HÖGSKOLAN
I SKÖVDE

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 20230821

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 LMN 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!**

LMN AB är ett litet företag som utvecklar och marknadsför en populär mobilapp för hälsa och välbefinnande. Företaget grundades 2019 av tre vänner som såg en möjlighet att skapa en app som hjälper människor att förbättra sin livskvalitet genom att erbjuda personlig rådgivning, motivation och feedback baserat på användarnas data.
Företaget har idag 15 anställda, varav 10 är utvecklare, 3 är marknadsförare och 2 är administratörer. Företaget har sitt huvudkontor i Göteborg, men de flesta anställda arbetar på distans. Företaget har en platt och informell organisation där alla får vara delaktiga i beslutsfattandet och innovationen.
Företagets affärsidé är att erbjuda en app som fungerar som en digital coach för hälsa och välbefinnande. Appen heter LMN och är tillgänglig för både Android och iOS. Appen samlar in och analyserar stora mängder data om användarnas beteende, preferenser och hälsostatus, såsom steg, sömn, puls, stress, humör, kost, aktiviteter, mål och utmaningar. Appen ger sedan användarna personlig rådgivning, motivation och feedback för att hjälpa dem att nå sina mål och förbättra sin livskvalitet. Appen använder sig av artificiell intelligens, maskininlärning och big data för att skapa individuella profiler och planer för varje användare.
Företaget har idag över 100,000 användare i Sverige och Norge, och planerar att expandera till fler länder i Europa. Företaget har ett freemium-affärsmodell där appen är gratis att ladda ner och använda, men användarna kan betala för att få tillgång till premium-funktioner, såsom personlig coaching, avancerad analys, extra utmaningar och rabatter på hälsoprodukter. Företaget har även samarbeten med olika företag och organisationer som erbjuder appen som en del av sina hälsoprogram eller välgörenhetsprojekt. LMNs framtidsplan är att ta emot VIP-kunder och erbjuda mer personlig coachning, även på plats i företagets lokaler.

Företagets nyckelpersoner är:
Anna Andersson: VD och medgrundare. Hon har en bakgrund inom psykologi och beteendevetenskap, och ansvarar för företagets vision, strategi och ledarskap.
Björn Berg: CTO och medgrundare. Han har en bakgrund inom datavetenskap och artificiell intelligens, och ansvarar för företagets tekniska utveckling, innovation och kvalitet.
Carl Carlsson: CFO och medgrundare. Han har en bakgrund inom ekonomi och entreprenörskap, och ansvarar för företagets finansiering, affärsmodell och partnerskap.
Diana Dahl: CMO. Hon har en bakgrund inom marknadsföring och kommunikation, och ansvarar för företagets marknadsföring, varumärke och kundrelationer.
Erik Eriksson: CSO. Han har en bakgrund inom sociologi och statistik, och ansvarar för företagets dataanalys, forskning och etik.

Företagets planer för framtiden är att fortsätta att utveckla appen med nya funktioner, språk och design som gör den mer attraktiv, användarvänlig och anpassningsbar. Företaget vill också öka sin användarbas genom att marknadsföra appen mer effektivt, skapa en lojal och engagerad community och etablera sig som en trovärdig och ansvarsfull aktör inom hälsobranschen. Företaget har även ambitioner att utforska nya affärsmöjligheter, såsom att erbjuda appen som en plattform för andra hälsorelaterade tjänster, produkter och innehåll.
Företagets teknikplattformar består av följande komponenter:
Appen: Appen är skriven i Kotlin för Android och Swift för iOS. Appen använder sig av olika bibliotek och ramverk för att implementera funktioner som gränssnitt, nätverk, databas, lagring, kryptering, notifikationer, betalningar och tester. Appen kommunicerar med företagets backend via en RESTful API.
Backend: Backend är skriven i Python och använder sig av Django som webbramverk. Backend hanterar logik, beräkningar, autentisering, auktorisering, datahantering och integration med externa tjänster. Backend använder sig av PostgreSQL som relationsdatabas och MongoDB som dokumentdatabas. Backend körs på Amazon Web Services (AWS) som molntjänstleverantör.
Artificiell intelligens: Artificiell intelligens är skriven i Python och använder sig av TensorFlow som maskininlärningsramverk. Artificiell intelligens ansvarar för att samla in, bearbeta, analysera och generera data om användarnas hälsa och välbefinnande. Artificiell intelligens använder sig av olika algoritmer och modeller för att utföra uppgifter som klassificering, regression, klusteranalys, rekommendationssystem, naturlig språkbehandling och bildigenkänning. Artificiell intelligens körs på Google Cloud Platform (GCP) som molntjänstleverantör.
Big data: Big data är skriven i Java och använder sig av Apache Spark som big data-ramverk. Big data ansvarar för att lagra, bearbeta, analysera och visualisera stora mängder data om användarnas hälsa och välbefinnande. Big data använder sig av Apache Hadoop som distribuerat filsystem och Apache Kafka som distribuerat meddelandesystem. Big data körs på Microsoft Azure som molntjänstleverantör.

Företaget har haft två stora säkerhetsincidenter som har påverkat dess verksamhet och rykte:
Dataintrång: I mars 2021 upptäckte företaget att en obehörig person hade lyckats bryta sig in i företagets backend och få tillgång till användarnas personuppgifter, såsom namn, e-postadresser, lösenord, telefonnummer och hälsodata. Personen hade även försökt att utpressa företaget genom att hota med att offentliggöra eller sälja datan om företaget inte betalade en lösensumma. Företaget anmälde händelsen till polisen och Datainspektionen, informerade användarna om intrånget och bad dem att byta lösenord, samt vidtog åtgärder för att stärka sin säkerhet genom att bland annat införa tvåfaktorsautentisering, kryptera datan i transit och vila och anlita en extern säkerhetsexpert för att granska företagets system och rutiner. Företaget utsattes för hård kritik från användarna, medierna och myndigheterna för att ha brustit i sitt ansvar att skydda användarnas integritet och säkerhet.
Denial-of-service-attack: I juni 2022 utsattes företaget för en kraftig denial-of-service-attack som överbelastade företagets backend och gjorde appen otillgänglig för användarna i flera timmar. Attacken var riktad mot företagets API och syftade till att

förhindra användarna från att kommunicera med företagets backend. Företaget upptäckte attacken genom att övervaka sin trafik och prestanda, och försökte att motverka attacken genom att bland annat filtrera ut falska förfrågningar, distribuera sin last över flera servrar och använda sig av en tjänst för att skydda sig mot denial-of-service-attacker. Företaget lyckades till slut återställa sin normala drift, men förlorade många användare och intäkter på grund av attacken. Företaget kunde inte identifiera vem som låg bakom attacken eller vad motivet var, men misstänkte att det kunde vara någon som ville sabotera företagets framgång eller konkurrera med företagets app.

Om du saknar någon information om företaget du behöver för att svara på en fråga får du fritt anta 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.

Du får inte återanvända exempel mellan olika frågor. Du får således inte exempelvis ge använda angrepp från Fråga 5 i varken tidigare eller senare frågor, så läs igenom alla frågor innan du börjar svara på dem.

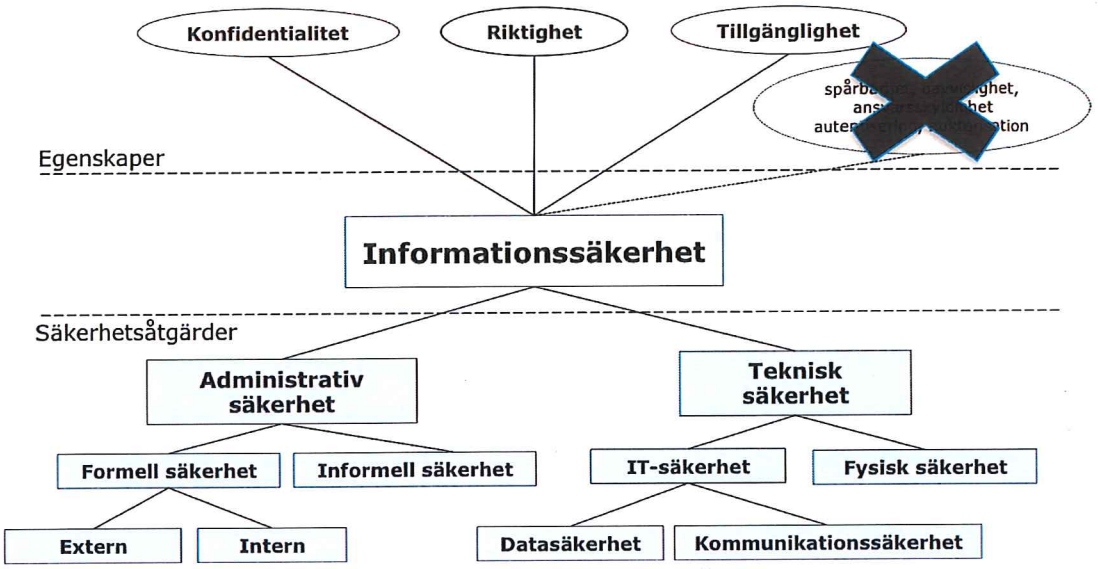
I själva utmaningen med att svara på tentafrågor ligger att planera din tid korrekt; du hinner kanske inte skriva allt du kan om området, men syftet är att du ska lyfta fram det som är viktigt för frågan!

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 romber) 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. *Notera att du alltså måste ge ett exempel för varje begrepp för att få poäng och att de ska knytas till caset!* (7 p)

Utöver detta ska du också definiera och exemplifiera följande begrepp:

b) Beskriv *hot* och *risk* och förklara vad som är skillnaden. (2 p)

c) Informationstillgång (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) Nämn och förklara tydligt två skäl till varför just LMN bör vara motiverade att genomföra en riskanalys innan expansion sker. (2 p)

b) Identifiera två områden som är särskilt viktiga för caset att börja genomföra riskanalyser inom, motivera varför just dessa är särskilt viktiga! (2 p)

c) 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 LMN. (6 p)

Fråga 3 (10 p) **Standarder**

a) Inför en framtida expansion av LMN vill din chef ha svar på följande frågor:

•Vad är ett LIS och vilket konkret värde kan det ha för LMN?
•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 LMN, 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 man lämpligen kan få ledningens engagemang i LMN. (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? (2 p)

b) Ge exempel på vad som enligt Dataskyddsförordningen är ”särskilda personuppgifter”? (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 LMNs verksamhet. (2 p)

d) Om något händer i LMNs system, kan de behöva genomföra effektiva incidentutredningar. Då vill LMN 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 engineering**

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 LMN hade kunnat bli attackerat via det.
- Ge ett förslag på skydd som hade kunnat hindra angreppet
- Ge exempel på vem som skulle kunna använda angreppet
- Förklara varför angriparen hade använt detta angrepp

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

a) ”Microsoftbedrägeri” (2 p)

b) Spear Phishing (2 p)

c) Road Apple (2 p)

d) Dumpster Diving (2 p)

e) Ge ett eget förslag på något angrepp som skulle kunna ske mot LMN baserat på social informationssäkerhet (undantaget de nämnda ovan och på andra platser i tentafrågor) och beskriv detta på samma sätt som de övriga. (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 LMN syftar vi på caset på första sidan).

Fråga 6 (10p) **Nätverkssäkerhet**

a) Förklara utförligt för LMN vad en brandvägg är, hur den fungerar och vilka typer som finns, samt ge ett förslag på bästa brandväggslösningen (typ och placering) för LMN. (4 p)

b) Ge minst tre exempel på hårdvarulösningar för autentisering? Det räcker inte här att bara nämna lösningen, du måste också beskriva var och hur i systemet den kan användas, vad som är bra med den, och vilka potentiella nackdelar den har. (6 p)

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

Fråga 7 (10 p) **Datasäkerhet**

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

a) LMN är bekymrade över om de gör tillräckligt för att skydda sin data. De har hört talas om att ”Hashing” och ”saltning” är användbart i deras app-utveckling. Beskriv utförligt vad ”hashing” och ”saltning” är, hur de fungerar och om de skulle kunna användas i LMNs app, och i så fall var och till vad? Vad kan vara dåligt med ”hashning” och ”saltning”? (6 p)

b) Nämn *två* andra *tekniska* sätt att angripa LMN, 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 angreppet. Inget av de angrep du anger får användas i andra frågor, varken tidigare eller senare. (4 p)

Fråga 8 (10 p) **Kryptering**

a) Förklara och beskriv kortfattat vad asymmetrisk kryptering, symmetrisk kryptering samt PKI är, och hur de relaterar till varandra? Kan något av dessa användas av LMN? Hur? (6 p)

b) LMN kan komma att genomföra en rejäl satsning på informationssäkerhet och vill förbättra sitt egenutvecklade system inför expansionen. Då de har planerat för att ta emot VIP-kunder framöver vill de givetvis ha en hög säkerhetsnivå rörande dessa (och andra konton). Nämn fyra viktiga delar i LMNs system som de bör kryptera. Motivera också varför de bör göra det! (4p)

Fråga 9 (10 p) **Fysisk säkerhet**

Eftersom LMN ska lyckas locka VIP-personer som kunder behövs nya lokaler, snygga och coola lokaler som ska vara lockande att besöka men också ha en hög säkerhetsnivå. Det måste också finnas som dessutom ska vara lätta att besöka, men de ska också vara rymliga med plats för många fler anställda. Ledningen trycker dock mycket tungt på att det inte får kännas som en "bunker", det ska vara "coolt" att besöka lokalerna men också "tryggt och säkert".

a) LMN vill veta vad det finns för *grundkategorier av fysiska skydd*, och vad de omfattar? Detta är något ni har gått igenom på en föreläsning… (2 p)

b) En viktig del av skyddet mot brand rör att välja rätt typ av brandsläckare. Vilken typ av brandsläckare skulle du välja, och varför, vid kontorslandskapet och vid kontorets kök? (2 p)

c) Fysisk säkerhet anses vara viktigt och utmanande. Något som LMN har problem med är hur besökare ska hanteras. Det finns en ovana hos vissa VIP att de besöker LMN:s lokaler när de behöver hjälp, i stället för att göra en normal ärendeanmälan via appen. Det blir således mycket mer besök i lokalerna än vad LMN hade tänkt från början. Detta gör att LMN behöver hjälp med vad som är viktigt att tänka på när företagets personal och besökare går in och ut ur kontoret. Ge en förklaring på vad som är viktigt att tänka på här, varför det är viktigt, och vad ska LMN kräva finns i de nya lokalerna/hur ska de vara designade för att minimera risker med detta, och hur ska de balansera säkerhet och "snygg design"? (6 p)

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 där frågan är att du ska förklara utifrån Caset, så 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!

Vi vill också påminna om att du inte får återanvända exempel mellan olika frågor. Du får således inte exempelvis ge använda angrepp från fråga 5 i senare frågor.

Lycka till!