

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 20250203

Tentamenstid: 8:30 – 14:30

Ansvarig lärare: Marcus Nohlberg

Berörda lärare: Jonas Ingemarsson

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 svarsapper, 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!

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!**

Live Media Network AB (LMN) är ett litet svenskt företag som specialiserar sig på att streama hyperlokala evenemang, såsom fotbollsmatcher i division 2, konstutställningar, lokala konserter och teaterföreställningar. Företaget grundades 2018 av syskonen Fatima och Karim Al-Hassan i syfte att göra lokala evenemang tillgängliga för personer med funktionsnedsättningar som annars inte kunde delta. Efter Covid19-pandemin ökade efterfrågan på streamingtjänster, och LMN expanderade snabbt till att täcka fler typer av evenemang.

LMN har sitt huvudkontor i Växjö och 10 anställda, varav de flesta arbetar med teknisk utveckling, produktion och support. Företaget erbjuder en enkel men professionell streamingplattform där varje evenemang säljs individuellt. Kunden betalar en premiumsumma, vanligtvis mellan 300–500 kronor per evenemang, och får tillgång till en högkvalitativ livesändning. Kunder har konton i LMNs system där de kan lagra betalinformation, eller så lägger de in ny betalningsinformation för varje beställning.

Affärsidé

LMN:s vision är att skapa en plattform för hyperlokal streaming där människor kan ta del av unika evenemang oavsett var de befinner sig. Företaget fokuserar på att erbjuda en personlig och högkvalitativ upplevelse för tittarna samtidigt som de stödjer lokala arrangörer att nå en bredare publik.

Tjänster och Infrastruktur

Streamingplattformen är egenutvecklad och molnbaserad, byggd på AWS för skalbarhet och säkerhet. Varje evenemang säljs via en betalvägg som stöder kortbetalning, Swish och PayPal. Kunden får en unik åtkomstkod för evenemanget. LMN arbetar också med lokala filmteam och egen personal för att säkerställa högkvalitativ produktion av evenemang. Tjänsterna inkluderar livesändningar och inspelningar som kan ses i efterhand. Bland de hyperlokala evenemangen som LMN streamar finns:

- Division 2-fotbollsmatcher.
- Konstutställningar och vernissager.
- Små konserter och lokala festivaler.
- Lokala föreläsningar och kulturarrangemang.

Tidigare incidenter och utmaningar

1. Ett försök att komma åt användardata via ett phishing-angrepp mot företagets betalvägg 2021 hanterades snabbt, och inga känsliga uppgifter läckte. Företaget förbättrade därefter MFA och implementerade starkare lösenordspolicyer.

2. En teknisk glitch 2022 ledde till att en livesändning av en lokal konsert misslyckades, vilket skapade missnöje bland kunderna. Efter detta införde företaget redundanta servrar och bättre testprocedurer innan evenemang.

3. Under 2023 skickades falska e-postmeddelanden till kunder som påstod sig erbjuda återbetalningar. Företaget genomförde informationskampanjer för att utbilda kunder i att känna igen phishing.

4. En oväntad topp i efterfrågan under en populär fotbollsmatch 2024 överbelastade plattformen, vilket ledde till driftstopp i 30 minuter. Företaget implementerade därefter en CDN-lösning (Content Delivery Network).

Organisationsstruktur

- VD: Fatima Al-Hassan – Ansvarig för strategi och affärsutveckling.
- COO: Karim Al-Hassan – Ansvarig för produktion och operativa processer.
- CISO: Lars Holm – Hanterar säkerheten och molnplattformens integritet.
- Supportchef: Mia Andersson – Leder kundsupportteamet.
- Marknadschef: Elin Persson – Ansvarar för att nå lokala arrangörer och kunder.

Vision och Framtid

LMN:s mål är att fortsätta växa genom att bli det självklara valet för arrangörer av lokala evenemang som vill nå en bredare publik. Företaget planerar att utveckla en mobilapp med bättre integration för betalning och streaming samt erbjuda fler interaktiva funktioner, såsom live-chattar och omröstningar under evenemang. De arbetar också på att inkludera automatiserad textning för att göra evenemangen ännu mer tillgängliga.

Säkerhetsstrategi

För att säkerställa säkerheten för både kunder och arrangörer har LMN implementerat följande:

- Zero Trust-arkitektur för att säkerställa att inga enheter eller användare är betrodda utan verifiering.
- Regelbundna säkerhetsutbildningar för personal, särskilt teknisk support och kundservice.
- Snabb respons på tekniska och säkerhetsrelaterade incidenter genom kontinuerlig övervakning och simulerade övningar.
- Samarbeten med externa säkerhetskonsulter för regelbundna revisioner och penetrationstester.

Utmaningar

Som ett mindre företag kämpar LMN med begränsade resurser för att möta den växande efterfrågan på tjänster. Att balansera mellan tillväxt och investeringar i säkerhet och teknisk infrastruktur är en ständig utmaning. Företaget måste också hantera lokala lagar och förordningar för dataskydd i olika regioner.

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!

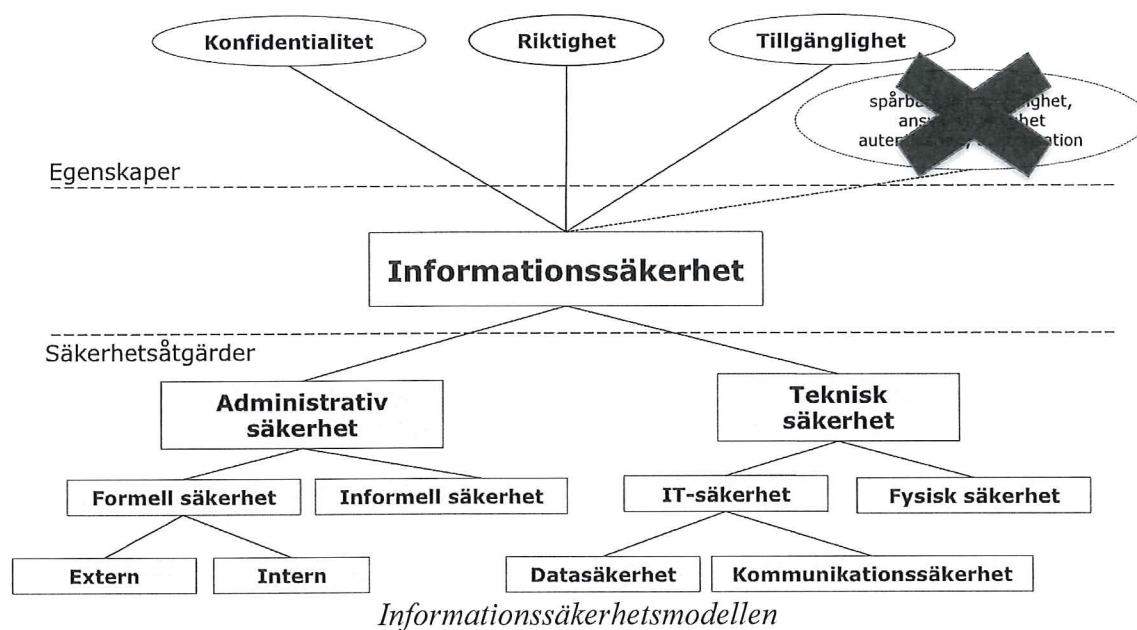
Ni måste skriva läsbart. Är det otydligt får ni noll poäng. Ni måste också lämna in svaren i ordning (fråga 1 – 9). Varje svar måste vara tydligt numrerat, även delfrågor. Saknar ni detta kommer ni inte få poäng för mer än maximalt första delfrågan.

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



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 är ”särskilda personuppgifter” enligt GDPR? (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-artister för att kunna sända deras arrangemang, behövs nya lokaler, snygga och coola lokaler som ska vara lockande att besöka men också ha en hög säkerhetsnivå. Det måste också 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 artister, men även hos några kunder, att de fysiskt besöker LMN:s lokaler när de behöver hjälp, i stället för att göra en normal ärendeanmälan via nätet. Det blir således mycket mer besök i lokalerna än vad LMN hade tänkt från början. 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.

Ni måste skriva läsbart. Är det otydligt får ni noll poäng. Ni måste också lämna in svaren i ordning (fråga 1 – 9). Varje svar måste vara tydligt numrerat, även delfrågor. Saknar ni detta kommer ni inte få poäng för mer än maximalt första delfrågan. Det är inte vår uppgift att leta efter era svar, så lämna helt enkelt in väl numrerat, i ordning, även med delfrågor. Lycka till