HÖGSKOLAN
I SKÖVDE

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 2024 ›0603

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!**

Företagsbeskrivning: PetCare Online AB (PCOAB)
PetCare Online AB är ett framgångsrikt e-handelsföretag baserat i Malmö som specialiserar sig på försäljning av produkter för husdjur. Företaget grundades 2015 och har snabbt vuxit till att bli en ledande aktör inom sin nisch. PetCare Online AB har 80 anställda och en årlig omsättning på omkring 150 miljoner kronor.

Ledningen
VD: Amina Kahn - Med bakgrund inom både detaljhandeln och IT, leder Lisa företaget med en kundfokuserad strategi.
CIO: Carlos Mendes - Ansvarig för företagets IT-strategi och tekniska infrastruktur.
CFO: Lisa Eriksson - Hanterar företagets finansiella planering och ekonomi.
CMO: Johan Persson - Ansvarar för marknadsföring och kundrelationer.

Affärsidé
PetCare Online AB:s affärsidé är att erbjuda ett omfattande sortiment av högkvalitativa produkter för husdjur via en användarvänlig e-handelsplattform. Företaget fokuserar på att ge husdjursägare en bekväm och pålitlig shoppingupplevelse. Det som gör PetCare Online AB unika på marknaden inkluderar:

Produktutbud
Brett Sortiment: Företaget erbjuder allt från husdjursmat och leksaker till vårdprodukter och specialtillbehör för olika typer av husdjur, inklusive hundar, katter, fåglar och reptiler.
Premiumvarumärken: PetCare Online AB samarbetar med kända premiumvarumärken och erbjuder exklusiva produkter som ofta inte finns tillgängliga hos konkurrenter.
Egna Märkesvaror: Utveckling av egna märkesvaror som kombinerar hög kvalitet med konkurrenskraftiga priser.

Kundupplevelse
Anpassade Prenumerationstjänster: Kunder kan teckna prenumerationer för regelbundna leveranser av husdjursmat och andra förbrukningsvaror, vilket ger en bekväm lösning för upptagna husdjursägare.
Personlig Kundservice: Ett dedikerat kundserviceteam som erbjuder personlig rådgivning och support via chatt, e-post och telefon.
Interaktiva Funktioner: En användarvänlig webbplats och mobilapp med funktioner som personliga rekommendationer baserade på tidigare köp och husdjursprofiler.
Miljövänliga Förpackningar: Användning av återvinningsbara och biologiskt nedbrytbara förpackningar för att minska miljöpåverkan.
Lokala Partnerskap: Samarbeten med lokala producenter och leverantörer för att stödja hållbara affärsmetoder och minska transportutsläpp.

Marknad
Företaget har en stark närvaro i Norden men expanderar snabbt till andra europeiska länder. Kunderna består främst av privatpersoner som äger husdjur, med en stor del av försäljningen via deras webbplats och mobilapp.

IT-Infrastruktur
PetCare Online AB:s IT-infrastruktur är en hybridlösning som kombinerar lokala servrar med molnbaserade tjänster:
Servrar: HP ProLiant-servrar för lokala datacenter.
Nätverk: Ubiquiti-switchar och brandväggar för nätverksinfrastruktur.
Molntjänster: AWS (Amazon Web Services) för skalbar lagring och databehandling.
Säkerhetslösningar: Kombination av egenutvecklade lösningar och tjänster från företag som Fortinet och McAfee.

Programvaror och Plattformar
Företaget använder flera olika programvaror för att driva sin verksamhet:
ERP-system: Microsoft Dynamics 365 för affärsprocesser.
CRM-system: HubSpot för kundhantering.
E-handelsplattform: Magento för webbshopen.
Projekthanteringssystem: Egenutvecklat system som körs som webtjänst. Här planeras och styrs alla utvecklingsprojekt i företaget. Det planeras att användas även för att styra och hantera informationssäkerheten i företaget.
Kommunikation: Google Workspace för intern kommunikation och samarbete.

Ransomwareattacken
I januari 2024 utsattes PetCare Online AB för en förödande ransomwareattack som nästan drev företaget i konkurs. Attacken började med att en anställd klickade på en skadlig länk i ett phishing-mejl, vilket installerade ransomware på företagets nätverk. Angriparna använde sedan verktyg som Mimikatz för att stjäla autentiseringsuppgifter och sprida ransomware till flera servrar och arbetsstationer. Angriparna lämnade ett meddelande där de krävde 30 miljoner kronor i Bitcoin inom 72 timmar, annars skulle data förbli krypterad och potentiellt läckas online.

Konsekvenser
Attacken ledde till att webbplatsen stängdes ner under flera veckor, vilket resulterade i stora ekonomiska förluster. Flera kunder valde att avsluta sina prenumerationer och beställningar på grund av osäkerheten kring deras personliga uppgifter.
Företaget tvingades anlita externa säkerhetsexperter och juridisk rådgivning för att hantera krisen. Trots att PetCare Online AB inte betalade lösensumman, lyckades de återställa delar av sin data från äldre backuper som inte var fullständiga, vilket ledde till ytterligare problem med kunddata och orderhantering.
Attacken satte även företagets rykte på spel, vilket krävde omfattande PR-arbete för att återvinna kundernas förtroende.

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.

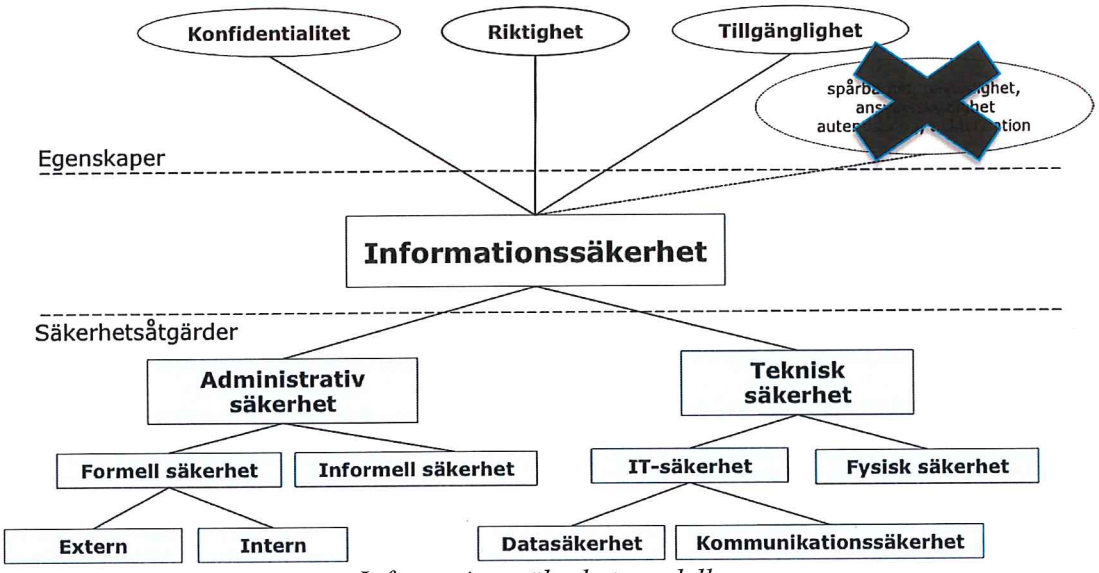
Ni måste lämna in svar på frågorna i ordning (fråga 1 – 9), och ni måste tydligt numrera vilka frågor ni faktiskt svarar på. Om ni inte har numrerat vilken fråga ni svarar på vet vi ju inte att ni börjar svara på ny fråga, då kan ni inte få poäng på detta. Ni får inte heller svara på delfrågorna A, B, C i en enda textmängd utan att tydligt visa vilken delfråga 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) Cybersäkerhet (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 PCOAB?
- 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 PCOAB 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) Vem har (om inte annat avtalats) rättigheterna till programvara som tas fram av:
1) arbetstagare som är anställd för att programmera? (1p)
2) annan arbetstagare? (1p)
3) extern konsult som anlitats för att programmera? (1p)

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 PCOAB 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 PCOAB 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) Whaling (2 p)

b) Tailgating (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 eller vara listat i caset. (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 PCOAB: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)

b) 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 PCOAB. (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**

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

Förklara och beskriv följande begrepp kortfattat. Ange dessutom ett konkret exempel för varje begrepp på hur de skulle kunna hota PCOAB datasäkerhet:

a) Dataförlust (2p)

b) Dataläckage (2p)

c) Rootkits (2p)

d) Beskriv fyra sätt – tekniska och/eller administrativa – som PCOAB skulle kunna använda för att skydda sig mot dessa sorters hot. (4p)

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 PCOABs lösningar.

a) Symmetrisk kryptering (2p)

b) AES (2p)

c) Hashning (2p)

d) PCOAB ska genomföra en rejäl satsning på informationssäkerhet och vill förbättra det 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. (4p)

Fråga 9 (10 p) **Fysisk säkerhet**

PCOAB 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!