HÖGSKOLAN
I SKÖVDE

Institutionen för informationsteknologi

TENTAMEN

Kurs: Informationssäkerhet - Intro

Examinationsmoment: Salstentamen

Kurskod: IT139G

Högskolepoäng för examinationsmomentet: 6

Datum: 20240819

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 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 14

Om caset – läs hela denna text noga!

I samtliga frågor som följer i tentan där vi refererar till ett Case eller SSTAB 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!**

SecureSoft Technologies AB (SSTAB)

Affärsidé: SecureSoft Technologies AB är ett svenskt företag specialiserat på utveckling av avancerade säkerhetslösningar för företag. Deras huvudsakliga produkter inkluderar antivirusprogram, brandväggar, och krypteringsverktyg för företagsnätverk. Företaget erbjuder också konsulttjänster inom IT-säkerhet och riskhantering.

Ledningsstruktur och Nyckelpersoner

Verkställande Direktör (VD): Priya Sharma
Ekonomichef (CFO): Murad Lundgren
Teknisk Chef (CTO): Karin Bergström
Säkerhetschef (CSO): Alejandro Martínez
IT-chef: Lotta Svensson

Styrelse: Består av fem medlemmar inklusive VD, med en extern ordförande som har lång erfarenhet inom teknik- och säkerhetsbranschen.

IT-infrastruktur

SecureSoft Technologies AB använder en hybrid IT-infrastruktur som kombinerar både lokala servrar och molntjänster. Företagets datacenter är beläget i Stockholm och säkerhetskopieras regelbundet till en sekundär anläggning i Malmö. För att hantera sin IT-miljö använder de följande programvaror och tjänster:

- **Operativsystem:** Windows Server 2019, Linux Ubuntu
- **Molntjänster:** Microsoft Azure, Amazon Web Services (AWS)
- **Säkerhetsprogramvara:** Egenutvecklade lösningar, samt tredjepartsprogram från Symantec och Palo Alto Networks
- **Samarbetsverktyg:** Microsoft 365, Slack, Jira
- **Databaser:** Microsoft SQL Server, MongoDB
- **Backup-lösningar:** Veeam Backup & Replication

Incidenten med Industrispionage

År 2022 drabbades SecureSoft Technologies AB av ett allvarligt fall av industrispionage. En anställd som arbetade som systemadministratör blev mutad av en konkurrent och läckte företagshemligheter som omfattade produktplaner och säkerhetsprotokoll. Dessa hemligheter publicerades på darknet, vilket ledde till en omfattande kris.

Läckan resulterade i att företagets nya säkerhetsprodukt, SecureGuard 2023, blev försenad och deras rykte som en säkerhetsledare blev allvarligt skadat. Konkurrenter fick tillgång till deras innovativa teknologier och kunde snabbt släppa liknande produkter på marknaden. Följden blev en dramatisk minskning av marknadsandelar och en nästan total kollaps av verksamheten.

Åtgärder och Investeringar i Informationssäkerhet

Efter incidenten beslutade ledningen att genomföra omfattande åtgärder för att stärka företagets informationssäkerhet. Åtgärderna inkluderade:

1. **Utbildning:** Alla anställda genomgår nu obligatoriska kurser i informationssäkerhet, inklusive regelbundna uppdateringar och simuleringar av säkerhetshot.
2. **Tekniska investeringar:** Företaget har investerat miljontals kronor i ny säkerhetsinfrastruktur, inklusive avancerade intrångsdetekteringssystem (IDS), flerfaktorsautentisering (MFA), och förbättrade krypteringsmetoder.
3. **Fysisk säkerhet:** Företaget har även förbättrat den fysiska säkerheten på sina kontor med biometri, säkerhetskameror, och striktare åtkomstkontroller.
4. **Extern revision:** Regelbundna säkerhetsrevisioner utförs av externa experter för att identifiera och åtgärda potentiella svagheter.

Arbetsmiljö och Effektivitet

De omfattande säkerhetsåtgärderna har dock haft en negativ inverkan på arbetsmiljön. Anställda har uttryckt missnöje över de strikta säkerhetsrutinerna som nu måste följas. Bland annat har flerfaktorsautentisering och omfattande säkerhetskontroller lett till att dagliga arbetsuppgifter har blivit tidskrävande och ineffektiva. Det har rapporterats om långa väntetider för att få åtkomst till nödvändiga system och resurser, vilket har minskat produktiviteten och ökat stressnivån bland personalen.

Många anställda känner att den ökade säkerheten har skapat en byråkratisk arbetsmiljö där enkel kommunikation och samarbete har blivit svårare. Detta har i sin tur påverkat arbetsmoralen negativt, vilket kan leda till högre personalomsättning och svårigheter att behålla kvalificerad arbetskraft.

Juridiska Problem

Incidenten har också lett till flera juridiska problem för SecureSoft Technologies AB. Företaget står inför rättsliga åtgärder från kunder och partners som anser att företaget har brustit i sitt ansvar att skydda känslig information. Flera kunder har ansökt om skadestånd för förluster som orsakats av den läckta informationen. Dessutom har myndigheter inlett utredningar om huruvida SecureSoft Technologies AB har följt lagstiftningen kring dataskydd och integritet.

Företaget har också tvingats att genomföra omfattande interna undersökningar och samarbeta med rättsväsendet för att utreda händelsen. Detta har resulterat i ytterligare kostnader och resursanvändning, samt en ökad oro bland aktieägarna över företagets framtida ekonomiska stabilitet.

Ekonomiska Konsekvenser

De omfattande investeringarna i informationssäkerhet har medfört betydande kostnader, vilket har påverkat SecureSoft Technologies AB vinstmarginaler negativt. Trots detta har aktieägarna uttryckt oro för de höga utgifterna och den kortsiktiga lönsamheten. Det finns dock en optimistisk syn på företagets långsiktiga återhämtning och framgång.

Framtidsutsikter

Trots den senaste tidens motgångar har SecureSoft Technologies AB några mycket lovande produkter under utveckling. En av dessa är SecureVision AI, en banbrytande säkerhetslösning som använder artificiell intelligens för att proaktivt upptäcka och förhindra cyberattacker. Detta projekt behandlas med största möjliga försiktighet och omfattande säkerhetsåtgärder för att undvika ytterligare läckor.

Satsningen på SecureVision AI och andra innovativa produkter har potential att återställa företagets marknadsposition och vinstmarginaler. Om de lyckas lansera dessa produkter utan incidenter, kan SecureSoft Technologies AB åter bli en ledande aktör inom IT-säkerhet.

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 tentamen

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.

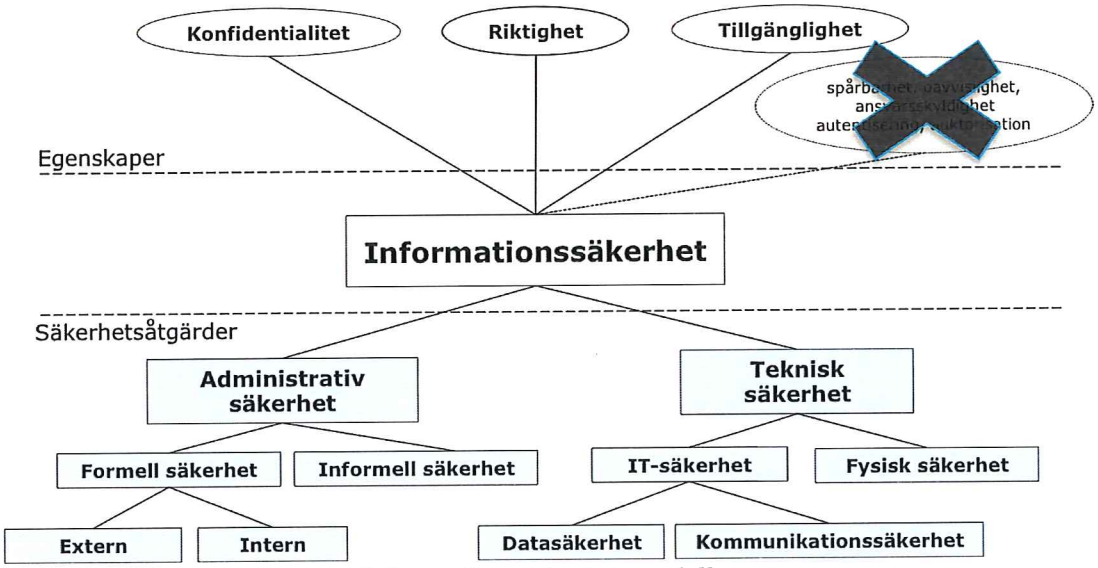
Ni måste lämna in svar på frågorna i ordning (fråga 1 – 9), och ni måste tydligt numrera vilka frågor ni faktiskt svarar på. Om ni inte har numrerat vilken fråga ni svarar på vet vi ju inte att ni börjar svara på ny fråga, då kan ni inte få poäng på detta. Ni får inte heller svara på delfrågorna A, B, 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 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 att just SSTAB bör vara motiverade att genomföra en riskanalys. (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 SSTAB. (6 p)

Fråga 3 (10 p) **Standarder**

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

- Vad är ett LIS och vilket konkret värde kan det ha för SSTAB?
- 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 SSTAB, 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 SSTAB. (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 SSTABs 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 manipulation**

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 SSTAB 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) Whaling (2 p)

b) Spear Phishing (2 p)

c) Road Apple/Baiting (2 p)

d) Dumpster Diving (2 p)

e) Ge ett eget förslag på något angrepp som skulle kunna ske mot SSTAB 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 SSTAB syftar vi på caset på första sidan).

Fråga 6 (10p) **Nätverkssäkerhet**

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

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

a) SSTAB 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 programvara. Beskriv utförligt vad ”hashing” och ”saltning” är, hur de fungerar och om de skulle kunna användas i SSTAB s programvara, och i så fall var och till vad? När kan vara negativt med ”hashning” och ”saltning”? (6 p)

b) Nämn *två* andra *tekniska* sätt att angripa SSTAB, 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 SSTAB? Hur och var? (6 p)

b) SSTAB kommer att genomföra en rejäl satsning på informationssäkerhet och vill förbättra sitt egenutvecklade system inför releasen. Nämn fyra viktiga delar i SSTABs system som de bör kryptera. Motivera också varför de bör göra det! Förklara också vilken typ av kryptering som är lämpligast, och varför. (4p)

Fråga 9 (10 p) **Fysisk säkerhet**

Eftersom SSTAB ska höja sitt generella säkerhetsläge, men också försöka kommunicera detta till sina kunder, vill de renovera sina lokaler så de blir både säkrare, men också ser säkrare ut. De har redan investerat mycket i säkerhetsprodukter, som nämns i caset, men de vill också att kontoret ska vara en inbjudande och kreativ arbetsplats. 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) SSTAB vill veta vad det finns för *grundkategorier av fysiska skydd*, och vad de omfattar? (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 SSTAB har problem med är hur besökare ska hanteras. Det finns en ovana hos vissa kunder att de besöker SSTAB :s lokaler när de behöver hjälp, i stället för att göra en normal ärendeanmälan. Det blir således mycket mer besök i lokalerna än vad SSTAB hade tänkt från början. Detta gör att SSTAB 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 SSTAB 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!