# Pitanja iz Sigurnosti Informacijskih Sustava

## Općenito o fizičkoj sigurnosti

1. 1. Što podrazumijeva fizička sigurnost u kontekstu informacijskih sustava?

* Mjere koje sprječavaju neovlašteni fizički pristup informacijama, opremi i prostorijama.
* Zaštitu od prijetnji kao što su krađa, oštećenja, požari i prirodne nepogode.
* Primjenu zaštitnih sustava poput kontrole pristupa, alarma i nadzora kako bi se osigurala sigurnost resursa i ljudi.

1. 2. Koji su osnovni ciljevi fizičke sigurnosti?

* Sprečavanje neovlaštenog ili nasilnog ulaska osoba u zaštićene prostore.
* Zaštita imovine, opreme i podataka od krađe, oštećenja ili gubitka.
* Otkrivanje, sprječavanje i reagiranje na sigurnosne prijetnje i zlouporabe.

1. 3. Koje su najčešće prijetnje fizičkoj sigurnosti informacijskih sustava?

* Prirodne nepogode poput poplava, potresa, požara, kao i ekstremnih vremenskih uvjeta koji mogu oštetiti opremu i podatke.
* Ljudske prijetnje, uključujući krađu, sabotažu, nemar, socijalni inženjering i neovlašteni pristup prostorijama i uređajima.
* Nepredviđene situacije poput kvarova na sustavima (električna mreža, plin, itd.) koje mogu uzrokovati oštećenje informacijskih resursa.

1. 4. Kako fizička sigurnost doprinosi cjelokupnoj informacijskoj sigurnosti?

* Fizička sigurnost osigurava da samo ovlaštene osobe imaju pristup informacijskim sustavima i opremi.
* Sprječava neovlašteni pristup, krađu, oštećenje opreme i podatka.
* Stvara sigurno okruženje koje podržava druge sigurnosne mjere i smanjuje rizik od sigurnosnih incidenata.

1. 5. Koja je razlika između fizičke i logičke sigurnosti?

* Fizička sigurnost obuhvaća mjere za sprječavanje neovlaštenog fizičkog pristupa opremi, prostorima i informacijama, uključujući zaštitu od krađe, oštećenja i prirodnih nepogoda.
* Logička sigurnost odnosi se na zaštitu pristupa informacijama i sustavima putem softverskih i mrežnih kontrola, kao što su lozinke, autentifikacija, enkripcija i upravljanje pristupnim pravima.
* Fizička sigurnost je temelj za logičku sigurnost jer se sprječava fizički pristup koji bi omogućio zaobilaženje logičkih kontrola.

1. 6. Koje su osnovne komponente fizičke sigurnosti?

* Pasivne mjere: korištenje arhitekture, okoliša i osvjetljenja za olakšanu detekciju upada i prijetnji.
* Aktivne mjere: sustavi i tehnike za detekciju i reakciju na prijetnje, uključujući nadzorne kamere, alarmne sustave, kontrolu pristupa i zaključavanje opreme.
* Fizički aspekt: zaštita imovine, primjerice zapošljavanje zaštitara.
* Tehnički aspekt: osiguranje usluga i elemenata koji podržavaju IT, poput sigurnosti soba s poslužiteljima.

1. 7. Kako se procjenjuje rizik u fizičkoj sigurnosti?

* Identifikacija rizika: prepoznavanje svih mogućih prijetnji, izvora opasnosti i njihovih posljedica, kao i postojećih zaštitnih mjera koje mogu smanjiti rizik.
* Analiza rizika: određivanje vjerojatnosti pojave prijetnji i njihovih potencijalnih posljedica, te evaluacija učinkovitosti zaštitnih mjera.
* Vrednovanje rizika: usporedba razine rizika s prihvatljivim kriterijima radi donošenja odluka o daljnjim sigurnosnim aktivnostima i potrebnim mjerama za smanjenje rizika.

1. 8. Koji su primjeri fizičkih kontrola pristupa?

* Vrata s ključevima ili lozinkama koja ograničavaju ulaz u prostorije.
* Elektroničke kartice za kontrolu pristupa i čitači kartica.
* Biometrijski sustavi kao što su skeneri otiska prsta, prepoznavanje lica ili šarenice oka.
* Sigurnosne ograde, barijere i čuvarska služba na ulazu u objekt.
* Video nadzor i alarmni sustavi za otkrivanje neovlaštenog pristupa.
* Zaključavanje ormara i serverskih ormana kao dodatna zaštita osjetljive opreme

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

* Fizička sigurnost štiti ključne resurse i infrastrukturu od prijetnji kao što su krađe, požari i prirodne katastrofe, osiguravajući time neprekinuto poslovanje.
* Mjere fizičke sigurnosti, poput kontrole pristupa i nadzora prostorija, uključene su u planove oporavka i oporavak nakon incidenata.
* Integracija fizičke sigurnosti omogućava pravovremenu reakciju i smanjenje šteta u kriznim situacijama, čime se skraćuje vrijeme zastoja i osigurava kontinuitet poslovnih procesa.

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

* Kompleksnost organizacijske strukture i nedostatak jasne odgovornosti za fizičku sigurnost, što otežava učinkovitu koordinaciju i provedbu mjera.
* Raznolike prijetnje, uključujući unutarnje ljudske faktore kao što su nemar i zloporaba ovlasti, te vanjske prijetnje koje zahtijevaju sveobuhvatan pristup zaštiti.
* Potreba za stalnim nadzorom i ažuriranjem sigurnosnih politika i mjera, uz edukaciju zaposlenika kako bi se smanjio rizik od nenamjernih ili namjernih sigurnosnih propusta.

## Definicije pojmova i tehnologija

1. 1. Što je kontrola pristupa i koje vrste postoje?

* Fizička kontrola pristupa: regulira pristup fizičkim prostorijama i resursima, npr. korištenjem ključeva, kartica, brava, nadzora i sigurnosnog osoblja.
* Logička kontrola pristupa: odnosi se na pristup informacijama i sustavima putem softverskih tehnologija poput lozinki, autentifikacije, biometrije i autorizacije prava korisnika.

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

* Biometrijska autentifikacija koristi jedinstvene biološke ili ponašajne karakteristike osobe (npr. otisak prsta, prepoznavanje lica, skeniranje šarenice) za provjeru identiteta.
* Pruža sigurniju i pouzdaniju metodu autentifikacije u odnosu na lozinke jer je teško krivotvoriti biometrijske podatke.
* U fizičkoj sigurnosti koristi se za kontrolu pristupa prostorima i resursima, omogućujući samo ovlaštenim osobama ulaz i smanjujući rizik od zloupotrebe.

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

* Omogućava beskontaktni i brz način identifikacije korisnika putem RFID kartica ili privjesaka.
* Pruža mogućnost praćenja tko i kada ulazi ili izlazi iz određenih prostora u stvarnom vremenu.
* Omogućava dodjelu prilagođenih razina pristupa prema ulogama korisnika, čime se povećava sigurnost i olakšava upravljanje pristupom.
* Može se integrirati s drugim sigurnosnim sustavima poput nadzora i evidencije radnog vremena za potpunu kontrolu sigurnosti objekata.

1. 4. Što je CCTV i kako doprinosi sigurnosti?

* Omogućava stalni vizualni nadzor prostora u stvarnom vremenu, što pomaže u prevenciji i otkrivanju kriminalnih aktivnosti.
* Djeluje kao sredstvo odvraćanja potencijalnih počinitelja zbog vidljive prisutnosti kamera.
* Snimke se mogu arhivirati i koristiti kao dokaz u istragama i sudskim postupcima.
* Omogućava daljinski nadzor više lokacija, što povećava učinkovitost sigurnosnog nadzora.

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

* Pasivni sigurnosni sustavi djeluju nakon nastanka incidenta i imaju za cilj smanjiti posljedice, npr. sigurnosni pojasevi, zračni jastuci, sigurnosna karoserija.
* Aktivni sigurnosni sustavi sprječavaju nastanak nesreća i incidenta, koristeći tehnologije kao što su sustavi za automatsko kočenje (ABS), kontrolu stabilnosti (ESC) i upozorenja vozača.
* Pasivni sustavi zaštite putnike tijekom i nakon nesreće, dok aktivni sustavi ciljaju na prevenciju i kontrolu vozila prije i tijekom opasnih situacija.

1. 6. Što su sigurnosne barijere i gdje se primjenjuju?

* Industrijska i radna mjesta za sprječavanje pristupa opasnim zonama ili strojevima (ograde, zaštitne mreže).
* Prometne površine i gradilišta za odvajanje vozila od pješaka i kontrolu protoka prometa (betonske barijere, stupovi, barikade).
* Protupožarne barijere u zgradama za sprečavanje širenja vatre i olakšavanje sigurne evakuacije (vatrootporni zidovi i vrata).

1. 7. Kako funkcionira sustav elektroničke kontrole pristupa?

* Korisnik koristi medij za identifikaciju, poput RFID kartice, biometrijske značajke ili drugog uređaja, koji se očitava na skeneru.
* Skener prosljeđuje informacije jedinici za upravljanje kontrolom pristupa (ACU), koja provjerava ovlaštenje korisnika uspoređujući podatke s bazom.
* Ako je korisnik ovlašten, ACU aktivira elektroničku bravu ili otvarač vrata, dopuštajući pristup; u suprotnom pristup se odbija.
* Sustav nadzire stanje vrata i brava, otkriva pokušaje neovlaštenog pristupa te može aktivirati alarme.
* Sustavi mogu raditi online s centraliziranim upravljanjem ili offline s lokalnim upravljačkim jedinicama i pohranom ovlaštenja na kartici.

1. 8. Što je sigurnosna zona i kako se definira?

* Područje s ograničenim pristupom i jasno definiranim pravilima za ulazak i kretanje.
* Služi za zaštitu osjetljivih podataka, objekata ili funkcija, primjerice vojnih lokacija, poslovnih prostora ili kritične infrastrukture.
* U pravilu se zona označava vizualnim i fizičkim sredstvima, te se u nju mogu ulaziti samo ovlaštene osobe s odgovarajućim certifikatima ili pod nadzorom.
* Vrste sigurnosnih zona mogu uključivati zone zabrane građenja, ograničenog građenja ili kontroliranog građenja, ovisno o stupnju sigurnosti i namjeni.

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

* ISO/IEC 27001:2013 — međunarodni standard za upravljanje informacijskom sigurnošću (ISMS) koji obuhvaća i fizičku sigurnost kao dio sveobuhvatne zaštite informacijskih resursa.
* ISO/IEC 27002 — smjernice za implementaciju kontrola sigurnosti iz ISO 27001, uključujući fizičke mjere poput kontrole pristupa i zaštite opreme.
* Ostali standardi i norme koji se mogu primijeniti ovisno o industriji i lokalnim propisima, često nadopunjuju ISO 27001 okvir za učinkovito upravljanje rizicima i sigurnosnim politikama.

1. 10. Što je tailgating i kako se može spriječiti?

* Postavljanje sigurnosnih vrata koja dopuštaju prolaz samo jedne osobe u jednom trenutku.
* Edukacija zaposlenika da ne dozvole ulazak neovlaštenim osobama i da budu oprezni prema nepoznatim osobama.
* Primjena stroge politike "bez značke nema ulaza" i provjera identiteta svih koji ulaze u zaštićene zone.
* Korištenje tehnologija poput biometrije, RFID kartica i nadzornih kamera za nadzor i kontrolu pristupa.
* Uvođenje sigurnosnog osoblja na važnim ulazima radi nadzora i sprječavanja tailgatinga

## Građevine, okoliš i prostorije

1. 1. Koji su kriteriji za odabir lokacije podatkovnog centra?

* Dostupnost i blizina: Lokacija treba biti lako dostupna za tehničko osoblje i održavanje, ali i za povezivanje s mrežom i korisnicima.
* Sigurnost od rizika: Procjena ugroženosti područja prirodnim katastrofama (poplave, zemljotresi, požari) i politička stabilnost regije.
* Infrastrukturna podrška: Dobro razvijena prometna, energetska i telekomunikacijska infrastruktura koja omogućuje neprekidan rad i brzu intervenciju u slučaju potrebe.
* Troškovi i financijski faktori: Troškovi izgradnje, rada, porezi, naknade i dostupnost radne snage.

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

* Oštećenja ili uništenje infrastrukture, što može dovesti do gubitka pristupa kritičnim resursima i prijetiti sigurnosti ljudi i opreme.
* Prekid komunikacija i energetskih sustava, što otežava ili onemogućava provedbu sigurnosnih mjera.
* Povećani rizik od sekundarnih opasnosti, kao što su požari, kemijska onečišćenja i drugi toksini koji mogu dodatno ugroziti sigurnost.
* Potrebu za unaprijed pripremljenim planovima za hitne intervencije, zaštitu i evakuaciju koji uzimaju u obzir specifičnosti prirodnih prijetnji.

1. 3. Koje mjere se poduzimaju za zaštitu server sobe?

* Fizička kontrola pristupa: korištenje sigurnosnih vrata s elektroničkim bravama, biometrijskom autentifikacijom ili kartičnim sustavima za ulaz samo ovlaštenim osobama.
* Nadzor okoliša: postavljanje senzora za praćenje temperature, vlage i dima te integracija s alarmnim sustavima za pravovremeno otkrivanje problema.
* Zaštita od požara: instalacija automatskih protupožarnih sustava, kao što su sustavi gašenja plinom, i protupožarni alarmi.
* Redovito održavanje i sigurnosne revizije: provjera svih sigurnosnih sustava i ažuriranje konfiguracija za zaštitu od neovlaštenih pristupa i drugih prijetnji.
* Sigurnosna oprema i infrastruktura: korištenje serverskih ormara za dodatnu zaštitu opreme i organizaciju kablova, kao i sigurnosne mreže i protokole za zaštitu podataka

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

* Fizička sigurnost zgrada uključuje slojevitu primjenu mjera zaštite koje se protežu od vanjskih granica poput vrata, ograda i prozora, do unutarnjih prostora kroz kontrolu pristupa i nadzor.
* Sigurnosne mjere uključuju protuprovalnu zaštitu vrata i prozora prema normi EN 1627:2011 koja definira razine otpornosti na provalu.
* Osiguranje evakuacijskih putova i instalacija, poput panik rasvjete i protupožarnih sustava, ključni su dijelovi sigurnosnih mjera za zaštitu stanara i korisnika.

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

* Osiguranje kontrole pristupa tako da neovlaštene osobe ne mogu lako ući u prostorije s važnim informacijskim sustavima; što uključuje strateško postavljanje kontrolnih točaka i barijera.
* Ugradnju nadzornih i alarmnih sustava na ključnim mjestima unutar prostorije za pravovremeno otkrivanje sumnjivih aktivnosti i mogućih prijetnji.
* Organizaciju prostora na način da se spriječi pristup osjetljivim uređajima i podacima, poput pozicioniranja računala tako da posjetitelji ne mogu vidjeti zaslone ili rukovati opremom, kao i korištenje ormarića s lokotima za dodatnu zaštitu.

1. 6. Kako se štite komunikacijski ormari i mrežna oprema?

* Sigurnost informacijskih sustava obuhvaća zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka kroz fizičke, tehničke i administrativne mjere tijekom cijelog životnog ciklusa sustava.
* Uključuje procjenu i upravljanje rizicima, nadzor nad prijetnjama i ranjivostima te primjenu međunarodnih standarda kao što su ISO/IEC 27001 i ISO/IEC 27002.
* Ključan je i ljudski faktor zbog čega su edukacija korisnika i praćenje sigurnosnih politika neizostavni dijelovi zaštite informacijskih sustava.

1. 7. Koje su preporuke za sigurnosnu rasvjetu oko objekta?

* Postavljanje sigurnosne rasvjete na evakuacijskim putovima i izlazima, osiguravajući dovoljno svjetla za sigurno kretanje u slučaju nestanka glavne rasvjete ili hitnih situacija poput požara ili potresa.
* Korištenje ravnomjerne rasvjete s minimalnim omjerom najniže i najviše osvijetljenosti od 1:40, te osiguravanje brzog paljenja rasvjete unutar 5 do 60 sekundi nakon prekida napajanja.
* Postavljanje sigurnosnih svjetiljki na ključnim mjestima poput stubišta, promjena smjera, blizu izlaza i sigurnosnih znakova kako bi se osigurala jasna vidljivost i identifikacija opasnosti ili opreme.

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

* Video nadzor: Korištenje CCTV sustava s visokorezolucijskim kamerama koje snimaju i prate aktivnosti na ulazima i izlazima, često integrirano s alarmnim sustavima za automatsku detekciju sumnjivih događaja.
* Kontrola pristupa: Sustavi kontrole pristupa koriste RFID kartice, biometrijske čitače ili kombinaciju tehnologija kako bi se osiguralo da samo ovlaštene osobe mogu proći, uz evidenciju ulaza i izlaza.
* Integracija sustava: Video nadzor, alarmi i kontrola pristupa povezani su u jedinstveni sustav koji omogućuje centralizirano upravljanje i brzo reagiranje na sigurnosne incidente.

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

* EN 14470-1: Europska norma koja specificira dizajn i kriterije ispitivanja za sigurnosne ormariće za skladištenje zapaljivih tekućina u laboratorijima, a može se primijeniti i na zaštitu opreme u određenim uvjetima.
* ISO 834-1 i EN 1363-1: Standardi koji definiraju metode ispitivanja otpornosti na vatru građevinskih elemenata, što uključuje i prostorije za smještaj kritične opreme.
* HRN EN ISO 1182 i HRN EN 1363 serija: Norme vezane uz ispitivanje negorivosti materijala i otpornosti prostorija na požar, osiguravajući da prostorije mogu izdržati određeno vrijeme izloženosti vatri radi zaštite opreme i osoblja.

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

* Kontrolu pristupa korištenjem privremenih iskaznica ili ovlaštenja za osobe koje imaju pravo ulaza, pri čemu se nadzor može vršiti putem zaštitara ili elektroničkih sustava.
* Primjenu slojevitih sigurnosnih mjera poput zaključavanja vrata, ugradnje video nadzora i detektora pokreta radi sprečavanja neovlaštenog pristupa i prijetnji.
* Planiranje sigurnosnih protokola prilagođenih specifičnostima privremenih objekata, uključujući osiguranje evakuacijskih putova i zaštitu kritične opreme od požara i krađe.