SIGURNOST INFORMACIJSKIH SUSTAVA

Međuispit 1

ISHOD 1

1. **Što je sigurnosna provjera?**

- Područje informacijske sigurnosti koje uključuje potpunu provjeru vezanu uz sigurnosne elemente neke organizacije.
- Provjera vlasništva, vlasnika, članova uprave, provjera savjetnika za informacijsku sigurnost, te sve osobe koje imaju pristup klasificiranim podacima.

2. **Što su mjere informacijske sigurnosti?**

- Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.
- Cilj im je osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, promjene ili uništavanja

3. **Koji se pojmovi i stupnjevi tajnosti utvrđuju Zakonom o tajnosti podataka?**

- Pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom ovoga Zakona.
- VRLO TAJNO, TAJNO, POVJERLJIVO, OGRANIČENO

4. **Koji podaci se klasificiraju stupnjem tajnosti VRLO TAJNO?**

Stupnjem tajnosti VRLO TAJNO klasificiraju se podaci čije bi neovlašteno otkrivanje **nanijelo nepopravljivu štetu** nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske, osobito sljedećim vrijednostima:

- Neovisnost, cjelovitost i sigurnost RH
- Međunarodni odnosi RH
- Obrambena sposobnost i sigurnosno-obavještajni sustav
- Sigurnost građana
- Osnove gospodarskog i financijskog sustava RH
- Znanstvena otkrića, pronalasci i tehnologije od važnosti za RH

5. **Koji podaci se klasificiraju stupnjem tajnosti TAJNO?**

- Stupnjem tajnosti TAJNO klasificiraju se podaci čije bi neovlašteno otkrivanje **teško naštetilo** prethodno navedenim vrijednostima iz članka 6. ZAKONA O TAJNOSTI PODATAKA.

6. **Koji podaci se klasificiraju stupnjem tajnosti POVJERLJIVO?**

- Stupnjem tajnosti POVJERLJIVO klasificiraju se podaci čije bi neovlašteno otkrivanje **naštetilo** prethodno navedenim vrijednostima iz članka 6. ZAKONA O TAJNOSTI PODATAKA.

7. **Koji podaci se klasificiraju stupnjem tajnosti OGRANIČENO?**

- Stupnjem tajnosti OGRANIČENO klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova iz članka 5. ZAKONA O TAJNOSTI PODATAKA**.**
- Područje obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ukoliko su podaci od sigurnosnog interesa za RH.

8. **U kojim vremenskim okvirima se provodi periodična procjena klasificiranih dokumenata?**

- Za stupanj tajnosti VRLO TAJNO – najmanje jednom u 5 godina
- Za stupanj tajnosti TAJNO – najmanje jednom u 4 godine
- Za stupanj tajnosti POVJERLJIVO – najmanje jednom u 3 godine
- Za stupanj povjerljivosti OGRANIČENO – najmanje jednom u 2 godine

9. **Objasniti tri aspekta sigurnosti CIA?**

- *Povjerljivost* (confidentiality) – podrazumijeva osiguranje tajnosti informacija, informacije (podaci) moraju biti dostupne isključivo subjektima kojima su te informacije namijenjen. Postoje dvije metode zaštite povjerljivosti informacija: korištenje kontrole pristupa (fizičke i logičke) i enkripcije.
- *Integritet* (integrity) – podrazumijeva da informacija (podaci) ne može biti promijenjena bez odgovarajućeg ovlaštenja, odnosno da su onemogućene promjene od strane neovlaštenih osoba ili neovlaštene promjene ovlaštenih osoba. Integritet se čuva istim principima kao i povjerljivost, upotrebom kontrole pristupa i enkripcijskim algoritmima.
- *Dostupnost* (availability) – osigurava dostupnost informacija (podataka). Računalna infrastruktura i mediji koji se upotrebljavaju za procesiranje i pohranu podataka te komunikacijski kanali kojima se isti prenose moraju biti dostupni u prihvatljivom vremenskom razdoblju. U tu svrhu danas se dizajniraju tzv. visoko dostupni sustavi (ispad jednog elementa ne smije ugroziti dostupnost kompletnog sustava)

10. Objasniti tri aspekta prijetnji DAD?

- *Razotkrivanje* (disclosure) – narušavanje tajnosti informacije te je na taj način izravno povezano s povjerljivošću.
- *Promjena* (alternation) – narušavanje integriteta informacije ili podataka.
- *Prekid* (disruption) – uzrokuje nedostupnost servisa ili podataka.

11. Što je sigurnosni rizik?

- Mogućnost realizacije neželjenog događaja koji može štetno utjecati na povjerljivost, integritet ili raspoloživost informacija.

12. Opisati ukratko proces upravljanja rizikom.

- *Procjena rizika* – uključuje identifikaciju i evaluaciju rizika te preporuke za implementaciju kontrola za umanjenje rizika.
- *Tretiranje rizika* – uključuje određivanje prioriteta, implementaciju i održavanje kontrola za umanjivanje rizika.
- *Evaluacija i nadzor rizika* – uključuje kontinuirano vrednovanje i nadzor rizika.

13. Navesti i opisati barem četiri kategorije resursa.

- *Resurs* – svako sredstvo u vlasništvu organizacije ili sredstvo kojim organizacija raspolaže.
- *Lokacija* - tipično u ovu kategoriju spadaju poslovni prostori u vlasništvu organizacije i svi ostali prostori na kojima se odvijaju poslovni procesi organizacije i prostori u kojima su smješteni ostali resursi organizacije
- *Ljudski resursi* – svi zaposlenici organizacije koji izvršavaju neku od poslovnih aktivnosti. Prilikom identifikacije ljudskih resursa preporučuje se identifikaciju napraviti prema ulozi koju zaposlenik obnaša u organizaciji
- *Infrastruktura* - u ovu kategoriju ulaze resursi poput alarmnog sustava, klimatizacijskog sustava, videonadzora i sl.
- *Mrežna infrastruktura* – sva pasivna i aktivna mrežna oprema nalazi se u ovoj kategoriji
- Hardver, softver, informacije, poslovni partneri

14. Što su ranjivosti? Na koje sve načine organizacija može dobiti informacije o potencijalnim ranjivostima?

- Ranjivost je svojstvo resursa. To je slabost u sustavu, sigurnosnim procedurama, dizajnu ili implementaciji resursa koja može biti iskorištena i rezultirati sigurnosnim incidentom.
- Ranjivosti nisu samo u tehničkim mjerama zaštite, brojne ranjivosti proizlaze iz loših operativnih procedura ili loše definiranih sigurnosnih politika

15. Što su prijetnje? Navedite na koje kategorije ih dijelimo? (pojasnite na primjerima)

- Prijetnja je mogućnost da izvor prijetnje iskoristi ranjivost i pri tome uzrokuje štetu resursu
- Izvor prijetnje može biti namjera i metoda usmjerena prema iskorištavanju ranjivosti, ili situacija te metoda koja slučajno iskorištava ranjivost.
- *Ljudske prijetnje* – događaj koji prouzrokuje čovjek, bilo da se radi o namjernim ili nenamjernim aktivnostima
- *Prijetnje iz okoline* – npr. dugotrajni ispadi struje, zagađenje i sl.
- *Prirodne nepogode kao prijetnje* – npr. poplava, potres, tornado i sl.
- Neovlašteni logički pristup, maliciozni softver, administratorska pogreška, ugrađeni backdoor

16. Što su kontrole? Kakve kontrole prema načinu djelovanja postoje?

- *Preventivne* – umanjuju vjerojatnost iskorištavanja ranjivosti (kontrole pristupa, enkripcija, autentikacija)
- *Detektivne* – omogućuju identifikaciju pokušaja iskorištavanja ili iskorištavanja prijetnji (IDS, IPS, log sustavi)
- *Korektivne* – umanjuju ranjivosti (procedure za oporavak podataka iz backup-a)
- *Kompenzirajuće* – nadomještaju povećani rizik dodavanjem kontrolnih koraka koji umanjuju rizik (dodavanje challenge-response komponente slabim kontrolama pristupa)
- *Kontrole za odvraćanje* – daju upozorenja koja mogu spriječiti napadače (zastrašivanje potencijalnih napadača)

17. Što je procjena štete i što se sve uzima u obzir kod nje?

- Procjena mogućih gubitaka ako prijetnja iskoristi neku od ranjivosti.
- U obzir treba uzeti:
    - namjenu resursa u poslovnim procesima u kojima se koristi
    - kritičnost resursa (njegova važnost za organizaciju)
    - osjetljivost resursa

18. Opisati kvantitativni izračun rizika.

- Temelji se na korištenju egzaktnih numeričkih vrijednosti.
- Vrijednost resursa se prikazuje u novčanim jedinicama.
- Ranjivost, prijetnje i posljedice se promatraju kao faktor izloženosti (EF) koji se izražavaju u postotku gubitka vrijednosti resursa.
- Vjerojatnost se obično promatra u zadanom vremenskom razdoblju.

19. Opisati kvalitativni izračun rizika.

- Ne koristi apsolutne vrijednosti parametara nego kvalitativno evaluira njihov utjecaj na rizik.
- Veliku važnost ima iskustvo, stručnost i sposobnost osoba koje provode procjenu rizika. Iako se procjena provodi kvalitativno, zbog lakše interpretacije rezultata, parametri se isto kao i procijenjeni rizik, kvantificiraju.
- Problem je subjektivnost jer svaka osoba drugačije procjenjuje rizik.

20. Napraviti matricu rizika za 3 razine vjerojatnosti, 5 razina šteta i 5 razina vrijednosti resursa. Koliki je minimalni i maksimalni rizik?

Prijetnja	**Vjerojatnost**	**1**					**2**					**3**				
	Šteta	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Vrijednost resursa	**1**	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75

21. Na koje sve načine je moguće tretirati rizik? Pojasnite

- *Umanjivanjem* – postiže se implementacijom kontrola za umanjivanje rizika. Rizik se također može umanjiti poboljšavanjem postojećih sigurnosnih kontrola
- *Prenošenjem* – rizik i opasnosti njegove realizacije se prenose na neku drugu organizaciju (osiguranje kod osiguravajuće kuće ili eksternalizacija)
- *Izbjegavanjem* – metode modifikacije procesa, odnosno procesni reinženjering.

ISHOD 2

1. **Što utvrđuje zakon o informacijskih sigurnosti?**
   Utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

2. **Na koga se primjenjuje Zakon o informacijskoj sigurnosti?**

- Na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.
- Na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

3. **Što je sigurnosna akreditacija informacijskog sustava?**

- Postupak u kojem se utvrđuje osposobljenost tijela i pravnih osoba iz članka 1. stavka 2. Zakona za upravljanje sigurnošću informacijskog sustava, a provodi se utvrđivanjem primijenjenih mjera i standarda informacijske sigurnosti.

4. **Koja je središnja uloga s naslova informacijske sigurnosti:**
   a. **Zavoda za sigurnost informacijskih sustava?**
      Zavod za sigurnost informacijskih sustava je središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama iz članka 1. stavka 2. Zakona o informacijskoj sigurnosti
   b. **Ureda vijeća za nacionalnu sigurnost?**
      UVNS je središnje državno tijelo odgovorno za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u RH, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između RH i stranih zemalja i organizacija.
   c. **Nacionalnog CERT-a?**
      CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s RH. Usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u RH te određuje pravila i načine zajedničkog rada.

5. **Koje aspekte informacijske sigurnosti uređuje Zakon o sigurnosno-obavještajnom sustavu RH?**

- Osnivaju sigurnosno-obavještajne agencije
- Sigurnosno-obavještajna agencija (SOA),
- Vojna sigurnosno-obavještajna agencija (VSOA)
- Njihov rad nadziru Hrvatski sabor, Predsjednik Republike, Vlada, Ured Vijeća za nacionalnu sigurnost, Vijeće za građanski nadzor sig-obav. Agencija

6. **Što predstavlja vitalne interese RH (sukladno važećoj strategiji nacionalne sigurnosti)?**

- Opstanak suverene, neovisne i teritorijalno cjelovite države sa svojim nacionalnim identitetom i temeljnim vrijednostima, te zaštita života i imovine njezinih građana.

7. **Koji aspekt informacijske sigurnosti uređuje Zakon o autorskom pravu i srodnim pravima?**

- Zakon o autorskom pravu i srodnim pravima s aspekta informacijske sigurnosti uređuje prava proizvođača autorskih djela, programa i baza podataka.

8. **Što je propisano Uredbom o mjerama informacijske sigurnosti?**

- Utvrđuju se mjere informacijske sigurnosti za postupanje s klasificiranim i neklasificiranim podacima.

9. **Što je propisano pravilnikom o standardima sigurnosti informacijskih sustava i na koji način?**

- Pravilnik se koristi u službene svrhe, označen je oznakom „Neklasificirano“ i ne objavljuje se u Narodnim novinama a dostavljen je svim tijelima koja po njemu moraju postupati. Te nije javno dostupan.

10. **Što sadrže mjere informacijske sigurnosti za područje sigurnost podataka?**

- Klasificiranje i deklasificiranje podataka, označavanje podataka
- Pristup podacima, zaštita podataka, sustav registara, evidencija korištenja klasificiranih podataka, postupanje u izvanrednim situacijama, ustupanje klasificiranih podataka drugoj državi ili međunarodnoj organizaciji

11. **Tko izdaje certifikat poslovne sigurnosti i koji mu je vijek trajanja?**

- Ured Vijeća za nacionalnu sigurnost
- Certifikat poslovne sigurnosti izdaje se na razdoblje od 5 godina.

12. Što je ISO 27001 norma i čemu služi?

- Skup najboljih praksi i preporuka za dizajn, implementaciju i održavanje sustava upravljanja informacijskom sigurnošću (ISMS)
- Okvir za uspostavu, implementaciju, nadzor, reviziju, održavanje i poboljšavanje sustava za upravljanje informacijskom sigurnošću

13. Objasniti procesni pristup ISO 27001 norme (PDCA ciklus).

- **P**LAN – Uspostava ISMS politike, ciljeva, procesa i procedura za upravljanje rizikom i poboljšanje informacijske sigurnosti.
- **D**O – Implementacija i rad ISMS kontrola, procesa i procedura.
- **C**HECK – Procjena i mjerenje učinkovitosti procesa, kontrola i ciljeva te priprema izvještaja za reviziju ISMS sustava.
- **A**CT – Poduzimanje korektivnih i preventivnih mjera na temelju rezultata interne revizije i revizije uprave i ostalih relevantnih informacija u cilju poboljšavanja ISMS sustava

14. Koje aktivnosti se poduzimaju prilikom određivanja opsega i izrade izjave o primjenjivosti?

- Granice usklađivanja s ISO 27001
- Obično samo kritični dijelovi
- Treba jasno definirati s obzirom na:
    - poslovne procese
    - Lokacije
    - infrastrukturu, hardver, softver
    - Informacije
    - vanjske partnere i
    - Zaposlenike

15. Pojasnite što je to program sigurnosnog osvješćivanja?

- Ljudi moraju postupati u skladu sa svojim ulogama i odgovornostima
- Moraju razumjeti sigurnosne prijetnje i rizike te kontrole
- Uspostavljanje sigurnosnih pravila za djelatnike
- Sigurnosno educiranje i stručno usavršavanje

16. Što je politika sigurnosti?

- Krovni, temeljni dokument
- Očekivanja, smjernice i namjere rukovodstva
- Sadrži temeljne high level koncepte informacijske sigurnosti
    - Namijenjena svim zaposlenicima kako bi postali svjesni važnosti
- Uzima u obzir zakonske i regulatorne zahtjeve
- MORA biti odobrena od najvišeg rukovodstva

17. Navedite savjete kojih se treba držati prilikom izrade sigurnosnih politika?

- Moraju biti realistične, primjenjive i izvedive
- Moraju biti jednostavne i lako razumljive
- Naći balans između produktivnosti i sigurnosti
- Ukoliko su zahtjevi za kontrolom prestrogi neće biti implementirani ili će zaposlenici naći način da ih zaobiđu (npr. mijenjanje zaporki svakih 30 dana)

18. Navedite i pojasnite temeljne odgovornosti uprave vezano za informacijsku sigurnost?

- Identifikacija sigurnosnih zahtjeva i integracija s poslovnim procesima
- Odobravanje sigurnosne politike
- Uspostava temeljnog okvira i organizacijske strukture
- Uspostava sustava uloga i odgovornosti
- Iniciranje security awareness programa
- Osiguravanje ljudskih, financijskih i informacijskih resursa
- Uprava imenuje osobu odgovornu za uspostavu i nadzor ISMS-a (CISO)

19. Navedite i pojasnite temeljne odgovornosti voditelja sigurnosti informacijskog sustava?

- Usklađivanje sigurnosnih ciljeva sa strategijom informacijskog sustava
- Izrada politika i procedura

- Nadzor i kontrola provedbe politika i procedura
- Izrada i periodička provjera analize rizika, ažuriranje promjena
- Planiranje i predlaganje aktivnosti vezanih uz sigurnost informacijskog sustava
- Prijedlog poboljšanja sigurnosnih kontrola
- Pomoć pri analizi sigurnosnih aspekata projekata informacijskog sustava
- Suradnja sa unutarnjim (revizija, IT) i vanjskim suradnicima (revizije).

20. Što je izjava o povjerljivosti?

- Između dvije ili više strana definira način rukovanja osjetljivim informacijama
  - Ugovorne se strane obvezuju da neće neovlašteno otkrivati informacije
  - Precizna specifikacija informacija
  - Vremensko razdoblje
  - Akcije i postupci u slučaju prekida valjanosti
  - Pravo na neovisnu reviziju
  - Proces obavješćivanja u slučaju kompromitacije
  - Postupci u slučaju kršenja
- Vrlo važno potpisati prije davanja pristupa

21. Zašto je važno nadzirati sigurnost trećih strana koje pristupaju našem informacijskom sustavu? Pojasnite navedeno na primjeru sigurnosnog incidenta tvrtke Target.

Nešto kao:
Ukoliko treća strana, koja nema dobru zaštitu svojeg informacijskog sustava, pristupa našem informacijskom sustavu, postoji opasnost da će napadač iskoristiti tu ranjivost i te na taj način pristupiti našem sustavu**.**

Target primjer:

- Gubitak kreditnih kartica i osobnih podataka za više od 110 milijuna korisnika
- Istraga pokazala da je ulaz u informacijski sustav omogućen putem mrežnih kredencijala od strane Fazio Mechanical (klima uređaji, …)
- Ukradeni dva mjeseca prije nego što je napad započeo → koristili besplatnu verziju antivirusnog progama (Malwarebytes Anti-Malware)
- Besplatna verzija nema real time protection
- Pristupali eksternom sustava plaćanja partnera
- Uspjeli se logirati na server koji je u internoj mreži
- Nije se koristila dvo-faktorska autentikacija → zahtjev PCI DSS
- "in rare cases" would Target have required a vendor to use a one-time token or other two-factor authentication approach.
- Target would have paid very little attention to vendors like Fazio, and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target."