Hemtentamen

HÖGSKOLAN I SKÖVDE

Hemtentamen: IT139G

Informationssäkerhet – Introduktion G1N

Grundnivå 6 högskolepoäng

VT-21

Student: Anton Karlsson

Personnummer: 940916-7534

Tentamendatum: 2021-06-04

Del A (10p)

Fråga 1 (10p)

a) (7p)

Fysisk säkerhet – Så som kassaskåp och inbrottssäkra dörrar, ett fysisk ”skal” som skyddar mot tillgång. RiMaRe behöver ha en byggnad eller avdelning där det finns fysisk säkerhet så som inbrottssäker dörr med lås, de datorer/ipads som är på lagning bör förvaras på ett extra säkert sätt då de ofta är mål för stölder om det finns vetskap om dem.

Tillgänglighet – Att filer och information ska vara tillgängliga för rätt personer, alltså de som behöver ha tillgång och inga andra. Till exempel de i RiMaRe som jobbar med utveckling bör ha tillgång till koder och projektdetaljer om systemutvecklingen men inte de andra som inte jobbar på det. Samt tillgängligheten med administrativa behörigheter gäller också bara för de som jobbar med utveckling, eftersom de behöver den friheten medans de som bara jobbar med support inte behöver det. Rätt tillgänglighet för rätt personer i företaget helt enkelt!

Konfidentialitet – Att data och information samt filer som bör hållas hemliga eller inte spridas till de som absolut inte verkligen behöver det. Till exempel att anställda som har sjukdomar och har statligt bidrag för mediciner vill ha sin data konfidentiell, den informationen bör förvaras tryggt och som nämnt i ovanstående exempel att tillgängligheten ska begränsas till endast de som det är absolut nödvändigt för. Kan även vara utvecklings projektet på system och mjukvara som de lagt ned mycket tid och resurser (pengar) på vill man hålla konfidentiellt (källkoden) så ingen kopierar eller stjäl den. Om källkoden läcker kan säkerhetsbrister enklare hittas.

Extern – Externa säkerhetsåtgärder kan vara att följa lagar och riktlinjer satta utav landet i fråga (tvärtemot interna regler och riktlinjer (policies)). RiMaRe’s molntjänster i fråga bör hållas koll på vart de är placerade och vilka regler och lagar det landet följer om informationslagring och datahantering, även följa det egna landets lagar och regler m.m. För deras egen utvecklade webblösning för de följa lagar och regler om datahantering på personalens beställningar, antagligen står anställningsnummer, personnummer och dylikt med i beställningen, kanske även befattning. Om detta är outsourcat kan det vara bra att se till att denna informationen inte lagras utomlands på ett osäker sätt.

Intern – interna riktlinjer så som policies, är det ramverk som satts upp utav företaget/föreningen själva. RiMaRe bör ha egna policies som de anställda följer, om till exempel hur förvaring utav de utgivna it-produkter (hp laptop, iphone, ipad) ska ske, samt användning av dessa produkter. Om det är okej att ta med sig dem hem och använda för privatbruk eller om de är strikt endast för arbetsplatsen och jobbuppgifter.

IT-säkerhet – att ha ett anti-virus och brandvägg på datorn för att skydda sin teknik mot obehörig tillgång utifrån samt lösenord eller kod för lokal tillgång till datorer och dylikt. Kan även vara tillgång till server på nätverket. Hos RiMaRe bör det finnas kod/lösenord för alla laptops så att inte vem som helst som har kommit över en av deras laptops kan gå in och börja kolla runt. Gärna använda två faktors autentisiering (med deras iphones). VPN-tillgång med användarnamn och lösenord för externa lagringsservrar för att bibehålla säkerhet och även spårbarhet.

Riktighet – att man ska kunna lita på att informationen är korrekt och fri från fel. De på RiMaRe behöver kunna lita på att deras filer och data är korrekta som är lagrade, detta område tangerar även tillgänglighet (att rätt personer ska ha rätt tillgång), bara de personer som absolut behöver redigerings privilegier ska ha det, resterande som endast behöver ha läsbehörigheter ska ha det. Då blir chansen för handhavande fel markant mindre, de som inte ska in och ändra i filer ska inte ha den behörigheten. Även att kolla upp riktigheten till exempel vid beställning utav hårdvara via webbtjänsten så bör beställningar kollas upp så att anställda inte beställer på andras anställningsnummer etc, då kan ett telefonsamtal göras till respektive kund för att säkerställa att beställning är korrekt.

b) (2p)

Tillgång är att ha fysisk tillgång och tillgänglighet till att nyttja till exempel datorer och nätverk. Medan informationstillgång är behörighet att få läsa dokument eller filer. Till exempel som anställd kan du ha tillgång till nätverket och dess server genom din HP laptop, men du har inte informationstillgång för de filer som innehåller information om de anställda, den informationstillgången är enbart tillgänglig för chefer. Kan även vara icke tekniska tillgångar, det ryktas om varsel på jobbet och den informationstillgången är endast för de högt upp i det administrativa på RiMaRe till exempel.

c) (1p)

Oavvislighet är att man ej ska kunna förneka något, till exempel om ett meddelande har skickats på företagets interna chat nätverk eller ett klassiskt email från jobbkontot så finns det spårbarhet och ett innehåll i meddelandet som inte kan förnekas. Har en anställd på RiMaRe skickat något dumt eller stötande till en kollega så syns detta och kan bevisas. Om spårbarhet erhålls kan till exempel det synas att någon har gått in och tagit bort en fil som är viktig, då ska det synas att ”Olof Karlsson” har varit inne och tagit bort en fil, då finns det en klar oavvistlighet gentemot honom.

Del B (40p)

Fråga 2 (10p)

a) (4p)

I RiMaRe's riskanalys bör de gå över riskerna med att gå ifrån ”vanliga datorer” till Ipad, kan ipadsen hålla en tillräcklighet hög säkerhetsnivå och relians. Kommer det finnas bra antivirus och brandväggs ”appar” att installera för att höja säkerheten. Kommer det även ha en kompatibilitet med det nuvarande nätverket eller kommer de inte funka så att en gammal dator får stå kvar för att ha tillgång till den gamla servern som då blir en säkerhetsrisk istället.

Databasen med alla ärenden och individens kunskapsnivå är något man bör göra en riskanalys på, eftersom datan där i kan hålla känsllig information. Eftersom RiMaRe har att göra med kommunanställda samt POLITIKER kan information där i vara något som politikerna inte vill ska komma ut. Exemplen är många men ett kan vara att det står att en politiker har fått virus och därför fått support för att få bukt med detta (viruset kan ha kommit från att ha laddat ned suspekta filer eller olämplig webbsurfning på jobbet). Detta kan minst sagt vara problematiskt och är något de inte vill att det ska stå om i tidningen att hen har porrsurfat på jobbet och fått virus och hens ”kunskapsnivå” är väldigt låg om IT-säkerhet. Eftersom politiker är publika och relativt utsatta figurer så kan detta vara en säkerhetsrisk som bör ses över i riskanalysen.

Processen för riskanalysen bör skötas av ett konsultbolag inom IT-säkerhet som har tidigare kunskap om detta, ge dom den information och tillgång som är nödvändig för att kunna utföra riskanalyser på de nedanstående punkterna. Eftersom IT-supportarbetarna på RiMaRe behöver fortsätta att just supporta, samt de har ingen tidigare erfarenhet inom just säkerhet. Möjligvis nyanställningar och utbildning inom säkerhet kan vara ett annat val men betydligt längre tidsram krävs då. Konsulterna behöver även prata med supportarbetarna och administrativa personalen för att få ”hela bilden”.

Riskanalysen bör baseras på tidigare undersökningar om ipad säkerhet (IOS och apple enheter överlag) samt se över om det finns rapporter på tidigare säkerhetsproblem inom RiMaRe med dessa produkter. Samma gäller databasen med ärenden, har den blivit hackad förut? Kolla upp rapporter och undersökning om liknande servrar, om det finns sårbarheter och om de är lätttillgängliga för att hacka sig in på servern. Kolla om det funnits hack-försök tidigare eller obehörig access. Samt processen för riskanalysen

Resultaten från rapporter och undersökning kan hjälpa till att beräkna riskerna och sannolikheten för att det ska inträffas, så att man vet vilken grad av säkerhet och investering som behövs på de olika områdena. Lagom mängd säkerhet är alltid bäst, istället för att lägga alla sina pengar på att skydda något som inte är så värdefullt eller är extremt låg risk.

b) (6p)

Allmänna mål – Vad ska primärt uppnås med säkerhetsarbetet, det är viktigt att RiMaRe vet vilka mål som gäller och ska uppfyllas. Till exempel målet kan vara att inget data

läckage ska ske, då behöver all personal veta om detta så att samtliga kan jobba med detta och företaget kan jobba åt samma håll.

Omfattning – För vilka delar av verksamheten gäller policyn? Väldigt viktigt att veta för personalen på RiMaRe att om en del policies inte gäller för ens egna avdelning, eller en policy som finns och enbart gäller för de som sysslar med utveckling. Då är det viktigt att de som sysslar med utveckling vet om att den policyn gäller just dem.

Fastställande av ansvar – Mycket viktigt att fastställa vad för ansvar de anställda har, ett exempel kan vara att sista person som går hem för dagen ska låsa dörren. Såklart finns det mer tekniska aspekter på det hela, om att man inte ska lämna datorn olåst eller att inte ge närstående access till datorn om de får ta med sig datorn hem och använda för personligt bruk. Samt om dessa policies skulle brytas så vet personalen om att de bär det yttersta ansvaret eftersom de brutit policyn.

Fråga 3 (10p)

a) (6p)

LIS är ett ledningssystem för informationssäkerhet som innehåller riktlinjer och policies, för RiMaRe har det ett bra värde att om expansioner fortsätter i högfart så blir det svårt att gå igenom alla policies som gäller för varje individ. Då finns detta styrdokument på plats för att informera personal om vad som gäller, LIS kan gå igenom till exempel användning av internet och e-post på arbete, åtgärder till skydd mot skadlig kod, incidenthantering och loggning m.m. Värdet är högt då all personal vet vad som gäller och förhoppningsvis minska risken för incidenter och onödiga samtal om till exempel internet användningen med mera.

Instruktioner – Ett LIS bör innehålla instruktioner för säkerhetsarbetet, vilket kan komma väl tillhands när expansionen kommer igång så att instruktioner finns redo att tillhandahållas till de nyanställda. Även instruktioner över andra delar där det är kritiskt att arbetet sker på rätt sätt, till exempel vid hantering utav ordrar på RiMaRe.

Rutiner – Ett LIS bör innehålla de rutiner som RiMaRe har, som är godkända utav ledningen. Visserligen kan det finnas rutiner på arbetsplatsen som inte är godkända utav ledningen i ett säkerhetsperspektiv. Det är viktigt att de rutiner som är korrekta och godkända finns nedskrivna och tillgängliga, då blir det enklare att slussa bort de dåliga rutiner som finns när man kommer in som nyanställd, finns rutinerna inte med i LIS så är de inte korrekta och stödda utav ledningen.

Policy – de allmänna säkerhetsregler och riktlinjer RiMaRe jobbar med, en policy kan vara att man aktivt ska jobba med ISO 27001 och 27002. Man behöver skriva upp de riktlinjer och policies man vill ha på RiMaRe som är stödda av ledningen för samtliga arbetare och hur man ska efterleva ISO standarderna.

Först och främst skulle jag börja med att skriva upp de instruktioner som är kritiska för de nya arbetarna att kunna och känna till, så att transitionen blir så smidig som möjligt och inte hela tiden får felhantering utav ny personal. Utan det ska finnas klara och tydliga instruktioner hur arbetet och dess säkerhet ska fortgå.

b) (4p)

Metodstödet bygger redan på ISO/IEC 27001 ledningssystem för informationssäkerhet, därför om RiMaRe implementerar och jobbar med metodstödet från informationssäkerhet.se så har det en god grund att jobba med, metodstödet är upplagt mer som ett projekt än policies och riktlinjer så som ISO standarderna. Det finns såklart skäl till att använda båda för att ha en högre säkerhet och följa ISO standarden kan man få en ISO certifiering på RiMaRe. Fördelar är en högre standard och säkerhet samt certifiering för att visa utåt mot kunder att man har en bra informationssäkerhet, nackdel är att det blir mycket mera jobb, kan behövas anställas konstulter för att driva projektet på en tillräckligt hög nivå, och blir därför mycket dyrt.

Fråga 4 (10p)

a) (8p)

Se till att verksamheten har tillräckligt bra skydd för personuppgifter i IT-systemen, de personuppgifter RiMaRe tar in på sina beställningar behöver lagras på ett säkert sätt och minska tillgång till de som behöver det.

Undersöka om vi behandlar personuppgifter med rätt rättsligt stöd, kan hända att man har flera alternativa grunder för sin behandling. Om RiMaRe har personuppgifterna lagrat på en molntjänst i ett annat land kan det finnas flera grunder för personuppgiftsbehandlingen. Viktigt att ta reda på vad som gäller i landet, samt följa det som gäller i Sverige.

Ta reda på vilken information och data som hanteras inom olika delar av din organisation, man behöver då veta att det är RiMaRe's server och nätverks avdelning som sköter detta (vi antar att de skapar denna avdelning i expansionen) primärt och hushåller datan, men sedan kan denna datan användas på andra håll i verksamheten, detta behöver då vetas om och dokumenteras samt att de andra avdelningar måste också veta om vad som gäller om de hushåller denna datan någon annanstans också!

Undersöka hur dataskyddsförordningen kan påverka RiMaRe och om det behövs fler resurser för att kunna anpassa sig till kraven. Om det då kommer fram att RiMaRe måste hushålla all personuppgiftsdata i en lokal server så kan det behövas investeras mycket pengar i just ett bättre server nätverk, detta kan medföra platsbrist och stora omkostnader, går det att genomföras blir då frågan.

b) (2p)

Det krävs att RiMaRe får det skriftligt att upphovsmannen (anlitade leverantören) tilldelar de fulla rättigheterna till verket, eller ensamrätten och detta gäller då produkten visar individuell särpregel att det just är gjort för RiMaRe och ingen annan.

Fråga 5 (10p)

a) (2p)

Ett exempel på VD-bedrägeri är där att man på något sett gör en e-postadress med en anknytning till Lennart Lång (VD för RiMaRe AB). Sedan skickas ett e-post där det står att en stor summa pengar ska överföras snabbt till ett annat konto för en betalning för något. Detta är då ett fake-konto som vill ha pengar till ett fake företag.

Ett skydd mot detta är att enbart ta emot jobb mail från de riktiga jobbmails adressen till exempel @rimare.se och har de inte denna domän så filtreras de bort. Eftersom de inte är jobbrelaterade är de inte heller releventa för ekonomi avdelningen. Samt digitala signaturer är en bra skyddsfaktor, att VDn själv måste godkänna med en digital signering.

VD bedrägeri skulle kunna uttnytjas av de flesta med företagskunskaper samt tekniska kunskaper för att kunna efterlika en person så mycket som möjligt tekniskt sett.

Att utbilda och informera om att dessa bedrägerier finns och är relativt vanliga i dagsläget höjer medvetenheten inom RiMaRe och kan då få personal att flagga eller dubbelkolla för att säkerställa att detta inte är ett lurendrejeri.

b) (2p)

Spear Phishing kan ske genom att en hacker kan få reda på information om att RiMaRe utvecklar en ny programvara och förväntar sig nya filer eller dokumentation från leverantör, då kan en person utge sig för att vara just den leverantören och istället skicka skadliga filer så som malware eller randomware eller andra typer av infekterade filer med skadligt uppsåt.

Denna kan vara svår att skydda sig emot, då återigen för man dubbelkolla epost-adressen eller där man har sig fildelning, om man har fildelningen via molnet istället så som dropbox eller github ska de på RiMaRe se till att enbart den betrodda levenrantören har tillgång och om någon ny kommer och frågar om tillgång ska man ta det som ett hot.

Här är det de med extremt hög teknisk kunskap som har kunnat övervaka RiMaRes aktiviteter eller sitter på insider information som kan göra detta, om informationen inte stämmer blir det svårt att lyckas genomföra ett spear phishing försök, det blir då alltför suspekt med rätt bakgrundsinformation.

Utbilndning på att endast dela med sig utav känslig informatin igenom rätt kanaler för att hålla känslig information mindre benägen till att övervakas/läckas.

c) (2p)

Ett exempel på ID stöld kan vara att någon får åtkomst till en jobbmail på RiMaRe och sedan utgör sig för att vara mig och skicka epost från anton@rimare.se och säger att hen har glömt inlogget till laptopen och får det utskickat från support. Då har denna personen fulltillgång till min laptop om hen skulle komma i kontakt med den eller om den är så pass teknisk att den kan sätta upp remote access.

Ett realistiskt skydd för detta är att påtvinga 2FA på alla jobbkonton, då minskar risken avskyvärt för otillåten kontoåtkomst.

Någon som vill ha åtkomst till RiMaRe's dator och ta reda på mera information, personen behöver hög teknisk kunskap för att lyckas med detta.

Utbilda om att inte bli phishad eller lurad av någon som skriver att hen behöver åtkomst från företaget, samt inte spara lösenord uppskrivet så att någon kan se det.

d) (2p)

RiMaRe kan bli DOS attackerade, en person eller ett företag kan sen lägligt skicka epost och skriva att det är experter på att DOS säkra servrar, de kan då blir anlitade mitt i DOS attacken för att de är desperata på RiMaRe, då kan dessa som då attackerade från början få jobbet och tillgång till deras server och nätverk.

Ett realistiskt skydd mot detta är att kolla upp de företag man anlitar och betror med information och tillgång, de ska funnits med och verka riktiga. Samt ta information om de anställda som det anlitade företaget skickar ut så man har en spårbarhet på att det är en anställd person och inte en bedragare som utgers sig för att jobba på till exempel Telia. Samt även ha ett bra DOS skydd från första början.

Någon som vill stjäla information från servern, företagsspionage kan vara en möjlighet gentemot RiMaRe.

Utbilda personalen på RiMaRe att klara av nätverksattacker inhouse och slippa outsourcea detta till andra företag som då kan vara en säkerhetsrisk.

e) (2p)

RiMaRes anställda kan bli måltavlor för tailgating om skalskyddet inte är tillräckligt bra, eller om de blir förföljda och spionerade på utanför RiMaRes lokaler. Förövaren kan klä ut sig till en vaktmästare eller städare och sedan gå runt och spionera på kontoren. Förövaren kan då se eller höra känsliginformation samt få tillgång till olåsta datorer.

För att skydda sig mot detta krävs passerkontroller för de anställda och id bekräftelse, fast någon som faktiskt jobbar som en vaktmästare men blir kontaktad för att spionera kan bli väldigt svårt att förhindra, nästintill omöjligt.

Personer som jobbar och har tillgång till RiMaRes lokaler.

Utbilda i att dessa sociala attacker finns, och riktlinjer om att alltid låsa datorer som inte används för stunden samt inte prata om känslig information i närheten av personer du inte känner till eller vet inte har behörighet till informationen.

Del C (40p)

Fråga 6 (10p)

a) (2p)

När ett lösenord sparas i hashat format blir det då mycket svårare att avläsa lösenordet om någon skulle få åtkomst till datorns filer, står den i klartext ser man direkt att lösenordet är ”hej123” till exempel istället för en sträng med oklar text.

Vid inloggning så hashas lösenordet för att sedan matchas mot det lagrade hashade lösenordet, om de överensstämmer så loggas man in. Vilket används på RiMaRes laptops vid inloggning.

b) (2p)

Brandvägg fungerar som ett filter som filtrerar paket mellan externa och interna källor. Paketfiltrering är den lättaste typen av skydd och kollar på paketets header (namn). Brandväggar gör filtrering för att avgöra om datan ska släppas förbi till användaren eller inte. De här besluten är baserade på regler som fastställts av administratören när datorn och brandväggen konfigureras (brandväggar för personligt bruk är oftast konfigurerade från start). Brandväggen skyddar mot väldigt basic threats, avancerade nya hot kommer den inte att kunna filtrera bort.

RiMaRe bör använda någon form utav brandvägg på samtliga HP laptops och nätverket på kontoret, en lokal brandvägg på laptopsen kan skydda dom vid användning hos andra kunder på deras nätverk.

c) (6p)

Tre olika hårdvarulösning för autentisering är USB-nycklar som innehåller en inloggningstoken, Fingeravtrycksläsare som gör det möjligt att logga in med sitt fingeravtryck så som mobiler (RiMaRes iphone 12 t.ex.). Accesskort (fungerar ihop med bluetooth i ett chip på något vis), som jag vet med egen erfarenhet finns tillgängliga att använda ihop med HP Security, att man då med hjälp av ett accesskort kan ge åtkomst till HP laptopen om man inte vill använda sig utav de ovanstående exmplen eller lämna ifrån sig biometrisk data.

Att man behöver använda sig av fingeravtrycksläsare enbart på sin jobbtelefon (iphone 12) kan vara användbart, då kan absolut ingen utom en själv komma in. Att införa passerkontroller med fingeravtryck till kontor och dylikt på RiMaRe kan vara en bra idé med tanke på att fingeravtrycksläsare inte längre är så dyra.

USB-nyckel med inloggningstoken är ett bra sätt att enbart ge den personen som besitter USB-stickan åtkomst till datorn, dock behöver man då vara mycket noga med vart man placerar denna och inte tappar bort den. Fungerar bra till RiMaRes laptops som ett kompliment till användarnamn och lösenord, blir då en två faktors autentisiering.

Att ha flertal nycklar på USB-nyckeln så kan man implementera att för att få lokal tillgång till deras egna server på RiMaRe som finns kvar så behövs en USB-nyckel samt inloggningsuppgifter.

Fråga 7 (10p)

a) (4p)

Ett hot som finns är att om personalen på RiMaRe skulle dra på sig skadliga filer eller kod så finns det en spridningsrisk via molnet, om detta laddas upp till deras molntjänst och sedan kommer nästa användare och förutsätter att allt är frittfrån virus och synkar dessa filer med sin egna laptop så har då viruset spridit sig.

För att skydda sig mot detta är det bästa man kan göra att ha ett bra anti-virus program och brandvägg på alla datorer och molnsynkade apparater för att minimera risken att infekterade filer laddas upp på molntjänsten detta är såklart också aplicerbart på den lokala servern på RiMaRe.

Ur ett administrativt säkerhetssätt så kan man överlåta uppladningen till en som är mycket insatt i skadliga filer som får rannsaka de filer som ska laddas upp till molnet och godkänna dem innan det blir ”commitat” (så som github fungerar med push och commit)

Ett sätt som är ganska långsökt kan vara att någon köper en liknande HP dator som är infekterad från början och sedan utger sig för att vara en kommunanställd och behöver support på sin dator och vill få lämna in den. Datorn kan då vara infekterad med rootkits, malware, ransomware med mera så att vid aktivering och uppkoppling mot RiMaRe’s nätverk kan den då få tillgång och göra skada när den skadliga koden körs och sedan infektera alla apparater på nätverket.

För att motverka detta behöver man kolla upp vem det är som lämnar in datorn på support hos RiMaRe (spårbarhet) och matcha mot kommunens anställda om detta stämmer, samt ha någon typ av hårdvaru matchning. Det bör finnas en inventeringlista på alla laptops och telefoner med serienummer eller någon typ av nummrering. Om nummreringen då inte stämmer kan man då se att denna laptopen inte tillhör något kommunaltanställd eller anställd på RiMaRe. Detta kan göras i en elektronisk lista eller databas så man enkelt kan matcha serienummren.

Administrativt sätt kan man sätta krav på att få behörighet från ledningen att lämna in sin laptop på support, finns inte behörigheten så får laptopen inte komma på support. Då kan inte heller vem som helst komma och lämna av laptops från första början, då kan RiMaRe neka att ta emot laptopen.

b) (6p)

Ett real-life trojansk angrepp, där infekterad hårdvara tar sig in på kontoret och aktiverad i en enhet på RiMaRes nätverk som ett ärligt misstag, där en anställd hittat en usb-sticka liggandes på golvet eller utanför lokalerna. Svagheten här är okunskap hos personal, utbildning och policies i att inte använda okänd hårdvara på RiMaRes datorer och nätverk.

Fråga 8 (10p)

a) (2p)

En digital signatur är en signatur som ges med hjälp av ett digitalt identifikations program så som bankID, där man med hjälp av en lösenordskord och ett utfärdat bankID som bara du har tillgång till kan användas till att signera saker. Vid påskrivningar utav dokument eller färdiga ordrar kan de på RiMaRe signera deras arbete och då vet man att det är ju denna personen som gjort detta. Eller låta VDn på RiMaRe signera dokument på avstånd så han inte måste åka in till kontoret varje gång.

b) (2p)

Steganografi handlar om att dölja information, så att den inte syns. Krypterad information ser man men man kan inte avläsa den. Här är det tvärtom, om du hittar den kan du avläsa den, men tanken är att gömma information. Till exempel gömma data i en mp3 fil.

Steganografins användsningsområde känns lite uråldrigt för dagens företag, men RiMaRe kan använda det för att gömma en lösenordslista över alla användarna i ett dokument som heter Städlista.pdf, de flesta hackersen skulle antagligen inte leta där eller leta där sist!

c) (2p)

PKI kan vara användbart att använda för RiMaRe på deras domän så som webbtjänst och epost för att verifiera identiter så som beställarna på webbtjänsten och kan då också använda sig utav signerad e-post med hjälp av CA-certifikat. Detta är dock bara relevant om de står för hostningen själva, om allt outsourceas kommer detta antagligen att tillhandahållas av leverantören utav tjänsterna.

d) (4p)

Symmetrisk kryptering använder sig bara utav en nyckel för att kryptera och dekryptera, medan assymterisk använder sig utav två olika nycklar, en för kryptering och en för dekryptering. För RiMaRe passar assymetrisk bäst då den har generellt högre säkerhet eftersom det är två nycklar involverat. Ett företag som bearbetar personuppgifter och dylikt bör hålla en hög säkerhet (följa ISO standard 27000).

Enkel förklaring till VDn på RiMaRe: Det är bättre att använda en säkerhetsmetod där man behöver två olika nycklar för två dörrar, istället för en metod där en nyckel går till två olika dörrar, för säkerheten på företaget.

Fråga 9 (10p)

a) (4p)

Skalskydd – så som dörrar, väggar och lås. Ett skydd runt sin verksamhetslokaler så obehöriga ej kan ta sig in.

Larmskydd- i form av larm, detektorer som triggar larmet, kan även vara kameror med mera.

Punktskydd – Lokala skalskydd där man behöver extra skydd och förvara värdefulla föremål eller känsligdata.

RiMaRes verksamhet blir påverkad så att de bör införa passerkontroller i de nya lokalerna för att öka skalskyddet samt minska tillgängligheten för obehöriga. De på RiMaRes kommer också behöva larma deras nya lokaler vid slutet av arbetsdagen, de behöver anlita en larmfirma som kan svara på larm vid inbrott. RiMaRe kan behöve investera i ett kassaskåp för att förvara USB-nycklar och passerkort som är aktiva men inte i bruk för att minimera risken att de kommer i obehörigas händer, även dyr elektronisk utrustning kan vara bra att låsa undan.

b) (4p)

I ett seriöst och stort företag så som RiMaRe siktar på att bli så bör passerkontroll implementeras och loggning utav besökare. Om en besökare ska få komma in måste den bli hämtad vid entré av en i personalen och säkerställa att besökaren inte är ett hot mot verksamheten (RiMaRe). Ett foto eller kamera i en bra vinkel som kan spela in personen som kommer på besök för spårbarhet vid incident, men för att göra detta krävs en framtaget dokument som besöker behöver skriva på och acceptera bilden/övervakningen. Generellt sett bör inte en arbetsplats vara videoövervakad, därför ska kameror endast sitta utomhus för bevakning eller i entré hallen mot dörren för att se inpasserande i RiMaRes nya lokaler. Kameran utomhus kan då också säkerställa att besökaren har lämnat lokalerna.

Passerkort för varje rum är att föredra (liknande passerkontrollen på Högskolan i Skövde för varje studierum och lektionssal) gärna med spårbarhet, så man kan se vilken anställd var det som gick in i rummet när till exempel en incident skett.

Passerkorten bör också ha olika behörigheter i de nya lokalerna, till exempel bör inte support personalen på RiMaRes komma in på VDns kontor.

c) (2p) För att enbart kunna släcka en mindre brand inne på RiMaRes kontorslandskap skulle jag välja en koldioxid släckare eftersom det finns elektronik och man vill helst inte smutsa ned och förstöra hela kontoret för en mindre brand och förstöra all elektronik. Koldioxidsläckaren släcker flammor snabbt och rent men är inte så bra på glöd, men om det är i papper det har börjat brinna så är det antagligen ingen glöd då det snabbt flammar upp samt tyger så som köksdukar och dylikt.

(Vattenslang ikopplad till vattenledningen i köket på RiMaRes nya lokaler kan vara ett alternativ om branden börjar bli större och att rädda elektroniken känns orelevant).