HÖGSKOLAN
I SKÖVDE

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 20240115

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 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!**

GreenStream Innovations AB – Ledande inom Smarta Energilösningar
GreenStream Innovations AB är ett svenskt teknikföretag som har blivit en tongivande aktör inom utvecklingen av avancerade system för hantering av förnybar energi. Företaget har på bara några år etablerat sig som en pionjär inom sektorn för smarta energilösningar och har skapat sig ett namn genom att erbjuda integrerade lösningar för smarta energinät, energieffektivisering och stöd för övergången till grön energi. Med huvudkontor i Uppsala och satellitkontor i Linköping samt Luleå, har företaget varit en drivande kraft bakom den gröna omställningen i Skandinavien.
GreenStream Innovations AB har cirka 200 anställda och är stolta över att ha en diversifierad och kvalificerad arbetsstyrka som består av experter inom teknik, förnybar energi, affärsutveckling och informationssäkerhet. Företagets VD, Jamal Aziz, baserad i huvudkontoret i Uppsala, leder företagets strategiska riktning och tillväxtinitiativ. Karim Bergström, CFO, är ansvarig för ekonomistyrning och finansiella strategier från företagets huvudkontor. Inom ledningsgruppen finns även Lisa Eriksson, COO, som ansvarar för företagets operativa verksamhet och är baserad på huvudkontoret. På informations- och cybersäkerhetsområdet är det DU som är CISO (Chief Information Security Officer), en central nyckelperson som arbetar från huvudkontoret för att utforma och genomföra företagets säkerhetsstrategier och initiativ. Viktiga nyckelpersoner inkluderar även Sofia Andersson, ansvarig för produktutveckling och innovation, som leder ett team av ingenjörer och forskare från Uppsala-kontoret. På marknadsförings- och försäljningsavdelningen är Peter Johansson, marknadschef, baserad på kontoret i Linköping, ansvarig för att driva företagets marknadsföringsstrategier och kundrelationer. Detta geografiskt spridda ledningsteam och nyckelpersoner återspeglar GreenStreams närvaro i flera städer och visar deras engagemang för att dra nytta av kompetensen på olika platser.

Affärsmål och Produkterbjudande
Företagets affärsmodell är centrerad kring att hjälpa kunder att minska sin energianvändning och koldioxidutsläpp genom innovativa, tekniskt avancerade lösningar. Genom användning av AI och maskininlärning optimerar GreenStream energiförbrukningen hos sina kunder genom att förutsäga konsumtionsmönster och automatiskt justera energiflöden. Deras flaggskeppsprodukt är en AI-baserad plattform som integreras med smarta sensorer och enheter för att skapa självlärande energinät. Detta system har möjliggjort för företag och kommuner att drastiskt minska sitt slöseri med resurser och förbättra sin hållbarhetsprofil.
Strukturella Utmaningar
GreenStream har dock nyligen stött på implementeringsproblem med sitt interna egenutvecklade projekthanteringssystem. Säkerhetsbrister har upptäckts, vilket lett till både dataintrång och riskexponering av känslig information. Detta har resulterat i

förlorad data och oro bland kunder om företagets förmåga att hantera konfidentiell information.
Dessutom har företagets BYOD-policy visat sig vara ett dubbeleggat svärd. Å ena sidan har den främjat flexibilitet och hög personalnöjdhet, men å andra sidan har den skapat komplexitet och säkerhetsrisker. Med ett brett spektrum av personliga enheter som ansluter till företagets nätverk och system, inklusive Android- och iOS-smartphones samt olika versioner av Windows och Mac OS på privata laptops, har IT-avdelningen haft fullt upp med att täppa till säkerhetsluckor.

Teknisk Infrastruktur

För att hantera sin dagliga verksamhet och projektledning använder GreenStream en molnbaserad infrastruktur. Medan detta erbjuder skalbarhet och tillgänglighet, har det också ökat företagets angreppsyta för cyberhot. Nätverksinfrastrukturen på huvudkontoret är robust med redundanta uppkopplingar och avancerad nätverksutrustning, men de mindre kontoren saknar samma skyddsnivå, vilket skapar inkonsekvenser i säkerhetsstandarden över hela företaget.
Projekthanteringssystemet som används är webbaserat för att möjliggöra åtkomst var som helst, men det har blivit tydligt att systemet behöver starkare autentiseringsprotokoll och bättre kryptering för att skydda mot framtida överträdelser.

Säkerhetskulturen och Personalens Roll

För att bemöta säkerhetsriskerna med BYOD planerar GreenStream att byta till ett system där endast företagsägda enheter får användas. Detta kommer att inkludera utrullning av telefoner och laptops med förhandsinstallerade säkerhetsverktyg. Förändringen möts med blandade känslor från personalen som värderar den nuvarande flexibiliteten högt.
För att stärka säkerhetskulturen inom organisationen kommer företaget också att inrätta regelbundna säkerhetsutbildningar. Dessa syftar till att öka medvetenheten om faror som phishing, social manipulation, och andra cyberhot. En ny tjänst som Chief Information Security Officer (CISO) har nyligen skapas för att övervaka säkerhetsstrategin och säkerställa att alla aspekter av företagets säkerhetsrutiner är uppdaterade och genomförs effektivt.

Framtidsutsikter och Expansion

För det kommande året planerar GreenStream att lansera nya produkter och expandera internationellt, vilket innebär att komplexiteten i dataskydd och efterlevnad av regelverk kommer att öka. Med en vision om att fortsätta vara i framkant av den gröna teknikrevolutionen, förstår GreenStream betydelsen av att skydda sin information och sina system. Investeringar i säkerhet har blivit en prioritet för ledningen, och de förbereder sig för en framtid där deras tekniska lösningar kan levereras globalt utan att äventyra säkerheten och integriteten hos de data de hanterar.
Alla dessa utmaningar pekar på behovet av en heltäckande strategi för informationssäkerhet som inte bara fokuserar på tekniska aspekter utan även tar hänsyn till personalens beteende, policyer och processer. GreenStream står inför en spännande men utmanande tid där de måste balansera innovation med informations- och cybersäkerhet för att fortsätta vara ledande inom sitt område.

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.

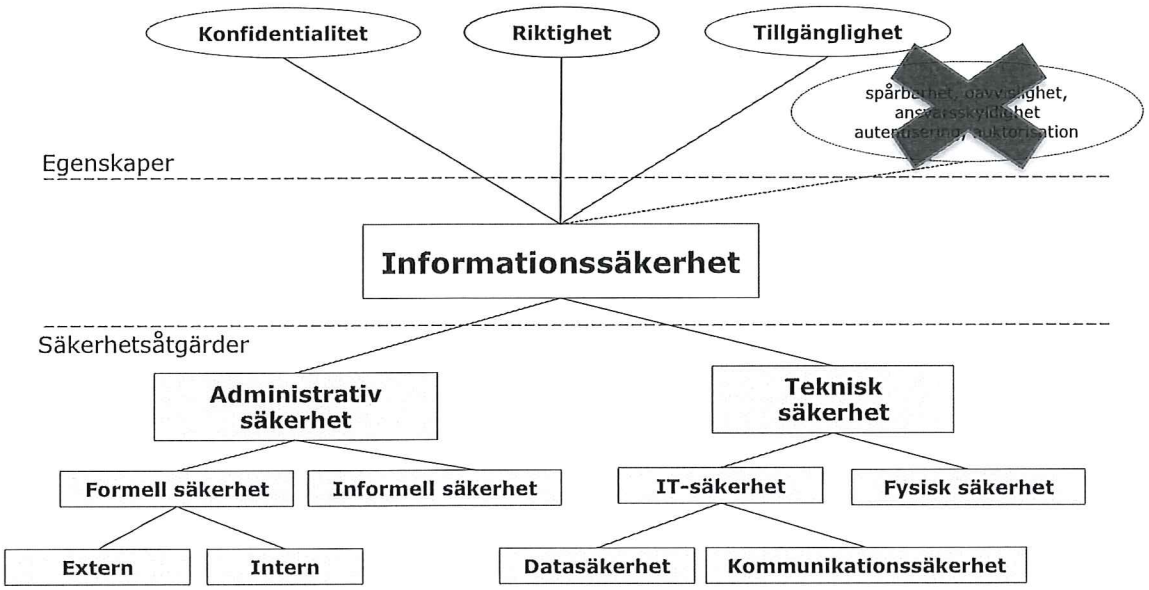
I själva utmaningen med att svara på tentafrågor ligger att planera din tid korrekt; du hinner kanske inte skriva allt du kan om området, men syftet är att du ska lyfta fram det som är viktigt för frågan!

Lycka till!

Del A (Fråga 1) Allmänt om informationssäkerhet

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

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 måste ge minst två 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) Databrottsling (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 har inte tidigare genomfört några 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 GreenStream Innovations AB?
- 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) En generell utmaning inom informationssäkerhetsarbete brukar vara att få ”ledningens engagemang”, dvs. att få högsta ledningen engagerad i att informationssäkerhetsarbete är viktigt. Förklara utförligt dels varför det är viktigt att få ledningens engagemang och ge dels detaljerade förslag på hur du lämpligen kan få ledningens engagemang i Caset. (4 p)

Fråga 4 (10 p) **Juridik**

a) Finns det konkreta säkerhetskrav i några lagar i Sverige? Vilka krav finns det och i vilka lagar? Är någon av dessa av extra vikt för GreenStream Innovations AB? (2 p)

b) Ge exempel på vad som enligt Dataskyddsförordningen är ”särskilda personuppgifter”? Är någon av dessa extra viktig att beakta för Caset? (2 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 caset 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**

Du är väl bekant med vikten av att arbeta med mänskliga aspekter rörande informationssäkerhet. För de angrepp som listas nedan ska du ge:

- Ett utförligt exempel på hur GreenStream Innovations AB 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) ”Microsoft bedrägeri” (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 GreenStream Innovations AB syftar vi på caset på första sidan).

Fråga 6 (10p) **Nätverkssäkerhet**

a) Är det någon skillnad om skadlig kod körs i kernel-mode eller user-mode på en dator? Beskriv vad skillnaden är mellan dessa två "modes" och vilka konsekvenser kan det leda till. (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 GreenStream Innovations AB. (2 p)

c) Ge minst tre exempel på hårdvarulösningar för autentisering. För var och en av dessa, ge två 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**

GreenStream Innovations AB 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 GreenStream Innovations AB (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. (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 GreenStream Innovations ABs lösningar.
a) Symmetrisk kryptering (2 p)
b) Asymmetrisk kryptering (2 p)
c) Digital Signatur (2 p)

d) GreenStream Innovations AB 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! (4p)

Fråga 9 (10 p) **Fysisk säkerhet**

GreenStream Innovations AB 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!