. **(1) Objasnite SANS (CIS) Top 20. Kako je podijeljen i zašto?**

Popis 20 ključnih sigurnosnih kontrola podijeljenih u osnovne, temeljne i organizacijske kontrole. Podjela pomaže u lakšoj implementaciji prema važnosti i složenosti.

8. **(2) Što je prijetnja? Kratko objasnite kategorije prijetnji.**

Svi negativni događaji koji mogu uzrokovati štetu na informacijskom sustavu, te se time narušava CIA trokut.
Kategorije: prirodne (poplava), ljudske (hakiranje), tehničke (kvar opreme), ...

9. **(1,5) Kratko objasnite ISO 27001. Koja je prednost/korist od njegovog uvođenja?**

Međunarodni standard za upravljanje informacijskom sigurnošću (lista kontrola koja se trebaju implementirati).
Prednost: poboljšava sigurnost, smanjuje rizike i povećava povjerenje klijenata.

Dodatno

1. **Zašto se CIS Top 18 smatra jednim od najboljih sigurnosnih kontrolnih okvira? Na koji način slijedi Paretov princip?**

Zato što jer je jasan, jednostavan i pokriva najvažnije dijelove kibernetičke sigurnosti s jasnim redoslijedom koraka. Podijeljen je u tri skupine prema veličini organizacije (IG1, IG2, IG3). Prati Paretov princip jer pokazuje da mali broj kontrola (20%) pruža veliku većinu zaštite (80%).

2. **Što je sigurnosni rizik? Kratko pojasnite faze upravljanje rizikom?**

Svaki događaj koji može ugroziti povjerljivost, cjelovitost ili dostupnost podataka (CIA).

Faze su:

- **Procjena** - otkrivanje rizika i preporuke za kontrole
- **Tretiranje** - određivanje prioriteta i primjena kontrola
- **Evaluacija i nadzor** - praćenje rizika kroz vrijeme

3. **Opisati kvalitativni izračun rizika.**

Kvalitativni izračun rizika određuje koliko nam nešto vrijedi u poslovnom smislu, a ne samo po novčanoj vrijednosti.

Primjer: računalo košta 1000 €, ali zbog važnih podataka na njemu za nas vrijedi puno više.