# Pitanja iz Sigurnosti Informacijskih Sustava

## Općenito o fizičkoj sigurnosti

1. Što podrazumijeva fizička sigurnost u kontekstu informacijskih sustava?

Fizička sigurnost obuhvaća mjere zaštite ljudi, prostora, opreme i resursa informacijskog sustava od fizičkih prijetnji poput krađe, požara, poplava, vandalizma ili neovlaštenog pristupa

2. Koji su osnovni ciljevi fizičke sigurnosti?

Zaštita ljudi i imovine. Sprječavanje neovlaštenog fizičkog pristupa. Osiguranje kontinuiteta rada informacijskog sustava.Smanjenje rizika od oštećenja ili gubitka podataka.

3. Koje su najčešće prijetnje fizičkoj sigurnosti informacijskih sustava?

Krađa i vandalizam. Požar, poplava, potres i druge prirodne nepogode. Neovlašteni fizički pristup prostorijama ili uređajima. Sabotaža i namjerno uništavanje opreme.

4. Kako fizička sigurnost doprinosi cjelokupnoj informacijskoj sigurnosti?

Bez fizičke sigurnosti, logičke i softverske mjere zaštite gube smisao. Ako netko može fizički ukrasti server ili disk, može zaobići sve digitalne zaštite. Dakle, fizička sigurnost je temelj cjelokupne informacijske sigurnosti.

5. Koja je razlika između fizičke i logičke sigurnosti?

Fizička sigurnost štiti prostorije, uređaje i infrastrukturu. Logička sigurnost štiti podatke i sustave putem softverskih i mrežnih mehanizama (lozinke, enkripcija, autentikacija).

6. Koje su osnovne komponente fizičke sigurnosti?

Kontrola pristupa (kartice, brave, biometrija). Videonadzor i alarmni sustavi. Vatrogasna i protupožarna zaštita. Klimatizacija i UPS (rezervno napajanje). Fizičke barijere (ograde, sefovi, zaključane prostorije).

7. Kako se procjenjuje rizik u fizičkoj sigurnosti?

Identificiraju se mogući incidenti (npr. požar, krađa). Analizira se vjerojatnost pojave i posljedice. Procjenjuje se izloženost i ranjivost sustava. Na temelju toga donose se mjere zaštite i planovi prevencije.

8. Koji su primjeri fizičkih kontrola pristupa?

Kartični sustavi i PIN kodovi. Biometrija (otisak prsta, skeniranje lica, šarenice). Sigurnosne brave i sefovi. Zaštitari i portiri. Videonadzor.

9. Kako se fizička sigurnost integrira u plan kontinuiteta poslovanja?

U plan kontinuiteta uključuju se sigurnosne mjere koje omogućuju nastavak rada u slučaju incidenta – npr. zaštita podatkovnog centra od požara i poplava, rezervno napajanje, sigurnosne kopije opreme i prostora, plan evakuacije i oporavka.

10. Koji su izazovi u implementaciji fizičke sigurnosti u velikim organizacijama?

Velik broj lokacija i zaposlenika. Visoki troškovi opreme i održavanja. Usklađivanje sigurnosti i produktivnosti (da zaštita ne ometa rad). Upravljanje različitim razinama pristupa. Potreba za stalnim ažuriranjem i usklađivanjem s propisima.

## Definicije pojmova i tehnologija

1. Što je kontrola pristupa i koje vrste postoje?

Kontrola pristupa je skup mehanizama i postupaka koji određuju tko smije ući u određeni prostor ili koristiti određene resurse. Vrste: Fizička kontrola pristupa (brave, kartice, biometrija). Logička kontrola pristupa (lozinke, PIN-ovi, autentikacija na računalnim sustavima).

2. Što je biometrijska autentifikacija i kako se koristi u fizičkoj sigurnosti?

Biometrijska autentifikacija koristi jedinstvene fizičke ili bihevioralne karakteristike osobe za potvrdu identiteta. Primjeri: otisak prsta, prepoznavanje lica, skeniranje šarenice, prepoznavanje glasa.  
U fizičkoj sigurnosti koristi se za **sprječavanje neovlaštenog pristupa** prostorijama i opremi.

3. Koja je uloga RFID tehnologije u kontroli fizičkog pristupa?

RFID (Radio Frequency Identification) omogućava identifikaciju putem kartica ili tagova s čipom koji odašilju signal čitaču. Koristi se za: Elektroničke kartice za ulaz/izlaz. Evidenciju dolazaka i odlazaka zaposlenika.

Automatsko otvaranje vrata ili rampi.

4. Što je CCTV i kako doprinosi sigurnosti?

CCTV (Closed-Circuit Television) je videonadzorni sustav. Doprinosi sigurnosti jer omogućuje: Nadzor prostorija i perimetra u stvarnom vremenu. Snimanje dokaza u slučaju incidenta. Prevenciju kriminala jer djeluje odvraćajuće.

5. Koja je razlika između pasivnih i aktivnih sigurnosnih sustava?

Pasivni sustavi: ne reagiraju automatski, već služe kao prepreka ili sredstvo dokazivanja (npr. brave, sigurnosne kamere). Aktivni sustavi: aktivno reagiraju na prijetnju (npr. alarmi, automatske brave, protupožarni sustavi).

6. Što su sigurnosne barijere i gdje se primjenjuju?

Sigurnosne barijere su fizičke prepreke koje sprječavaju ili otežavaju pristup. Primjena: Ograde i zaštitne mreže oko objekata. Sigurnosna vrata i sefovi. Stupići i rampe na parkiralištima.

7. Kako funkcionira sustav elektroničke kontrole pristupa?

Korisnik se identificira (kartica, PIN, biometrija). Sustav provjerava ovlaštenja u bazi podataka. Ako je pristup dopušten → vrata se otključavaju. Evidencija pristupa se bilježi radi nadzora i kasnije analize.

8. Što je sigurnosna zona i kako se definira?

Sigurnosna zona je fizički prostor s određenom razinom zaštite, gdje se primjenjuju posebne sigurnosne mjere. Definira se prema: Osjetljivosti podataka ili opreme u zoni. Razini prijetnji. Potrebnim kontrolama pristupa (npr. podatkovni centar vs. recepcija).

9. Koji su standardi i norme relevantni za fizičku sigurnost (npr. ISO 27001)?

ISO/IEC 27001 – standard za upravljanje informacijskom sigurnošću, uključuje i fizičku sigurnost. ISO/IEC 27002 – smjernice za implementaciju kontrola (uključuju fizičku i okolišnu sigurnost). EN 50132 – standardi za CCTV sustave. Nacionalni propisi (npr. zakoni o zaštiti na radu, zaštiti od požara).

10. Što je tailgating i kako se može spriječiti?

Tailgating je neovlašten ulazak osobe u zaštićeno područje tako da uđe “u stopu” iza ovlaštene osobe. Prevencija: Turniketi ili sigurnosna vrata koja propuštaju samo jednu osobu. Biometrija uz kartični sustav.

Edukacija zaposlenika da ne propuštaju druge osobe. Videonadzor i zaštitari.

## Građevine, okoliš i prostorije

1. Koji su kriteriji za odabir lokacije podatkovnog centra?

Udaljenost od područja sklonih poplavama, potresima, požarima ili industrijskim nesrećama. Stabilna i pouzdana opskrba električnom energijom. Dostupnost više neovisnih internetskih i komunikacijskih veza. Dobra prometna povezanost, ali ne previše izložena (npr. ne odmah uz autocestu). Mogućnost fizičke zaštite i kontrole pristupa.

2. Kako okolišni faktori (poplave, potresi) utječu na fizičku sigurnost?

Poplave mogu uništiti opremu, prekidati napajanje i dovesti do gubitka podataka. Potresi mogu fizički oštetiti zgrade, ormare i servere. Zbog toga se poduzimaju mjere poput podignutih podova, jačih temelja, otpornijih ormara i redundancije opreme na više lokacija.

3. Koje mjere se poduzimaju za zaštitu server sobe?

Kontrola pristupa (kartice, biometrija). Videonadzor i alarmni sustavi. Klimatizacija i kontrola vlage. Detekcija i gašenje požara (plin, CO₂, praškasti sustavi – nikako voda). Rezervno napajanje (UPS, agregat).

4. Kako se osigurava fizička sigurnost u zgradama s više korisnika?

Ograničeni pristup samo ovlaštenim osobama (posebne kartice, zone). Odvojene sigurnosne zone za različite organizacije. Videonadzor zajedničkih prostora. Posebno osigurani prostori za servere i komunikacijsku opremu.

5. Koja je uloga dizajna prostorije u sigurnosti informacijskih sustava?

Optimalan raspored opreme sprječava pregrijavanje i olakšava održavanje. Kabeli i ormari trebaju biti organizirani i označeni. Zidovi, vrata i podovi trebaju imati vatrootpornost i zvučnu izolaciju. Sigurnosne barijere (npr. dvostruka vrata, zaključani ormari).

6. Kako se štite komunikacijski ormari i mrežna oprema?

Zaključavanje ormara i pristup samo ovlaštenim osobama. Smještaj u sigurnosnim zonama (server sobe). Videonadzor i senzori otvaranja. Oznake i uredno vođenje kablova za sprječavanje manipulacije.

7. Koje su preporuke za sigurnosnu rasvjetu oko objekta?

Vanjska rasvjeta koja pokriva sve prilaze i kritične točke. Automatsko paljenje (senzori pokreta ili vremenski program). Kombinacija rasvjete i kamera za bolju vidljivost. Rezervno napajanje da svjetla rade i tijekom nestanka struje.

8. Kako se provodi nadzor nad ulazima i izlazima iz objekta?

Evidencija pristupa (kartice, biometrija). Videonadzor svih ulaza i izlaza. Portir ili zaštitar na glavnom ulazu.

Sustavi koji onemogućuju “tailgating” (npr. turniketi, sigurnosna vrata).

9. Koji su standardi za vatrootpornost prostorija s kritičnom opremom?

EN 1047-2 – standard za zaštitu IT prostorija od požara. ISO/IEC 27001 i 27002 – propisuju mjere zaštite, uključujući i protupožarnu sigurnost. Nacionalni propisi o zaštiti od požara. Preporuka: zidovi i vrata minimalno 60–120 minuta otpornosti na požar.

10. Kako se provodi fizička sigurnost u mobilnim ili privremenim objektima?

Korištenje kontejnerskih podatkovnih centara (modularnih, lako premjestivih). Pojačane brave, prijenosni alarmni sustavi i videonadzor. Zaštita od vremenskih uvjeta (krovne i bočne zaštite). Sigurnosne kopije podataka na udaljenim lokacijama (u slučaju oštećenja).