Säkerhetsrevision av informationssystem

-

Vilka aspekter bör beaktas?

(HS-IDA-EA-03-301)

David Alpsten (a00daval@student.his.se)

Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Examensarbete på det systemvetenskapliga programmet under vårterminen 2003.

Handledare: Gunnar Buason

Säkerhetsrevision av informationssystem

-

Vilka aspekter bör beaktas?

Examensrapport inlämnad av David Alpsten till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för Datavetenskap.

2003-05-21

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Säkerhetsrevision av informationssystem

-

Vilka aspekter bör beaktas?

David Alpsten (a00daval@student.his.se)

Sammanfattning

Information och data har i en allt större utsträckning blivit en resurs som organisationer är beroende av och grundar sin verksamhet på. Precis som andra värdefulla resurser så måste också denna skyddas mot obehörigas åtkomst. Detta examensarbete handlar om systemförvaltning och arbetet med att revidera säkerheten i ett datorsystem. Eftersom denna typ av revision är en väsentlig del av arbetet med att upprätthålla säkerheten i ett system, är det följaktligen viktigt att känna till hur en säkerhetsrevision genomförs. I resultatet presenteras ett antal olika aspekter och delområden som bör granskas vid en revision av säkerheten hos datorer i ett datorsystem. Resultatet visar även att det är svårt att finna någon enskild modell eller standard som täcker samtliga aspekter som bör undersökas vid en säkerhetsrevision.

Nyckelord: Säkerhetsrevision, informationssäkerhet, informationssystem, vårdsektor, ISO, GAO och CERT.

Innehållsförteckning

Tabellförteckning

Figurförteckning

1 Introduktion

Information och data har i en allt större utsträckning blivit en resurs som organisationer är beroende av och grundar sin verksamhet på. Den utgör ofta den värdefullaste resursen en organisation har. Precis som andra tillgångar så måste även denna resurs skyddas mot obehörigas åtkomst (Svensson, 1999). I takt med att mängden information och beroendet av den har ökat, så har också de system som administrerar den vuxit och det har blivit allt viktigare att förvalta dessa informationssystem för att säkerställa att de fungerar på ett tillfredställande och säkert sätt. Idag har användandet av informationssystem snart spridit sig till samtliga aktörer på marknaden och utgör en livsviktig del av många verksamheter. En av dessa aktörer är vårdsektorn, där informationssystem idag i stor utsträckning bidrar med att minska det administrativa arbetet. Vården är den sektor inom vilken detta examensarbete kommer att ha sin fokusering.

För att kunna skapa ett säkert informationssystem hävdar Schneider (2000) att det krävs en säkerhetspolicy som är baserad på en analys av tänkbara hot mot organisationen. Ett av dessa hot som finns mot informationssystemen inom vården är, enligt Lagerlund (1998), hotet om intrång. Detta kan exempelvis ske genom att förövaren lyckas använda systemet under falsk identitet, använda sig av virus eller hackar sig in i systemet.

En organisations säkerhetspolicy styr vilka motmedel som behövs mot eventuella hot, för att systemet ska klara av att leva upp till ställda säkerhetskrav (Schneider, 2000). Att regelbundet granska informationssystemet, med avseende på dess säkerhet, är en viktig del av systemförvaltningen. Denna del kallas för säkerhetsrevision. Då en säkerhetsrevision genomförs finns det olika modeller och standarder att följa, dessa sätter upp riktlinjer för hur arbetet kan bedrivas och vad som ska undersökas. Någon modell för hur arbetet speciellt bedrivs inom vårdsektorn, där kraven på informationssäkerhet är mycket hög, finns inte. Att ta reda på vad, vilka aspekter, som ska revideras hos ett system i denna miljö med avseende på intrång i värddatorerna utgör ansatsen i detta examensarbete. För att finna dessa aspekter används i huvudsak tre litterära källor; en informationssäkerhetsstandard, en statlig manual för revision av informationssystem och en samling moduler för förbättring av säkerheten i ett system.

Dessa tre källor tillsammans med en empirisk undersökning inom vården är tänkta att utgöra stommen i detta projekt. Resultatet från dem presenteras i form av tabeller innehållande olika aspekter på vad som bör revideras vid en säkerhetsrevision.

Rapporten inleds i kapitel 1 med en introduktion till området som examensarbetet behandlar följt av bakgrunden som beskrivs i kapitel 2. I kapitel 3 diskuteras problemområdet och den problemprecisering som arbetet har. Därefter följer metod kapitlet som behandlar alternativa och valda metoder. Hur dessa metoder har används i genomförandet redovisas i nästföljande kapitel. Resultatet från genomförandet samt en analys av det presenteras i kapitel 6 respektive 7, följt av slutsatsen som presenteras i kapitel 8. Slutligen följer en diskussion av examensarbetet i kapitel 9.

2 Bakgrund

Kapitlet presenterar centrala begrepp och teorier som ligger till grund för detta examensarbete. I avsnitt 2.1 beskrivs olika typer av hot samt säkerhetstjänster som svarar upp mot dessa, och i avsnitt 2.2 beskrivs IT-termer med utgångspunkt i vårdsektorn samt begreppet informationssäkerhet. Avsnitt 2.3 handlar om vikten av att förvalta ett informationssystem, och avsnitt 2.4 ger en beskrivning av hur arbetet med att bedriva en säkerhetsrevision kan se ut.

2.1 Hot och säkerhetstjänster

Betydelsen av nätverkssäkerhet har blivit större i takt med att allt fler verksamheter kopplar ihop sina system i nätverk och att informationsberoendet ökar. Nätverk kan definieras som: ”*Ett antal sammankopplade enheter som kan kommunicera och dela varandras resurser*” (Bandyo-padhyay, 2000, s. 157). Ett nätverk kan bestå av ett antal olika komponenter: värddatorer, terminaler, kablage, kommunikations processorer och mjukvaror. Ett ord som frekvent används när nätverk diskuteras är topologi. Med detta avses datorernas layout i ett nätverk. Dataföreningen i Sverige (SSR 97 ETT) menar att oavsett vilken topologi ett nätverk har, vilket kan vara – buss, ring, stjärna etc. – så har de något gemensamt. Denna gemensamma nämnare är bristen på säkerhet i dem.

Orsaken till att det överhuvudtaget bör finnas ett säkerhetstänkande är att det existerar en hotbild gentemot organisationer och deras nätverk. Schneider (2000) skriver att det inte är någon nyhet att det begås kriminella handlingar, så som stöld, intrång och förfalskning, utan hur dessa utförs och vilka hjälpmedel som används. Med tanke på den informationsmängd som kommuniceras och som finns lagrad i nätverk, är det inte så förvånande att brottsligheten har nått även dit.

Det finns fyra stycken olika typer av hot mot ett system. Med ett hot avses alla oönskade händelser eller situationer som kan störa verksamheten. Dessa fyra typer av hot kan beskrivas som (SSR 97 ETT):

- **Denial-of-service** – Alla trafik på nätverket blockeras, vilket innebär att ingen trafik kommer fram.
- **Modifiering** – Innan ett meddelande når sin mottagare kan det förändras.

- **Avlyssning eller upptagning** – Detta kan delas upp i två delar: trafikanalys där förövaren koncentrerar sig på att lära känna komponenter, användare och destinationer för informationen, och avlyssning av allt som trafikerar nätet.
- **Skapande eller förklädnad** – Genom att en dator utger sig för att vara en dator med behörighet kan falsk information skapas och spridas i nätverket.

Det finns ett antal olika säkerhetstjänster som är framtagna för att svara upp mot de hot som finns mot bland annat datorsystem. Dessa tjänster kan presenteras på lite olika sätt varav två har valts ut i detta arbete. Den första uppdelningen har gjorts av det amerikanska försvarsdepartementet, där säkerhetstjänsterna delas in i tre kategorier och nio säkerhetstjänster. (SSR 97 ETT, s. 67):

Tabell 1: Säkerhetstjänsterna delas in i tre kategorier och nio säkerhetstjänster.

Kategori	**Säkerhetstjänster**
Kommunikations-integritet	• *Autentisering*, säkerställande av persons identitet. • *Integritetsskydd*, förhindra otillbörlig förändring av information • *Oavvislighet*, inte kunna förneka ansvar för innehåll i viss informationsmängd
Denial-of-service	• *Tillgänglighet*, information ska kunna spridas och tas emot inom rimlig tid. • *Brandväggsfunktioner*, filtrerar trafik som passerar i nätverket. • *Nätverksadministration*, ansvarar för upprätthållande av nätverkets funktioner
Intrångsupptäckt	• *Datakonfidentialitet*, att skydda information från obehörigas insyn. • *Trafikflödesskydd*, hindrar avlyssning av trafiken på nätet. • *Selektivrouting*, selektion av vad som skickas vidare och inte.

I standard ISO 7498-2, från International Organisation of Standardization, beskrivs en annan uppdelning av säkerhetstjänsterna. (SSR 97 ETT, s. 67):

- *Åtkomstkontroll*, kontroll av vem som får tillträde till systemet.
- *Autentisering*, säkerställande av persons identitet.
- *Konfidentialitetsskydd*, skydd mot obehörigas insyn av data i systemet.
- *Integritet för data*, förhindra otillbörlig ändring av data.
- *Integritet för trafikflöde*, förhindra påverkan av trafiken på nätverket.
- *Icke förnekbarhet eller oavvislighet*, inte kunna avsägas ansvar för information som skickas.

Införandet av dessa säkerhetstjänster, vare sig det är amerikanska försvarsdepartementets eller ISO:s, så tjänar de till att skapa säkerhet i organisationers datorsystem. Behov av ökad säkerhet är ett resultat av att allt fler företag använder sig av IT-stöd i sin verksamhet. Detta stöd av IT har spridit sig till i princip samtliga aktörer på marknaden. Inom vårdsektorn exempelvis, där IT numera är en integrerad del av vårdprocessen, ställs enligt Lagerlund (1998), nya krav på informationssystemen, som menar att för att lyckas med informationshanteringen och IT-stödet så krävs det samverkan och överenskommelser på många nivåer inom organisationen. Denna ökande användning av informationssystem inom vården har lett fram till ett begrepp som kallas medicinsk informatik. Innebörden av detta begrepp beskrivs i nästa avsnitt.

2.2 Medicinsk informatik

Kostnaderna för att bedriva sjukvård är enormt stora för samhället och de tenderar att stiga i framtiden. För att råda bot på dessa kostnader har olika angreppssätt används. Peterson & Rydmark (1996) skriver att på 1980-talet försökte kostnaderna sänkas genom att göra vården mera marknadsmässig. På 1990-talet var angreppssättet interna revisioner för att öka effektiviteten med gemensamt utnyttjande av information. Trenden på 2000-talet verkar bli samverkan mellan olika sjukhus regioner, nationellt och internationellt. En betydande del av kostnaderna kommer från det stora administrativa arbete som utförs. Enligt Peterson & Rydmark (1996) går i dagsläget 25-50% av sjukvårdspersonalens tid åt till administrativt arbete, vilket har lett till ökade krav på effektiv medicinsk, omvårdnadsmässig och ekonomisk informationshantering.

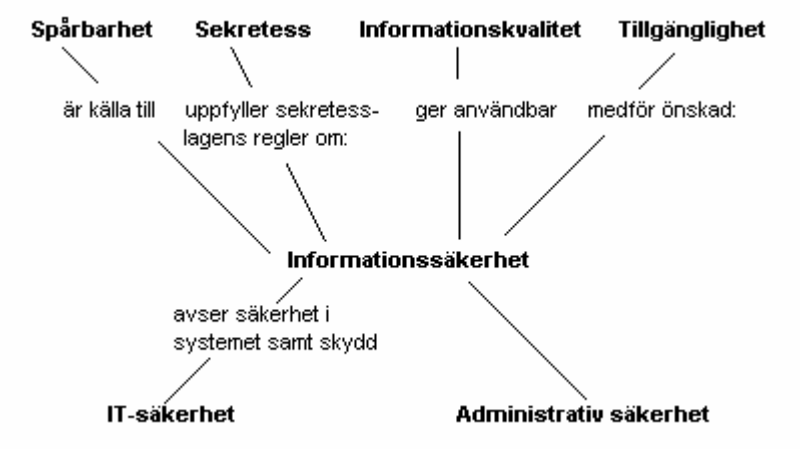
Den snabba utvecklingen inom IT-sektorn har resulterat i att datorer används i en allt större utsträckning även inom vården och är numera ett viktigt verktyg för att öka den administrativa effektiviteten. Ett begrepp som ofta används i detta sammanhang är medicinsk informatik. Enligt de Dombal (1996) betyder begreppet, användning och tillämpning av informationsteknologi och forskning inom område IT, som är specifik för vårdsektorn. I detta sammanhang blir datorn det centrala verktyget och patientjournalerna de centrala dokumenten.

Vid hantering av dessa centrala dokument, patientjournaler, finns det lager som styr hanteringen av informationen i dem. Den lag som i första hand är av intresse i detta sammanhang är patientjournallagen (SFS 1985:562). Lagen är inte beroende av någon

viss teknik utan tillämpas likadant oavsett om journalen är i pappers- eller elektronisk form. I 7 § föreskrivs att *varje journalhandling* ska hanteras och förvaras så att obehöriga inte får tillgång till den. Sekretesslagen (SFS 1980:100) har som utgångspunkt, för hälso- och sjukvården, att sekretess rör uppgifter om enskilds hälsotillstånd eller andra personliga förhållanden. Båda dessa lagar trycker på vikten av att information inte på något sätt får komma i felaktiga händer utan måste skyddas.

All datahantering inom sjukvården innebär integritets- och sekretess problem. För att vården ska kunna skydda sig mot eventuella intrång är arbetet med informationssäkerhet enormt viktigt.

Det har tidigare gjorts en del arbeten inom området informationssäkerhet med fokus på vården. Ett projekt som benämns SITHS (Björner, 1999), ett samarbete mellan Spri och fyra landsting, har haft som mål att utveckla modeller och metoder för att införa informationssäkerhet med hjälp av IT inom vårdsektorn. Att ge en enkel beskrivning på vad begreppet informationssäkerhet betyder är inte helt enkelt men SITHS har, ur ett större perspektiv, försökt ge en definition på det. Orsaken till att denna definition används är att den är framtagen av en projektgrupp som jobbade med inriktning mot vårdsektorn och därmed stämmer bra överens med fokusen på detta arbete. Figur 1 ger en beskrivning av hur SITHS definierar informationssäkerhet:



Figur 1: SITHS definition på informationssäkerhet (Björner, 1999)

Definitionen bygger på sex stycken olika områden utifrån vilka informationssäkerhet byggs upp: *spårbarhet, sekretess, informationskvalitet, tillgänglighet, administrativ- och IT säkerhet.* Med *spårbarhet* avses möjligheten att kunna spåra handlingar tillbaka till en enskild person som har genomfört dem. *Sekretess* handlar om att

skydda information från obehöriga. Genom att säkerställa *kvaliteten* på *informationen* garanteras korrekthet i data som lagras. Med *tillgänglighet* avses att systemet kan leverera det som det är till för utan avbrott som stör verksamheten. Handhavande av information exempelvis bredvid datorn och lösenord inbegrips i *administrativ säkerhet*. Slutligen området *IT-säkerhet* som avser säkerhet inom områden så som datorsystem och nätverk.

SITHS projektet har i sin rapport (Björner, 1999) lagt fram en *vision* för hur de ser på informationssäkerhet inom just vården. Den innehåller inga tekniska aspekter utan anger bara de krav som finns på informationshanteringen och ser ut som följer: ”*rätt information till rätt person vid rätt tid på rätt ställe*”. För att uppnå denna vision, och för att skapa ett säkert informationssystem, har SITHS fastslagit några viktiga funktioner:

- Spårbarhet: enskilda handlingar ska kunna spåras till person
- Integritet: skydd mot oönskade ändringar
- Sekretess: data får inte bli tillgänglig för obehöriga
- Oavvislighet: mottagande eller skickande av meddelande kan inte nekas
- Behörighet: användarens rätt att använda resurser i systemet
- Autenticitet: kontroll av identitet

Behovet av att skapa informationssystem som upprätthåller säkerheten inom vården styrks av Hayem (1996), som trycker på vikten av hur nödvändigt det är att skapa säkra informationssystem för att hindra tänkbara angrepp och hot mot de livsnödvändiga system som finns inom vården. Förutom att bara skapa ett säkert system pekar Hayam (1996) på behovet av säkerhetsrevisioner för att analysera systemet gentemot fastställda säkerhetsregler. I nästa avsnitt kommer vikten av att förvalta informationssystemen, som vuxit i takt med att storleken och betydelsen av dem har blivit allt större, att diskuteras samt innebörden av begreppet systemförvaltning.

2.3 Systemförvaltning

Det är allmänt erkänt att information är en tillgång som har fått allt större betydelse för många organisationer och att den ofta är den mest värdefulla (Svensson, 1999). Precis som andra tillgångar, så som lokaler, personal och produkter, är det viktigt att den förvaltas på rätt sätt. Informationen måste administreras på ett bra sätt för att säkra verksamhetens framgång och om det inte görs på ett riktigt sätt kan det få

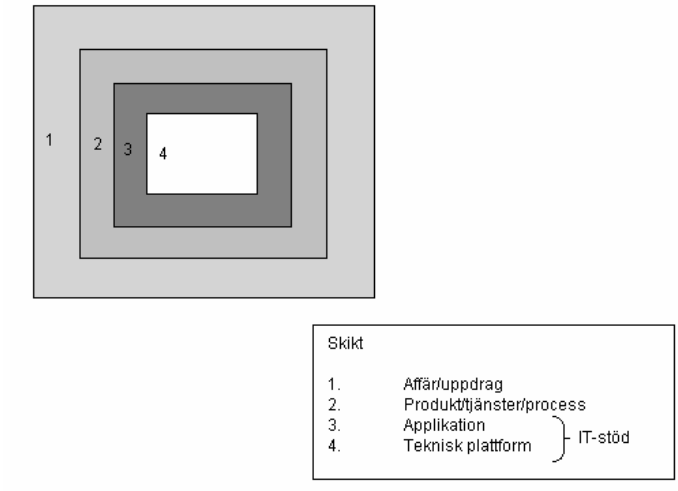
allvarliga följder på verksamheten (Ward, 1995). I takt med att informationsteknologin växte fram kom det nya fördelar som ett resultat av att bearbetningen och användningen av data blev mera effektiv och greppbar. Ward (1995) menar att informationssystemen idag har blivit en integrerad del av varje organisation. De ingår mer eller mindre i varje process i verksamheten. Men användningen av teknologier som påverkar alla dessa processer har också gjort att underhållet av informationssystemen har blivit ett område som kräver speciell uppmärksamhet.

Administreringen av ett datasystem kan även kallas för systemförvaltning. Enligt Andersen (1998) innebär förvaltning en uppföljning av driften med löpande korrigering, bedömning och större underhåll. Det innebär också att avgöra om informationssystemet lever upp till uppsatta krav eller inte. Begreppet systemförvaltning kan definieras på följande sätt: ”*Systemförvaltning är samtliga aktiviteter som görs för att styra, administrera och verkställa förändringsarbetet av existerande objekt och stödja användandet*” (Brandt, 1998, s. 11).

För att bättre förstå innebörden i detta citat klargör Brandt (1998) ytterligare vissa av delarna i det. Uttrycket s*amtliga aktiviteter* används för att det finns en mängd aktiviteter som kan utföras och det är inte möjligt att lista exakt alla av dem. Listan skulle bli mycket lång, eftersom det t.ex. i ändringsprocessen finns upp emot ett hundra aktiviteter. Med ändringsprocess avses alla aktiviteter som genomförs från att ett ändringsbehov uppstår tills att ändringen är genomförd. Att s*tyra, administrera och verkställa* är tre åtgärder som kan ingå i förvaltningen av systemet. De styrande åtgärderna utförs av dem som sitter i en ägarroll så som system- och produktägare. De administrativa åtgärderna ansvarar de som sitter på den administrativa nivån för. De som sitter på den verkställande nivån utför de verkställande åtgärderna, så som system- och teknikstöd. *Förändringsarbetet* är ett annat uttryck som används för systemförvaltningsarbetet, då det kan ses som en förändring av existerande system. Med *existerande objekt* vill Brandt (1998) trycka på att det inte enbart gäller förändring av informationssystem utan att även andra delar, så som kunskapsförändring, produkter och dokumentation kan inkluderas bland de objekt som kan förvaltas.

Enligt Nordström och Welander (2002) är det ett stort problem att många inte tillräckligt noga definierar detta förvaltningsobjekt. Idag är det vanligt att det enbart

sker förvaltning av den del som utgör IT-stödet. Vid sidan om denna del finns även områden så som verksamheten och dess affärer, produkter och tjänster. Om det sker en separering av dessa delar kan det leda till att IT-stödet inte fungerar tillfredställande inom dessa. Denna separering avses i samband med att en organisation lägger upp en strategi för vad som ska förvaltas. Figur 2 åskådliggör en modell av förvaltningsobjektet. Den presenterar ett sätt att se på förvaltningsobjektet bestående av fyra skikt. Dessa skikt utgör fyra olika nivåer med det tekniska skiktet längst in följt av applikationer och produkter och, organisationens affärer och dess uppdrag längs ut. De två innersta skikten utgör den del som också kallas för IT-stödet:



Figur 2: En modell av förvaltningsobjektet. Skikten i modellen utgör fyra olika lager som kan ingå i en säkerhetsrevision av objektet (efter Nordström & Welander, 2002, s. 46).

Ramarna för detta projekt ger inte utrymme åt någon närmare granskning av samtliga delar i förvaltningsobjektet. De områden som kommer vara föremål för granskning är områdena applikation och teknisk plattform, dvs. IT-stöd.

Det nämndes tidigare att systemförvaltning avser *samtliga aktiviteter*. Bland dessa aktiviteter är ändringshanteringen den mest frekvent förekommande. Till grund för varje ändring som sker finns det ett bakomliggande ändringsbehov. Det finns en mängd sådana varav några anges nedan (Nordström & Welander, 2002):

- Upptäckt av *brister i objekt* – någon upptäcker att någonting kan göras på ett bättre sätt. Detta motiverar en förändring av objektet för att samspelet mellan verksamhetsrutiner och applikationer ska fungera bättre. Detta kallas ofta för förbättringar.
- Upptäckt av *fel i objektet* – någon upptäcker ett fel som påverkar verksamheten i organisationen. Dessa fel upptäcks oftast i början när en

applikation används och minskar sedan med tiden. Behöver inte bara vara tekniska fel utan kan även innefatta rutiner. Dessa kallas ofta förändringar.

- *Förändringar i verksamheten och IT-stödet* genereras ofta utifrån marknadens krav på organisationen. De delar av verksamheten som behöver ändras kan skapa ett nytt behov eller en förändring av sitt IT-stöd. Dessa krav kan t ex vara lagar och skattesatser. Dessa ändringar brukar kategoriseras som anpassningar.

Ett sätt för att upptäcka dessa bakomliggande ändringsbehov, som utgörs av fel och brister i förvaltningsobjektet, är att genomföra en revision. En revisions syfte är att finna brister och felaktigheter i verksamhet, detta kommer ytterligare att behandlas i nästkommande avsnitt. Om revisionen görs inom området IT-stöd med fokus på säkerhet kan det kallas det för säkerhetsrevision, eftersom den berör organisationens nätverk och ingående datorsystem med avseende på hur deras säkerhet fungerar.

2.4 Säkerhetsrevision

Det har under senare år blivit allt vanligare att göra säkerhetsrevisioner och det kan ses som en trend hos företag att säkerhet inte längre uppfattas som något datateknikerna kan lösa med en nätverksmjukvara utan de har insett att det krävs större resurser för att leva upp till ställda säkerhetskrav (Vaas, 2000). Här fyller säkerhetsrevisionen en viktig roll och kan beskrivas som den revision som görs av en organisations nätverk och ingående datorsystem och kan ses som en viktig del i systemförvaltningen. Den första delen av ordet, *säkerhet*, trycker på att revisionen ska utföras på just detta område. Ordet *revision* ges i Nationalencyklopedin betydelsen *"…den granskning i efterhand av ett företags eller annan organisations redovisning och förvaltning som görs i syfte att ge upplysning om redovisningens tillförlitlighet och om ledningens sätt att förvalta organisationen*". (Nationalencyklopedin, 1994, band 15, s. 524) Det område som utsätts för en revision är således föremål för en närmare granskning med avsikt att upplysning om eventuella felaktigheter eller svagheter ska framkomma. Detta görs i syfte att organisationen i framtiden ska slippa upprepning av eventuella felaktigheter som har orsakat brister i tillförlitligheten och förvaltningen av verksamheten.

Brooks (1998) menar att innan någonting annat görs bör orsakerna till varför en säkerhetsrevision genomförs fastställas. Detta innebär att revisorn tillsammans med ledningen går igenom riskanalysen och säkerhetspolicyn hos organisationen. Oliver

Rist (2000) menar att syftet med den här typen av revision är att få en förståelse för var eventuellt förekommande svagheterna i nätverket finns, hur allvarliga de är och vad som behöver göras för att åtgärda dem.

Schneider (2000) säger att arbetet med en säkerhetsrevision inte är någon enkel process utan att den kan vara svår att genomföra. Men genom att använda metoder och standarder kan hjälp erhållas om hur ett visst problem ska angripas och vilka hjälpmedel som är lämpliga (Andersen, 1994). Den litteraturundersökningen som genomförts i detta arbete har inte funnit någon enskild standard för hur en säkerhetsrevision genomförs. Förslag från olika författare på principer och metoder för hur arbetet kan genomföras har dock identifierats. Två presenteras i denna rapport för att ge läsaren en övergripande bild av hur revisionsarbetet kan genomföras. Kapps modell, som presenteras i avsnitt 2.4.2 har en något mjukare vinkling med avseende på hur användare och ledning involveras i arbetet än vad Brooks modell i avsnitt 2.4.1 har, som fokuserar mera på att rätt programvara och teknisk plattform används. Ingen av dessa modeller går in på vilka aspekter det är som ska granskas då en säkerhetsrevision genomförs, utan fokus ligger på hur arbetsprocessen ser ut. Detta är orsaken till att dessa modeller inte har används i litteraturstudien, utan tre andra källor, som har mera fokus på vad som ska revideras men inte så mycket på genomförandet, har används.

2.4.1 Brooks modell för säkerhetsrevision

Modellen innehåller tre huvudsteg, *förberedelse, revision och rapport* (Brooks, 1998). Denna modell ger en generell bild av hur ett revisionsarbete kan se ut men gör inte anspråk på att vara den enda och riktiga modellen att göra en säkerhetsrevision på.

Förberedelse

I ett tidigt skede ska fastställande av orsaken till revisionen göras samt genomgång av riskanalys och organisationens säkerhetspolicy. Detta görs tillsammans med ledningen. Varje säkerhetsrevision bör baseras på en noggrann avvägning av vilka risker organisationens information kan utsättas för.

I denna förberedelsefas av arbetet behöver följande fyra frågor besvaras: *vem, vad, när* och *hur*. Den förstnämnda frågan om *vem* som ska utföra revisionen, är viktig eftersom det ofta krävs tillåtelse för att genomföra en revision över olika avdelningsgränser samt att viss information som är nödvändig för arbetet kan vara hemligstämplad. Frågan om *vad* som ska revideras har enligt Brooks (1998) ofta

klumpats ihop i tre kategorier: värddator, nätverk och brandvägg. *När* en säkerhetsrevision ska genomföras ska uttryckas i säkerhetspolicyn. Vissa generella tumregler säger att värddatorerna och nätverket ska revideras en gång per år medan brandväggen ska undersökas var sjätte månad. Frågan *hur,* syftar på vilka verktyg som ska användas. Det är av stor vikt att de verktyg som används, i efterhand inte kan ifrågasättas på något sätt då detta kan äventyra hela revisionens tillförlitlighet. Slutligen bör den plattform ifrån viken revisionen utförs från uppmärksammas. För att undvika att obehöriga ska störa arbetet ska den inte vara tillgänglig från det datorsystem som analyseras. Det ideala verktyget för en revision är en bärbar enhet som kan anslutas och kopplas bort från systemet på kort varsel. Denna enhet bör även vara föremål för en egen säkerhetsrevision.

Revision

Inom en säkerhetsrevision finns det både en teknisk och en icke-teknisk del. Den tekniska delen ses ofta som naturlig att genomföra medan den icke-tekniska lätt försummas. Men i varje revision bör det ingå att en visuell översyn görs av anläggningen för att finna användarmönster, privilegierade användare, kritiska system och deras funktioner samt nyckelpersoner. Personalens medvetenhet om organisationens säkerhetspolicy bör även kontrolleras. Efter att den icke-tekniska delen av revisionen har genomförts är det dags för den tekniska.

Brooks (1998) säger att revisionsverktyg i själva verket används för att minska den enorma tid det skulle ta att göra alla kontroller manuellt. Dessa kan innefatta allt från kontroll av systemloggar och filintegritet till att kontrollera sårbarheter och fel som har hittas av tillverkaren eller andra företag som letar fel i t.ex. programvaran. En annan författare (Hutt, 1997), delar upp dessa olika kontroller i tre kategorier. Dessa inkluderar *förebyggande kontroll*, som hindrar att icke-önskvärda händelser inträffar, *undersökande kontroll*, som upptäcker händelser medan de sker, och *korrigerande kontroll*, som återställer situationen till normalläge efter att något oönskat har inträffat. De flesta verktyg som används för att utföra dessa kontroller har ett intuitivt grafiskt gränssnitt vilket underlättar användningen av verktygen och gör att revisionen kan komma igång snabbt. Beroende på hur stort det aktuella systemet är tar det olika lång tid för ett verktyg att göra sitt arbete men generellt kan sägas att det är ganska tidskrävande. En fördel med de flesta verktyg är att användaren kan köra igång dem

och sedan gå därifrån för att syssla med något annat medan programmet sköter sig självt.

På marknaden finns det ett stort antal revisionsverktyg där vissa är så kallade gratisprogram (eng. freeware) medan andra måste köpas. Det är viktigt att i förberedelserna ha i åtanke att tillförlitligheten och kontrollen hos gratisprogram kan vara lägre än hos programvaror som har köpts. Dessa verktyg skiljer sig en del från varandra och kan därefter delas upp i kategorier beroende på vilken arkitektur de har (Brooks, 1998):

- *Manager/agent*. Med denna typ av verktyg sker revisionen från en central dator. Denna centrala enhet reviderar individuella värddatorer med hjälp av information som skickas till den från ett program, så kallad agent, som installerats i den värddator som är föremål för revision. Nackdelen med denna typ av verktyg är att ett program måste installeras i den dator som ska revideras, medan fördelen är den detaljerade information som erhålls. Ett exempel på verktyg med denna arkitektur är, Axent Technologies' Enterprise Security Manager (ESM).
- *Network scanners*. Vid användning av denna typ av verktyg behöver det inte ske installering av någon programvara i datorn som ska revideras. Fördelen med dessa verktyg är att arbetet kan komma igång snabbt och att samtliga datorer som ingår i nätverket kan revideras utan någon fysisk kontakt med dem. Nackdelen är att den information som erhålls från de datorer som revideras är begränsad till den typen av information som kan kommas åt via fjärranslutning (eng. remote access). Exempel på verktyg som jobbar på detta sätt är: SATAN, Internet Security Systems' Internet Scanner och WheelGroup's NetSonar.

Rapporten

Resultatet från revisionsverktygen blir ofta enorma mängder med papper och grafer över alla tänkbara svagheter i systemet. Det är enligt Brooks (1998) extremt viktigt att detta material inte hamnar i fel händer där det skulle kunna orsaka stor skada. Distribution av materialet ska göras endast till dem som verkligen behöver det samt att de måste signera varje kopia de får. Dessa kopior ska inte vara i elektronisk form utan på papper. Original handlingarna ska förvaras på ett säkert ställe och användas för jämförelse vid nästa revision.

Beroende på vilka verktyg som används presenteras resultatet på olika sätt. Det är viktigt att ha detta i åtanke då ett enda verktyg kanske inte är tillräckligt utan behöver kompletteras med ett eller flera andra. För revisorerna är det en stor utmaning att tolka det material som har genereras för att därigenom kunna föreslå en plan på hur eventuella brister ska hanteras.

2.4.2 Kapps modell för säkerhetsrevision

I den här modellen presenteras det flera steg som ska gås igenom i samband med en revision (Kapp, 2000). Modellen innehåller åtta steg, *förberedelse, granskning av policy och dokument, intervjuer och samtal, teknisk undersökning, granskning av data, sammanställning av material, rapportpresentation, och efterarbete*. Dessa presenteras i tabell 2:

Tabell 2: Steg som ska gås igenom vid en säkerhetsrevision. För var och ett av dessa anges den procentuella andel tid respektive steg beräknas ta i anspråk (efter Kapp, 2000, s. 4).

Steg	% av total tid
Förberedelse	10
Granskning av policy o dokument	10
Intervjuer och samtal	10
Teknisk undersökning	15
Granskning av data	20
Sammanställning av material	20
Rapportpresentation	5
Efterarbete	10

Förberedelse

En förutsättning för en lyckad revision är att från början fastställa hur djupt den ska gå. Ett informationssystem består av ett antal olika komponenter, exempelvis värddatorer, servrar, brandväggar och nätverk. Inom vart och ett av dessa ska djupet fastställas. Vissa system måste revideras djupare än andra för att fastslå viktiga säkerhetsfrågor. Vidare måste det ske en planering av när revision ska göras för att störa verksamheten så lite som möjligt men ända att viktiga personer ur personalen finns anträffbara. Att kontrollera de verktyg som kommer att användas under revisionen är enormt viktigt. Dels att de passar det system som ska undersökas och dels att ingen har manipulerat med dem. En aspekt att ha i åtanke här är om verktyget är köpt eller om det är ett gratisprogram (se avsnitt 2.4.1).

Granskning av policy och dokument

När en revision genomförs är säkerhetspolicyn utgångspunkten i arbetet. I början av revisionen ska säkerhetspolicyn ses som ett hot. Detta för att kunna fastställa om den täcker alla grundläggande dokument som en policy ska innehålla. Kan en säkerhetspolicy vara ett hot? Kapp (2000) menar i sin rapport att den kan vara det. En säkerhetspolicy som är dåligt skriven och saknar viktiga dokument kan vara mycket sämre än ingen policy alls. Om en organisation saknar en policy eller har en som inte fungerar bör övervägning göras om en sådan bör skapas innan revisionen påbörjas då detta är ett mycket viktigt dokument. Att undersöka dokument som specificerar vilka som har tillstånd och behörighet i systemen ger en bra bild av systemets gränser.

Intervjuer och samtal

En säkerhetsrevision bör innehålla intervjuer med personal på ett informellt sätt. Enligt Kapp (2000) är detta en aspekt av revisionen som ofta förbises men som är mycket viktig. De personer som samtal och intervjuer förs med, ska inte enbart utgöras av den tekniska personalen utan även vanliga användare och ledningen. Det är viktigt att i dessa intervjuer avgöra om personalen har sett och läst säkerhetspolicyn.

Teknisk undersökning

Den tekniska undersökningen bör innehålla en avsökning (eng. scanning) av nätverket med någon typ av revisionsverktyg. Dessa verktyg generera en stor mängd information baserat på vad de är förprogrammerade att undersöka. Genomgången av denna information ligger i ett senare steg av revisionen varför det är viktigt att all information sparas på ett lättöverskådligt och säkert sätt. Vidare ska genomgångar av systemloggarna göras för att finna eventuella mönster som kan tyda på otillåten användning. Kontroll av uppstartningsprocesser ska göras för att finna eventuella processer som inte ska vara där. Kontrollen görs genom att jämföra vilka uppstartsprocesser som finns där, med de applikationer som ska vara installerade eller med vad som finns dokumenterat sen tidigare. Det finns en mängd områden i systemet som undersöks i denna del av revisionen och det ges inte utrymme här för att gå in på samtliga.

Granskning av data

För att resultatet från revisionen ska vara användbart krävs det noggrann analys och genomgång av informationen som har genererats. Detta är ett tidskrävande arbete och

kräver noggrannhet och kunskap för att kunna upptäcka eventuella svagheter i systemet. All data som genereras under revisionen, i elektronisk eller pappersform, ska sparas för att kunna användas som referens material i framtiden. Den ska sparas på ett säkert ställa där inga obehöriga kan komma åt den (Kapp, 2000).

Sammanställning av materialet

Rapporten bör vara skriven på ett sådant sätt att det tekniska djupet ökar ju längre in i den läsaren kommer. De flest i ledningen behöver inte känna till de tekniska detaljerna, så att presentera det de behöver veta i de första kapitlen är viktigt. Rapporten bör ha en logisk struktur. Detta innebär bland annat en sammanfattning åt ledningen och en lista över prioriterade rekommendationer. Uppgifter om de verktyg som har används ska finnas med som bilaga.

Rapportpresentation

Rapporten ska presenteras av revisorerna inför berörd personal och ledning. Genom att ledningen låter rapporten presenteras av revisorerna ger det signaler till övrig personal om att ledningen tar det utförda arbetet på allvar. I samband med att presentationen sker ska det ges möjlighet till att ställa frågor till revisorerna för att klargöra eventuella oklarheter eller funderingar.

Efterarbete

När rapporten har presenterats bör ansvarig personal sätta sig ner för att diskutera eventuella åtgärder som revisorerna presenterar. Det är viktigt att det finns datum på när olika åtgärder ska ha genomförts för att detta arbete ska gå snabbt och inte dra ut på tiden.

2.4.3 Jämförelse mellan Brooks och Kapp

Det går att se tydliga skillnader i dessa två modeller av hur en säkerhetsrevision ska genomföras. Som tidigare nämndes har Kapp en annan syn på medverkan av användarna och ledning i revisionsarbetet. Kapp trycker på vikten av att dessa ska ingå i intervjuer och samtal samt att rapporten ska presenteras för berörd personal och ha ett upplägg som underlättar för läsarna. I Brooks modell syns en tydligare inriktning på de tekniska aspekterna av revisionen, så som vikten av rätt programvara och tekniska plattform. Brooks ger vidare inga uttryck för hur resultatet ska

presenteras, utan verkar lita på att läsarna själva ska förstå och kunna hantera de slutsatser som revisorerna anger i sin rapport. Nedanför följer en kort jämförelse mellan de tre stegen, *förberedelse, revision*, och *rapport*, i Brooks modell och Kapps motsvarande. Denna jämförelse presenteras också översiktligt i tabell 3.

Det första steget i Brooks modell är *förberedelse*. Här fastställs orsaken till varför revisionen ska göras samt att de fyra frågorna *vem, vad, när* och *hur* ska besvaras. Motsvarande del i Kapps modell består av *förberedelse* och *granskning av policy och dokument.* Här lägger Kapp större vikt än Brooks vid att säkerhetspolicyn ska granskas och att den bör ligga till grund för revisionsarbetet. Båda trycker på att det är viktigt att avgöra när revisionen ska genomföras för att övrig verksamhet ska störas så lite som möjligt och att rätt revisionsverktyg väljs.

Det andra steget i Brooks modell är *revisionen*. Denna består av två delar: dels den tekniska delen och dels den icke-tekniska. Denna icke-tekniska del motsvaras i Kapps modell av det tredje steget som heter *intervjuer och samtal* och den tekniska delen ser i stort sett likadan ut hos de båda. Den stora skillnaden i genomförandet av revisionen är att den mjuka delen, i form av intervjuer och samtal, upptar större plats hos Kapp än den gör hos Brooks samt att Brooks lägger större vikt vid hanteringen av revisionsverktygen.

Det sista steget som Brooks presenterar är *rapporten.* Motsvarande stycke hos Kapp består av *granskning av data, sammanställning av material, rapportpresentation* och *efterarbete.* Brooks nämner vid flera tillfällen hur viktigt det är att materialet från revisionen skyddas från att komma i orätta händer och att kompletterande verktyg kan behövas för att få ett bra material att presentera. Kapp å andra sidan har, genom sin uppdelning av detta stycke i fyra steg, visat att granskning och rapportering av det material som genereras från revisionen utgör en stor del av hela revisionsarbetet. En punkt som Kapp har med men som saknas hos Brooks är *efterarbetet*. Här menar Kapp att ansvarig personal ska sätta sig ner och diskutera resultatet och eventuella åtgärder som presenterats för att på så sätt få till ett snabbt förändringsarbete.

Tabell 3: Jämförelse mellan stegen i Brooks och Kapps modeller

Brooks	**Kapp**
Förberedelse	Förberedelse Granskning av policy och dokument
Revision (teknisk och icke-teknisk)	Intervjuer och samtal Teknisk undersökning
Rapporten	Granskning av data Sammanställning av material Rapportpresentation
	Efterarbete

3 Problem

I detta kapitel beskrivs det problemområde samt det problem som detta arbete syftar till att besvara. Vidare finns det i kapitlet motivering till varför det anses vara ett problem samt hur avgränsningen har gjorts. Kapitlet avslutas med förväntat resultat och en beskrivning av hur problemet kommer att angripas.

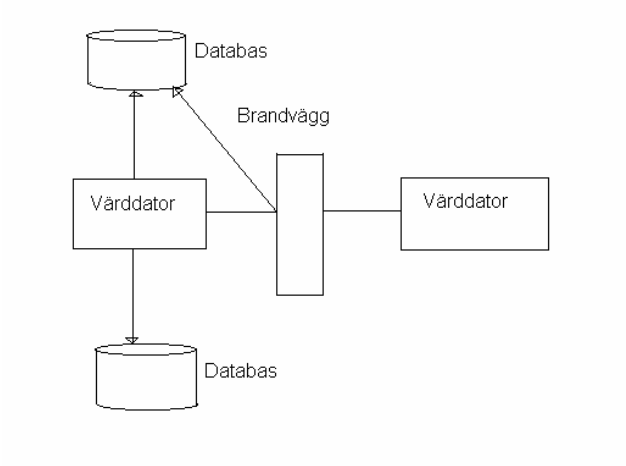
3.1 Problemområde

Organisationer har i en allt större utsträckning blivit beroende av information. Arthur E. Hutt (1997) säger i sin bok att information är en av de viktigaste tillgångarna för en organisation och att den därför ska skyddas. För att kunna skydda informationen måste organisationen känna sin omgivning och de hot som den kan utsättas för. Genom att göra en analys av möjliga hot kan en modell skapas som ger en bra bild av omgivningen. Schneider (2000) menar att om omgivningen inte är känd så går det inte att skapa en trovärdig säkerhetspolicy eftersom möjliga hot och attacker inte är kända. Baserat på denna modell, kan en säkerhetspolicy skapas och användas för att finna de rätta motmedlen för att undvika lyckade attacker på systemet (Schneider, 2000). Det räcker dock inte med att ha en bra säkerhetspolicy och att ha infört säkerhetsåtgärder i datorsystemet, det krävs också förvaltning av systemet. En viktig del av förvaltningen är att följa upp hur säkerheten stämmer överens med uppsatta säkerhetskrav. Rist (2000) menar att det enda sättet att få en bra uppskattning av systemets säkerhet är att låta en säkerhetsspecialist göra en säkerhetsrevision.

En säkerhetsrevision kan beskrivas som den revision som görs av säkerheten hos en organisations nätverk och ingående datorsystem. Vilka områden som ska vara föremål för revisionen råder det delade meningar om men oftast delas de upp i de tre huvudområden: värddatorer, nätverk och brandväggar (se avsnitt 2.4.1). Vart och ett av dessa huvudområden innehåller ett antal aspekter på vad som ska revideras inom dem.

3.2 Problemavgränsning

Som nämns i inledningen är det ofta tre huvudområden som en säkerhetsrevision inriktar sig på: värddatorer, nätverk och brandväggar. Enligt avsnitt 2.1 bildar flera sammankopplade enheter ett nätverk. Figuren 3 ger en övergripande illustration av hur dessa hänger samman.



Figur 3: Illustration av huvudområden vid säkerhetsrevision (Brooks, 1998).

Figuren beskriver hur flera värddatorer kan vara sammankopplade så att de bildar ett nätverk med hjälp av olika nätverkskomponenter. Som en del av sammankopplingen mellan datorerna finns det brandväggar som är till för att filtrera kommunikationen mellan de olika värddatorerna i nätverket. En brandvägg kan beskrivas som en eller flera komponenter som begränsar åtkomsten mellan ett skyddat nätverk och Internet, eller mellan olika delar av nätverket (Chapman & Zwicky, 1995). Inom många datorsystem finns det också gemensamma databaser som kan nås av de datorer som ingår i systemet. Var och en av dessa delar behöver vara föremål för säkerhetsrevision för att säkra systemets tillförlitlighet.

Det kommer i detta arbete inte att ske någon undersökning av brandväggar och vad som ska granskas hos dem i samband med en revision. Vidare ligger inte området nätverk inom ramen för detta projekt vilket innebär att nätverksutrustning så som routrar, switchar, hubbar och kablage inte kommer att behandlas. Det huvudområde som arbetet kommer att inriktas på är värddatorerna i systemet. Orsaken till att detta huvudområde väljs är att en av utgångspunkterna i arbetet är hot mot systemet i form av intrång. Lagerlund (1998) skriver att intrång kan ske genom att förövaren uppträder under falsk identitet eller via hackers och virus. Genom att exempelvis

uppträda under falsk identitet kan förövaren använda sig av en dator som är behörig i systemet. Dataföreningen i Sverige (1997) trycker på vikten av kontroll av vilka datorer och användare som har rätt till viss information i systemet. Men denna kontroll är enbart intressant så länge det är känt vem som arbetar utifrån värddatorn. Om ett intrång sker i någon av dessa så är kontrollen av rättigheter inte längre intressant eftersom någon annan än den tänkta användaren jobbar utifrån den. Således utgör värddatorerna en inkörsport för intrång in systemet.

Arbetet med att undersöka denna del av systemet kommer att bedrivas med inriktning mot vårdsektorn. Den information som till stor del hanteras inom vården och som ska skyddas är sekretessbelagd patientinformation. I de journaler som förs inom vården lagras information om patientens identitet, uppgifter om bakgrund till vården, diagnoser etc. För sjukvårdens förtroende är det viktigt att säkerheten kring patientinformationen kan garanteras så att inga uppgifter kommer till obehörigas kännedom (Petersson & Rydmark, 1996). Den här typen av information kommer att vara den andra utgångspunkten i detta arbete.

3.3 Problemprecisering

De undersökningar som ska bedrivas i detta projekt kommer att utgöras av litteraturstudier och intervjuer. Syftet med undersökningarna är att ta fram de aspekter som ska undersökas då en säkerhetsrevision görs av värddatorerna i ett informationssystem inom vårdsektorn. Förslag och riktlinjer på hur säkerhet uppnås i system och vad som ska revideras ges av flera olika författare, bland annat av Weber (1999) och TK99 AG6 (2002). De riktlinjer och förslag som presenteras av dessa författare och i annan litteratur avser vanligtvis inte något enskilt område av ett informationssystem, så som värddatorerna, utan tittar på systemet som helhet. Detta kan eventuellt få till följd att detaljer missas då fokus ligger på helheten snarare än ett visst område av systemet.

Det första målet med arbetet är att finna de aspekter, hos värddatorerna, som föreslås ingå vid en generell säkerhetsrevision utan hänsyn tagen till avgränsningarna som är uppsatta för projektet. När detta är uppnått kommer det andra målet vara att utöka eller reducera dessa aspekter baserat på resultat från intervjuer med personal inom vårdsektorn. Detta görs för att bättre spegla vad en revision ska undersöka då den utförs på informationssystem inom vården med utgångspunkt i hot om intrång i systemet.

3.4 Förväntat resultat

Med en klar inriktning mot vårdsektorn och deras värddatorer och med utgångspunkt i hotet om intrång kan resultatet i detta arbete ge en ny infallsvinkel med bättre fokusering på vilka aspekter som ska väljas när en säkerhetsrevision ska genomföras. Målsättningen är att presentera vilka aspekter som ska beaktas vid en revision samt varför de ska ingå in en säkerhetsrevision. De tekniska detaljerna kring varje aspekt kommer inte vara föremål för närmare granskning i detta projekt.

3.5 Angreppssätt

För att genomföra arbetet kommer en empirisk undersökning, av hur revisioner inom vårdsektorn görs, att utföras tillsammans med en litterär översikt. Den empiriska undersökningen kommer att göras i form utav intervjuer av personal som jobbar med datorsystemen inom vården. Önskan är att dessa ska dela med sig av erfarenheter de har och information om vilka områden och aspekter inom dessa som de undersöker i samband med revision av sina datorsystem. Under förutsättning att rapporter från gjorda säkerhetsrevisioner inom vården kan erhållas, kommer dessa att utgöra en viktig källa till information om vad som bör ingå i en revision. Den teoretiska delen av undersökningen kommer att innefatta böcker, artiklar och rapporter.

4 Metod

I den första delen av detta kapitel beskrivs möjliga metoder som skulle kunna användas i detta examensarbete. Dessa består av *litteraturstudier, intervjuer, enkäter* och *jämförelse av revisionsverktyg.* Orsaken till att dessa redovisas är att de kan fungera som en hjälp vid eventuella fortsatta arbeten. I efterföljande avsnitt beskrivs vilka metoder som har valts samt motivering till varför det blev just de.

4.1 Möjliga metoder

Paulsson (1999) menar att metodproblem innebär att det finns ett val, mellan olika alternativ av metoder, om vilka som ska användas i en viss situation. När detta uppstår är det viktigt att presentera de olika alternativ som finns för att visa på en metodmedvetenhet. Utifrån dessa ta fram för- och nackdelar med respektive metod, ange vilka alternativ som väljs samt motiveringen till varför vissa val gjorts. De metoder som väljs bör leva upp till de krav som ofta ställs på metoder i akademiska sammanhang. Paulsson (1999) ger några exempel på de vanligaste kraven: *kontrollerbart, upprepningsbarhet och individoberoende.* Så länge metoder som i nuläget anges i metodböcker används, brukar det inte vara svårt att få metoden accepterad, däremot går det ofta att diskutera metodens lämplighet i en viss situation (Paulsson, 1999).

4.1.1 Litteraturstudier

En litteraturstudie innehåller två stycken olika huvudkomponenter: *litteratursökning* och *litteraturgranskning*. Det som innefattas i begreppet litteratursökning är att söka efter, sortera, hantera och sammanfatta litteraturen. Den granskande delen består av förståelse, kritisk värdering, konceptualisering och presentation av funnet material. För att knyta samman dessa delar spelar referenshanteringen en avgörande roll (Dawson, 2000). Orsaken till att en litteraturstudie görs motiveras enligt Dawson (2000) av de tre olika punkter som presenteras nedan:

- Den motiverar ett arbete – genom litteraturstudierna visas att området som behandlas är uppmärksammat och betydelsefullt och att arbetet därmed är värt att genomföras.

- Den sätter arbetet i relation till tidigare genomförda studier genom att diskutera och kritisk granska dessa. Genom denna jämförelse sätts arbetet in i ett större sammanhang och fungerar som ett bidrag till aktuellt område.
- För att andra forskare ska kunna fortsätta där arbetet slutar, ger litteraturstudien en startpunkt där andra kan ta vid samt att den ger uppgifter om vilken litteratur som är intressant och relevant.

Vid genomförande av en litteraturstudie finns det en rad olika källor som kan användas, exempelvis *böcker, tidningar och tidskrifter, forskningsartiklar och uppsatser*. *Böcker* utgör enligt Dawson (2000) ofta startpunkten för en litteraturstudie. Dessa bidrar med en bra överblick över det aktuella området, men kan lida av nackdelen att de inte är helt aktuella. Att granska aktuella *tidningar* och *tidskrifter* ger en bra uppfattning om vad som händer inom ett givet utredningsområde. Detta kan gälla både ämnesområdet och utredningsmetoder som används. Vidare ger det uppslag till annat material som kan studeras för djupare kännedom (Eriksson & Wiedersheim-Paul, 2001). Det kan lätt uppfattas som skrämmande att läsa de senaste *forskningsartiklarna* inom ett område då dessa representera det allra nyaste rönen som framkommit och därmed håller en hög nivå. Efterhand tenderar dock dessa artiklar användas mera då personen som utför arbetet får en ökad kunskap inom område och därmed kan tillgodogöra sig kunskapen i dem (Dawson, 2000). Användandet av *uppsatser*, gjorda vid högskolor och universitet, kan ge bra hjälp till att finna relevanta referenser. Dessa arbeten kan också bidra med tankar och idéer inom området som studeras (Dawson, 2000).

För att litteraturstudien ska fylla sin funktion är det enormt viktigt att det sker en kritisk granskning av det material som samlats in. När en sådan görs finns det en mängd frågor som kan ställas. Några exempel på sådana är: Är författaren erkänd inom området? Vad ger artikeln för bidrag? Har resultatet begränsningar, kan det författaren skriver endast användas under vissa förutsättningar? Huvudsyftet med att göra en kritisk granskning, av materialet från litteraturstudien, är att tanken på vad som har lästs ska väckas och mana till eftertanke (Dawson, 2000).

4.1.2 Intervjuer

Enligt Patel & Davidsson (1994) innebär en intervju direktkontakt mellan den person som utför intervjun och de som är föremål för den. Kontakten är direkt så till vida att

samtal förs mellan de två parterna, det behöver dock inte innebära att de fysiskt träffas. En intervju kan även utföras via telefon, Internet eller TV. En intervju som utförs kan enligt Olsson & Sörensen (2001) vara standardiserad och strukturerad. Med standardiserad innebär att intervjun är väl planerad för att minska respondentens inflytande på intervjun. Graden av strukturering anger hur stort utrymme det ges åt den som svarar att själv tolka innebörden i frågan. Enligt Patel & Davidsson (1994) finns det några negativa aspekter då denna metod används för informationssamling. Resultatet från intervjun är avhängigt hur villig respondenten är att svara på frågor och medverka till att relevant information framkommer. Personen som utför intervjun kan ha stor påverkan här beroende på hur denna agerar vid intervjutillfället. Vidare så är tidsaspekten en faktor som ofta uppfattas som negativ då intervjuer tenderar att ta stor tid i anspråk. Å andra sidan så kan denna tidsfaktor leda till att eventuella oklarheter kan redas ut så att missförstånd undviks. Vid utformande av frågor är det viktigt att ha i åtanke den påverkan som formuleringen av frågan kan ha. Eriksson & Wiedersheim-Paul (2001) trycker på vikten av att inte ställa flera frågor samtidigt eller överbelasta frågorna och att inte lägga in värderingar och överdrifter i dem.

4.1.3 Enkät

Enkäter är en undersökningsteknik som bygger på att samla information med hjälp av frågeformulär. Dessa skickas ut till respondenterna som får svara på dem innan formulären samlas in och sammanställs. Denna teknik lämpar sig att användas då ett stort antal personer ska ingå in undersökningen. Orsaken till detta är att sammanställningen av resultatet från enkäterna går snabbt att göra. En nackdel med denna teknik är att de som svarar på frågorna kan missuppfatta dem och därmed ge missvisande svar. Det går heller inte att ställa följdfrågor till respondenten om eventuella förtydliganden eller fördjupningar kring någon intressant synpunkt (Patel & Davidsson, 1994). Eftersom enkäter bäst lämpar sig att används då statistiskt material ska tas fram, är det enligt Bell (1995) viktigt att avväga om enkäter verkligen passar undersökningens målsättning och ger den information som behövs.

4.1.4 Jämförelse av mjukvara

Då säkerhetsrevisioner utförs används ofta någon typ av verktyg i form av en programvara. Dessa verktyg används för att undersöka och samla in data kring vissa områden av systemet som skulle ta lång tid att genomföra manuellt. Hur dessa verktyg

fungerar beror på den arkitektur de har (se avsnitt 2.4.1). Det gemensamma för dem är att de analyserar olika områden och aspekter av ett system för att kunna fastställa svagheter i systemet och ge en bild av dess säkerhet. Genom att jämföra områden och aspekter som analyseras av olika revisionsverktyg skulle förståelse kunna skapas kring vad dessa anser vara mest väsentligt att revidera. Denna information tillsammans med den som framkommer av litteraturstudier och intervjuer skulle kunna ge en god bild av hur en säkerhetsrevision ska genomföras och vilka aspekter i ett informationssystem som bör ingå. Om programvaror ska användas i ett projekt bör dessa införskaffas i ett så tidigt skede som möjligt för att undvika en situation, där programvaran inte längre är tillgänglig eller att den har blivit för dyra att få tag på, uppstår. Information och tips om olika programvaror och verktyg finns att tillgå på en rad olika ställen, exempelvis från Internet och företag eller specifika intresseorganisationer (Dawson, 2000).

4.2 Val av metod

Det finns några olika aspekter som ligger till grund för vilken eller vilka metoder som väljs då ett projekt ska genomföras. Bell (1995) menar att beroende på vilken typ av svar som förväntas, är vissa typer av undersökningsmetoder mer lämpliga. Vilken typ av svar som förväntas har att göra med hur preciseringen av problemet har gjorts. En annan aspekt som avgör valet av metod är enligt Patel & Davidsson (1994), de resurser som finns till förfogande samt hur mycket tid som finns disponibel. Det finns dock möjlighet att anpassa en viss metod efter det problem som ska lösas, men för att lyckas med detta är det viktigt att känna till metodens för- och nackdelar.

De metoder som har valts för detta examensarbete är *litteraturstudier* och *intervjuer.* Nedanför följer motiveringar till varför dessa har valts samt hur de ska användas specifikt i detta projekt.

4.2.1 Intervjuer

Den empiriska delen av undersökningen kommer att genomföras med hjälp av intervjuer. Det finns flera skäl till att denna metod har valts. För det första ger intervjuer information om hur säkerhetsrevisioner genomförs i praktiken, vilka aspekter som beaktas och om det sätt de arbetar på inom vården stämmer överens med resultatet från den teoretiska undersökningen. För det andra finns det begränsat med litteratur som enbart berör vårdsektorns säkerhetsarbete. Genom intervjuer går det att

få reda på vad som är speciellt och utmärkande för denna. Detta är av intresse eftersom en del av avgränsningen handlar om att undersökningen ska beröra just vårdsektorn. Genom att samtala med och intervjua personer, som jobbar med säkerhet inom vården, erhålls större förståelse och insikt om området som helhet, vilket förhoppningsvis ska bidra med att slutresultatet blir mer tillförlitligt.

Arbetet med att intervjua folk är tänkt att genomföras hos personer som sitter i positioner där de har en överblick över förvaltningen av systemet och då särskilt rörande säkerhetsaspekterna. Dessa intervjuer kommer i första hand inte inrikta sig på frågor som berör hur revisioner genomförs rent praktiskt utan på vilka aspekter som uppmärksammas då de genomförs. Förhoppningen är att få ta del av checklistor som används inom vården, som beskriver vilka områden och aspekter som analyseras i samband med en säkerhetsrevision.

4.2.2 Litteraturstudier

Orsakerna till att litteraturstudie väljs som metod för detta examensarbete är flera. Dels finns det de skäl som Dawson (2001) anger i avsnitt 4.1.1 men det finns också andra som är mer specifika för detta projekt.

Som nämns i avsnitt 3.2 så finns det sedan tidigare en del skrivet om vilka aspekter som bör beaktas vid en revision. För att kunna titta närmare på dessa och finna olika infallsvinklar krävs det studier av en rad olika litterära källor. Utifrån dessa är tanken att de aspekter som är mest frekvent förekommande och som har starkast argument för att revideras, ska ingå i resultatet av detta examensarbete. Vidare ger litteraturstudien, i form av tidskrifter och forskningsartiklar, information om det senaste som händer inom området säkerhet. Medvetenhet om detta är av vikt, då dessa kan presentera sådant som bör revideras, men som ännu inte förekommer frekvent i annan litteratur eller i checklistor som används av organisationer i det arbete som bedrivs idag.

Litteraturstudier kan således ge information om hur revisioner genomförs idag men även om hur de bör se ut i framtiden.

5 Genomförande

I detta kapitel beskrivs hur valda metoder har används vid genomförandet av examensarbetet. De metoder som ligger till grund för arbetet är litteraturstudier, som utgör huvuddelen, men även en empirisk undersökning i form av intervjuer har genomförts. En redogörelse för den litteratur som ingått i litteraturstudien kommer också att presenteras.

5.1 Empirisk undersökning

Syftet med den empiriska undersökningen i form av intervjuer, som tidigare tagits upp i avsnitt 4.2.1, var att få en bild av hur säkerhetsrevisioner genomförs i praktiken samt att få den speciella vinklingen mot vårdsektorn som beskrivs i problempreciseringen.

För att genomföra den empiriska undersökningen var tanken att ett antal personer, med kunskap om säkerhetsarbetet med informationssystem inom vården, skulle kontaktas. En förutsättning för att denna del av examensarbetet skulle fungera var att rätt personer med rätt kunskap var villiga att samarbeta och bidra med sin kännedom. För att finna dessa personer kontaktades Västra Götalandsregionens kontor i Göteborg, Landstinget i Blekinge, några lokala sjukhus samt en insatt person på Högskolan i Skövde. Vid förfrågningar hos dessa, och i vissa fall upprepade sådana, rekommenderades ett antal olika personer som ansågs ha de arbetsuppgifter och den kunskap som undersökningen krävde. Var och en av dessa kontaktades personligen, via besök eller via e-post. Resultatet av dessa kontakter varierade. I de flesta av fallen, där respondenten erhöll en förfrågan om eventuellt samarbete via e-post, tog det lång tid att få svar. I vissa fall kom detta svar överhuvudtaget inte alls. Vid flertalet utskick svarade personen som hade kontaktats att de, på grund av den mycket pressade arbetssituationen, inte hade möjlighet att bidra i undersökningen. I något fall berodde det även på den höga belastningen av sjukskrivningar på det aktuella sjukhusets IT-avdelning. Arbetet med att finna personer som kunde ingå i den empiriska undersökningen har, vilket framgår av beskrivningen ovan, varit svårt och många gånger frustrerade.

Sökandet har dock resulterat i att några stycken personer har varit villiga att svara på frågor i viss utsträckning. En av dem jobbar med säkerhetsfrågor, så som risk- och sårbarhetsanalyser, inom Landstinget i Blekinge. En annan jobbar för en intern konsultfirma inom Västra Götalansregionen. Denna enhet kallas för IT-centrum och

är en liten enhet med få anställda som jobbar för att gå i bräschen för säkerhetsarbetet inom regionen. Även IT-säkerhetschefen på Sahlgrenska i Göteborg har varit med och gett information kring arbetet med säkerhetsrevisioner. Resultatet som framkommit i kontakten med dem presenteras i kapitel 6.

Som ett resultat av svårigheterna med att finna villiga respondenter till undersökningen, har den empiriska delen av examensarbetet fått en mera tillbakadragen roll i resultatdelen. Detta påverkar i sin tur hur väl genomförandet svarar mot, den i avsnitt 3.3 beskrivna problempreciseringen. En djupare diskussion kring detta kommer att föras i diskussionen (se kapitel 9).

5.2 Litteraturstudie

Syftet med litteraturstudien, som tidigare beskrivits i avsnitt 4.1.1, var att finna material som finns skrivit om vilka aspekter som bör beaktas vid en säkerhetsrevision och att finna olika infallsvinklar till dessa. Genom att söka efter olika litterära källor kan arbetet med att finna de vanligast förekommande och mest väl motiverade aspekterna börja.

För att inte överbelasta läsaren med källor, och för att inte skapa ett hopplock av referenser, valdes från början av genomförandet att ett begränsat antal litterära källor skulle användas. Dessa skulle utgöra stommen i undersökningen och kompletteras med andra, för arbetet mindre betydande, när så behövdes. Vid en litteraturstudie är det brukligt att presentera och argumentera för de källor som har bäring på problemställningen och som används i genomförandet (Eriksson & Wiedersheim-Paul, 2001). Denna presentation följer längre fram i rapporten under avsnitt 5.3.

De källor som skulle utgöra grunden för arbetet behövde, till viss utsträckning, vara allmänt vedertagna och erkända. Om så inte var fallet skulle detta kunna ses som ett skäl till att inte finna resultatet fullt trovärdigt. För att finna dessa källor användes inledningsvis Högskolan i Skövdes bibliotek med tillhörande databaser. Det visade sig relativt omgående att det material som fanns att tillgå, i form av böcker, inte svarade upp mot de uppsatta målen med litteraturstudien. Detta grundar sig i första hand på att dessa, i stor utsträckning, inte var helt aktuella utan hade flera år på nacken. Eftersom utvecklingen inom det datavetenskapliga området, och då inte minst inom säkerhet, går mycket fort upplevdes dessa böcker många gånger inte vara helt relevanta. Även mängden av litteratur som fanns att tillgå var begränsad. Denna

granskning resulterade dock i att en av de källor som har används i undersökningen hittades. Denna källa är standarden ISO 17799, som presenteras i avsnitt 5.3.4, och utgör en av de mest erkända riktlinjerna inom informationssäkerhet.

För att finna flera erkända källor inom området användes databaser och Internet i en allt större utsträckning. Genom att söka efter publikationer och artiklar i dessa databaser, som många gånger är mycket omfattande, framträdde efterhand en organisation som omnämndes i flera olika sammanhang. Denna organisation CERT®, ett rapporteringscentra för säkerhet, verkade vara en auktoritet inom området informationssäkerhet. Eftersom det inte fanns några böcker att tillgå på biblioteket om dem, det gjordes vid senare tillfälle inköp, så användes Internet för att finna mer information. På deras hemsida (se avsnitt 5.3.3), och i en bok som senare köptes in (Allen, 2001), presenteras en modell som har används som en av huvudkällorna i detta projekt. Vid det fortsatta letandet efter relevant litteratur visade det sig att en av vår tids största myndigheter, den amerikanska staten, har ett särskilt organ som ansvarar för granskning och revision av statens verksamheter. Detta organ, General Accounting Office (GAO), har gett ut en manual som beskriver riktlinjer för hur interna kontroller, som styr integritet, sekretess och tillgänglighet på data, ska utvärderas vid en revision. Denna manual blev den tredje och sista av de källor som utgör stommen i detta examensarbetes genomförande.

Det har under arbetets gång visat sig att mycket av det material som finns inom området informationssäkerhet, och som delvis används i litteraturstudien, inte ensidigt behandlar den inriktning som beskrivs i problempreciseringen. Perspektivet på den information som studerats är många gånger mera generell än den som detta examensarbete ger uttryck för. Det har därför fått ske en avvägning om det material som presenteras är applicerbart eller inte.

När den litteratur som skulle användas var funnen var det dags att börja studera den mer ingående. Var och en av de tre källorna, CERT, ISO och GAO, studerades närmare i syfte att, dels få en bättre förståelse kring vem de riktade sig till och deras syfte, men också deras innehåll. Med utgångspunkt i problempreciseringen började sedan arbetet med att finna de aspekter som skulle ingå i en säkerhetsrevision. Att finna dessa var inte helt trivialt då det många gånger är svårt och komplicerat att avgöra huruvida en viss aspekt är tillräckligt starkt knuten till problempreciseringen för att tas med i resultatet eller inte. Efterhand som arbetet fortskred utkristalliserade

sig ett tiotal aspekter som verkade vara relevanta för resultatet. Med dessa som utgångspunkt fortsatta arbetet med att granska källorna för att finna vad hos respektive källa som gav stöd åt dessa aspekter. Det uppvisades variationer mellan CERT, GAO och ISO ifråga om fokusering på vissa av aspekterna, vilket är en av orsakerna till att aspekter ser ut att stödjas starkare av vissa källor än av andra.

5.3 Litteraturpresentation

Nedanför följer en presentation av de organisationer och myndigheter vars standarder och manualer utgör basen för genomförandet av examensarbetet. Dessa är *GAO, ISO* och *CERT*. Orsaken till att dessa tre har valts grundar sig delvis på att de till sin natur är vitt skilda åt. Den ena av dessa källor är en myndighet, Gereral Accounting Office, en annan är en stor internationell institution för standarder, Internationella Standardiserings Organisationen, medan den sista är en fristående organisation för säkerhetsfrågor rörande datorer, CERT® Coordination Center. Genom denna bredd ges det ett stort spektra av infallsvinklar. Dessa infallsvinklar kan bidra med att öka förståelsen av vilka aspekter som är viktiga att analysera vid en säkerhetsrevision inom vården.

5.3.1 General Accounting Office

General Accounting Office (GAO) är en myndighet som arbetar för den amerikanska regeringen. GAO är en självständig och politiskt oberoende myndighet som fungerar som den utredande delen av kongressen. De jobbar med att studera regeringens åtgärder och dess förbrukning av offentliga resurser. De ger råd till regeringen och de olika myndigheterna rörande hur det statliga arbetet kan skötas mer effektivt och ansvarsfullt. En del av myndighetens arbete handlar om revision av statens utgifter men även av dess informationssystem (http://www.gao.gov).

5.3.2 Internationella Standardiserings Organisationen

Internationella Standardiserings Organisationen (ISO) är en världsomspännande organisation som består av standardiseringsorgan från 140 olika länder, ett från varje land. ISO är en icke-statlig organisation som grundades 1947 med målsättning att främja utvecklingen av standarder i världen. ISO's arbete resulterar i internationella överenskommelser som publiceras som Internationella Standarder. ISO har under åren

gett ut en mängd olika standarder var av de mest kända torde vara ISO 14000 och ISO 9000 som utgör miljö- och kvalitetsstandarderna (http://www.iso.org).

5.3.3 CERT® Coordination Center

CERT® Coordination Center är en av de största rapporteringscentrarna för säkerhetsproblem förknippade med Internet. De arbetar med att ge teknisk rådgivning, identifiering av trender rörande intrång i datorsystem, samarbete med andra experter för att lösa säkerhetsproblem och att sprida information till den breda allmänheten. CERT®/CC analyserar också olika produkters sårbarhet, publicerar artiklar och jobbar med utbildning inom säkerhet. De finns placerade på institutet för mjukvaruutveckling på Carnegie Mellon Universitetet, som också är huvudmännen bakom centrat. Finansiering av verksamheten står till stor del det amerikanska försvarsdepartementet för, samt några olika statliga verk (http://www.cert.org).

5.3.4 ISO 17799, FISCAM och CERT

Var och en av ovanstående källor, ISO, CERT & GAO har givit ut någon typ av vägledning i form av en manual, standard eller modell. Dessa har till viss del olika användningsområden inom informationssäkerhetsarbetet samtidigt som samtliga ger bra information om vad som ska analyseras i en säkerhetsrevision. En jämförelse mellan dessa manualer, standarder och modeller kan bidra till att öka förståelsen till varför det finns avvikelser i deras presentation av revisionsaspekter. Den här presentationen och jämförelsen syftar till att lyfta fram de olikheter och likheter som finns mellan dem och hur de tillsammans kompletterar varandra.

ISO 17799

Detta är en internationellt erkänd informationssäkerhets standard. Den består av en omfattande samling av de bästa tillämpningarna inom informationssäkerhet. Dess föregångare, BS7799, har funnits under ett antal år utan att få någon större genomslagskraft. År 2000 blev den dock erkänd som ISO-standard och fick namnet ISO 17799, och det blev möjligt att certifieras och ackrediteras enligt den.

Syftet med denna standard är att specificera hur en verksamhet kan bygga upp ett ledningssystem för informationssäkerhet. En viktig del i detta arbete utgörs av en aktiv riskanalys. Denna analys syftar till att verksamheten ska identifiera sina informationstillgångar och att finna och förstå de risker som är förknippade med dem.

ISO 17799 ger handfast och praktiskt stöd gällande hur riktlinjer och rutiner införs och hur en verksamhet ska arbeta för att minska sårbarheten på sina informationstillgångar (TK99 AG6, 2002).

ISO 17799 har inte något enskilt kapitel som behandlar arbetet med revision av informationssystem. I kapitel 12.2, Granskning av säkerhetspolicy och teknisk efterlevnad, ges en kortare beskrivning av vikten att säkerställa att system följer organisationens säkerhetspolicy och säkerhetsnormer. Det anges bland annat att granskningen bör innefatta informationssystemet men även dess leverantörer, ägare och användare. Vidare ska även en teknisk kontroll göras för att säkerställa att säkerhetslösningen är korrekt implementerad. Denna tekniska kontroll kan dels göras manuellt men också med hjälp av olika mjukvaruverktyg.

Eftersom det inte klart och uttryckligt anges hur denna granskning ser ut och vad den ska innehålla så får andra delar i standarden fungera som riktlinjer. Exempelvis kapitel 9 som är en av de mest relevanta delarna för detta projekt, handlar om styrning av åtkomst till systemet. Här ger exempelvis standarden anvisningar om hur lösenordshanteringen ska gå till. Genom att studera de rutiner och regler som måste följas enligt standarden går det att få en bra bild av hur granskningen av säkerhetspolicyn och den tekniska efterlevnaden ska genomföras.

FISCAM

Detta är en akronym som står för *Federal Information System Controls Audit Manual* och är en manual utgiven av den amerikanska regeringens revisions organ, General Accounting Office, GAO. Den modell som beskrivs i manualen ger riktlinjer för revisorer då de ska utvärdera interna kontroller som styr integritet, sekretess och tillgänglighet på data som förvaras i de system som regeringen använder. FISCAM är primärt framtagen för att granska och utvärdera finansiella system. Metodens applicerbarhet på detta projekt är dock god då kraven på säkerheten inom den ekonomiska sektorn, i likhet med vårdsektorn, är mycket hög. Det uttrycks också i manualen att modellen kan användas då andra informationssystem ska granskas. FISCAM utges inte för att vara någon standard utan ska fungera som en guide vid informationssystemsrevisioner.

Manualen är tänkt att användas av systemrevisorer och finansrevisorer som sedan tidigare har nödvändiga kunskaper, färdigheter och förmåga att genomföra revisioner i en datorbaserad miljö. GAO menar att manualen ska fungera som ett gemensamt språk och en guide, för de i revisionen ingående revisorerna, så att de på ett effektivt sätt kan arbeta tillsammans som ett team, förstå uppgiften som ska lösas och nå gemensamma mål. Modellen går igenom de mål som ska uppnås när datorsystem granskas, den ger exempel på tekniker som kan användas och förslag på hur själva revisionen ska genomföras. Vissa områden i datorsystem anses vara så svåra att revidera att specialkompetens i form av tekniker kan behövas.

Manualen listar specifika kontrollaspekter och föreslår tillvägagångssätt för hur dessa ska revideras. De tillvägagångssätt som föreslås är beskrivna på en hög nivå och förutsätter kunskap om området för att kunna genomföras på ett effektivt sätt. Mera detaljerade beskrivningar kan behöva göras av revisorn, dessa ska baseras på de hård- och mjukvaror som den aktuella verksamheten använder sig av samt på deras säkerhetspolicy. För att få ut bästa möjliga resultat av den modell som beskrivs i manualen förutsätter GAO att revisorerna ska utföra utvärderingen med en viss nivå av skepsis, kritiskt tänkande och kreativitet.

CERT® Security Improvement Modules

CERT har givit ut en samling av moduler som ska hjälpa verksamheter att förbättra säkerheten i sina nätverk. Orsaken till att begreppet modul används är att varje sådan tar upp ett viktigt men väl definierat område som utgör ett problem inom nätverk. Dessa moduler är var för sig fristående och om någon anses som mera relevant kan denna användas skilt från de andra. Tanken är dock att de tillsammans utgör ett kraftfullt instrument för att förbättra nätverkssäkerheten.

Modulerna är uppbyggda på följande sätt. Varje modul representerar, som tidigare nämndes, ett viktigt men väldefinierat problemområde. Modulen består i sin tur av tre olika delar: *sammanfattning, praktiska tillämpning och implementationsdetaljer*.

- Den inledande *sammanfattningen* ger en beskrivning av problemet och en introduktion till problemområdet. Den drar även upp generella riktlinjer för hur problemet ska lösas.

- Den andra delen beskriver problemet mera i detalj. Den innehåller en kort beskrivning av vad som ska göras, det specifika säkerhetsproblemet som tas upp, dvs. varför det är ett problem och en eller flera metoder för hur de *praktiskt ska tillämpas*.
- *Implementationsdetaljerna* beskriver hur ovanstående tillämpningar ska genomföras för en specifik teknologi; exempelvis, Sun, Solaris, UNIX och Windows. I de flesta fall är de inte teknikberoende. Hur en verksamhet i praktiken tar tillvara på och inför dessa praktiska tillämpningar beror till stor del på vilken typ av nätverk och datorutrustning de har.

CERT modulerna är i första hand skrivna för att användas av system- och nätverkstekniker då det är dessa som i det dagliga arbetet installerar, konfigurerar och underhåller datorerna och nätverket. Det sätt på vilket de är skrivna och presenterade gör att även vanliga användare kan använda sig av dem. Dessa moduler finns att tillgå i en något förkortad version i boken *The CERT Guide to System and Network Security Practices av* Allen, H. J. (2001).

Jämförelse ISO, CERT och GAO

Vid en första anblick kan dessa tre källor ses som relativt snarlika. Detta kan till vis del stämma då de alla tre handlar om hur informationssäkerhet ska uppnås i en verksamhets system. Det finns dock även en del skillnader mellan dem. En jämförelse mellan ISO, GAO och CERT med utgångspunkt i några olika områden kan se ut som följer (se tabell 4):

Tabell 4: Jämförelse mellan de källor som används i litteraturstudien.

Område	**ISO**	**CERT**	**GAO**
Utgivare, typ av organisation	Internationell organisation	Icke-statligt rapporteringscentra	Statlig myndighet
Målgrupp	Företag, organisationer och myndigheter	Företag och privatpersoner	Staten
Syfte	Hjälpa organisationer att bygga upp ett ledningssystem för informationssäkerhet.	Fungera som ett stöd vid konfigurering av säkerhetsinställningar och vid uppföljning av tidigare gjorda sådana.	Fungera som en manual åt revisorer vid granskning av interna kontroller.
Upplägg	Lätt överskådlig	Lätt överskådlig	Något mera komplex
Hela eller delar av systemet	Hela systemet	Fokus på värddatorn	Hela systemet
Nivå	Goda förkunskaper	Vissa förkunskaper	Goda förkunskaper
Detaljrikedom	God, men inte fullständig	God	God
Exempel på genomförande	Ja, men i en separat handbok till standarden	Ja, ger exempel	Begränsat

Med utgångspunkt i några olika områden görs här en jämförelse mellan ovan presenterade källor.

De utgivare som står bakom de tre olika huvudkällor som används i genomförandet har varierande bakgrund. Det handlar om en internationell standardiseringsorganisation, ett icke-statlig rapporteringscentra och en statlig myndighet. Beroende på denna variation går det att se skillnader i vilka målgruppen för de olika modellerna och standarderna är. ISO standarden riktar sig i första hand till större verksamheter som önskar att bli certifierade enligt en erkänd standard medan GAO:s modell är tänkt att i första hand användas av statliga myndigheter som stöd för revisorer. CERT moduler kan användas av såväl privatpersoner som företag som önskar vägledning i säkerhetsarbetet med bland annat konfigureringar och säkerhetsinställningar. Beroende på målgruppen för dessa källor varierar den kunskapsnivå som krävs för att kunna använda dem på ett tillfredställande sätt. Även upplägget och den detaljrikedom som presenteras i dem varierar. Standarden från ISO är lättöverskådlig med sin uppdelning i välstrukturerade kapitel men det krävs god kännedom inom området för att fullt ut kunna använda den. Även den statliga modellen från GAO kräver goda förkunskaper. Orsaken till detta är att den i första hand är tänkt att användas av revisorer som har jobbat med liknande uppgifter

tidigare. Dock finns det brister i hur modellen är strukturerad och kan därför upplevas som svår att få ett grepp om hur den hänger samman. Modulerna från CERT ligger på en nivå där det inte krävs lika goda kunskaper som för de två tidigare nämnda, detta då den ska kunna användas av privatpersoner. Även dess upplägg och de exempel som anges i den bidrar till att den är lätt att använda.

6 Resultat

Resultatet från genomförandet av den litterära och den empiriska undersökningen presenteras i detta kapitel. Det mesta av resultatet baseras på den förstnämnda undersökningen vilket därmed gör resultatet mera generellt än vad som var tänkt från början. Tanken med resultatet, som framgår av problempreciseringen, var att finna aspekter hos värddatorerna som skulle undersökas vid en säkerhetsrevision av vårdsektorns datorsystem. Beroende på att den empiriska undersökningen inte har fortskridit enligt planerna så ser resultatet något annorlunda ut.

Med utgångspunkt i de manualer, modeller och standarder som används, och det tillvägagångssätt som beskrivs i föregående kapitel har följande resultat framkommit. Det presenteras utifrån tio olika aspekter. Detta antal är ett resultat av hur de olika delområdena har slagits samman för att bilda den grupp av delområden som kallas aspekter. Var och en av dessa aspekter innehåller en introduktion till det område som den berör samt en motivering till varför det anses befogat att den aspekten bör ingå i en revision. Inom varje aspekt finns det ett antal olika delområden som mer i detalj går in på vad som ska undersökas vid en revision. De delområden som finns med inom respektive aspekt, gör det för att de stämmer överens med den avgränsning som examensarbetet har. Deras medverkan i resultatet stöds i vissa fall av samtliga av de tre källor[1] som ligger till grund för arbetet, medan de i vissa fall enbart finner stöd hos en. En djupare diskussion gällande detta kommer att föras i kapitel 7.

6.1 Resultat från litteraturstudien

Resultatet utgörs av tio aspekter (se tabell 5) vars innehåll grundar sig på det material som framkommit i studierna av ISO, CERT och GAO:s utgivningar. Detta resultat har inte någon vinkling mot vårdsektorn utan är generell i avseende på vilken typ av organisation det är tillämpbart på. Den vinkling som finns i denna del av resultatet, handlar om att de aspekterna som presenteras berör värddatorerna i ett system med avseende på hot om intrång. Resultatet presenteras i tio tabeller som var och en utgör en aspekt. Inom varje aspekt finns ett eller flera delområden som mer i detalj redogör för vad som ska revideras i en säkerhetsrevision. Det anges för varje sådant delområde

[1] GAO - General Accounting Office
ISO - Internationella Standardiserings Organisationen
CERT - CERT® Coordination Center

vilken eller vilka av källorna som stöder dess medverkan i resultatet. Efter varje tabell följer en analys och beskrivning av det som presenteras i tabellen.

Tabell 5: Sammanfattning av de tio aspekterna med respektive delområden

Aspekt	**Delområde**
Behörighetsprofiler och konton	Behörighetsprofiler Konton Filer
Fjärranslutning	Distansarbete Mobil dator användning
Inloggning	Inloggningsrutiner
Virus	Installering av programvara (icke godkänd) Installering av programvara (godkänd) Installering av virusprogram
Loggning	Vad som loggas Händelser som loggas
Lösenord	Lösenord
Nätverkstjänster	Identifiera alla nätverkstjänster Identifiera alla nätverkstjänster som automatiskt är aktiverade. Sätt ur stånd och ta bort alla nätverkstjänster som inte ska användas. Konfigurera kvarvarande nätverkstjänster så åtkomst och exponering begränsas.
Systemmjukvara	Systemmjukvara
Uppdatering av programvara	Uppdatering av programvara
Säkerhetskopiering	Säkerhetskopiering

6.1.1 Behörighetsprofiler och konton

Inloggning och verifiering sker vanligtvis genom att användaren anger ett användarlogin och ett lösenord. Vid inloggningen verifierar systemet användarens identitet. Antingen så blir användaren positivt verifierad alternativt får användaren inte tillgång till systemet. Vid godkänd verifiering tilldelas en behörighetsprofil innehållande aktuella verksamhetsroller för användaren (Lagerlund, 1998).

En behörighetsprofil skapas och underhålls av ansvarig personal genom att respektive användare blir tilldelad viss behörighet. Denna behörighet baseras bland annat på roller, befattningar, arbetsuppgifter och behov. När en användare försöker att använda en resurs i systemet så kontrolleras det om användaren har behörighet till den, denna

behörighet tilldelas användaren av resursägaren. Behörigheten som en användare har specificeras i en så kallad *åtkomstkontrollista* (eng. access control list). Den innehåller för varje resurs i systemet, en beskrivning på vilka användare som har behörighet att använda den. Beroende på hur användarens behörighetsprofil ser ut ges olika behörighet till systemets resurser.

De ovan beskrivna behörighetsprofilerna anger till vilka delar av systemet en användare har behörighet. De anger inte vilka åtgärder som användaren har rättighet att utföra på dessa resurser, denna rättighet anges utifrån så kallade konton. Varje användare av systemet är tilldelad ett konto. Konton avgör vilka rättigheter som användaren har att utföra vissa åtgärder i systemet. Det finns olika typer av konton med varierande grad av rättigheter, exempelvis: användarkonton, gästkonton och administratörskonton. Vanligtvis har användar- och gästkonton en låg grad av rättigheter medan administratören har fulla rättigheter. För att underlätta arbetet med tilldelning av rättigheter används något som kallas grupper. Varje grupp tilldelas vissa rättigheter och hit kan användare anslutas. En användare kan vara ansluten till flera olika grupper och därigenom erhålla olika grader av rättigheter (Stinson, 1994).

Motivering

En av revisorns viktigaste uppgifter är att avgöra vilka inställningar som har gjorts och om de överensstämmer med de åtkomsträttigheter som upprättats av de olika resursägarna (se tabell 6). Om behörighetsprofilen inte stämmer överens med en användares åtkomsträttigheter ökar risken för att obehöriga kommer åt information och program i datorn.

Tabell 6: Aspekten behörighetsprofiler och konton med tillhörande delområden**.**

Aspekter	**Delområde**	**Stöds av**
Behörighetsprofiler	Delad åtkomst av information ska ha godkänts av ägaren.	GAO, CERT
	Uppdatera listor med användargrupper och deras åtkomsträttigheter.	CERT, GAO, ISO
	Alla filer ska tillhöra en säkerhetskategori, denna lista ska uppdaterats regelbundet.	GAO
	Styrning av särskilda rättigheter till information och programvara ska kontrolleras extra noga. Exempelvis programvara som kan gå runt normala säkerhetskontroller.	CERT, GAO, ISO
	Jämför åtkomsträttigheter med åtkomstaktiviteter.	GAO, ISO
	Kryptera behörighetsprofilerna.	CERT, GAO
	Följs riktlinjerna/policyn för tilldelning av åtkomsträttigheter.	ISO, GAO, CERT
	Fördelning av privilegierade rättigheter bör kontrolleras för att avgöra att de inte erhållits obehörigt.	ISO
	Delad åtkomst av information ska ha godkänts av ägaren.	GAO, CERT
Konton	Ta bort/avaktivera konton som inte används.	CERT, GAO
	Kontrollera inställningarna i säkerhetsprogramvaran (access control software) om de stämmer med givna rättigheter. Ex. R, W, X till vissa filer.	CERT, ISO
	Undvik delade användarkonton	CERT
Filer	Skriv/ändrings rättigheter får inte finnas på körbara filer.	CERT
	Operativsystemets källfiler har endast administratören åtkomst till.	CERT
	Lista med vilka som har åtkomst till filer ska regelbundet kontrolleras.	GAO
	Kontrollera åtkomst genom arv då nya kategorier av filer och användare har skapats.	CERT
	Kontrollera de punkter som är känsliga i åtkomstvägarna.	GAO

Samtliga källor återkommer flera gånger till vikten av att följa upp de listor som anger en användares rättigheter och behörigheter som tilldelats av resursägare och administratörer. Det är utifrån dessa listor som en stor del av systemets säkerhet byggs. Felaktig behörighet i dessa listor resulterar i att detta fel kommer att sprida sig till resten av systemet och leda till att obehöriga får åtkomst till delar i systemet som

de inte ska ha. Det handlar även om uppdatering och kryptering av behörighetsprofiler och kontroll av att interna riktlinjer följs. Denna aspekt finner stort stöd hos alla de källor som studerats. De konton i systemet som inte längre använts ska snarast möjligt tas bort eller avaktiveras för att inte kunna användas av obehöriga. Det kan handla om tillfälliga gästkonton eller om konton som har tillhört anställda som har slutat. Denna punkt tas inte upp i ISO standarden men anses ända vara av så pass viktigt att det bör revideras. ISO standarden går heller inte in på hanteringen av enskilda filer, så som källfiler och körbarafiler. Dessa berörs i större utsträckning av CERT och GAO som anser att åtkomst samt skriv- och ändringsrättigheter på dessa filer ska revideras med jämna mellanrum. Vissa delområden som behandlas i denna aspekt berörs inte av samtliga källor, men det finns ändå en stor enhet kring vikten av att granska och följa upp behörighetsprofiler och användarkonton.

6.1.2 Fjärranslutning

Fjärranslutning spelar en viktig roll vid bland annat administrering av ett nätverk, exempelvis vid underhåll av dess värddatorer. Att administrera värddatorer kan innebära undersökning av loggar, uppdatering av information rörande användarkonton, installering och uppdatering av mjukvara och konfigurering av olika inställningar. Dessa uppgifter kan dels skötas från den enskilda datorn men också från en annan dator via en nätverkskoppling, så kallad *fjärranslutning.* Det har enligt CERT blivit allt vanligare med fjärranslutningar, och detta ses som ett resultat av de kostnadsbesparingar som kan göras. Fjärranslutning används också för att utföra andra arbetsuppgifter vid sidan av de rent administrativa.

Beroende på vilka mjuk- och hårdvaror som används, för att sköta fjärranslutningen, finns det skillnader mellan vilka aspekter som ska beaktas. De aspekter som presenteras nedan är några huvuddrag (se tabell 7). För att fullt ut klara av en revision av detta område kan det många gånger behöva anlitas en expert inom området datakommunikation.

Motivering

En dator som vid normal användning är säker kan vid administrativt arbete, som nämndes ovan, vara i ett tillfälligt sårbart läge. Detta är extra tydligt om det sker hos enheter utanför företaget via fjärranslutning, eftersom arbetet då inte sker innanför organisationens egna brandväggar, vilket kan öppna dörrar för intrång. Detta kan

resultera i att sekretessbelagd information exponeras eller att informationens integritet kompromissas, inkräktaren får åtkomst till resurser på det interna nätet, eller kan använda enskilda datorer som tillfälliga värdar för attacker på andra interna eller externa datorer.

Tabell 7: Aspekten fjärranslutning med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Distansarbete	Datorers identitet ska verifieras för att begränsa åtkomsten från specifik dator.	GAO, ISO, CERT
	Användare ID och lösenord ska verifieras vid åtkomst till applikationer.	GAO, ISO
	Kontrollera åtkomsten mellan systemet som ansluter och värddatorn, överföringar bör vara krypterade.	GAO, CERT
	Anslutningen ska avslutas automatiskt efter sessionens slut eller inte används under viss en tid.	GAO, CERT
	Kontrollera lista över behöriga som får fjärranslutas.	GAO
	Definitioner av tillåtet material och arbetsuppgifter som får utföras.	ISO
	Skydda känslig data under överföringen	GAO
	En applikations användning av nätverkets resurser, så som interna system och tjänster, ska vara begränsad.	GAO,ISO
	Automatisk terminalidentifiering för autentisering av förbindelsen.	ISO
	Rutiner för säkerhetskopiering	ISO
	Kontrollera att interna policys och säkerhetsprocedurer följs.	ISO, GAO, CERT
Mobil datoranvändning	Kontrollera att de interna riktlinjerna följs	GAO, CERT

Alla källor trycker på vikten av att datorers identitet så väl som användarens lösenord verifieras vid distansarbete för att undvika obehörigas åtkomst. När en anslutning väl finns mellan två datorer ska det material som skickas mellan dem vara i krypterad form och fjärranslutningen bör enligt GAO och CERT avbrytas automatiskt efter sessionens slut. Eftersom säkerhetsrisken är högre vid fjärranslutning än vid intern användning av systemet, anses det i ISO standarden vara viktigt att det finns begränsningar i datorn för vilket material och vilka arbetsuppgifter som får utföras vid sådan uppkoppling. Ingen av källorna kan gå in på alla detaljer eftersom det finns stora variationer beroende på vilken utrustning som används och hur verksamheten i övrigt ser ut, därför anger samtliga behovet av att följa upp de riktlinjer som finns i

respektive verksamhet. Det samma gäller den mobila användningen av datorer och hur dessa ska hanteras för att trygga informationens säkerhet.

6.1.3 Inloggning

När en användare ska använda en tillgång finns det mekanismer med hjälp av vilka användaren bevisar sin rätt att använda tillgången. När det handlar om åtkomst till ett datorsystem finns det normalt två steg i denna process (Caelli, 1991):

- användaren anger sin identitet, vanligtvis genom en användarlogin eller någonting som innehåller användarens identitet, exempelvis ett kort eller en nyckel.
- användaren bevisar sedan att han eller hon har rättighet att kräva den åtkomst som stämmer överens med angiven användarlogin.

Att kunna bevisa identiteten på användaren är en grundläggande process inom dator- och nätverkssäkerhet. Men om säkerheten i samband med inloggning är för besvärlig och upplevs som ett hinder av användarna kan detta istället få motsatt effekt. Användarna kan då på olika sätt försöka ta sig förbi och göra genvägar genom säkerhetssystemet för att underlätta inloggningen. Detta kan exempelvis göras genom att datorer lämnas upplåsta utan att användaren är i närheten, bakdörrar i systemet skapas eller att lösenord skrivs på en lapp bredvid datorn (Caelli, 1991).

Motivering

Om obehöriga kan komma åt de bevis som krävs av en godkänd användare så har hela säkerhetssystemet fallerat. Om detta inträffar kan förövaren genomföra otillåtna ändringar, få insyn i sekretessbelagd information och orsaka förlust av data. För att skydda sig mot detta kan ett antal motåtgärder användas (se tabell 8).

Tabell 8: Aspekten inloggning med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Inloggning	Antal försök att logga in ska vara begränsat.	CERT, GAO, ISO
	Ingen systeminformation visas förrän inloggning är klar.	ISO
	Inloggning få endast ske på fastställda tider.	ISO, GAO
	Kontroll av inställningar och se om dessa stämmer med de, av resursägaren, uppsatta regler.	GAO
	Automatisk utloggning när terminalen inte används.	GAO, ISO, CERT
	Tidsfördröjning vid misslyckad inloggning.	ISO
	Text på skärmen ska visa att åtkomst till datorn endast får ske av behöriga användare.	ISO
	Max- och minimitider för inloggningsrutiner	ISO
	Inloggningsinformation ska valideras först efter all data inmatats.	ISO
	Kontrollera efterlevnad av interna regler och policys	CERT, ISO, GAO

Eftersom lösenord går att gissa sig till ska det enligt CERT, GAO och ISO inte vara möjligt att på detta sätt ta sig in i dator. Som ett resultat av detta anser de allihop att det maximala antalet försök att logga in i en dator inte ska överstiga tre. ISO standarden går så långt som att säga att dator ska vara inställd så att det råder en viss tidsfördröjning efter varje misslyckad inloggning och att ingen information ska visas på skärmen förrän fullgod inloggning är genomförd. En användare som är inloggad men som inte använt datorn under en viss tid ska automatiskt loggas ut för att undvika att någon obehörig ska kunna använda den. Även här ska det undersökas så att de interna riktlinjerna och reglerna för inloggning efterlevs.

6.1.4 Virus

Datorer är skapade för att följa vissa givna instruktioner. Dessa instruktioner utför oftast det som användaren tror att programmet ska utföra, exempelvis någon beräkning, filradering eller handhavande av en databas. Ibland kan dessa instruktioner vara felaktiga och därmed utföra operationer som de inte är tänkta att göra. Detta kan dels bero på att programvaran innehåller buggar eller att programmet på något sätt skadats. Men det kan också bero på att programvaran medvetet har ändrats för att utföra operationer som inte överensstämmer med användarens bild av vad den ska göra. När sådant inträffar kallas programkoden för skadlig kod (Garfinkel & Spafford, 1996). Det finns rad olika hot som uppkommer genom programvaror och dessa kan

delas upp i ett antal olika kategorier men i dagligt tal kallas de ofta för virus. Garfinkel & Spafford (1996) ger nedan en beskrivning av de vanligast förekommande definitionerna på skadliga program:

- *Säkerhetsverktyg*, som är skapade för att användas i syfte att säkra ett system kan också användas av obehöriga för att undersöka ett system i syfte att hitta svagheter som kan utnyttjas vid intrång.
- *Logisk bomb*, är kod som är gömd i programvaran och som utför en viss handling när rätt omständigheter inträffar.
- *Bakdörr*, tillåter obehöriga åtkomst till systemet.
- *Virus*, eller program som ändrar andra program på datorn, genom att kopiera in sig själv i dem.
- *Maskar*, program som förökar sig från dator till dator på ett nätverk, utan att nödvändigtvis ändra några program på måldatorn.
- *Trojanska hästar*, program som utger sig för att ha en funktion men som egentligen utför någon annan.

Flera av de hot som nämns ovan har även icke-destruktiva användningsområden. Det som gör ett program till ett hot är inte hur det fungerar utan syftet som ligger bakom användandet av det.

För att kunna skydda sig mot skadliga program måste det finnas kännedom om varifrån de kommer för att rätt motmedel och skydda ska kunna sättas in. Det finns enligt Garfinkel & Spafford (1996) tre vanliga sätt för skadliga program att komma in i en dator:

- *Inifrån systemet* – bakdörrar och trojanska hästar finns oftast i systemet därför att det är där de har skrivits från början.
- *Installering av programvara* – genom att installera program som inte har undersöks noggrant kan vanliga användare vara med och sprida virus, maskar, och andra sådana hot. Detta kan exempelvis ske genom nedladdning av programvaror från Internet.
- *Nätverk* – program som skrivs på utsidan av nätverket kan ta sig in via olika kopplingar som finns mellan datorerna.

Vad som kan hända när dessa skadliga programvaror tar sig in i en dator diskuteras i stycket nedanför.

Motivering

De hot från programvaror som gåtts igenom kan orsaka betydande skador på en dator och det system den ingår i. Sekretessbelagd information kan vidareförmedlas, känslig information kan ändras, och inställningar på datorn kan modifieras så att otillåten åtkomst medges och därmed leda till intrång. Genom kännedom om vad som ska undersökas vid en säkerhetsrevision kan riskerna från dessa hot minska (se tabell 9).

Tabell 9: Aspekten virus med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Installering av programvara (icke godkänd)	Kontrollera att policyn och regler som berör installering av mjukvaror efterlevs. Utseendet på reglerna varierar mellan organisationer.	GAO, CERT, ISO
	Kontrollera att policyn som berör nedladdning av datafiler och program från eller via externa nätverk och andra medium efterlevs.	ISO, CERT
Installering av programvara (godkänd)	God dokumentation av alla förändringar.	GAO, ISO
	Uppdatering av programvarubiblioteket.	GAO
	Kontrollera att installerad programvaran är testad och godkänd.	GAO, CERT, ISO
Installering av virusprogram	Kontrollera och uppdatera programvaran regelbundet.	CERT, GAO, ISO
	Gör periodiska kontroller av systemet med hjälp av off-line kopior av virusprogrammet.	CERT
	Kontrollera att de senaste versionerna av virusprogrammet är installerat.	CERT
	Virusprogram ska kontrollera bifogade filer i e-post.	ISO

Samtliga källor står bakom uppfattningen att de regler som finns inom en verksamhet gällande installering och nedladdning av program ska granskas för att se att de efterlevs. Tyvärr är det inte alla verksamheter som har fastställt hur dessa regler ska se ut, vilket medför att det står användarna fritt att ladda ned det som de hittar på Internet, får via e-post eller har med sig på disketter. Det anses även vara av stor vikt att kontrollera att den programvara som redan är installerad verkligen är godkänd och testad. Detta kan den vanlige användaren inte göra så mycket åt utan det ligger på systemadministratörernas ansvar. GAO och ISO menar även att det noggrant bör följas upp om eventuella förändringar av godkända program görs. Vad gäller virusprogram som är till för att skydda datorn, så ska det enligt CERT regelbundet avgöras om det är de senaste versionerna som finns installerade i datorn. Det finns inte mycket angivet om vad ett virusprogram ska innehålla och vad det ska klara av

att göra. ISO säger dock att programmet ska kunna kontrollera filer som är bifogade i e-post.

6.1.5 Loggning

Loggning innebär, att föra en kontinuerlig förteckning över de händelser som inträffar medan ett program eller ett system körs. De händelser som inträffar under körningen lagras i så kallade loggar. Det finns en mängd olika typer av loggar som var och en används för olika ändamål. Några exempel på sådan är säkerhets-, drifts-, debiterings- och transaktionsloggar. Den typ som är intressant att titta på vid en säkerhetsrevision är säkerhetsloggen. De säkerhetsloggar som förs måste ha en hög autenticering, vara lätta att hantera och att analysera. Vad dessa loggar innehåller baseras på säkerhetspolicyn och regler uppsatta att styra loggningen. Det finns en mängd händelser som behöver loggas (se tabell 10), bland annat beroende på en verksamhets säkerhetsnivå, och dessa kan utgöras av inloggningar, ändringar i säkerhetsprofiler och åtkomst till känsligt material.

Motivering

Syftet med att föra loggar ur ett säkerhetssammanhang är (SSR 97 ETT, s. 93):

- att kontrollera åtkomstmönster hos individuella objekt samt åtkomsthistorik över processer, individer och hur olika skyddsmekanismer används,
- att kunna se om någon har försökt ta sig förbi skyddsmekanismerna i systemet,
- avgöra om en användare försökt skaffa sig högre behörighet än denne är tilldelad,
- att kunna ingripa om någon vanemässigt försöker ta sig förbi skyddsmekanismerna,
- att visa för användarna att alla försök att ta sig förbi skyddsmekanismerna loggas och medför upptäckt

De händelser som loggas kan efterhand behöva förändras som ett resultat av utveckling av informationssystemet, införande av ny applikationer eller att förövare angriper via ny metoder. Om detta inte görs, kan händelser som skulle kunna avslöja eventuella intrång förbises, och därmed inte loggas.

Tabell 10: Aspekten loggning med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Vad som loggas	• användar-ID • använda resurser • vad som ändrats • datum • tid • dator	GAO, ISO
Händelser som loggas	Ickebehöriga försök till åtkomst	GAO
	Åtkomsttrender och avvikelser från dem	GAO, ISO
	Åtkomst till data och andra resurser	GAO, ISO
	Högkänslig privilegierad åtkomst, så som möjlighet att ta sig förbi säkerhetssystemet.	GAO, ISO
	Åtkomstmodifieringar gjord av säkerhetspersonalen.	GAO
	Misslyckade och lyckade försök till inloggning	GAO, ISO
	Brott mot interna säkerhetsregler inom organisationen	GAO
	Systemlarm och larm utlösta pga. intrång i systemet.	ISO
	Alla användning av system-hjälpmedel	ISO, GAO
	Utnyttjande av systemansvarigs-konto.	ISO, GAO
	Meddelanden från nätverksportar och brandväggar.	GAO, ISO
	Överträdelser mot åtkomstregler	ISO

Detta är en aspekt som överhuvudtaget inte tas upp av CERT och orsaken till detta är oklar. De två andra källorna säger det är svårt att i förväg avgöra vad som ska loggas hos en dator efter som det finns stora variationer mellan olika verksamheter och att det styrs av interna riktlinjer. Inom exempelvis vården handlar mycket av loggningen om hur patientjournaler hanteras, vilket intet är något som behandlas inom verksamheter som tillverkningsindustrin. ISO och GAO är dock överens om att sådant som användaridentitet, tid, datum och resurser som används ska loggas när vissa aktiviteter utförs. Vad gäller dess aktiviteter så råder det relativt stor överensstämmelse mellan de olika källorna. Exempelvis anser de båda att aktiviteter så som åtkomsttrender och avvikelser, brott mot interna säkerhetsregler och användandet av systemansvarigs konto ska loggas. Men det finns även aktiviteter som enbart stöds av en av källorna.

6.1.6 Lösenord

Identifiering är en process som skiljer en användare från de andra. Detta görs vanligtvis genom användning av någon typ av användarnamn. Användarnamnet är viktigt eftersom det är via det som specifika rättigheter tilldelas och känns igen av datorn, men det är oftast inte hemligt. Därför används det andra sätt för att avgöra om en användare är den han utger sig för att vara. Det mest frekventa sättet att göra detta på är användning av lösenord, vars utseende bestäms av uppsatta regler (se tabell 11). Genom att användaren anger användarnamn tillsammans med korrekt lösenord ges denne tillträde till systemet (Silberschatz, 2003).

Motivering

Obehöriga kan sätta säkerheten på spel genom åtkomst av information som finns lagrad i datorn eller som kan nås från den. För att förhindra detta måste en dator konfigureras så att användarens autenticitet kan bekräftas och därmed hindra att någon obehörig kommer in i den. Detta kan göras om användningen av lösenord sker korrekt.

Tabell 11: Aspekten lösenord med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Lösenord	Unikt för varje individ	ISO, GAO,
	Byte efter viss tid ex. 30 dagar	CERT, ISO, GAO
	Ej återanvändning inom visst antal generationer.	GAO, CERT, ISO
	Längden på lösenordet	GAO, CERT, ISO
	Inga fabriksinställda lösenord	ISO, GAO
	Användning av ord och namn är förbjudet, ev. en lista med förbjudna lösenord	GAO, ISO
	Lösenordsfiler är krypterade	GAO, ISO
	Lösenordspolicyn ska implementeras så att lösenord som inte uppfyller kraven avisas.	CERT,
	Vem som får ändra lösenorden	CERT
	Ändra lösenord och namn på default konton	CERT

Användandet av lösenord är kanske den aspekt där det råder störst överensstämmelse mellan ISO, GAO och CERT. Orsaken till detta kan vara att det är en aspekt som är lätt att greppa och att dess regler inte är så svåra att fastställa, det är heller ingen större variation på hur lösenord hanteras från system till system. Det som de anser ska granskas vid en revision är att det byts med jämna mellanrum, att det inte återanvänds

inom ett visst antal generationer och dess längd. Vidare finns det starkt stöd för att inga fabriksinställda lösenord får användas, att lösenordsfiler ska krypteras samt hur utseendet på lösenordet får vara. CERT menar även på att det ska kontrolleras vilka som har rätt att ändra lösenord samt att intern lösenordspolicy efterlevs.

6.1.7 Nätverkstjänster

Många datorer innehåller ett brett utbud av nätverktjänster och servermjukvara som är förinstallerade för att datorn ska kunna användas som:

- en persondator som endast använder nätverkstjänster som en klient
- en persondator som förser och använder tjänster från andra arbetsstationer
- en dator som fungerar som en server

De flesta datorerna behöver inte ha alla nätverkstjänster som är förinstallerade. Dessa tjänster kan utgöras av Internettjänster så som FTP[1], WWW[2] och fjärranslutning eller filhantering, elektronisk post, databasåtkomst och utskriftshantering. Därför bör alla tjänster som inte är nödvändiga tas bort. Hur detta kan genomförs presenteras i tabell 12. Det är svårt att säga vilka tjänster som ska och inte ska tas bort, beroende på att en dator kan ha så varierande användningsområden (Allen, 2001).

Motivering

Datorer som utför tjänster såsom fildelning måste känna igen och lita på andra datorer den kommunicerar med. Varje tjänst som finns på en dator kan vara en inkörsport för obehöriga användare och vara ett potentiellt säkerhetsproblem för den datorn och andra datorer på ett lokalt nät. Det är därför viktigt att endast tillåta de tjänster som krävs för att datorn ska kunna användas till det den är till för.

[1] File Transfer Protocol
[2] World Wide Web

Tabell 12: Aspekten nätverkstjänster med tillhörande delområden

Aspekter	Delområde	Stöds av
Identifiera alla nätverkstjänster	De nätverkstjänster som är tillgängliga i systemet.	CERT
Identifiera alla nätverkstjänster som automatiskt är aktiverade.	Scanning av portarna	CERT
	Kontroller personliga WWW och FTP servrar.	CERT
Sätt ur stånd och ta bort alla nätverkstjänster som inte ska användas.	Finn onödiga tjänster.	CERT
	Ta bort dessa tjänsters körbara filer.	CERT
	Ta bort dess konfigureringar och datafiler.	CERT
Konfigurera kvarvarande nätverkstjänster så åtkomst och exponering begränsas.	Begränsa vilka som har tillgång till tjänsten	CERT
	Kan endast användas av datorer med autenticierad uppkoppling.	CERT
	Begränsa graden av tillgång	CERT

Denna aspekt tas enbart upp av CERT. Detta kan vara ett resultat av att de har större fokusering på just värddatorerna i ett system. Den här aspekten anses som så viktig att den ändå ingår i resultatet. Det som CERT säger är att det första som ska göras vid en revision är att fastställa vilka nätverkstjänster som finns och vilka som automatiskt är aktiverade enligt förinställningar. Utifrån resultatet från detta ska de tjänster som inte är nödvändiga avaktiveras och tas bort. De tjänster som sedan återstår ska konfigureras på ett sätt så att åtkomst och exponering av dem begränsas. Om detta görs kan mjukvarukomponenter som annars utgör en inkörsport för intrång avlägsnas eller konfigureras på ett sådant sätt att de kan användas säkert.

6.1.8 Systemmjukvara

Systemmjukvaror är program som är designade att styra och kontrollera processer i datorutrustningen. Enligt Svensk Standard SS 01 16 01 avses främst operativsystemet men även andra program som är av grundläggande betydelse för att ett datorsystem ska kunna utnyttjas. Dessa program brukar ofta användas för att stödja och köra applikationer som körs på samma dator. De används till allt från att koordinera in- och utmatningar till att ändra data och programkod utan att lämna spår efter sig. Några exempel på systemmjukvaror:

- Operativsystem
- Programbiblioteksystem

- Filunderhållsystem
- Säkerhetssystem
- Databashanteringssystem

Motivering

Om systemmjukvaran inte skyddas kan en obehörig få tillträde till dessa. Förövaren kan då ta sig runt olika säkerhetsåtgärder som skyddar operativsystemet och gå in och ändra i åtkomstkontrollen som skyddar olika programvaror. Här ifrån kan individen läsa, ändra och förstöra programvaror och viktiga datafiler samt ta bort alla spår på att intrång har skett. Det behövs således åtkomstkontroll av samtliga av systemmjukvarorna. Om detta skydd inte är fullgott kan skador uppstå på enskilda komponenter i systemet eller så kan vissa komponenter användas för att skapa åtkomst till förbjudna delar av systemet.

Tabell 13: Aspekten systemmjukvara med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Systemmjukvara	Endast viss godkänd personal har åtkomst till dem, uppdateras.	ISO, GAO
	Godkännandena ska finnas sparade i filer.	ISO, GAO
	Kontrollera alla åtkomstvägar	GAO,
	All åtkomst loggas	GAO,
	Noggrann övervakning ska göras av dess användning.	ISO, GAO
	Operativsystemet ska vara konfigurerat så att det inte går att ta sig förbi säkerhets mjukvaran	GAO,

Eftersom dessa mjukvaror är extra kraftfulla vad gäller möjligheten att påverka en dator bör de också utsättas för noggrann övervakning. Både ISO och GAO trycker på vikten av att endast viss personal ska ha åtkomst till dessa mjukvaror samt att deras åtkomst ska vara godkänd av ansvarig personal. När mjukvaran väl används ska det ske övervakning och loggning av de aktiviteter som utförs med hjälp av dem. Enligt GAO bör åtkomstvägar till dessa mjukvaror kontrolleras så att det inte går att ta sig förbi de säkerhetsspärrar som finns.

6.1.9 Uppdatering av programvara

Många leverantörer av komponenter till datorer kommer med jämna mellanrum med uppdateringar av sina produkter. Eftersom mjukvaror är enormt komplexa dröjer det ofta till efter lanseringar innan vissa säkerhetsrelaterade fel upptäcks. De flesta leverantörer av mjukvaror är dock snabba med att informera när fel upptäcks, ofta via sina hemsidor eller någon leverantörs (se tabell 14). När en uppdatering kommer bör denna utvärderas, dess lämplighet avgöras och beslut tas ifall den ska installeras. Men det kan ofta bli ett visst glapp innan den uppdaterade versionen installeras hos användaren. För att minimera detta glapp bör följande beaktas (CERT, kapitel 2):

- att vara medveten om när säkerhetsrelaterade problem som berör systemet publiceras
- känna till åtgärder som kan vidtas för att minska risken att utsättas för eventuella attacker innan uppdatering hinner ske
- känna till bestående förändringar som leverantören gör

Många av de åtgärder som görs gällande uppdatering av programvara görs utanför den enskilda värddatorn. Detta inkluderar bland annat test och godkännande, och genomförs innan installering sker.

Motivering

När en uppdatering släpps blir den tillgänglig för samtliga aktörer på marknaden, däribland personer som är intresserade av att göra intrång i datorer. Genom att utnyttja säkerhetsluckor, som åtgärdats i den uppdaterade versionen men inte i den tidigare, kan obehöriga användare tas sig in i datorerna. Därför är det av största vikt att följa med i uppdateringar så att det inte lämnas några möjligheter till intrång via nyupptäckta fel i programvaran.

Tabell 14: Aspekten uppdatering av programvara med tillhörande delområden

Aspekter	Delområde	Stöds av
Uppdatering av programvara	Lista över aktuella sidor som tillkännager de senaste uppdateringarna.	CERT
	Integritets kontroll – det kan ha skett oönskade ändringar av filer och bibliotek i samband med uppdatering. Återverkningar.	CERT, ISO,
	Dokumentera driftsrutiner, säkerställa att erforderlig säkerhetsnivå kan upprätthållas även i samband med förändring av utrustning och systemet. Kräver systemgodkännande av ledningen.	ISO
	Att det finns backup av datorn innan uppdateringen sker.	CERT

Denna aspekt berörs inte i materialet från GAO utan tas enbart upp i viss utsträckning av ISO och CERT. Orsaken till detta har inte framkommit vid studien av deras material. I samband med att en uppdatering har skett anser båda källor att det måste ske en kontroll av integriteten på data som finns lagrad i datorn. Detta för att fastställa att den inte har påverkats vilket kan leda till oönskade ändringar av den. Som en del i arbetet med uppdateringar menar CERT att det ska föras listor över sidor på nätet som anger de senaste uppdateringarna. Dessa listor ska vara så aktuella så att inga uppdateringar förbises. I ISO-standarden anges det att det ska finnas rutiner som gör att säkerhetsnivån ska kunna upprätthållas även om det görs förändringar av utrustningen i systemet och i datorn.

6.1.10 Säkerhetskopiering

I arbetet med att finna lösningar på hur inbrott och intrång i systemet ska upptäckas, undersökas och kunna leda till eventuella åtgärder, är det viktigt att tänka på hur verksamheten ska kunna fortsätta utan att störas i en allt för stor utsträckning, om ett eventuellt intrång sker. Det som bör beaktas är hur systemet och integriteten på dess data ska kunna säkerställas. Brister i detta kan generera stora kostnader om det får till följd att datorer och systemet som helhet står still under en längre tid. Därför är det av största vikt att en dator som utsatts för intrång så snabbt som möjligt kan komma i drift igen. Det finns enligt Icove (1995), några olika aspekter på vad som behövs göras för att denna återstart ska gå så snabbt som möjligt. En av dessa är säkerhetskopiering av alla program och datafiler. De andra två är:

- att ha tillgång till andra datorer och annan utrustning så att verksamheten kan fortsätta.
- att känna till hur ett system undersöks för att upptäcka brott som har genomförts mot det.

Säkerhetskopiering innebär att det alltid finns en kopia av den senaste versionen av ett program eller en datafil. Denna kopia ska förvaras på en plats som är skild från resten av datorutrustningen i systemet. Om de förvaras på ett icke-tillfredställande sätt kan det inträffa att både originalet och kopian skadas vid en olycka (Icove, 1995). Det är av största vikt att de kopior som sparas alltid är de senaste ändrade för att undvika att systemet inte ska gå att återstarta i det tillstånd det hade innan det eventuella intrånget (Silberschatz, 2003).

Motivering

Vid ett eventuellt intrång kan data, på ett eller annat sätt skadas. Med hjälp av säkerhetskopior är det möjligt att återskapa systemet till det tillstånd som rådde innan det utsattes för en attack.

Tabell 15: Aspekten säkerhetskopiering med tillhörande delområden

Aspekter	**Delområde**	**Stöds av**
Säkerhetskopiering	Säkerhetskopierad information ska förvaras så den inte kan skadas.	ISO
	Tre generationers säkerhetskopior bör finnas för viktiga tillämpningar.	ISO
	Regelbunden testning av den säkerhetskopierade informationen ska göras för att säkerställa dess korrekthet.	ISO, CERT
	Återstart med säkerhetskopierad information bör göras med jämna mellanrum för att fastställa tillförlitlighet.	ISO, CERT
	Klarar säkerhetskopieringen de krav som anges i verksamhetens avbrottsplan.	ISO
	Alla säkerhetskopior ska förvaras krypterade.	CERT
	Kontrollera att det går att återskapa enskilda filer.	CERT, ISO

6.2 Resultat från empiriska undersökningen

Mot bakgrund av de svårigheter som förekommit i denna del av examensarbetet kommer detta resultat att utgöra en mindre del än vad tanken var ifrån början. Inledningsvis skulle det resultat som framkom i den litterära undersökningen jämföras med det som kom fram i den empiriska för att på så sätt avgöra vilka aspekter som bör revideras hos värddatorer inom vården. Skillnaden hos det resultat som presenteras i denna del av undersökningen mot vad som var tänkt från början, är den att det inte kunnat ske någon jämförelse med de aspekter som framkom i den litterära undersökningen. Orsaken till detta är delvis att arbetet med säkerhetsrevisioner inom vården inte har nått tillräckligt långt ännu. Denna del kommer därför att beröra hur långt detta arbete har kommit samt behovet av att genomföra säkerhetsrevisioner.

En av de personer som har bidragit med information i den empiriska undersökningen heter Thomas Pehrsson och jobbar inom Landstinget i Blekinge med risk- och sårbarhetsanalyser. Vid förfrågningar om hur de i dagsläget jobbar med att revidera säkerhetspolicyn och dess efterlevnad framkom det att de överhuvudtaget inte har gjort någon sådan granskning ur ett användarperspektiv. Det säkerhetsarbete som de idag bedriver handlar mycket om de risk- och sårbarhetsanalyser som nämndes ovan. Utifrån resultatet av dessa analyser har de kunnat skapa sig en bra bild av hur säkerhetsarbetet fungerar i praktiken. Det har även lett fram till att konkreta handlingsplaner, som exempelvis införande av användarrutiner för vissa olika delar av systemet, har införts. Vissa områden har ännu inte blivit föremål för fastställande av användarrutiner, detta handlar bland annat om Internet-användningen.

De personer som i första hand har försökts kontaktas i samband med den empiriska undersökningen har jobbat inom Västra Götalandsregionen. Denna region bildades relativt nyligen genom sammanslagning av flera landsting samt sjukvården i Göteborg stad. Enligt Fredrik Rasmusson som jobbar inom regionen, på en enhet som kallas IT-centrum, resulterade denna sammanslagning i vissa problem rörande säkerhetsarbetet. Tidigare hade varje landsting och sjukhus ansvarat för sin egen säkerhet med egna rutiner och krav. I samband med sammanslagningen hann dessa regler inte göras enhetliga utan de regler som finns inom den nya regionen varierar från sjukhus till sjukhus. För att råda bot på detta pågår det i dagsläget två parallella projekt som syftar till att skapa enhetliga rutiner för säkerhetsarbetet. Som ett resultat av dessa projekt

har en ny enhet inom regionen skapats, som heter Säkerhetsstrategiska enheten, vars mål är att driva detta arbete framåt. I arbetet med att skapa enhetliga regler så har regionen fastslagit att den arbetsmodell som ska användas är ISO standarden *ISO 17799*. Fredrik Rasmusson sa också att när det gäller just säkerhetsrevisioner så bedrivs det inte något sådant arbete från centralt håll. Som övrigt säkerhetsarbete så har detta område, innan sammanslagningen till Västra Götalandregionen, varit ålagt varje lokal enhet att bedriva. I framtiden är tanken att detta ska styras centralt. På grund av att sammanslagningen skedde relativt nyligen har denna centralisering inte hunnits med ännu.

Efter att ha fått viss insikt i hur arbetet med säkerhetsrevisioner ser ut inom regionen som helhet kontaktades flera sjukhus, bl.a. kärnsjukhuset i Skövde, sjukhuset i Lidköping och Sahlgrenska i Göteborg. Det enda av dem som inte gav ett avböjande svar var Sahlgrenska. Efter diverse förfrågningar och kontakter blev det Barbro Laurin som delade med sig information om arbetet med säkerhetsrevisioner. Barbro jobbar som IT-säkerhetschef på Sahlgrenska, vilket gör att hon har god inblick i det arbete som bedrivs. På frågan om de genomför revisioner av säkerheten i sina datorsystem, angav hon att de inte utför något sådant idag. Däremot påpekade hon vikten av arbetet med säkerhetsrevisioner och uppföljning av verksamhetens säkerhetspolicy samt att det finns ett stort behov av detta, dels på Sahlgrenska men även inom regionen som helhet. Ännu har inte deras säkerhetsarbete nått dit, vilket antagligen kan ses som ett resultat av den genomförda sammanslagningen, men de revisorer som ska arbeta med säkerhetsrevisioner har precis tangerat området. Inom en snar framtid kommer de således att påbörja detta arbete.

7 Analys

I samband med presentationen av resultatet från den teoretiska undersökningen i stycke 6.1, finns det en mindre analys av respektive aspekt som lades fram. Vid sidan om det som skrevs där sker här en fortsättning på analysen men som i större utsträckning utgår ifrån den empiriska undersökning som gjorts. Denna undersökning är till sin utsträckning begränsad såtillvida att antalet personer som har samtalats med inte är särskilt stort samt att det i huvudsak enbart berör Västra Götalandsregionen. Detta kan naturligtvis ses som en nackdel då underlaget för det resultat som framkommer inte baseras på så många källor och dels inte berör sjukvården som helhet utan ett begränsat område. Å andra sidan kan den begränsade geografiska spridningen ses som en fördel då en större sådan hade kunnat resultera i avvikelser på grund av variationer mellan olika regioner. Det kan således vara bättre att ha fokus på ett mindre område för att skapa en rättvisare bild av det säkerhetsarbetet som bedrivs. De personer som har deltagit är, som tidigare nämndes, till sitt antal inte många men de sitter på positioner som gör att de har god inblick och kan därmed betraktas som tillförlitliga i sin bedömning av läget.

Fredrik Rasmusson förklarar att regionen har som mål att jobba med ISO 17799 som arbetsmodell. Denna standard är också en av de källor som utgör grunden för detta examensarbetes teoretiska undersökning. Som en följd av denna överensstämmelse blir det resultat som framkommit mer relevant för vårdsektorn än om denna standard inte hade ingått i undersökningen.

Enligt Barbro Laurin, som jobbar som IT-säkerhets chef på Sahlgrenska, är vikten av säkerhetsrevisioner stor. Detta visar på relevansen av att göra en jämförelse mellan olika källor gällande aspekter som ska revideras. Enligt den litteraturstudie som gjorts i detta examensarbete så är det ingen av de tre källorna, ISO, GAO och CERT, som klarar av att täcka alla de aspekter som borde vara föremål för en säkerhetsrevision. Det kan därför ses som nödvändigt med en jämförelse för att kunna avgör vilken av dem som bäst täcker de behov som finns inom just vården.

Orsaken till att det i dagsläget inte genomförs regelbundna säkerhetsrevisioner har inte helt framkommit i undersökningen. Till viss del kan förklaringen ligga i det faktum att de tidigare enskilda enheterna nu ska samarbeta centralt istället för separat vilket skedde tidigare. Detta kan ha resulterat i att vissa delar av säkerhetsarbetet har fått stå tillbaka till förmån för andra. Denna brist på revisioner kan ses som en

indikering på att vården inte har full koll på hur väl deras säkerhetsarbete fungerar. Rist (2000) säger att det enda sättet att få ett grepp om ett nätverks säkerhet är att genomföra säkerhetsrevisioner. Även Barbro Laurins uttalande om vikten av att genomföra säkerhetsrevisioner ger ytterligare indikering på att detta är något som snarast borde genomföras inom vårdsektorn. För så länge som de själva inte är fullt medvetna om hur väl de efterlever de säkerhetskrav som satts upp kan de heller inte skydda sig fullt ut mot eventuella intrång i systemet.

I resultatet från den teoretiska undersökningen presenteras en rad olika aspekter och delområden som ska undersökas i samband med en säkerhetsrevision. Varje delområdes medverkan i resultatet stöds av en eller flera av de tre huvudkällor som har används. Detta resultat har framkommit genom en subjektiv bedömning av det som presenteras i respektive källa och visar på att det finns avvikelser mellan de olika modeller och standarder som presenteras i dem. Orsakerna till detta torde vara flera men delvis beror det på att de har olika upphovsmän och därmed olika fokus. Det är dock noterbart att vissa delområden överhuvudtaget inte behandlas av vissa källor medan andra lägger relativt stor vikt på dem. Detta ger en antydan om vikten för en organisation att kontrollera flera modeller och standarder innan de slår fast hur en säkerhetsrevision ska genomföras. Om detta inte görs kan det få till följd att viktiga detaljer missas som senare kan utgöra brister i systemet där intrång kan ske. Det bör även anges att kompletterande litteratur som är mer produkt- och teknikspecifik kan användas för att skapa en bättre förståelse för vad som ska undersökas vid en säkerhetsrevision.

8 Slutsats

I detta kapitel redovisas de slutsatser som kan dras utifrån den teoretiska och empiriska undersökning som har genomförts i detta examensarbete. Det är problempreciseringen, som beskrivs i avsnitt 3.3, som ligger till grund för de slutsatser som dras gällande enskilda standarder och metoders tillräcklighet, möjligheten att anpassa resultatet mot vårdsektorn och behovet av att införa säkerhetsrevision som en del i deras säkerhetsarbete.

De litterära källor som i huvudsak har används i den teoretiska undersökningen består av utgivningar från tre tillförlitliga institutioner. Dessa är den internationella standardiseringsorganisationen ISO, det erkända rapporteringscentrat för säkerhet CERT och den amerikanska regeringens revisionsorgan GAO. Var och en av dem har givit ut en standard eller modell för hur informationssäkerhet ska uppnås i datorsystem. Det är med dessa som utgångspunkt detta arbetes resultat har formats. Enligt problempreciseringen är syftet med undersökningarna, att ta fram de aspekter som ska undersökas då en säkerhetsrevision görs av värddatorerna i ett informationssystem inom vårdsektorn. Då dessa källor har studerats närmare och de aspekter som framkommer från dem har sammanställts, har det visat sig att det i vissa fall finns betydande avvikelser mellan dem. Detta handlar om att vissa aspekter som tas upp av två av källorna men inte ens berörs av den tredje, trots att vissa av dem är tillsynes viktiga aspekter vid säkerhetsrevisioner. Som exempel kan hanteringen av tillåtna nätverkstjänster anges. Den variation som uppvisas mellan de olika modellerna och standarderna tyder på att det inte entydigt behöver vara så att en av dem enskilt klarar av att täcka upp alla de aspekter som bör granskas vid en säkerhetsrevision. En slutsats som framkommit är att de genom att komplettera varandra kan bidra till att bättre täcka in helheten av ett system. Detta är något som antyddes redan i avsnitt 3.3 där det argumenterades för att om fokus ligger på helheten snarare än vissa delar av systemet kan det inträffa att detaljer förbises.

Som tidigare nämndes i slutsatsen ska det enligt problempreciseringen vara en vinkling av resultatet mot vårdsektor. Detta skulle uppnås genom en granskning av hur säkerhetsrevisioner idag genomförs hos dem. Som en följd av tidigare resonemang, angående bristen på denna typ av revisioner, har denna granskning inte fullt ut kunnat genomföras. Genom detta konstaterande går det att ana en brist och ett behov inom vårdens säkerhetsarbete med avseende på just säkerhetsrevisioner. Detta

är något som också har uppmärksammats av bl.a. Barbro Laurin på Sahlgrenska, då hon uttryckligen angav detta som viktigt och att det fanns ett stort behov av det samt att revisorerna just har tangerat området. Slutsatsen blir den att säkerhetsrevisioner är något som snarast borde börja genomföras inom vården för att kontrollen över systemen ska kunna upprätthållas och att eventuella intrång ska upptäckas samt kunna förebyggas. Den samordning av säkerheten och då inte minst säkerhetsrevisioner, som är tänkt att ske inom Västra Götalandsregionen, var något som togs upp redan 1996 av Petersson & Rydmark(se avsnitt 2.2).

9 Diskussion

I detta kapitel kommer det resultat som framkommit i examensarbetet att diskuteras. Diskussionen kommer att föras i tre steg; *värdering av resultatet, resultatets relevans* och *metodkritik*. Denna diskussion kommer bland annat att föras med utgångspunkt i arbetets problemprecisering. Vidare kommer det även att framföras förslag på *fortsatt arbete*.

9.1 Värdering av resultatet

Eftersom arbetet till stor del bygger på litteraturundersökning kan resultatets tillförlitlighet till viss del härledas till vilka källor som har används. Dess tillförlitlighet påverkas också av hur dessa källor har används och vilka metoder som har tillämpats för att nå fram till resultatet.

Vad gäller de källor som används och deras trovärdighet så torde den vara hög. Till att börja med så används en internationellt erkänd standard från ISO, en manual från den amerikanska regeringens revisionsorgan samt en modell från ett stort rapporteringscentra för säkerhet. Vad avser användningen av källorna så finns det ett par aspekter som kan inverka på värderingen av resultatet. I exempelvis ISO 17799 så uttrycks det inte klart vad som ska revideras vid en säkerhetsrevision. Det som har fått göras är en värdering av de regler och krav som föreslås i ISO 17799. Dessa regler och krav ska följas för att en organisation ska kunna certifieras enligt ISO 17799, därmed bör det också vara de som ska undersökas vid en säkerhetsrevision. Dessa krav har alltså fått utgöra underlag till resultatet och pekar således på de aspekter som ska beaktas vid en revision. Vidare har ingen av de källor som använts den avgränsning i sitt material som har beskrivits i detta arbetes problemavgränsning. Därför har det behövts en subjektiv bedömning för att kunna avgöra vilka aspekter hos källorna som är relevanta för resultatet och inte. På grund av detta går det att föra diskussioner där argument läggs fram för att vissa delar av resultatet inte anses lämpligt och borde tas bort eller att vissa borde läggas till. En rättvis och korrekt bedömning har dock försökt göras av de delar som ska ingå i resultatet. Vad avser Kapps och Brooks modeller som presenteras i avsnitt 2.4, så utgör de inte en del av resultatet i den bemärkningen att de bidrar till utformningen av de aspekter som presenteras i resultatet. Orsaken till detta är att de snarare ger en beskrivning av hur genomförandet och arbetsprocessen vid en säkerhetsrevision ser ut, än en beskrivning av vad det är som ska revideras, dvs. vilka aspekter. Detta är något som i större

utsträckning behandlas av GAO, ISO och CERT som istället lägger mindre vikt vid genomförandeprocessen.

Delvis på grund av examensarbetets tidsbegränsning har de metoder som används inte varit fullt tillräckliga. Detta handlar i första hand om den bristande jämförelsen med hur revisioner idag utförs inom vården samt en praktisk tillämpning av resultatet. Detta har fått till följd att resultatet inte har kunnat verifieras mot vårdsektorn och därmed heller inte fått den vinkling som var tänkt i från början.

Tillvägagångssättet att genomföra litteraturstudien utifrån tre olika källor, se avsnitt 5.3, har på flera sätt bidragit till att öka resultatets trovärdighet. Dels kompletterar de varandra väl, vilket behövs då ingen av dem enskilt täcker samtliga aspekter vid en säkerhetsrevision och dels så ger var och en av källorna sin vinkling på hur problemet ska angripas, detta som ett resultat av de olika utgivarnas karaktär. När dessa tre tillsammans bidrar till resultatet så finns möjligheten att det bästa från var och en av dem kan användas. Om så är fallet är för tidigt att avgöra i detta examensarbete.

9.2 Resultatets relevans

Som uttrycks i förväntat resultat i avsnitt 3.4, så är målsättningen att kunna presentera vilka aspekter som ska beaktas vid en revision med avseende på den avgränsning som gjorts. Lever då det resultat som presenteras här upp till denna målsättning så att det kan användas i de sammanhang det är avsett för? Denna fråga är svår att besvara innan resultatet har används i praktiken eller i en större utsträckning jämförts med hur revisioner idag genomförs inom vården. Den sammanslagning av flera olika källor som har gjorts i arbetet kan vara en faktor som påverkar dess användbarhet då resultatet har en bred täckning. Orsaken till att detta gjordes är som tidigare nämndes den att ingen av de modeller och standarder som har använts enskilt täcker upp alla de aspekter som kan tänkas ingå i en säkerhetsrevision. Anledningen till detta är bl.a. att de har fokusering på olika områden av ett nätverk, den nivå de är skrivna på tillåter inte att de går in på detaljer eller att de är tänkta att fungera som vägledning snarare än mallar som helt ska följas. Genom att då jämföra det material som presenteras i dem går det dels att få en bild av de olika källornas inriktning, men också information om eventuellt viktiga aspekter som kan saknas i någon av de andra källorna. Nackdelarna med att göra denna typ av jämförelse är att det är svårt att avgöra huruvida en viss aspekt ska inkluderas eller inte, vilket resulterar i att det får avgöras utifrån en subjektiv bedömning.

Som nämndes i resultatet från den empiriska undersökningen så genomförs det i dags läget inte några direkta säkerhetsrevisioner inom vårdsektorn. I avsnitt 2.2 uttrycker Hayem (1996) att säkerhetsrevisioner ska genomföras för att skapa säkra system och för att analysera systemet gentemot fastställda säkerhetsregler. Den brist på säkerhetsrevisioner som visat sig förekomma inom vårdsektorn, är således något som snarast borde åtgärdas. Detta håller på att förbereds inom Västra Götalandsregionen och de har som mål att jobba med ISO 17799 som arbetsmodell. Eftersom resultatet från litteraturstudien visade att ingen av källorna, däribland ISO 17799, täcker samtliga aspekter kan det vara av intresse får vårdsektorn att se att det finns alternativa modeller. Detta examensarbete gör inte på något sätt anspråk på att fullt ut förklara vad som ska ingå in en säkerhetsrevision, utan det kan snarare fungera som en tänkeställare om att ingen standard eller modell är fullständig. För att fullt ut kunna fastställa vilka aspekter som bör ingå i en säkerhetsrevision behövs det en betydligt större undersökning och hjälp från experter inom de olika områdena av ett nätverk.

Samtidigt som det har diskuterats att det kan vara en fördel för resultatets tillförlitlighet att tre olika källor har används kan det också utgöra en nackdel vid användningen av det. Orsaken till detta är att en verksamhet hellre använder sig av en standard eller modell istället för av tre. Vid exempelvis en certifiering enligt ISO 17799 så följs enbart denna standard. Det används då inga kompletterande modeller till den som verksamheten bestämt sig för att certifieras enligt. Det resultat som presenteras i detta arbete har däremot använt sig av tre olika modeller och standarder och kan således ses som svårare att applicera på en verksamhet.

9.3 Metodkritik

I problempreciseringen uttrycks det att de undersökningar som ska göras kommer att bestå av litteraturstudier och intervjuer. Den förstnämnda av dessa har genomförts enligt planerna och resultatet från den finns att läsa i avsnitt 6.1. Den största delen av litteraturstudien utfördes på tre litterära källor, vilka är ISO, GAO och CERT. Genom att använda dessa har det skapats en bredd i resultatet som hade varit svår att uppnå om enbart en modell eller standard hade används. Det resultat som framkom av denna del av examensarbetet utgör, vilket framgår av problempreciseringen, det första målet med undersökningarna, dvs. vad som bör ingå i en säkerhetsrevision utan hänsyn till avgränsning mot vårdsektorn. Den empiriska delen, som utgörs av intervjuer, har däremot inte fortskridigt enligt planerna. Från ett tidigt skede i examensarbetet har en

mängd personer kontaktats med en förfrågan om de är villiga att svara på frågor rörande systemförvaltning och säkerhetsrevisioner. Överlag så har det varit tidskrävande att få svar och i flertalet fall har de förfrågade gett ett avböjande svar. Detta har bland annat berott på tidsbrist och sjukskrivningar eller att de överhuvudtaget inte har jobbat med denna typ av revisioner. I slutändan så handlar det inte om mer än ett fåtal personer som har kunnat bidra till den empiriska undersökningen. Detta faktum har resulterat i att det i efterhand går att betrakta metod valet som delvis misslyckat, men å andra sidan var detta inte möjligt att förutsäga innan genomförandet.

Med utgångspunkt i problempreciseringen så framstår ändå dessa två metoder, litteraturstudie och intervjuer, som de bäst lämpade för att uppnå examensarbetets förväntade resultat. Möjligtvis hade någon typ av praktisk tillämpning av resultatet varit önskvärd men detta har inte varit möjligt med tanke på tidsramen för arbetet.

9.4 Förslag på fortsatt arbete

Utgångspunkten för detta examensarbete var att skapa ett resultat som i stor utsträckning var fokuserat på vårdsektorn. Detta kunde inte till fullo uppfyllas på grund av omständigheter som beskrivits ovan. Trots de svårigheter som har förekommit och trots att det vid upprepade tillfällen gjorts gällande att säkerhetsrevisioner inte utförs finns det med största sannolikhet mycket nyttig information att hämta hos dem som jobbar med systemförvaltning inom vården. Att ta del av denna information och utifrån den skapa en mindre generell bild av säkerhetsrevision än vad detta arbete har gjort är av stort intresse inte minst för vårdsektor.

Ett informationssystem består av en mängd olika delar, en kort beskrivning av detta ges i avsnitt 3.2 , och detta arbetes fokus ligger på värddatorerna. Att undersöka vilka aspekter som ska ingå vid en säkerhetsrevision av andra delar av systemet är av största intresse, detta eftersom en revision normalt sett inte utförs på enbart en del av systemet.

Det resultat och de aspekter som presenteras i denna rapport grundar sig på det som framkommit i de modeller och den standard som används. Men för att få en djupare förståelse för många av de aspekter som ska undersökas vid en säkerhetsrevision, krävs det god teknisk kännedom och det är svårt som lekman att avgöra om det som presenteras i resultatet i tillräckligt stor utsträckning täcker det aktuella området. För

att kunna avgöra detta skulle det vara önskvärt om experter inom olika områden av ett informationssystem kunde ge sin bedömning av de aspekter som detta examensarbete lägger fram.

Under arbetets gång har det visat sig att det i dagsläget inte utförs säkerhetsrevisioner i någon större utsträckning inom vården. Detta har varit ganska så förvånande då det utgör en enormt viktig del i säkerhetsarbetet med ett informationssystem. Det skulle vara intressant att göra en noggrannare undersökning om denna tendens återkommer inom flera regioner och landsting. Om så är fallet, granska framtida planer för hur deras fortsatta säkerhetsarbete ser ut samt vad det skulle kunna få för konsekvenser om de inte börjar genomföra säkerhetsrevisioner.

I ett tidigt skede av examensarbetet var det tänkt att de skulle göras en undersökning av och en jämförelse mellan olika mjukvaruverktyg som används i samband med säkerhetsrevisioner. Detta har på grund av arbetets omfattning inte hunnits med. Genom att göra en jämförelse mellan vilka aspekter olika program beaktar skulle en sammanställning av dessa kunna göras för att finna de aspekter som tillsammans ger den bästa täckningen av ett informationssystem. Dessa skulle sedan kunna användas som underlag vid beslut om hur en säkerhetsrevision ska genomföras. En enkel beskrivning av detta förkommer i stycket som beskriver möjliga metoder (se avsnitt 4.1).

Referenser

Allen, H. J. (2001) *The CERT Guide to System and Network Security Practices*, SEI series in software engineering, Addison-Wesley, USA.

Andersen, S. E. (1994) *Systemutveckling – principer, metoder och tekniker*. Studentlitteratur, Lund.

Bandyo-padhyay, N. (2000) *Computing for non-specialists*. Pearson Education Limited, Harlow, England.

Bell, J. (1995) *Introduktion till forskningsmetodik*. Studentlitteratur, Lund.

Björner, O. (1999) *Begrepp för IT-säkerhet*. Rapport nr 2 från SITHS-projektet.

Brandt, P. (1998) *Systemförvaltningshandoken*, ITligence HB, Stockholm.

Brooks, T. & Scambray, J. (1998) Computer Networks - Security Measures. *InfoWorld, 11*.

Caelli, W., Longley, D. & Shain, M. (1991) *Information Security Handbook*, MacMillan Publishers Ltd., Hants, England.

Chapman, B. D. & Zwicky, D. E. (1995) *Building Internet Firewalls*. O'Reilly & Associates, Inc., USA.

Dawson, C., W. (2000) *The essence of computing projects: A student´s guide*. Prentice Hall, Pearson Education Limited, Harlow, England.

De Dombal, F. T. (1996) *Medical informatics: the essentials*. Reed Education and Professional Publishing Ltd, Cornwall, England.

Eriksson, L., T. & Wiedersheim-Paul, F. (2001) *Att utreda, forska och rapportera*. sjunde upplagan, Liber Ekonomi, Malmö.

Garfinkel, S. & Spafford, G. (1996) *Practical Unix & Internet Security*, O´Reilly & Assiciates, Inc., Sebastopol, USA.

Hayam, A. (1996) Security Audit – a suggested model for effective audit strategies in healthcare informatics. *International Journal of Biomedical Computing, 35*.

Hutt, E. A., Bosworth, S. & Hoyt, B. D. (1997) *Computer Security Handbook*. John Wiley & Sons, Somerset.

Icove, D., Seger, K. & VonStorch, W. (1995) *Computer Crime – a crimefighter´s handbook*, O´Reilly & Associates, Inc., Sebastopol, USA.

Kapp, J. (2000) How to conduct a security audit, *PC Network Advisor, 120*, 3-4.

Lagerlund, B.(1998) *Informationssäkerhet i vårdprocessen*. Rapport nr 1 från SITHS-projektet.

Nordström, M. & Welander, T. (2002) *Affärsmässig förvaltningsstyrning*. Studentlitteratur, Lund.

Olsson, H., & Sörensen, S. (2001) *Forskningsprocessen: Kvalitativa och kvantitativa perspektiv*. Liber AB, Stockholm.

Patel, R. och Davidsson, B. (1994) *Forskningsmetodikens grunder*. Studentlitteratur. Lund.

Paulsson, U. (1999) *Uppsatser och rapporter – med eller utan uppdragsgivare*. Studentlitteratur, Lund.

Peterson, G. & Rydmark, M. (1996) *Medicinsk informatik*. Almquist & Wiksell Medicin, Liber Utbildning, Stockholm.

Rist, O. (2000) A case for a network security audit, *InternetWeek, 837*.

Schneider, B. (2000) *Secrets and lies – digital security in a networked world*. John Wiley Sons Inc., New York, USA.

SFS 1980:100. *Sekretesslagen*, Justitiedepartementet L6 1980, Omtryck SFS 1992:1474.

SFS 1985:562. *Patientjournallagen*. Rixlex, Sveriges Riksdag.

Silberschatz, A., Galvin, P. B. & Gagne, G. (2003) *Operating System Concepts*, Sixth Edition, John Wiley & Sons, Inc., New York, USA.

Stinson, C., Blaszczak, M., McKinney, B. & Woodcock, J. (1994) *Windows NT*, Microsoft Press, Redmond, USA

Svensk Standard SS 01 16 01, utgåva 4 (1989), *Informationsteknik - Ordlista*, Standardiseringskommissionen i Sverige, Stockholm.

Svensson, T. (1999) *Företagens skydd och säkerhet*. Industrilitteratur AB, Stockholm.

SSR97ETT. (1997) *Riktlinjer för god informationssäkerhet*. SIG Security Studentlitteratur, Lund.

TK99 AG6 (2002) *Handbok i informationssäkerhetsarbete – baserad på standarden SS ISO/IEC 17799 och SS 66 77 99-2*, Docusys, Stockholm.

Vaas, L. (2000) Security Checkup, *eWeek, 17*, 49.

Ward, J. & Nellis, G. J. (1995) *Principles of information system management*. Routledge, London, UK.