HÖGSKOLAN
I SKÖVDE

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 20240307

Tentamenstid: 8:30 – 14:30

Ansvarig lärare: Marcus Nohlberg

Berörda lärare

Hjälpmedel/bilagor

Engelsk/svensk, svensk/engelskt lexikon.

Övrigt

Skriv läsbart med tydlig penna, ej ljus blyerts. Oläsbara svar bedöms alltid som noll poäng. Nytt blad för varje fråga. Numrera dina svar noga, även a/b/c-frågor och *lämna in svaren i ordning*. Skriv namn och personnummer på samtliga inlämnade blad. Alla svar ska skrivas på svarspapper, inga svar till tentamensfrågor skrivna i tentahäftet kommer rättas.

Anvisningar

- ☐ Ta nytt blad för varje lärare
- ☒ Ta nytt blad för varje ny fråga
- ☒ Skriv endast på en sida av papperet.
- ☒ Skriv namn och personnummer på samtliga inlämnade blad.
- ☒ Numrera lösbladen löpande.
- ☒ Använd inte röd penna.
- ☒ Markera med kryss på omslaget vilka uppgifter som är lösta.

Poänggränser

45 p = G (minst 5p från del A och 20p från del B och 20 p från del C).

76 p = VG (minst 5p från del A och 20p från del B och 20 p från del C).

Skrivningsresultat bör offentliggöras inom 18 arbetsdagar

Lycka till!

Antal sidor totalt 13

Om caset – läs hela denna text noga!

I samtliga frågor som följer i tentan där vi refererar till ett Case eller företagsnamnet är det Caset nedan som avses! **Det är viktigt att du läser igenom *hela* denna text och bekantar dig med verksamheten innan du svarar på övriga frågor!**

GreenHarvest AB (GHAB) har revolutionerat livsmedelsindustrin med dess hållbara affärsmodell som kombinerar passionen för ekologi med teknologisk innovation. Företaget grundades av Sofia Rodriguez, före detta agronom med en doktorsgrad i ekologiskt jordbruk; Kenji Takahashi, en MBA-utbildad affärsstrateg med en bakgrund inom förnybar energi; och Amina Yusuf, en marknadsföringsexpert med erfarenhet från stora FMCG-företag.
Affärsidé och Verksamhet: GreenHarvest AB erbjuder ett brett sortiment av ekologiska produkter, från frukt och grönsaker till förpackade varor som ekologisk müsli och plantbaserade snacks. De samarbetar nära med certifierade ekologiska bönder och har etablerat en transparent leveranskedja där kunder kan spåra sina livsmedels ursprung genom QR-koder på förpackningarna. All försäljning sker online via deras egen e-handelsplattform eller via utvalda ekologiska butikskedjor.
Ledning: Sofia Rodriguez fungerar som VD, med ansvar för företagets strategiska riktning och övervakning av produktkvalitet. Kenji Takahashi styr de dagliga operationerna och ansvarar för att hållbarhetsmål infrias, medan Amina Yusuf leder företagets marknadsföring och kundengagemang.
Säkerhetsorganisation: Företagets säkerhetsorganisation är robust och mångfacetterad. CSO Jamal Patel och hans team ansvarar för att skydda företagets digitala infrastruktur och fysiska tillgångar. De implementerar regelbundna penetrationstester, upprätthåller en strikt bring-your-own-device (BYOD) policy, och utbildar personal i säkerhetsmedvetenhet.
Fysisk Miljö: GreenHarvest Cos huvudkontor är ett exempel på grön arkitektur med sensorstyrd belysning, effektiva HVAC-system och ett grönt tak. Företaget har ett centralt lager för distribution och ett nätverk av kylförvaringsenheter hos sina partnerbönder.
Digitala System:

- ERP-system: GreenHarvest AB använder NetSuite för att hantera allt från lagerhantering till ekonomi.
- CRM-plattform: HubSpot CRM hjälper teamet att spåra kundinteraktioner och optimerar försäljningsprocessen.
- E-handelsplattform: Shopify Plus används för e-handel, med anpassade plugins för lagerintegration och spårning.
- Kryptering & Dataanalys: Företaget använder AES-kryptering för data i vila och TLS för data i transit, och Tableau för dataanalys.

GreenHarvest Co. är inställda på att expandera och stärka sin position inom den ekologiska livsmedelssektorn genom flera strategiska initiativ.
Produktutveckling: De planerar att utvidga sitt sortiment med nya ekologiska och veganvänliga alternativ för att attrahera en bredare kundbas.

Internationell Expansion: Företaget siktar på att nå nya marknader genom att etablera partnerskap med internationella distributörer och utöka sitt distributionsnätverk.
Teknologiinvesteringar: För att öka transparensen i leveranskedjan kommer GreenHarvest Co. att investera i blockchain-teknologi, samtidigt som de förstärker sina cybersäkerhetssystem med avancerade skyddsåtgärder, inklusive AI-baserad intrångsdetektering.
Hållbarhetsåtaganden: Ett långsiktigt mål är att uppnå koldioxidneutralitet genom att integrera förnybar energi i alla operationer och minska företagets miljöavtryck.
Personalens Utveckling: Genom att erbjuda kontinuerlig utbildning och karriärmöjligheter för sina anställda, strävar GreenHarvest Co. efter att både främja internt engagemang och attrahera talang.
Dessa planer visar GreenHarvest Co:s engagemang för hållbar tillväxt, innovation, och en stark företagskultur som värdesätter både människor och planeten.

Säkerhetsincidenter:

1. *Tekniskt Angrepp:* En SQL-injektion utfördes mot GreenHarvest Co:s databas genom deras e-handelsplattform. Angriparen utnyttjade en sårbarhet i ett tredjeparts plugin som inte hade uppdaterats med den senaste säkerhetspatchen. Attackeraren kunde extrahera kunddata, inklusive namn och emailadresser. Företaget svarade snabbt genom att stänga ner det berörda systemet, informera berörda kunder och myndigheter samt genomföra en utredning för att stärka sina system och processer.
2. *Nätfiskeangrepp & Ransomware:* En anställd föll offer för ett nätfiske-mail som utgav sig för att komma från företagets IT-supportavdelning. Anställdens inloggningsuppgifter kapades och användes för att sprida ransomware över nätverket, vilket krypterade viktiga filer och orsakade driftstopp. Företaget tvingades stänga sin e-handelsplattform temporärt och aktiverade sin katastrofåterställningsplan inklusive att återställa data från säkerhetskopior. Efter incidenten intensifierade GreenHarvest AB sina utbildningsprogram för anställda om nätfiske och uppdaterade sina säkerhetsprotokoll.

Dessa incidenter har lärt GreenHarvest AB vikten av kontinuerlig övervakning, uppdatering av sina system samt regelbunden utbildning av personalen i cybersäkerhet. De har även lett till en översyn av deras incidenthanteringsplaner för att bättre hantera framtida hot.

Om du saknar någon information om företaget du behöver för att svara på en fråga får du fritt anta rimliga saker, så länge du noga redovisar att det är just antaganden du gör, och förklarar vad du grundar dem på!

Generellt om tentan

Denna tentamen är baserad på caset ovan. Det innebär att du förväntas knyta dina svar till caset, och också redovisa hur du resonerar, tänker och argumenterar. Här ligger en utmaning kring att planera din tid under tentamen. Givetvis förväntar vi inte längre svar än du hinner skriva under den tid som finns på tentamen, men du har själv ansvar för att planera att du utnyttjar tiden effektivt. *Det är möjligt att du känner igen caset från tidigare tentamina, men notera att viktiga detaljer kan ha ändrats i caset, så läs caset noga!*

En klok strategi är att planera hur lång tid du har att svara på varje fråga och göra en struktur över vad du vill ha med i dina svar, innan du börjar skriva för att säkerställa att du hinner svara på alla frågor och inte lägger för mycket tid på någon enskild fråga.

I själva utmaningen med att svara på tentafrågor ligger att planera din tid korrekt; du hinner kanske inte skriva allt du kan om området, men syftet är att du ska lyfta fram det som är viktigt för frågan!

Några viktiga påminnelser:
Ni får inte återanvända exempel från caset i era svar. Exempelvis får ni inte poäng för att ge samma exempel på angrepp som ges i caset i era svar på frågor längre fram. Ni kan inte heller använda samma exempel i flera olika frågor, då får ni bara poäng första gången ni gör det.

Ni måste skriva läsbart. Är det otydligt får ni noll poäng.

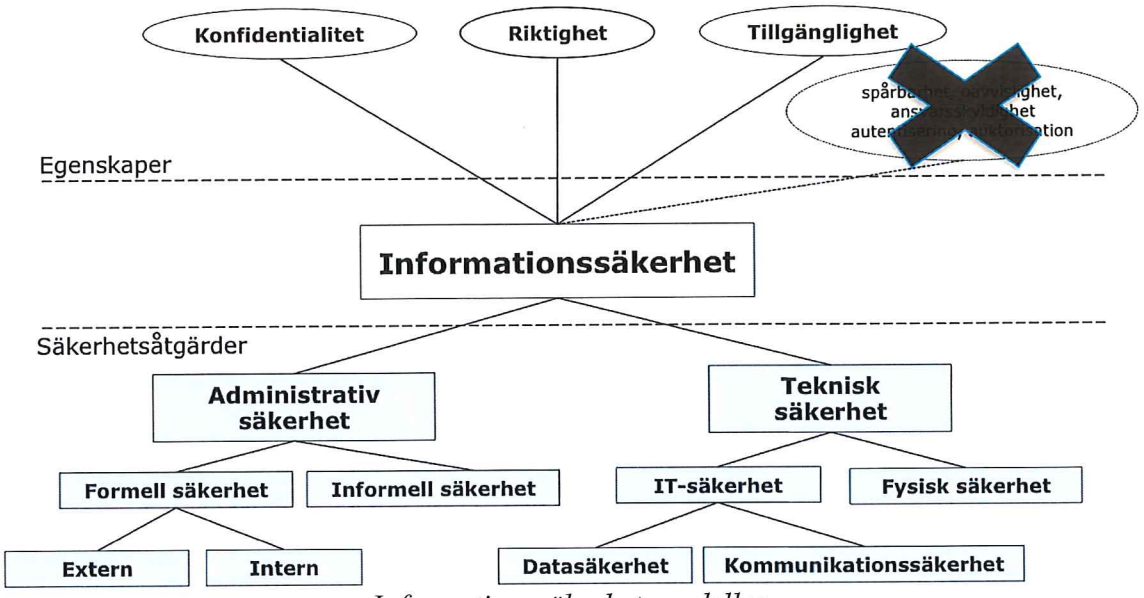
Ni måste lämna in svar på frågorna i ordning (fråga 1 – 9), och ni måste tydligt numrera vilka frågor ni faktiskt svarar på. Om ni inte har numrerat vilken fråga ni svarar på vet vi ju inte att ni börjar svara på ny fråga, då kan ni inte få poäng på detta. Ni kan inte heller svara på delfrågorna A, B, C i en enda textmängd utan att tydligt visa vilken fråga ni faktiskt svarar på.

Lycka till!

Del A (Fråga 1) Allmänt om informationssäkerhet

(Denna del måste klaras till 50 % för att få godkänt på hela tentamen.)

Fråga 1 (10 p) **Allmänt**



Informationssäkerhetsmodellen

I kursen har vi använt den modell som finns ovan för att beskriva informationssäkerhet.

a) Välj själv ut sju begrepp (dvs. boxar eller ovaler) ur figuren ovan (undantaget den överkorsade) och definiera och exemplifiera dessa nedan.

Skriv tydligt för varje begrepp vilket du valt, och beskriv varje begrepp på ny rad. Du ska också ge exempel på vad detta begrepp är/kan vara för Caset. Du ska ge minst ett exempel per begrepp!
*Notera att du alltså **måste** ge ett exempel ur caset för varje begrepp för att få poäng!* (7 p)

Utöver detta ska du också definiera och exemplifiera följande begrepp:

b) Beskriv *tillgång* och *informationstillgång* och förklara vad som är skillnaden. (2 p)

c) Oavvislighet (1 p)

Del B (Fråga 2 - 5) Administrativ säkerhet

(Denna del måste klaras till 50 % för att få godkänt på hela tentan.)

Fråga 2 (10p) **Riskanalys**

a) Caset vill genomföra nya riskanalyser. Identifiera två delar/enheter/tillgångar i verksamheten du vill prioritera att göra riskanalyser på först. Motivera dina val noga. Beskriv också hur du vill strukturera riskanalysprocessen för Caset. Vad ingår i de riskanalyser du ska genomföra? Vad är nyttan med resultaten och hur kan Caset använda resultaten på bästa sätt? (4 p)

b) Informationssäkerhetspolicy är ett fundamentalt viktigt dokument i arbetet med strukturerat informationssäkerhetsarbete. Informationssäkerhetspolicyn ska omfatta ett antal områden (fem) för att faktiskt vara en informationssäkerhetspolicy. Nämn tre av dessa områden och förklara varför just dessa är viktiga att ha med i informationssäkerhetspolicyn specifikt för Caset. (6 p)

Fråga 3 (10 p) **Standarder**

För att trygga sin verksamhet kan det bli aktuellt att följa någon form av standard för Caset.

a) Inför den framtida expansionen vill Caset börja arbeta med ett LIS. Inför detta arbete vill din VD ha svar på följande frågor:

- Vad är ett LIS och vilket konkret värde kan det ha för GHAB?
- Vad ingår i ett LIS, vad behöver utföras? Beskriv på rubriknivå.
- Vad av det som ingår i ett LIS skulle du välja att börja med för Caset, och varför? (6 p)

b) Vad är skillnaden på ISO-standarderna inom 27000-serien och det metodstöd som tagits fram av MSB (www.informationssäkerhet.se)? På vilket sätt kan GHAB använda sig av standarderna och metodstödet för att arbeta med informationssäkerhet. Hur skiljer sig användningen och resultatet mellan de två? (4 p)

Fråga 4 (10 p) **Juridik**

a) GHAB funderar på att i framtiden outsourca en del av mjukvaruutvecklingen till ett bolag i Tidaholm. Enligt upphovsrättslagen (URL), vem tillfaller upphovsrätten om ett avtal inte skrivs?" (3 p)

b) Ge exempel på vad som enligt Dataskyddsförordningen är "särskilda personuppgifter"? (1 p)

c) I Dataskyddsförordningen är grundprincipen att all behandling av personuppgifter är förbjuden. Lagen anger dock två undantag när behandling av personuppgifter är tillåten. Vilka är dessa två undantag samt ge minst ett konkret exempel på hur detta skulle kunna vara applicerbart i GHAB verksamhet. (2 p)

d) Om något händer i Casets system, kan de behöva genomföra effektiva incidentutredningar. Då vill de kunna använda den information de har i sina system. Har de alltid rätt att använda all sådan information i incidentutredningarna? Förklara den juridiska aspekten på detta! (4 p)

Fråga 5 (10 p) **Social informationssäkerhet**

För de angrepp som listas nedan ska du ge:

- Ett utförligt exempel på hur GHAB hade kunnat bli attackerat via det.
- Ge ett förslag på (för caset realistiskt) skydd som hade kunnat hindra angreppet
- Ge exempel på vem som skulle kunna använda angreppet
- Ge exempel på utbildningsåtgärd som hade kunnat förhindra angreppet

Var noga med att knyta dina förslag till caset, enbart generella beskrivningar ger noll poäng.

a) Smishing (2 p)

b) Spear Phishing (2 p)

c) ID-stöld (2 p)

d) ”Vishing” (2 p)

e) Ge ett *eget förslag* på något angrepp som skulle kunna ske mot Caset baserat på social informationssäkerhet (undantaget de nämnda ovan) och beskriv detta på samma sätt som de övriga. Detta exempel får inte användas i övriga frågor på denna tentamen. (2 p)

Del C (Fråga 6-9) Teknisk säkerhet

(Denna del måste klaras till 50 % för att få godkänt på hela tentan. Även i denna del när vi refererar till Caset eller företaget GreenHarvest AB syftar vi på caset på första sidan).

Fråga 6 (10p) **Nätverkssäkerhet**

a) Vad är en bra lösenordspolicy för GHAB:s anställda? Vilka krav ska ställas, och hur ska de anställda fås att följa den? Finns det några andra sätt att göra det säkrare än att enbart arbeta med lösenord? Vilka? (2 p)

a) Förklara överskådligt för Caset vad en brandvägg är, hur den fungerar och vilka typer som finns, samt ge ett förslag på var en brandvägg ger störst nytta för GHAB. (2 p)

c) Ge minst tre exempel på hårdvarulösningar för autentisering. För var och en av dessa, ge två detaljerade exempel på tillfällen när de hade varit användbara för Caset? (6 p)

Var noga med att knyta ditt resonemang till den aktuella verksamheten!

Fråga 7 (10 p) **Datasäkerhet**

GHAB ser stora utmaningar för att kunna skydda sin data mot hackers och är således engagerade även i tekniken de väljer.

a) Skadlig kod kan spridas på massor av sätt. Identifiera två sätt som skadlig kod skulle kunna spridas i Caset. Beskriv hur den skulle kunna spridas, men också hur de skulle kunna skydda sig, både via tekniska och administrativa lösningar. (4 p)

b) Nämn *tre* andra relevanta *tekniska* sätt att angripa GHAB (som inte nämns i andra frågor eller i dina svar till denna tenta). Förklara *hur* angreppet skulle kunna ske, vilka *svagheter som skulle kunna utnyttjas*, och *ge för varje svaghet förslag på åtgärder* som skulle kunna skydda mot angreppen och beskriv hur och var dessa åtgärder kan implementeras i GHAB. (6 p)

Fråga 8 (10 p) **Kryptering**

Förklara och beskriv följande begrepp kortfattat. Ange dessutom exempel på var/hur de tillämpas eller var de bör tillämpas i GHABs lösningar.
a) PKI (2 p)
b) Digital Signatur (2 p)

c) GHAB ska genomföra en rejäl satsning på informationssäkerhet och vill förbättra sitt egenutvecklade projekthanteringssystem som beskrivs i Caset. De vill givetvis ha en hög säkerhetsnivå rörande detta. Nämn fyra viktiga delar i deras system som de bör kryptera. Motivera också varför de bör göra det och vilken kryptering de bör använda, och varför. (6p)

Fråga 9 (10 p) **Fysisk säkerhet**

GHAB funderar på att flytta till nya, ändamålsbyggda lokaler där hela deras verksamhet kan samlas i en byggnad.

a) Förklara vad fysisk säkerhet innebär i ett informationssäkerhetsperspektiv och vilka principer som ligger till grund för den. Ge exempel på tre fysiska hot mot informationstillgångar och hur de kan förebyggas eller minskas (6p)

b) Ge förslag på hur caseföretaget ska implementera fysisk säkerhet i sin verksamhet. Beskriv minst tre åtgärder som caseföretaget bör vidta för att skydda sina informationstillgångar och hur de bidrar till att uppnå företagets mål och krav. Beskriv också vad som är viktigast att börja med och varför. (4p)

Här vill vi än en gång påminna om att det är viktigt att i *samtliga* frågor där vi ställer frågan utifrån Caset att du där förhåller dig till det i ditt svar. **Notera att detta innebär att om du enbart svarar med en definition, men inte förhåller dig till caset kommer du inte få poäng alls för ditt svar.** Läs alltså noga igenom Caset och läs noga igenom frågorna ifall du ska svara generellt eller utifrån Caset!

Lycka till!