Risk Management - Kvalitativ Utvärdering av Verktyg och Metoder för Riskanalys

(HS-IDA-EA-99-306)

Magnus Ekman (a96magek@ida.his.se)

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

Examensarbete på det systemvetenskapliga programmet under vårterminen 1999.

Handledare: Anders Eklund

Risk Management - Kvalitativ Utvärdering av Verktyg och Metoder för Riskanalys

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

1999-06-11

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: _____

Risk Management - Kvalitativ Utvärdering av Verktyg och Metoder för Riskanalys

Magnus Ekman (a96magek@ida.his.se)

Sammanfattning

Denna rapport ingår tillsammans med en muntlig presentation som examination i kursen *Examensarbete i ADB, 20p* vid Högskolan i Skövde. Kursen ingår som slutmoment på det systemvetenskapliga programmet.

Undersökningen, vilken genomfördes i samarbete med företaget Arthur Andersen, hade som syfte att utvärdera verktyg och metoder för riskanalys av verksamheters informationssäkerhet.

Medelst intervjuer av 5 experter inom området, samt med en dokumentstudie, utvärderades problemställningen kvalitativt. Resultatet blev en analys av existerande verktyg och metoder för riskanalys, med avseende på deras olika fördelar och nackdelar, samt deras resultat.

Nyckelord: Informationssäkerhet, Risk Management, Riskanalys

Innehållsförteckning

1 Inledning

För 10 år sedan sparades, enligt Olovsson (1998), alla organisationers viktiga dokument i pappersform. Idag blir det allt vanligare att verksamhetskritiska dokument lagras i datorsystem, som förväntas skydda mot obehörig tillgång. Samtidigt blir allt fler personer i sitt dagliga arbete beroende av att datorsystemen fungerar. Man behöver inte gå så långt som till börser eller banker för att hitta verksamheter där tillgången till datorsystemen är kritisk. Sjukvård, offentlig förvaltning, försäkringsbolag och andra helt vanliga företag har stora delar av sin verksamhet datoriserad. Prislistor, kundregister, lagerregister, m.m. finns ofta inte ens i pappersform längre.

När beroendet av informationstekniken ökar, blir säkerheten allt viktigare för i princip alla sorters verksamheter. Tidningen Computer Sweden (1998) presenterade 1998 en enkät genomförd bland svenska företag. 68 procent av de tillfrågade hade infört elektronisk affärskommunikation i någon form, eller kommer att införa det i framtiden. Av de tillfrågade uppgav 61 procent att de måste höja säkerhetskraven i organisationen. Vissa hävdade till och med att den bristande tilltron till säkerheten förmodligen skulle avhålla dem från satsningar på elektronisk affärskommunikation.

Dock bör man vara medveten om att statistik som rör informationssäkerhet sannolikt ofta är snedvriden. Det finns förmodligen ett stort mörkertal i många undersökningar, beroende på att företagen inte vill förlora sitt anseende:

> […] in the event of a crime, some companies will not investigate or prosecute, for fear that it will damage their public image (Pfleeger, 1989:2).

Statistik som jag funnit visar att brott mot informationssäkerheten är ett växande hot. Computer Security Institute (1998), CSI, som är en amerikansk intresseförening för informationssäkerhet, publicerade 1998 undersökningen: *1998 CSI/FBI Computer Crime and Security Survey.* Undersökningen, som gjordes i samverkan med FBI, hade som mål att höja säkerhetsmedvetandet och avgöra mängden av datorbrott i USA. I undersökningen, som gjordes med hjälp av enkäter, svarade 520 respondenter med säkerhetsrelaterat arbete. Nedan redovisas några av undersökningens resultat:

- 64% av respondenterna rapporterade att brott i deras IT-säkerhet hade skett inom de senaste 12 månaderna. Detta var en ökning på 16% i jämförelse med 1997 års undersökning, och en ökning med 22% i jämförelse med den första undersökningen 1996.
- 72% av respondenterna sade att de led finansiell skada av brotten, men bara 46% av respondenterna kunde kvantifiera förlusterna i dollar. Den totala finansiella förlusten hos de 241 organisationer som kunde kvantifiera dessa summerades till ett värde av $136.822.000.
- Säkerhetsbrotten som respondenterna hade upptäckt bestod av en mängd olika sorters allvarliga attacker. T.ex. rapporterade 44% av respondenterna att de anställda hade haft obehörig tillgång till information, 24% rapporterade att systemen attackerats utifrån, 18% rapporterade stöld av viktig information, 15% rapporterade att finansiella bedrägerier skett, och 14% rapporterade sabotage av data eller nätverk.
- De största finansiella skadorna uppstod genom obehörig tillgång från anställda, stöld av viktig information, bedrägerier inom telekommunikation, och finansiella bedrägerier.

- Antalet organisationer som rapporterade Internetkopplingen som en frekvent attackpunkt ökade från 47% under 1997 till 54% 1998. 1996 var samma procenttal 37%. Antalet rapporterade Internetattacker var 1998 uppe i samma antal som de rapporterade attackerna på de interna systemen.

Den bristfälliga informationssäkerheten kostar således enorma summor varje år. Att informationssäkerheten är bristfällig i svenska företag visar en undersökning som företaget Ernst & Young (1997) gjorde 1997. Syftet med undersökningen var att beskriva status och trender inom informationssäkerheten i de undersökta organisationerna, samt att ge en bild av hur svenskt näringsliv står sig säkerhetsmässigt i jämförelse till Europa och resten av världen. Undersökningen gjordes i form av en enkät, som skickades till cirka 3000 befattningshavare på svenska företag. Av de tillfrågade svarade 541 på enkäten. Undersökningen visade att:

- Virus är ett stort problem: 46% av respondenterna angav att de lidit stor skada av virus, respektive 35% av makrovirus. Detta trots att 94% använde sig av aktivt virusskydd.
- Hoten finns inne i organisationerna. Det var inte obehöriga, utan behöriga användare och anställda som uppfattades som det största hotet mot informationssäkerheten.
- Incidentuppföljning är bristfällig. Endast 5 av 10 tillfrågade angav att incidenter beträffande informationssäkerheten rapporteras och följs upp.
- Vart fjärde företag i undersökningen saknade en formell data- eller säkerhetspolicy.

Ovanstående undersökningar visar att bristfällig informationssäkerhet är ett stort problem. Hur skall då säkerheten höjas? Det finns givetvis många svar på den frågan. Grunden för att kunna öka graden av informationssäkerhet i en verksamhet bygger, anser jag, på att man vet vilka hot och sårbarheter som finns i informationssystemen. Genom att identifiera dessa underlättas arbetet med att finna lämpliga skyddsåtgärder. Detta arbete kallas för riskanalys och är en del av en organisations riskhantering, även kallad *Risk Management*. Syftet med denna rapport är att utvärdera olika verktyg och metoder som kan användas för att utföra en riskanalys av en verksamhets informationssäkerhet.

2 Bakgrund

I detta kapitel kommer jag att beskriva den bakgrundsinformation som är nödvändig att känna till för att förstå min problemställning. Jag börjar med att påvisa att vårt samhälle blir allt mer sårbart i och med att beroendet av informationstekniken ökar. Denna sårbarhet skapar ett behov av en standard för informationssäkerhet, vilket påvisas i kapitel 2.2. Därefter beskrivs, i kapitel 2.3, mer ingående vad informationssäkerhet innebär. Till sist, i kapitel 2.4, förklarar jag vad en riskanalys är.

2.1 Informationssamhället är sårbart

Börjesson (1998) anser att mycket pekar på att det idag pågår en samhällsförändring. Den industrialiserade delen av världen går från ett industrisamhälle till ett informationssamhälle. Caelli et al (1994) hävdar att samhällen och organisationer blir mer och mer beroende av informations- och kommunikationssystem, med ständigt ökande komplexitet och sårbarhet. Det är denna sårbarhet jag vill belysa i detta kapitel.

Statskontoret (1998a) fick 1997 i uppdrag av regeringen att utarbeta en strategi för samhällets IT-säkerhet. I den färdiga rapporten *Sammanhållen strategi för samhällets IT-säkerhet* identifierar utredningen olika hot mot informationssamhället. Nedan följer ett sammandrag av dessa hot. Om inget annat anges är källan till den resterande delen av detta kapitel: Statskontoret (1998a).

De allvarligare hoten som kan drabba informationssamhället är störningar i olika typer av samhällsviktiga funktioner eller kritiska infrastrukturer. Det gäller t.ex. avbrott i elförsörjningen, störningar i transporter (av komponenter, drivmedel, dagligvaror etc.), avbrott i infrastrukturen för data- och telekommunikation, störningar i betalningsväsendet och störningar i den offentliga förvaltningens tjänster.

Ett exempel på en incident som lett till stor påverkan på samhället är ett elavbrott i Auckland, Nya Zeeland. De centrala delarna av Auckland lades i mörker den 20 februari 1998. Elavbrottet berörde uppskattningsvis 50 000 arbetstagare och 6 000 boende i citykärnan. Det tog cirka 10 veckor innan problemen var lösta.

Ett annat exempel på en omständighet som kan leda till allvarliga störningar i samhället är om omställningen av informationssystemen till år 2000 inte sker fullt ut och i tid. Statskontoret har i en rapport till regeringen (*Skiftet till år 2000. Läget i myndigheter och samhällsfunktioner)* gjort bedömningen att svåra störningar inom flera vitala samhällsfunktioner inte kan uteslutas.

De öppna kommunikationsstandardernas snabba utveckling har vidare inneburit att gårdagens system med stordatorer i stor utsträckning ersatts av distribuerade system för persondatorer i nätverk. Detta har medfört en högre grad av informationsutbyte inom och framför allt mellan organisationer. Nya tjänster växer fram genom Internet. Sammankopplingen av kommunikationen mellan system ökar exponeringen av den information som hanteras. Detta för med sig att hoten mot och säkerhetsbristerna i systemen ändrar karaktär.

De vanligaste störningarna beror på brister i programvaror. Bara under första kvartalet 1998 publicerades det från US Department of Energy fler än 50 rapporter om allvarliga fel i olika typer av programvaror m.m. Programvarufelen kan, om de utnyttjas, leda till att angripare får tillgång till lösenord, webbsidor och kan störa eller

helt avbryta webbtjänster, och på så vis sprida felaktig eller i värsta fall medvetet manipulerad information.

Angrepp via Internet sker i en betydligt större omfattning än vad man kan vänta sig. Ett exempel på en attack som riktats mot företag och organisationer via Internet i USA inträffade i slutet av 1996. Då förändrades CIA:s webbsida av vad som visade sig vara svenska hackers som ville protestera mot en svensk åklagares förundersökning riktad mot hackers i Sverige.

Samhällets grundläggande infrastrukturer hotas också av informationskrigföring. Informationskrigföring handlar om åtgärder för att komma åt, påverka eller utnyttja andra aktörers information och informationssystem, samtidigt som man skyddar sin egen information och sina egna informationssystem. Informationskrigföring är ett av de allvarligaste hoten som i dagsläget finns mot samhällets informationsförsörjning. Cohen (1995) tar upp ett exempel där informationskrigsföring använts, nämligen Gulfkriget. I detta krig riktade USA i första hand sina attacker mot kommunikations-anläggningar, som användes för styrning av Iraks trupper.

Företag och myndigheter verksamma i Sverige är i allt högre utsträckning beroende av leverantörer och aktörer i andra länder. Traditionell infrastruktur som transport och distribution är i hög grad beroende av funktionen i infrastrukturerna för tele- och data-kommunikation. Dessa blir i sin tur alltmer sammanflätade. Mängden leverantörer av transmission, samt operatörer av tjänster för tele- och datakommunikation, ökar också komplexiteten. Detta är faktorer som medverkar till att tillvägagångssättet vid förmedlingen av en viss information blir svåröverskådligt.

Sammanfattningsvis kan det konstateras att samhället är betydligt mer sårbart på vissa punkter än tidigare, samtidigt som möjligheten till kontroll försvårats. Statskontoret (1998a) anser att risken för störningar i informationssystemen ökar om inte säkerhets-arbetet håller jämn takt.

2.2 Behov av standard

En metod för att granska säkerheten i en produkt, ett system eller i en organisations användning av IT-system är, enligt Statskontoret (1998b), certifiering. Certifiering innebär att ett antal kriterier anges som beskriver den önskvärda säkerhetsnivån. Granskning görs sedan av om system och organisation uppfyller kriterierna. Upptäckta brister vid granskningen måste åtgärdas innan certifikatet kan utfärdas. Certifieringen kan således ses som en kvalitetsstämpel på en produkt, ett system eller en organisation.

Enligt Statskontoret (1998b) ger certifiering av informationssäkerheten i en orga-nisation en bra grund för att lägga fast en gemensam grundsäkerhetsnivå. En standard för detta ändamål har ett stort egenvärde även om den inte är perfekt. Det viktiga är att standarden är tillräckligt bra, att många använder den, samt att arbete pågår att successivt förbättra den och anpassa den till förändrade behov.

Alla samhällsviktiga funktioner skall, enligt Statskontoret (1998a), på sikt vara certifierade med avseende på säkerhet, kvalitet och tillgänglighet. En sådan certifiering skall innebära att kontrollerad säkerhet finns och kan upprätthållas även i krissituationer. Vilka krav som skall ställas i samband med certifiering skall preciseras. Det kan t.ex. handla om att tillämpa en standardmodell med grundkrav och olika tilläggskrav beroende på systemtyp och risker.

Även för företag är behovet av en standard för informationssäkerhet stor. Säkerhet är, menar jag, ett kvalitetsattribut och någon form av certifiering kommer förmodligen att krävas från aktieägare och andra intressenter i framtiden. Olovsson (1998) anser att säkerhet snart kommer att bli ett viktigt konkurrensmedel.

2.2.1 BS 7799

1995 publicerades *Code of Practice for Information Security Management; BS 7799* av British Standards Institution som brittisk standard för informationssäkerhet. BS 7799 innehåller ett stort antal säkerhetskontroller. Boken är uppbyggd som en strukturerad lista med råd till företag och organisationer om hur de bäst skall hantera sin informationssäkerhet. Totalt beskrivs drygt 100 råd inom 10 huvudgrupper. 10 av säkerhetskontrollerna karakteriseras som ”nyckel”-kontroller. Dessa kontroller bör, enligt standarden, i första hand införas i företaget som en basnivå för informationssäkerheten. De 10 nyckel-kontrollerna är enligt British Standards Institution (1995): *dokumenterad säkerhetspolicy, ansvarsfördelning, utbildning och övning, rapportering för säkerhetsincidenter, viruskontroll, plan för fortsatt affärsverksamhet vid allvarlig störning, kopieringsskydd av programvara, skydd av viktiga handlingar och register, dataskydd* och *efterlevnad av säkerhetspolicyn*.

Enligt Statskontoret (1998a) är Storbritannien, Nederländerna och Australien de länder som har kommit längst med implementeringen av BS 7799. Där har de första certifieringarna redan genomförts. Andra länder som visar stort intresse är bl.a. Norge, Estland och Israel. Standarden börjar således få allt större internationellt genomslag. I Sverige har Allmänna Standardiseringen (STG) från och med oktober 1997 ansvaret för den svenska utvecklingen av BS 7799. Statskontoret (1998a) tror att BS 7799 kommer att bli svensk standard under mitten av 1999.

Om BS 7799 blir en svensk standard som får stor spridning inom näringslivet, bör den enligt Statskontoret (1998a) införas som obligatoriskt regelverk inom de delar av den offentliga förvaltningen som är strategiska för samhällets informationsförsörjning.

BS 7799 är dock inte den enda standarden som rör informationssäkerhet. Exempel på andra standarder är COBIT, INFOSEC och ITSEC. Anledningen till att jag bara berör BS 7799 är att det verkar som om det är BS 7799 som kommer att få störst genomslag, både i Sverige och internationellt.

2.3 Informationssäkerhet

I detta kapitel börjar jag med att definiera vad informationssäkerhet är. Sedan beskriver jag en arbetsprocess som kan tillämpas för att uppnå god informationssäkerhet. Detta gör jag för att påvisa var riskanalysen kan utföras. Därefter definierar jag vad en tillgång är. Sedan går jag igenom ett antal hot och sårbarheter som kan hota tillgångarna. Till sist ger jag en översikt över vilka skyddsåtgärder som kan användas för att skydda tillgångar mot hot och sårbarheter.

2.3.1 Definition

Information är, enligt British Standards Institution (1995), en viktig tillgång, och som alla andra tillgångar som en organisation förfogar över, har informationen ett värde. Det är därför viktigt att skydda informationen på ett lämpligt sätt. Begreppet informationssäkerhet rör detta skydd av information.

Det finns ingen enhetlig eller allmänt vedertagen definition av informationssäkerhet. Dock används ofta den definition som *Information Technology Security Evaluation Criteria* (ITSEC) fastställt, menar Olovsson (1998). ITSEC är en europeisk standard som innehåller kriterier för evaluering av IT-säkerhet. Informationssäkerhet kan enligt ITSEC (1991) definieras med hjälp av tre distinkta krav:

Sekretess: att hålla information och resurser otillgängliga för obehöriga.

Integritet: förhindrande av otillåten modifiering av information och resurser.

Tillgänglighet: att hålla information och resurser tillgängliga för behöriga.

Denna definition används även i Informationstekniska standardiseringens (1994), (ITS), rapport *Terminologi för Informationssäkerhet – rapport ITS 6,* vars syfte är att skapa en enhetlig terminologi för området informationssäkerhet.

SIG Security, som är en intressegrupp för informationssäkerhetsfrågor inom Dataföreningen i Sverige, definierar informationssäkerhet såsom:

> Säkerhet vid hantering av information för önskad tillgänglighet, riktighet, sekretess och spårbarhet. Informationssäkerhet kan uppdelas i administrativ säkerhet och IT-säkerhet (SIG Security, 1997:xii).

Informationssäkerhet är således ett paraplybegrepp som innefattar ett antal underliggande begrepp. För att klargöra den något vida definitionen av informationssäkerhet, definierar SIG Security (1997) även de delbegrepp definitionen innehåller:

Tillgänglighet: Säkerställer att behöriga användare har tillgång till de resurser de är behöriga till i rätt tid och omfattning.

Riktighet: Säkerställer att data inte ändras eller modifieras.

Sekretess: Ska säkerställa att ingen obehörig person kommer åt den information som finns i informationssystemet.

Säkerhet: Det arbete som verkar mot våld, stöld, sabotage, ekonomisk och organiserad brottslighet. Dessutom inkluderas säkerhetsskydd i begreppet.

Administrativ säkerhet: Säkerhet som huvudsakligen uppnås med hjälp av administrativa regler och rutiner.

IT-säkerhet: Säkerhet i IT-system. IT-säkerhet kan delas upp i ADB-säkerhet och kommunikationssäkerhet.

ADB-säkerhet: Säkerhet för skydd av data och system mot obehörig åtkomst eller oavsiktlig förändring eller störning vid databehandling.

Kommunikationssäkerhet: Säkerhet i samband med överföring av information eller styrsignaler. Syftet med kommunikationssäkerhet är att förhindra att känslig information kommer obehöriga till del, att information förvanskas eller inte når mottagaren, men också att missledande information eller signaler introduceras i kommunikationen eller systemet.

SIG Securitys definition av informationssäkerhet bygger på ITS och ITSEC:s definition av informationssäkerhet, med begreppen *sekretess*, *integritet* och *tillgänglighet* som grundstenarna i definitionen. Så som jag tolkar det är begreppen *integritet* och *riktighet* synonymer i SIG Securitys och ITS definitioner. Tyvärr definierar SIG Security inte vad de menar med begreppet *spårbarhet*, som återfinns i

deras definition av informationssäkerhet. Det gör dock Informationstekniska standardiseringen (1994):

Spårbarhet: princip innebärande att verksamheten och tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer.

ADB-säkerhet och Kommunikationssäkerhet kan även delas in i fysisk- och logisk säkerhet, menar Olovsson (1998):

Fysisk säkerhet: Fysisk säkerhet handlar om att skydda systemet mot fysiska angrepp som t.ex. stöld och brand.

Logisk säkerhet: Logisk säkerhet innefattar alla mekanismer och all teknik som tas till hjälp för att lösa säkerheten i systemet.

Jag kommer att använda mig av SIG Securitys definition i denna rapport. Jag anser att den täcker begreppet informationssäkerhet väl och den är baserad på ITSEC:s definition som förmodligen är den mest vedertagna definitionen internationellt, samt på ITS definition. Dessutom gör den en distinktion mellan IT-säkerhet och administrativ säkerhet, vilket kommer visa sig vara värdefullt längre fram i rapporten. I figur 1 i bilaga 1 finns en sammanfattande illustration över begreppet informationssäkerhet och dess komponenter, så som jag kommer att tolka begreppet i denna rapport.

2.3.2 Arbetsprocess

I skriften *Företagsledningen och informationssäkerhet*, som utgavs av STG 1998, beskrivs en arbetsprocess utformad för att ge god informationssäkerhet i en verksamhet. Processen är baserad på riktlinjerna från BS 7799. Processen är, enligt STG – Allmänna Standardiseringsgruppen (1998), indelad i 7 steg:

1. *Skriva ett policydokument*. Ledningen bör ha en tydlig inriktning och visa sitt stöd för informationssäkerhetsarbetet genom att skriva ett policydokument och se till att all personal får ta del av det.
2. *Sätta upp en organisation*. Ett ledningsorgan för att införa säkerheten bör införas. Beroende på företagets storlek kan det vara nödvändigt att inrätta ledningsgrupper för att godkänna riktlinjer, fördela arbetsuppgifter och ansvar och koordinera införandet av skyddsåtgärder. En specialfunktion kan också behöva etableras i företaget.
3. *Göra en riskbedömning*. Det bör råda balans mellan kostnaderna för säkerheten å ena sidan, och värdet av de tillgångar som skall skyddas och konsekvenserna av att misslyckas å den andra. En riskanalys bör utföras för att bestämma vilka skyddsåtgärder som behövs och prioriteringen i införandet av dem.
4. *Införa säkerheten*. Skyddsåtgärder enligt BS 7799 bör sedan införas. Tänk igenom vilken vägledning som de anställda behöver. Olika kategorier kan ha olika krav, problem och prioriteter beroende på roller och IT-miljö. Befattningsbeskrivningar med individuella riktlinjer kan behöva upprättas.
5. *Upprätta en avbrottsplan*. Inrätta en procedur för avbrottsplanering, d.v.s. att utveckla och underhålla lämpliga avbrottsplaner för att skydda kritiska affärsrutiner från olyckor och katastrofer.

6. *Utbilda personalen*. Gör ett lämpligt utbildningsprogram om informationssäkerhet för de anställda och säkerställ att alla användare är övade i korrekt och säker användning av IT-resurserna. Alla skall veta hur de skall handla i fall av misstänkta eller konstaterade säkerhetsincidenter.
7. *Kontrollera efterlevnaden*. Se till att informationshanteringen regelbundet granskas mot säkerhetspolicyn, gällande normer och andra regler.

Notera att steg 4 inte nödvändigtvis behöver göras före steg 5. I figur 2 i bilaga 1 finns en övergripande illustration av processen.

Det finns givetvis andra åsikter om hur en arbetsprocess för informationssäkerhet optimalt bör vara utformad, men det ligger utanför denna rapports ramar att göra en fullständig beskrivning av detta område. Syftet med beskrivningen är att ge läsaren en föreställning om hur en arbetsprocess *kan* se ut. Det viktiga är att förstå var riskbedömningen (riskanalysen) utförs i ett större perspektiv.

2.3.3 Tillgångar

Vad en tillgång är anser jag beskrivs bra i boken *Computer Security Handbook*. I den säger författarna Hutt et al (1995) att en tillgång är en del av ett system som av organisationen anses ha ett värde för verksamheten. Exempel på tillgångar är enligt Hutt et al (1995) t.ex. information/data, hårdvara, mjukvara, kommunikationsutrustning, dokumentation, personal, infrastruktur, goodwill, pengar och kunder.

Pfleeger (1989) hävdar att de viktigaste tillgångarna i ett datasystem är hårdvaran, mjukvaran och datan. Jag tolkar det som att författaren här avser de viktigaste tillgångarna i ett datasystem (computing system), ej för hela informationssystem. Jag anser att människorna är en av de viktigaste tillgångarna i ett informationssystem. För att data skall bli information krävs det alltid en tolkning, gjord av en människa.

2.3.4 Hot och sårbarheter

Det finns en stor mängd potentiella hot mot en verksamhets informationssystem. Det ligger utanför denna rapports ramar att ge en fullständig redogörelse av alla hot. Syftet med detta kapitel är att generellt påvisa vilka typer av hot en verksamhets informationssäkerhet kan ställas mot. Men först kommer jag att definiera vad ett hot och vad en sårbarhet är.

Ett hot definieras av ITS som:

> Möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten (Informationstekniska standardiseringen, 1994:19).

Ett närliggande begrepp till hot är begreppet sårbarhet. En sårbarhet definieras av ITS som:

> Svaghet i system eller i en verksamhet, i form av bristande förmåga att motstå hot (Informationstekniska standardiseringen, 1994:25).

Dessa definitioner tycker jag är användbara och de kompletterar varandra bra[1]. Det är i princip omöjligt att räkna upp alla hot som kan finnas mot en verksamhets informationssystem. Ett system är dock oftast inte säkrare än sin svagaste punkt:

> In any security system, the *weakest point* is the most serious vulnerability. A robber intent on stealing something from your house will not attempt to penetrate a two-inch thick metal door if a window gives easier access (Pfleeger, 1989:3).

Man kan kategorisera hoten på ett antal sätt. I boken *IT-säkerhet för ditt företag* identifierar författarna tre övergripande kategorier av hot mot informationssystemen i en organisation (Borg et al, 1997):

Riktade hot: Till denna kategori räknas beställningsbrott, datorintrång på beställning, industrispionage, hackers eller crackers som bryter sig in i organisationer med t.ex. hög profil i media eller som hävdat att de har hög säkerhet.

Oriktade hot: Hit räknas virus, slumpmässiga intrång, hackers eller crackers som bryter sig in ”bara för att det går”.

Olyckor och katastrofer: Till detta räknas oriktade hot som inte direkt är orsakade av människor, till exempel strömavbrott, översvämningar, åsknedslag, eldsvådor, jordbävningar, vulkanutbrott eller råttor som gnager av kablar.

Hot kan även kategoriseras som *externa*- eller *interna*. Dessa definieras av ITS som:

> Internt hot - hot mot säkerheten som orsakas av insiders. En insider är en person med anknytning till verksamheten som utför eller planerar otillåtna ingrepp i informationssystem (Informationstekniska standardiseringen, 1994:20f).
>
> Externt hot - hot som orsakas av aktiviteter utanför organisationen. (Informationstekniska standardiseringen, 1994:26).

Pfleeger (1989) delar in hoten mot ett datorsystem i 7 kategorier; *hot mot hårdvara, mjukvara, data, lagringsmedia, nätverk, otillåten tillgång* och *nyckelresurser*. I efterföljande underkapitel kommer jag att beskriva dem. Jag använder mig av Pfleegers bok eftersom jag har fått uppfattningen att detta är en av de mest centrala böckerna inom området. Exempelvis används boken på universitetskurser i IT-säkerhet och den citeras i flertalet av min övriga litteratur. Enligt min tolkning rör Pfleegers hot enbart IT-säkerheten, inte hela informationssäkerheten.

Hot mot hårdvara

Eftersom fysiska enheter är så synliga är de enkla att angripa, menar Pfleeger (1989). En typ av ”angrepp” är de ofrivilliga angreppen. Datorer har dränkts med vatten, brunnit upp, elektrifierats av blixtar eller andra elkällor. Människor har spillt drickor, chips och andra typer av föda över datorer. Möss har gnagt sig igenom kablar. Alla

[1] Jag kommer i fortsättningen, gällande mindre centrala begrepp, använda mig av ITS definitioner. Eftersom syftet med ITS rapport är att skapa en enhetlig terminologi för området informationssäkerhet anser jag att den är lämplig för detta. För mer centrala begrepp kommer givetvis även andra källor att beaktas.

dessa typer av förstörelse hamnar, enligt Pfleeger (1989), under kategorin *ofrivilliga angrepp*, som är olyckliga händelser vars syfte inte var att skada hårdvaran.

En allvarligare typ av angrepp är, anser Pfleeger (1989), de *medvetna angreppen*, där förövaren verkligen vill skada systemet. Datorer har blivit skjutna med vapen och huggna med kniv. Bomber och bränder har förstört datorrum. Vanliga pennor, nycklar och skruvmejslar har använts för att kortsluta kretskort och andra komponenter. Stöld av datorer är också vanligt förekommande.

Hutt et al (1995) tar upp ett annat hot mot hårdvaran som Pfleeger (1989) inte berör, nämligen att hårdvaran kan gå sönder. Detta hot anser jag alltid bör beaktas. Även om garantier kan ge ersättning för hårdvaran, så kan systemets tillgänglighet hotas vid hårdvarufel.

Hot mot mjukvara

Mjukvara kan förstöras uppsåtligen, men också raderas, modifieras eller tappas bort av misstag. Resultatet blir dock alltid det samma enligt Pfleeger (1989); tillgängligheten i systemet hotas.

Det är mycket lätt att av misstag ta bort, eller spara fel version av en viktig fil över den riktiga filen, menar Pfleeger (1989). Det tror jag nästan alla som använder datorer har varit med om.

Modifiering av program kan, enligt Pfleeger (1989), innebära att programmet ändras så att det slutar att fungera, eller så att dess funktionalitet förändras. T.ex. kan programmet modifieras av en illasinnad person så att det fungerar som det skall för det mesta, men slutar att fungera vid någon specifik händelse, t.ex. när ett visst datum inträder. Detta kallas för en *logisk bomb*. Detta är en form av *virus*. Virus är det grundläggande exemplet på så kallad skadlig kod. Virus är ett program eller en del av ett program som kan kopiera sig själv till ett annat program, och modifiera det. Virus kan, enligt SIG Security (1997) göra samma saker som andra program och det samma som användare, men det agerar utan användarens tillstånd eller vetskap, och fullständigt oberäkneligt. Viruset kan förstöra det infekterade programmet eller samexistera med det så att det själv uppför sig som ett virus. SIG Security (1997) klassificerar virus som antingen *transienta* eller *residenta*. Ett transient virus körs och avslutas när det infekterade programmet körs och avslutas. Ett resident virus lägger sig i arbetsminnet och blir kvar där, även om det infekterade programmet avslutats. Ett annat kännetecken för virus, som företaget PricewaterhouseCoopers (1998) tar upp i sin årliga rapport *Technology Forecast: 1999*, är att virus oftast replikerar sig själva. Förutom logiska bomber finns det ett antal andra sorters virus, exempelvis:

Trojansk häst: Program som skenbart eller reellt utför en förväntad, önskad funktion men som även utför oönskade operationer (Informationstekniska standardiseringen, 1994).

Lönndörr: Programmets designer kan ha lagt in ett hemligt säkerhetshål, som bara han/hon vet om. En farlig variant av lönndörrar är de som inkluderats i en kompilator, på så sätt kan en programmerares egna program smittas utan att han/hon vet om det (Silberschatz, 1998).

Mask: Program som sprider kopior av sig själv i nätverk. Till skillnad från andra virus är maskar självständiga program, de är därför inte gömda i någon program- eller datafil. De måste startas av en agent. Resultatet av maskar blir oftast att prestandan i

systemet minskar. I vissa fall är avsikten att helt fylla en datorresurs, exempelvis en hårddisk (SIG Security, 1997).

Makrovirus: Makron eller mallar som innehåller infektionsmekanismer, som följer med i dokument. Detta medför att viruset sprids till de datorer som öppnar det smittade dokumentet. Traditionella virus var bundna till ett operativsystem och infekterade bara programfiler. Makrovirus kan infektera flera typer av operativsystem och gömma sig i datafiler (PricewaterhouseCoopers, 1998).

Med Internets hjälp har det blivit mycket lättare att skicka information mellan användare. Därmed har också det blivit större utrymme för virus att sprida sig, menar PricewaterhouseCoopers (1998). Antalet virus ökar hela tiden. PricewaterhouseCoopers (1998) tar upp en undersökning gjord av tidningen *Virus Bulletin*, som rapporterar att mellan 1987 och 1998 dubblerades antalet virus ungefär var 10:e månad. PricewaterhouseCoopers (1998) citerar även tidningen *PC Magazine*, som enligt citatet rapporterat att det tillkommer mer än 200 nya virus varje månad. Virus är ett stort problem för företag. I Ernst & Youngs (1997) undersökning, som jag beskrev i kapitel 1, uppgav 46% av respondenterna att de lidit stor skada av virus respektive 35% av makrovirus. Detta trots att 94% använde sig av aktivt virusskydd.

Ett annat hot mot mjukvara är stölder, menar Pfleeger (1989). Stöld kan innebära att program obehörigt kopieras, och används eller säljs.

Hutt et al (1995) anser att ett annat hot som måste beaktas är att mjukvaran kan ha inbyggda fel. Programvaror förr i tiden var relativt små och antalet programrader räknades ofta i tusentals rader kod. Ett helt Unix-system bestod i mitten av 1980-talet av ca 25.000 rader kod. Idag (1998) har antalet rader i programvarorna formligen exploderat och programmen har blivit gigantiskt stora. Antalet programrader räknas istället i miljontal. Windows 2000 (Windows NT 5) uppges innehålla ungefär 25 miljoner rader kod.

Hot mot data

De tre faktorer som informationssäkerhet bygger på: *integritet, sekretess* och *tillgänglighet,* kan alla vara potentiella hot mot data.

Hot mot integriteten, d.v.s. att datan blir otillåtet modifierad, kräver större skicklighet av förövaren än t.ex. stöld av data, menar Pfleeger (1989). Förövaren måste ha kunskap om tekniken där datan skickas eller är lagrad, samt i många fall vilket format den är lagrad, för att kunna modifiera den. Den största andelen av hot mot data-integriteten består av virus, felaktiga lagringsmedium och felaktiga kommunikations-anläggningar.

Data är mycket sårbar för modifieringar, anser Pfleeger (1989). Små, och skickliga modifieringar kan förbli oupptäckta utan att någon märker det. Ett exempel på detta, som Pfleeger (1989) tar upp, är så kallade *salamiattacker*. Ett exempel på en salami-attack är om det ligger inlagt i ett banksystem att 1 öre från varje kunds ränta skickas till ett annat konto. Det är osannolikt att någon kund skulle märka det, eller klaga på det om han/hon mot all förmodan skulle upptäcka det.

Hot mot sekretessen, d.v.s. att data blir tillgänglig för obehöriga, kan uppstå på många sätt. Exempel kan vara avlyssnade kablar, mutor av personal, avkänning av elektro-magnetisk strålning eller stöld, menar Pfleeger (1989). Även optisk strålning från

bildskärmar kan, enligt Johansson (1998), avläsas från långt håll om de är olämpligt placerade, exempelvis vid ett fönster.

Pfleeger (1989) tar tyvärr inte upp vilka hot mot tillgängligheten av data som kan finnas, men det gör Caelli et al (1996). Sabotage, fel på kommunikationsanläggningar, virus, och av misstag bortagna filer är alla hot som kan störa tillgängligheten av data för behöriga, menar de.

Hot mot lagringsmedia

Det lagringsmedium där datan lagras är också ett potentiellt hot, menar Pfleeger (1989). Disketter och hårddiskar kan gå sönder, cd-skivor repas m.m., vilket kan medföra att datan blir oläsbar.

Hot mot nätverk

När man kopplar samman datorer i nätverk ökar hoten:

> Networks simply multiply the problems of computer security. Lack of physical proximity, use of insecure, shared media, and need to identify remote users are all security problems that are made more difficult in computer networks (Pfleeger, 1989:11).

Caelli et al (1996) identifierar ett antal egenskaper, som förklarar varför hoten ökar i nätverkssystem i jämförelse mot system där datorerna inte är sammankopplade med varandra:

Delning: Målet med nätverk är att dela på resurser och arbetsbelastningar, och som ett resultat av detta kan fler användare få tillgång till en nätverksansluten dator.

Komplexitet: Eftersom nätverk ofta är stora och komplexa är det svårare att upprätthålla säkerhetspolicyn (om sådan finns) än i ett endatorsystem.

Flytande gräns: Det är ofta svårt att avgöra var ett nätverk börjar och var det slutar. En dator kan utgöra en nod eller en brygga i två olika nätverk, så att resurserna i det ena nätverket av misstag kan bli tillgängliga för användare i det andra nätverket.

Många potentiella attackpunkter: Tidigare konstaterades att ett system inte är säkrare än sin svagaste punkt. Om data t.ex. måste skickas genom flera värddatorer för att komma fram till mottagaren, är datan inte säkrare än den svagaste länken i kommunikationskedjan.

Hoten är större om systemet är kopplat mot omvärlden, exempelvis via Internet, än om det bara är ett lokalt nätverk (LAN). Med koppling mot omvärlden tillkommer risken för externa angrepp.

En vanlig typ av externa angrepp, som PricewaterhouseCoopers (1998) tar upp, är så kallade *denial of service-attacks.* Dessa attackers syfte är att minska systemets tillgänglighet genom ett flertal olika metoder. Exempel på metoder är (PricewaterhouseCoopers, 1998):

E-post bomber: Denna metod går ut på att skicka hundratals brev eller stora filer till servern vilket kan medföra att filsystemet fylls eller att mailservern överbelastas, vilket gör dem otillgängliga för användarna.

Ping of Death: Slår ut nätverksservrar genom att överbelasta dem med otillåtet stora ping-paket. ”Ping” står för *Packet Internet Groper*, och är ett kommando som används

för att testa om en IP-adress är uppkopplad. En variant av denna metod modifierar IP-paketen så att servern tror att det skall komma fler paket, vilket det inte gör. Servern väntar på paket som inte kommer, och därmed minskas dess tillgänglighet att behandla ”riktiga” paket.

Hoten från kopplingar mot omvärlden verkar öka konstant. Enligt undersökningen som Computer Security Institute (1998) gjorde ökade antalet organisationer som rapporterade Internetkopplingen som en frekvent attackpunkt från 47% under 1997 till 54% 1998. 1996 var samma procenttal 37%. Antalet rapporterade Internetattacker var i undersökningen 1998 uppe i samma antal som de rapporterade attackerna på de interna systemen.

Otillåten tillgång

Otillåten tillgång till datorutrustning är ett hot. Inkräktaren kan, menar Pfleeger (1989), stjäla dyrbar datortid. Ett annat hot är att inkräktaren kan förstöra data, eller stjäla viktig information. En obehörig användare kan även hindra en behörig användare att få tillgång till systemet.

Nyckelresurser

Om bara en person vet hur ett speciellt program används eller underhålls är detta ett hot, menar Pfleeger (1989). Personen i fråga är då en *nyckelperson*. Problem kan uppstå om nyckelpersonen t.ex. blir sjuk, råkar ut för en olycka eller slutar. Jag anser dock att även andra saker än personer kan vara av nyckelkaraktär. Vissa resurser som t.ex. en viss hårdvara kan vara kritisk för verksamhetens funktion. Detta är då en nyckelresurs, som, enligt mig, är viktig att skydda.

Förutom de hot som Pfleeger (1989) beskriver går det att identifiera andra hot mot informationssäkerheten. Pfleeger (1989) berör ju som sagt bara IT-säkerheten. Jag kommer att gå igenom några andra typer av hot nedan.

Felaktigt ledarskap

Ett av de största hoten mot informationssäkerheten är dålig, eller felaktig ledning och styrning av säkerhetsarbetet i organisationen, menar Hutt et al (1996). Ansträngningarna att bibehålla eller att öka graden av informationssäkerhet kommer ofta till korta på grund av dålig ledning och styrning. Ibland beror problemet enbart på slöhet. Lika farligt är det när ledningens beslut bara är ”tomma ord” som ej tas på allvar eller efterlevs. I allt för många fall tas informationssäkerheten inte på allvar av ledningen, menar Hutt et al (1996). De räknar upp ett antal anledningar och ursäkter som kan ligga till grund för ledningens bristande säkerhetsengagemang:

”Det har inte behövts förut”: Ledningen är konservativ och tror att om det har gått bra förut så kommer det att gå bra i framtiden.

Motstridiga mål: Säkerhetsarbetet använder resurser som kan användas till annat. Om säkerheten upplevs mer som en börda än en integrerad del av affärsprocessen, finns det risk att säkerhetsarbetet blir negligerat eller uppskjutet.

Inget uppenbart ekonomiskt bidrag till verksamhetens resultat: Om varje skyddsåtgärd måste kostnadsberättigas som en oberoende aktivitet, kan den utsättas för (ekonomiska) nedskärningar.

Ovilja att lägga pengar på säkerhet: Ofta är ledningen, av olika anledningar, ovillig att bekosta alla de skyddsåtgärder som behövs för att säkerställa säkerheten.

Hot mot extern exekverbar programvara

Ett hot mot datorer som är kopplade mot omvärlden är, enligt Olovsson (1998), extern exekverbar programvara som t.ex. ActiveX-komponenter, Java-applets m.m., där vare sig funktion eller säkerhet normalt kan verifieras. Detta hot tror Pricewaterhouse-Coopers (1998) kommer att öka i framtiden, med den ökade användningen av Internet.

År 2000-problemet

År 2000-problemet är, enligt Överstyrelsen för civil beredskap (1999), ett hot mot IT-systemen med anledning av att IT-utrustning med tillhörande maskin- och programvaror i många fall innehåller datumlogik som eventuellt inte kommer att fungera normalt efter övergången till år 2000. Det grundläggande skälet till detta är att datum många gånger representeras med endast två siffror för årtal i applikationer.

Det finns givetvis ett stort antal andra hot och sårbarheter som bristande rutiner, ovetande användare, rena misstag, slarviga installationer, avsaknad av säkerhets-uppdateringar, ambition, kunskap, industrispionage, o.s.v. Det ligger som sagt utanför denna rapports ramar att ge en fullständig redogörelse av alla hot och sårbarheter.

2.3.5 Skyddsåtgärder

För att skydda sig mot potentiella hot mot informationssäkerheten i verksamheten kan man vidtaga skyddsåtgärder. Skyddsåtgärder definieras av ITS som:

> Åtgärder och kontroller som vidtas för att uppfylla för systemet specificerade säkerhetskrav (Informationstekniska standardiseringen, 1994:25).

Skyddsåtgärder kan, enligt Informationstekniska standardiseringen (1994), omfatta organisation och ansvar, administrativa rutiner, personalsäkerhet, fysiskt skydd, drifts-rutiner samt utrustnings- och programbaserade funktioner. Skyddsåtgärderna kan klassificeras som *förebyggande*, *återställande* eller *detekterande*. Detta tycker jag ger en bra indelning av skyddsåtgärderna. Dock bör man vara medveten om att en skydds-åtgärd t.ex. både kan vara detekterande och återställande. I figur 3 i bilaga 1 finns en illustration över denna klassificering.

I efterföljande underkapitel kommer jag beskriva några möjliga skyddsåtgärder. Jag har inga ambitioner att göra en komplett beskrivning av alla möjliga skyddsåtgärder, syftet är att påvisa exempel på sådana.

Utbildning

Utbildning av personalen krävs för att allt arbete som lagts ner på säkerhet inte skall förstöras i ett slag, på grund av något misstag som enkelt kunde förebyggts med kunskap. Borg et al (1997) menar att det finns två saker som motiverar till utbildning. Det första är att höja säkerhetsmedvetandet. Säkerhetsmedvetandet är grunden till ett säkerhetsfrämjande beteende hos samtliga anställda i organisationen. Vissa kunskaper om säkerhet måste vara kända och respekterade av var och en som har tillgång till informationssystemen. Detta skydd anser jag faller in under typen förebyggande åtgärder.

Det andra motivet till utbildning är, enligt Borg et al (1997), bevakning av datorresurser. Ansvaret för detta ligger traditionellt på systemadministratören, som förmodligen har störst möjlighet att upptäcka säkerhetsbrister och intrång i datorsystemen. Ju fler ögon som vakar över olika datorresurser, desto större är chansen att upptäcka påbörjade intrång. Detta skydd anser jag faller in under typen detekterande åtgärder. Utbildning kan således leda till både ett förebyggande- och ett detekterande skydd.

Revision

Ett sätt att höja säkerheten i organisationen, som Borg et al (1997) beskriver, är att någon dag om året simulera olyckor eller dataintrång genom scenarior. Genom att utsätta organisationen för en säkerhetsrisk på låtsas, kan säkerhetsluckor uppenbaras. Inte minst syns det om personalen vet vad den skall göra i en sådan situation. Detta förfarande kallas säkerhetsrevision och bör, enligt Borg et al (1997), genomföras i samarbete med någon utomstående part, lämpligen en säkerhetskonsult. Revision anser jag faller in under både detekterande- och förebyggande skyddsåtgärder eftersom en revision både kan upptäcka en existerande säkerhetslucka, samt förhållanden som kan leda till en säkerhetslucka, t.ex. för dåligt utbildad personal.

Fysiskt skydd

Exempel på förebyggande skyddsåtgärder som syftar till fysisk säkerhet är, enligt Informationstekniska standardiseringen (1994) brandskyddsväggar, säkerhetsskåp, och olika typer av tillträdesskydd som dörrar och lås. Ett annat skydd, som Johansson (1998) beskriver, är avskärmning av strömförande ledare, för att förhindra avlyssning. Exempel på detekterande skyddsåtgärder som syftar till fysisk säkerhet är, enligt Informationstekniska standardiseringen (1994) olika typer av inbrotts-, brand- och övervakningslarm.

Kryptering

Ett mycket kraftfullt sätt att skydda data på, som Johansson (1998) beskriver, är kryptering. Kryptering är en mekanism baserad på en matematisk algoritm med vars hjälp en läsbar datamängd (klartexten) kan omvandlas till en oläsbar datamängd (kryptotexten). Kryptotexten kan sedan lagras eller skickas utan att obehöriga kan ta del av innehållet. Den behörige användaren eller mottagaren kan omvandla kryptotexten till klartext när han/hon så önskar. Alla krypteringsmetoder, fortsätter Johansson (1998), bygger på minst en hemlighet, en krypteringsnyckel, som delas mellan parterna. Säkerheten vid kryptering är helt beroende på att nyckeln är hemlig och inte kommer i orätta händer eller enkelt kan listas ut. Därför är nyckelgenerering, nyckelhantering och nyckelutbyte lika viktigt som hur starkt själva kryptot är. Detta är något som ofta förbises av användare. Hur svårt det är att lösa krypteringen utan att ha tillgång till nyckeln kan karakteriseras som en funktion av krypteringsalgoritmens komplexitet och nyckelns längd, menar PricewaterhouseCoopers (1998). I de flesta fall gäller att ju längre nyckel som används, desto svårare är det att dekryptera datan.

Ett krypterat meddelande kan, enligt Pfleeger (1989), inte läsas av obehöriga, kryptering skyddar således datans sekretess. Det går inte heller att modifiera datan på något ”intelligent” sätt, därmed skyddar kryptering även datans integritet. Däremot går det naturligtvis att stoppa eller radera meddelandet, så att det aldrig når sin adressat

menar Johansson (1998). Därmed skyddar kryptering inte datans tillgänglighet. Kryptering är, enligt mig, en förebyggande skyddsåtgärd.

Autentisering

En annan förebyggande skyddsåtgärd är, enligt Johansson (1998), autentisering. Med autentisering menas fastställandet av en identitet eller verifierande av en identitet, t.ex. då man fastställer identiteten på användaren av ett system. Eftersom autentiseringen skall vara unik för varje enskild person, måste de data eller fakta som autentiseringen bygger på vara unika för varje enskild person. Autentisering kan bygga på tre olika principer:

Någonting man kan: utgår från en unik kunskap som individen har, exempelvis ett lösenord (Silberschatz et al, 1998).

Någonting man har: utgår från att endast ägaren har tillgång till ett speciellt fysiskt passerobjekt, ett bevis eller ett kännetecken, som används för autentisering. Typiska passerobjekt är nycklar, brickor, passerkort och aktiva kort (Johansson,1998).

Någonting man är: utgår från att personliga egenskaper och karaktärsdrag är unika för varje människa. Metoder som mäter någon biologisk egenskap kallas för *biometriska metoder*. Det finns ett antal biometriska metoder. Exempelvis existerar metoder som använder fingeravtryck, näthinnan, iris, ansiktet, rösten, tangenttryckningar eller handskrift, för autentisering (Computer Sweden, 1999).

Även kombinationer av ovan nämnda principer kan användas. I en artikel i Computer Sweden (1999) beskriver författarna olika sådana, t.ex. kombination av aktiva kort och biometrisk autentisering.

Digitala signaturer

En speciell form av autentisering, som används för att verifiera att meddelanden och filer är äkta, kallas för digitala signaturer. Johansson (1998) beskriver att en digital signatur åstadkoms med hjälp av kryptering. Först beräknas en kontrollsumma som utgår från all information i meddelandet. Avsändaren skapar sedan en signatur genom att kryptera kontrollsumman med hjälp av en hemlig nyckel som bara är känd för honom. Mottagaren dekrypterar signaturen med en allmän nyckel och får på så sätt fram den ursprungliga kontrollsumman. Mottagaren kan sedan generera en ny kontrollsumma, och om de båda överensstämmer med varandra kommer meddelandet från rätt avsändare. Digitala signaturer gör således att man kan säkerställa att ett meddelande kommer från rätt avsändare. De ger även ett visst integritetsskydd, eftersom om meddelandet ändrats under överföringen kommer kontrollsummorna att bli olika.

Brandväggar

En brandvägg används traditionellt för att skydda en verksamhets interna nätverk från externa angrepp, exempelvis från Internet. Vissa verksamheter behöver även, enligt SIG Security (1997), använda brandväggar internt för att skilja olika domäner åt, så kallade säkerhetsdomäner. En brandvägg består, enligt SIG Security (1997), huvudsakligen av två beståndsdelar. Filter har till uppgift att blockera överföring av viss trafik. Den andra delen är en *gateway* som låter vissa tjänster passera men under övervakning. Gatewayen är ett komplement till filtret.

Antivirusprogram

Antivirusprogram är förmodligen den vanligaste återställande skyddsåtgärden. De flesta antivirusprogram letar bara efter kända virus, beskriver Johansson (1998). För varje sådant virus har man identifierat någon karakteristisk teckensträng som är unik för just detta virus. Antivirusprogrammen söker igenom minnesutrymmet och letar efter dessa strängar. Om någon av dessa strängar hittas i minnet har antivirus-programmet detekterat ett virus och ett larm ges till användaren. Borttagandet av viruset görs sedan oftast manuellt av användaren. I alla fall får användaren ett förslag till åtgärd från programmet och rensning sker först sedan användaren givit sitt klartecken. Det finns även program som automatiskt rensar bort upptäckta virus, menar Johansson (1998). Antivirusprogram är således både en detekterande och en återställande skyddsåtgärd.

2.4 Riskanalys

En riskanalys genomförs, enligt SIG Security (1997), för att verksamheten skall få en uppfattning om vilken säkerhetsnivå man har för tillfället, vilka brister som måste åtgärdas med skyddsåtgärder, och i vilken prioritetsordning detta skall ske. En annan beskrivning gör Gilbert (1995), som menar att det yttersta syftet med riskanalysen är att välja rätt skyddsåtgärder:

> The ultimate purpose of risk analysis is to help in the selection of cost-effective safeguards that will reduce risks to an acceptable level (Gilbert, 1995:A2.1).

Gilbert (1995) menar alltså att riskanalyser i slutändan går ut på att finna de mest kostnadseffektiva skyddsåtgärderna. Detta syfte anser jag inte vara den enda anledningen till att utföra en riskanalys. Jag tycker att SIG Securitys beskrivning är bättre. I kapitel 2.4.5 kommer jag att behandla några av riskanalysens andra positiva effekter.

2.4.1 Definition

ITS definierar begreppet riskanalys såsom:

> I riskhantering systematisk metod för att i beslutsprocessen fastställa risk för system eller funktion (Informationstekniska standardiseringen, 1994:22).

För att förstå ITS definition av riskanalys måste man veta vad ITS menar med en risk. En risk är enligt ITS:

> Produkten av sannolikheten för ett framgångsrikt angrepp och därmed uppkommande skadekostnad (Informationstekniska standardiseringen, 1994:22).

I princip använder sig Olovsson (1998) av samma definition som ITS, fast med enklare ord:

> Risk = (sannolikheten för en oönskad händelse) $\times$ (graden av skada), där graden av skada mäts i något lämpligt mått, som exempelvis kronor (Olovsson, 1998:23).

Sammanfattningsvis kan sägas att: risken = sannolikheten $\times$ konsekvensen (för ett hot eller en sårbarhet). Riskanalysen utförs i steg 3 av den arbetsprocess för informations-

säkerhet som jag beskrev i kapitel 2.3.2. Riskanalysen är en del av en organisations riskhantering. Riskhantering definieras av ITS som:

> Aktiviteter på ledningsnivå som omfattar riskanalys samt åtgärder som följd av denna. I begreppet ingår olika sätt att hantera riskerna, t.ex. avbrottsplanering, förstärkning av skyddsåtgärder, skadefinansiering och eventuellt försäkringsskydd (Informationstekniska standardiseringen, 1994:23).

2.4.2 Arbetsprocess

Hur utförs då en riskanalys? Det finns inget enkelt svar på den frågan. I de böcker jag läst beskrivs arbetsprocessen på olika sätt. Dock går det att finna gemensamma arbetsmoment som de flesta metoder för riskanalys innehåller. I boken *Risk Analysis and the Security Survey* beskriver Broder (1984) 4 grundläggande moment som bör utföras i en riskanalys. De är:

1. Identifiera tillgångar
2. Identifiera hot och sårbarheter
3. Bedöma hoten och sårbarheternas sannolikhet
4. Bedöma konsekvensen av hoten och sårbarheterna

Efter att dessa grundläggande moment utförts kan man sedan på olika sätt analysera vilka risker som är viktigast att åtgärda, och vilka skyddsåtgärder som skall användas. I figur 4 i bilaga 1 finns en illustration över dessa grundläggande moment.

De flesta verktyg och metoder för riskanalys kan, enligt Gilbert (1995), klassificeras som *kvantitativa* eller *kvalitativa*. Vissa producerar resultat uttryckt i monetära- eller ekonomiska termer (kvantitativa), medan andra använder sig av kvalitativa uttryck eller approximeringar, ofta är det lingvistiska uttryck som t.ex. ”liten risk” eller ”mycket stor risk”.

2.4.3 Generella metoder för riskanalys

Det finns ett antal olika generella metoder som kan användas i riskanalyser. En riskanalysmetod är ofta sammansatt av flera av dessa generella metoder. I efterföljande underkapitel kommer jag att beskriva exempel på dessa generella metoder.

Checklistor

Checklistor ställer frågor om hot och sårbarheter och utgör en kontroll av säkerhetsnivån i verksamheten. Ofta utvärderar checklistorna säkerheten gentemot någon fastlagd standard, säger Hamilton (1996). En sådan standard kan t.ex. vara BS 7799. Hamilton (1996) menar att fördelen med checklistor är att risken minskar att man glömmer något hot eller någon sårbarhet i systemet. Dessutom blir resultatet från analyser av olika system jämförbara. En nackdel är dock att frågeformuläret kan ha förbisett någon väsentlig fråga. Därför anser jag att det kan vara farligt att helt förlita sig till färdiga checklistor. En möjlighet är att varje verksamhet anpassar checklistan till sin speciella kontext.

Scenarior

SIG Security (1997) beskriver hur scenarior kan användas som analysmetod. I en scenarioanalys samlas kunniga personer och personer med specialistinriktning från den verksamhet som skall analyseras. Gruppen går sedan igenom olika scenarior med olika typer av risker och deras konsekvenser. Därefter skapar man lösningar och tar fram aktiviteter som vägs samman till en åtgärdsplan. Scenarioanalyserna kan, enligt SIG Security (1997), genomföras som ”brainstorming” eller med hjälp av analysblanketter. När brainstorming används kallas detta, enligt Hamilton (1996), för *Delphi-teknik*.

Trädanalys

En annan analysmetod som SIG Security (1997) beskriver är trädanalys. Trädanalysen går till på så sätt att man benar upp ett problem steg för steg, genom att ge olika typer av svar på frågeställningar som uppstår på vägen. Trädanalys kan utföras av en ensam person, eller av flera som arbetar i grupp. Ett enkelt exempel på trädanalys kan se ut så här (SIG Security, 1997):

- Fel - datorn fungerar inte.
- Första steget – Beror det på datorfel eller finns det andra orsaker?
- Genom bedömningen att det handlar om något annat än datorfel, går man ett steg vidare och bedömer om det är användaren som gör fel, fel på kablaget eller fel i administrationen o.s.v.

Transaktions- eller processanalys

Den tredje formen av analysmetod som SIG Security (1997) beskriver är transaktions- eller processanalys. I en transaktions- eller processanalys identifieras själva processen. Det kan exempelvis röra sig om ett pengaflöde eller någon annan typ av transaktionskedja. Först identifieras ett antal punkter där problem kan uppstå, eller där det kan finnas inbyggda brister. Med denna beskrivning i botten kan sedan andra generella riskanalysmetoder användas, t.ex. checklistor, trädanalyser o.s.v., för att beskriva de olika risker som kan finnas i de olika delarna av processen.

Kostnadsnyttoanalys

Den kanske vanligaste generella metoden för riskanalys är den så kallade kostnadsnyttoanalysen. Detta är, enligt Hutt et al (1995), den traditionella formen av riskanalys. De årliga kostnaderna för skyddsåtgärderna jämförs med de förväntade kostnaderna för förluster i samband med att hot inträffar.

Den grundläggande formeln för kostnadsnyttoanalys är, enligt Hutt et al (1995):

$$ALE = SK$$

ALE står för den årliga förväntade förlusten (Annual Loss Expectancy), S är sannolikheten att ett hot kommer att inträffa under ett år, och K är kostnaden som tillkommer om hotet inträffar.

Vanligtvis implementerar företaget inte en skyddsåtgärd om den årliga kostnaden för skyddsåtgärden överstiger den årliga förväntade förlusten, menar Hutt et al (1995).

2.4.4 Verktyg för riskanalys

Det finns olika typer av mer eller mindre avancerade datorbaserade verktyg för att analysera risker, enligt SIG Security (1997). Verktygen erbjuder ofta en viss automatik och ger en automatiserad rapportering som resultat av analyserna. Datorbaserade verktyg kan ge en bra överblick över vilka brister och åtgärdsbehov som finns i verksamheten. I verktygen finns ofta möjlighet att utföra sannolikhetsbedömningar och med utgångspunkt från dessa även kostnadsberäkningar.

Gilbert (1995) identifierar tre funktioner som ett datoriserat verktyg för riskanalys bör ha implementerade:

Informationsinsamling: Verktyget bör ha en struktur för att samla information om systemet som studeras, antingen från text eller grafiskt. Denna funktion är nödvändig för att samla information om tillgångarna och deras värde för verksamheten. Det bör även vara möjligt att samla information om hot, sårbarheter och skyddsåtgärder.

Analys: I denna funktion analyseras relationen mellan tillgångarna, hoten, sårbarheterna, skyddsåtgärderna och eventuellt andra faktorer som kan påverka eventuella förluster, t.ex. sannolikhetsbedömningar.

Resultat: Den sista funktionen är presentationen av resultatet. Olika verktyg skiljer sig åt med avseende på vilka resultat de ger. Vissa verktyg ger ej förslag på skydds-åtgärder, medan andra har en komplett och grafisk utvärderingsprocess av olika skyddsåtgärder. Vissa verktyg tar med kostnaden för skyddsåtgärderna i beräkningen och presenterar deras kostnadseffektivitet.

2.4.5 Riskanalysens positiva effekter

Jag anser att riskanalysen ger ett viktigt, och i många fall nödvändigt beslutsunderlag för det fortsatta säkerhetsarbetet. Men riskanalysen ger även andra positiva effekter. En riskanalys kan enligt Olovson (1998):

Öka medvetenheten om riskerna: Organisationen tvingas tänka efter, och göra klart för sig vilka risker som egentligen finns.

Klargöra vilka tillgångar som finns: Många gånger är organisationen inte medveten om alla tillgångar som finns, och hur värdefulla de är. Detta gäller i synnerhet immateriella tillgångar som exempelvis goodwill.

Identifiera sårbarheter i systemet: Gäller både tekniska och organisatoriska svagheter.

Identifiera möjliga hot: Ett hot kan vara direkt kopplat till en sårbarhet, men behöver inte vara det.

Klargöra vilka styrmekanismer som finns och hur de kan användas för att förbättra säkerheten.

3 Problem

I detta kapitel kommer jag att beskriva den problematik som rapporten behandlar. Jag börjar med att generellt beskriva problemområdet. Därefter avgränsar jag problemområdet, och pekar ut mer specifikt vad det är jag kommer att analysera i min undersökning. Till sist gör jag en prognos över vilket resultat jag förväntar mig att få.

3.1 Problembeskrivning

Som jag beskrev i kapitel 2.1 är informationssäkerhet ett område som får större betydelse ju mer samhället blir beroende av informationsteknik. De allvarligare hoten som kan drabba informationssamhället är, enligt Statskontoret (1998a), störningar i olika typer av samhällsviktiga funktioner eller kritiska infrastrukturer. Det gäller t.ex. avbrott i elförsörjningen, störningar i transporter, avbrott i data- och telekommunikation, störningar i betalningsväsendet och störningar i den offentliga förvaltningens tjänster.

Även företag blir mer beroende av informationstekniken. Undersökningen Computer Security Institute (1998) genomförde, visade att datorbrotten i USA stiger för varje år. Den totala finansiella förlusten, under 1998, hos de 241 respondenter som kunde kvantifiera sina förluster summerades till ett värde av ca 136 miljoner dollar.

Med det ökande beroendet till informationstekniken ökar vikten av att företag och organisationer upprätthåller informationssäkerheten. I arbetet med informationssäkerhet är en av de mest kritiska komponenterna riskanalysen, d.v.s. vilken risknivå är acceptabel för respektive verksamhet/process, vilka skyddsåtgärder bör väljas, och i vilken prioritetsordning detta skall ske.

För att utföra riskanalyser av en verksamhets informationssäkerhet finns det ett antal kommersiella verktyg och metoder, med olika fördelar och nackdelar. Att det är relevant att utvärdera dessa verktyg och metoder baserar jag på den internationella standarden BS 7799, vilken är den standard för informationssäkerhet som förmodligen kommer att bli den standard som svenska företag kommer att certifiera sig mot i framtiden. För att bli certifierad mot BS 7799 måste organisationen göra en riskanalys:

> Management must assess the risks to the organization and implement appropriate controls to reduce the risks, depending upon the level of risk management has decided to accept (British Standards Institution, 1995:1).

Dock beskriver BS 7799 ej hur denna analys kan eller bör utföras, med avseende på metoder och verktyg. Även Statskontoret anser det vara viktigt att riskanalyser genomförs:

> Risk- och säkerhetsanalyser i samhällsviktiga system ska löpande och systematiskt genomföras. Varje organisation ombesörjer själv genomförandet av analyserna med stöd av ÖCB[2] vid behov. Resultatet av analyserna behövs som grund för beslut som fattas om säkerhetsåtgärder. (Statskontoret, 1998a:kap 6.3)

[2] Överstyrelsen för civil beredskap (egen anm.).

Varken BS 7799 eller Statskontoret beskriver hur en riskanalys kan eller bör utföras, med avseende på metoder och verktyg, trots att de säger att en riskanalys skall genomföras. Därför anser jag att metoder och verktyg för riskanalys är ett intressant ämne att studera närmare.

Min huvudfråga blir därför att utreda vilka verktyg och metoder för riskanalys det finns. Jag kommer att försöka undersöka vilka fördelar och nackdelar de olika verktygen och metoderna har. Jag kommer därtill försöka se vilket resultat som respektive verktyg och metod ger.

3.2 Avgränsning

Med avseende på de resurser och den tid jag har till förfogande, avgränsar jag mig till att enbart analysera stora och medelstora företag i Sverige, som genomfört eller planerat att genomföra någon form av riskanalys av sin informationssäkerhet. Att analysera företag som inte genomfört eller planerat att genomföra någon form av riskanalys anser jag inte är lämpligt för att besvara mina frågeställningar, eftersom de förmodligen inte har någon erfarenhet av metoder och verktyg för riskanalys. Det samma gäller för små företag, eftersom de förmodligen inte gör riskanalyser i samma utsträckning som stora och medelstora företag.

Jag kommer enbart att behandla verktyg och metoder för riskanalyser av en verksamhets informationssäkerhet. Jag kommer dock inte att begränsa mig till att analysera någon speciell typ av verktyg eller metod, exempelvis vill jag undersöka både kvantitativa och kvalitativa sådana.

3.3 Preciserade frågeställningar

Den huvudfrågeställning som jag i denna rapport vill svara på är således:

- Vilka verktyg och metoder för riskanalys av en verksamhets informationssäkerhet finns det?

Mina delfrågor till huvudfrågan är:

- Vilka fördelar och nackdelar har dessa verktyg och metoder?
- Vilket resultat ger de olika verktygen och metoderna?

3.4 Förväntat resultat

Eftersom detta är ett nytt område för mig, har jag svårt att föreställa mig vilket resultat min undersökning kommer att ge. Förhoppningsvis kommer jag att finna ett antal verktyg och metoder för riskanalys med olika fördelar och nackdelar. Jag tror att resultatet av undersökningen kommer att bli en utvärdering av dessa verktyg och metoder, med en rekommendation över vilka som är bäst lämpade för olika situationer och kontexter.

Om jag får svar på min frågeställning tror jag det kan ge ett stort bidrag till företag och andra organisationer som står i begrepp att utföra en riskanalys av informationssäkerheten i verksamheten.

4 Metod

Syftet med denna rapport är att genomföra en utredning av vilka metoder och verktyg för riskanalys som det finns, och vilket resultat de ger. Därtill skall de olika verktygens och metodernas fördelar och nackdelar utvärderas. Därför är metodvalet för denna analys viktigt då den skall belysa styrkor respektive svagheter i de olika metoder och verktyg som jag finner. Observera att ordet metod i detta avsnitt diskuteras med två olika betydelser, (a) metod för riskanalys, samt (b) metod för lösning av problemställningen. För att lösa detta begreppsproblem kommer jag i detta kapitel att ange den sistnämnda (b) som "undersökningsmetod".

I detta kapitel börjar jag med att beskriva olika forskningsansatser som kan användas för att vetenskapligt angripa ett problem. Därefter beskriver jag olika undersökningsmetoder som skulle kunna tillämpas i denna undersökning. Slutligen väljer jag den forskningsansats och de undersökningsmetoder som, enligt mig, passar bäst för undersökningen.

4.1 Forskningsansatser

Det finns ett antal olika sätt att på ett vetenskapligt sätt närma sig ett problem. Två vetenskapliga inriktningar är de kvantitativa och de kvalitativa forskningsansatserna. En undersökning kan även klassificeras som deduktiv och/eller induktiv.

4.1.1 Kvantitativ ansats

Med kvantitativt inriktad forskning menas, enligt Patel och Davidsson (1994), forskning som använder sig av statistiska insamlings-, bearbetnings- och analysmetoder. Grunden för den kvantitativa ansatsen är, enligt Bell (1993), att resultatet av undersökningen skall vara generell och gälla hela den undersökta populationen. Eftersom det ofta i praktiken inte är möjligt att undersöka en hel population tas ett stickprov, d.v.s. ett urval görs. Resultatet generaliseras sedan till att gälla hela populationen. Bell (1993) menar att de kvantitativa metoderna oftast går mer på bredden än på djupet, eftersom undersökningen riskerar att missa mångfalden i och med att ett urval gjorts.

Kvantitativ metod kan, enligt Repstad (1993), användas till att beskriva hur vanlig en företeelse är, för att få reda på fördelningar, samt för att finna statistiska samband eller korrelationer. Dessutom kan undersökningen upprepas vid ett senare tillfälle för att se om det har skett en förändring.

4.1.2 Kvalitativ ansats

Med kvalitativt inriktad forskning menas, enligt Patel och Davidsson (1994), forskning som använder sig av verbala analysmetoder. Syftet är att försöka förstå och analysera helheter. Den kvalitativa bearbetningen präglas av den person som genomför arbetet, menar Patel och Davidsson (1994). Själv anser jag att även kvantitativ forskning präglas av den som utför arbetet, men det sker förmodligen i större utsträckning i kvalitativ forskning.

Det som kännetecknar kvalitativ metod är, enligt Repstad (1993), att den går på djupet men inte på bredden. Det innebär att man enbart studerar en eller några få miljöer, men att de i stället studeras som en helhet med alla dess nyanser. I den kvalitativa

forskningstraditionen betonar man ett tätt och nära förhållande mellan forskaren och den miljö eller de personer som skall studeras.

Ytterligare ett kännetecken på kvalitativa metoder är, fortsätter Repstad (1993), deras flexibilitet. I en kvantitativ undersökning är det metodiskt sett en stor synd att ändra på frågorna när man t.ex. redan frågat hälften av populationen. Det innebär att man inte får jämförbara data, eftersom respondenterna ställts inför olika frågor. I en kvalitativ studie däremot är det inte särskilt problematiskt att ändra frågorna, eftersom man inte söker generalisera resultatet till en större population.

4.1.3 Deduktiv och induktiv ansats

Det mest använda sättet att utveckla teorier är, enligt Holme och Solvang (1991), det som kallas för *hypotetisk-deduktiv teoribildning*. Deduktion innebär att man ur befintlig teori härleder nya hypoteser. Dessa hypoteser prövas sedan med empiriska undersökningar. En risk med denna ansats är, enligt Patel och Davidsson (1994), att den redan befintliga teorin bestämmer vilken information som samlas in, hur den tolkas, och hur informationen sedan relateras till den befintliga teorin.

Den induktiva ansatsen är, enligt Patel och Davidsson (1994), deduktionens raka motsats. Forskaren studerar då forskningsobjektet utan att först ha förankrat undersökningen i befintlig teori. Istället formuleras en ny teori utifrån den insamlade informationen, d.v.s. utifrån empirin. Det finns risker även med denna ansats menar Patel och Davidsson (1994). En risk är att man inte kan veta något om den nya teorins räckvidd, eftersom den baserar sig på ett empiriskt underlag som är speciellt för en viss kontext. Dessutom finns risken att forskarens egna idéer och föreställningar färgar av sig på de teorier som produceras. Detta är dock, enligt mig, en risk även i deduktiv forskning.

Enligt Hemeren (1999) är kvalitativa undersökningar ofta induktiva, och kvantitativa undersökningar ofta deduktiva.

4.2 Undersökningsmetoder

Det finns ett antal olika vetenskapliga undersökningsmetoder för att insamla information. Patel och Davidsson (1994) menar att den som utför insamlandet måste veta vad han/hon egentligen gör. För det första måste forskaren veta att han/hon undersöker det som avses att undersökas, d.v.s. man måste ha god *validitet*. För det andra måste forskaren veta att undersökningen sker på ett tillförlitligt sätt, d.v.s. undersökningen måste ha god *reliabilitet*.

I efterföljande underkapitel kommer jag att beskriva de undersökningsmetoder som jag anser skulle kunna vara relevanta för min undersökning.

4.2.1 Enkät

En vanlig undersökningsmetod är enkäten. En enkät innebär vanligen att ett slumpmässigt urval av personer eller företag får ett frågeformulär att besvara. Bell (1993) menar att enkäten är en bra undersökningsmetod för att samla in information på ett snabbt och förhållandevis billigt sätt. Enkäter förutsätter dock att respondenterna kan läsa, att de tolkar frågorna på i stort samma sätt som frågeställaren, samt att undersökaren är tillräckligt disciplinerad för att utelämna onödiga frågor.

Det finns, enligt Dahmström (1996), tre olika sorters enkätundersökningar. De är post-, grupp- och besöksenkäter. Nedan följer en kort beskrivning av dessa.

Postenkät

En postenkät utgörs, enligt Dahmström (1996), av ett frågeformulär som skickas ut till t.ex. enskilda personer, företag eller myndigheter. För- och nackdelar med en postenkät är:

Fördelar:

- Billigt
- Möjligt att skicka enkäten till många respondenter
- Många slag av frågor går att ställa
- Handlingar/anteckningar kan konsulteras av respondenten
- Respondenten kan svara när han/hon har tid
- Ingen påverkan från intervjuare

Nackdelar:

- Risk för stort bortfall
- Kan ej göras allt för omfattande
- Tar lång tid
- Ingen finns till hands om frågorna är oklara
- Svårt att få svar på öppna frågor
- Man vet ej säkert vem som svarat

Gruppenkät

En gruppenkät genomförs, enligt Dahmström (1996), på en samlad grupp människor. Enkäten delas ut till samtliga närvarande. Exempel på grupper kan vara skolklasser, idrottslag och konferensdeltagare. För- och nackdelar med en gruppenkät är:

Fördelar:

- Många personer kan undersökas samtidigt
- Billigt och snabbt
- Litet bortfall på grund av vägran

Nackdelar:

- Risk för påverkan respondenterna emellan
- Anonymiteten kan ej alltid skyddas
- Risk för mätfel
- Ingen förnyad kontakt för granskning av oklara svar är möjlig

Besöksenkät

Besöksenkäter genomförs, enligt Dahmström (1996), på besökare till företag eller andra verksamheter. Besökarna får ett frågeformulär att besvara. Enkäten kan antingen besvaras direkt på platsen eller besvaras senare och återsändas. Ett exempel på besöksenkäter är valundersökningar som sker vid vallokalen. För- och nackdelar med en besöksenkät är:

Fördelar:

- Ingen ram över besökande behöver skapas i förväg
- Snabb redovisning

Nackdelar:

- Risk för stort bortfall
- Personalkrävande
- Beroendeställning mellan respondent och den som faktiskt fyller i enkäten

4.2.2 Intervju

Med en intervju menas vanligen, enligt Patel och Davidson (1994), ett personligt möte där intervjuaren ställer frågor till respondenten. Intervjuer kan även genomföras per telefon.

En stor fördel med intervjuer är, enligt Bell (1993), att det är en anpassningsbar och följsam undersökningsmetod. Intervjuaren kan följa upp idéer, sondera svar och gå in på motiv och känslor på ett sätt som är omöjligt i en enkät. Hur respondenten svarar (med avseende på t.ex. tonfall, mimik och pauser) kan ge information som ett skriftligt svar inte avslöjar. Svaren på enkätfrågor måste tas för vad de är, men i en intervju kan man komma med följdfrågor och svaren kan utvecklas och fördjupas. En annan fördel gentemot enkäten är, menar Bernard (1995), att man vet vem respondenten är.

Det finns givetvis även problem med intervjuer. Intervjuer tar, enligt Bell (1993), lång tid att genomföra, och är dessutom kostsamma. Därtill är det en subjektiv metod, vilket medför att risker för skevheter (*bias*) är stor. Det kan även visa sig vara svårt att analysera de svar man får, och formuleringen av frågorna tar lika lång tid att göra som vid enkäter.

Bell (1993) beskriver att olika former av intervjuer kan kategoriseras längs ett kontinuum som mäter olika grad av formalitet. På den ena ytterkanten hamnar en synnerligt formell intervju där intervjuaren så mycket som möjligt skall fungera som en maskin, en objektiv registrator. På den andra extremen finns en helt och hållet informell intervju som styrs av respondentens svar och reaktioner. Denna kategorisering benämner Patel och Davidson (1994) som graden av *standardisering*. Intervjuer med låg grad av standardisering sker när intervjuaren själv formulerar frågorna under intervjun och ställer frågorna i den ordning som är lämplig för varje specifik intervju. Vid helt standardiserade intervjuer ställs helt likalydande frågor i exakt samma ordning till varje respondent. Graden av standardisering har, menar Patel och Davidson (1994), sin utgångspunkt i principer om mätning varför helt standardiserade intervjuer oftast används i kontexter där intervjuaren vill kunna jämföra och generalisera sina resultat.

En annan aspekt på intervjuer är, fortsätter Patel och Davidson (1994), graden av *strukturering*. Strukturering handlar om vilket svarsutrymme som ges till respondenten. En helt strukturerad intervju lämnar ett mycket litet utrymme för respondenten att svara inom, och det kan redan före intervjuns genomförande förutsägas vilka svar som är möjliga. I en ostrukturerad intervju däremot lämnar frågorna maximalt utrymme för respondenten att svara inom. Om en fråga är ostrukturerad brukar den kallas för en *öppen* fråga.

Intervjuaren har, enligt Dahmström (1996), möjlighet att stötta och stimulera respondenten till att ge så kompletta svar som möjligt genom så kallade *probes* (”*probe*” = sondera, grundligt undersöka). Risken finns dock att intervjuaren styr det uppgivna svaret. Bernard (1995) tar upp ett antal olika probe-tekniker. Exempel på dessa är:

Silent probe

Detta är, enligt Bernard (1995), den svåraste probe-tekniken. Den går ut på att intervjuaren är tyst och väntar på att respondenten skall fortsätta. Detta kan ibland ge mer information än en direkt fråga. Ovana intervjuare tenderar att kasta sig på nästa fråga så fort respondenten blir tyst, trots att respondenten kanske funderar vidare på sitt svar till den förra frågan. En annan effekt av silent probe är att man ej styr respondenten att svara på ett visst sätt.

Echo probe

Denna teknik går ut på att repetera det sista som respondenten sade, och be honom/henne att fortsätta. Detta är särskilt effektivt när respondenten beskriver en process eller en händelse, menar Bernard (1995). Genom upprepningen visar intervjuaren att han/hon har förstått vad respondenten sagt än så länge, och uppmuntrar respondenten att fortsätta. Dock bör inte denna teknik användas för ofta, eftersom det kan reta respondenten.

"Uh-huh" probe

En undersökning har, enligt Bernard (1995), visat att när intervjuaren lägger in små uppmuntrande eller bekräftande ljud som t.ex. ”jag förstår” eller ”uh-hum” när respondenten talar, så blir svaren en tredjedel längre än när intervjuaren är tyst.

Phased assertion

En annan probe-teknik är, fortsätter Bernard (1995), *phased assertion*. Denna teknik går ut på att intervjuaren låtsas att han/hon redan vet något för att få respondenten att ”öppna upp sig”. Detta är speciellt effektivt när det gäller känsliga ämnen som respondenten kanske inte vill berätta. Ju mer respondenten tror att intervjuaren redan vet, desto mer berättar respondenten, menar Bernard (1995). Det är ju inte respondenten som ”skvallrar”, eftersom intervjuaren redan hört det från någon annan. En annan typ av *phased assertion* är när intervjuaren provocerar fram ett svar genom att påstå något som han/hon vet är falskt. På så sätt kan respondenten ledas till att svara på frågor som han/hon egentligen inte tänkt svara på.

Intervjuer kan, som jag nämnde i början av detta kapitel, utföras både på plats och per telefon. Dahmström (1996) beskriver skillnaderna mellan dessa två tekniker.

Besöksintervju

En besöksintervju genomförs vanligen så att intervjuaren söker upp respondenten och ställer frågor på plats. Besöksintervjuer kan, enligt Dahmström (1996), karaktäriseras som en dyrbar metod som ibland är nödvändig för att få utförliga svar med tillräckligt hög kvalitet.

Besöksintervjuns fördelar:

- Många och ”krångliga” frågor kan ställas
- Svarskort med bilder och övrig information kan visas
- Oklarheter i frågorna kan vanligen utredas enkelt
- Möjlighet att stötta och stimulera respondenten med probes finns
- Anonymitetsskyddet kan förstärkas

Besöksintervjuns nackdelar:

- Dyrt och tar lång tid
- Risk för intervjuareffekter, d.v.s. intervjuaren påverkar respondenten
- Risk för prestigebias, d.v.s. den skevhet med anledning av det sociala tryck att svara i enlighet med vedertagna sociala normer och förväntningar som respondenten kan uppleva

Telefonintervju

En telefonintervju innebär att intervjuaren ställer sina frågor per telefon. Precis som vid besöksintervjuer har intervjuaren, enligt Dahmström (1996), vissa möjligheter att medverka till att svaren blir av högre kvalitet än t.ex. vid en enkät.

Telefonintervjuns fördelar:

- Snabbt och billigt, speciellt i jämförelse med besöksintervjuer
- Oklarheter i frågorna kan vanligen utredas enkelt
- Möjlighet att stötta och stimulera respondenten med probes av intervjuaren

Telefonintervjuns nackdelar:

- Risk för stor andel oanträffbara personer
- Krav på kända och aktuella telefonnummer
- Ej möjligt med alltför lång intervju
- Ej alltför krångliga eller känsliga frågor
- Den omgivande miljön kan vara störande
- Risk för föga genomtänkta svar
- Inga anonymitetsskyddande åtgärder möjliga

4.2.3 Dokument

Begreppet *dokument* har, enligt Patel och Davidson (1994), traditionellt använts för att beteckna information som nedtecknats eller tryckts. Idag kan dock information lagras

på ett flertal andra sätt. Därför ingår även t.ex. filmer, bandupptagningar och fotografier i begreppets innebörd. En övergripande kategorisering av dokument kan se ut så här (Patel och Davidson, 1994):

- Statistik och register (t.ex. kundregister, mantalslängder)
- Officiella handlingar (t.ex. diarier, protokoll)
- Privata handlingar (t.ex. brev, dagböcker, självbiografier)
- Litteratur (t.ex. biografier, skönlitteratur, facklitteratur)
- ”Kortlivade” dokument (t.ex. tidningar, broschyrer)
- Bild-dokument (t.ex. filmer, kartor, foton)
- Ljud-dokument (t.ex. kassettband, grammofonskivor)

Dokument kan, enligt Patel och Davidson (1994), användas för att besvara frågeställningar kring faktiska förhållanden och faktiska skeenden. Då måste den som gör undersökningen försöka fastställa att de fakta som står i dokumentet är sannolika. Dokument kan också användas till att besvara frågeställningar som rör individers upplevelser av något förhållande eller skeende.

Man bör alltid förhålla sig kritisk till dokument, menar Patel och Davidson (1994). I källkritiken bör man ställa sig frågor som:

- När och var har dokumentet tillkommit?
- Vilket syfte hade upphovsmannen med dokumentet?
- Under vilka omständigheter tillkom dokumentet?
- Vem är upphovsmannen?
- Vilken relation till det som beskrivs hade upphovsmannen?
- Framställdes dokumentet under någon form av påverkan?

Närheten till ett dokument kan, fortsätter Patel och Davidson (1994), avgöra hur pålitligt det är, speciellt med avseende på förfalskningar. Ögonvittnesskildringar och förstahandsrapporteringar kallas *primärkällor*, övriga kallas *sekundärkällor*.

4.3 Val av forskningsansats och undersökningsmetoder

I detta kapitel kommer jag att presentera mitt metodval, med tillhörande motiveringar.

4.3.1 Kvalitativ ansats

Jag anser att mina frågeställningar lämpar sig bäst att undersökas med en kvalitativ forskningsansats. Frågeställningarna passar inte att besvara statistiskt, eftersom de inte är enkla och entydiga. De kan tolkas på många sätt, och kräver förmodligen i stor utsträckning att den som ställer frågorna har möjlighet att förklara dem ytterliggare. Exempelvis frågan som rör vilka fördelar och nackdelar respektive verktyg eller metod har, anser jag vara olämplig att försöka samla in en stor mängd av svar på och sedan försöka dra några generella slutsatser därifrån. T.ex. skulle en respondent kunna svara att metod X är bra för den tar 3 dagar att utföra, medan en annan respondent säger att metod X är dålig för den tar 3 dagar att utföra. Hur skulle detta tolkas? Med kvalitativ ansats får jag möjlighet att ställa följdfrågor och tränga djupare in i

problemområdet. Möjligtvis skulle min första frågeställning rörande vilka verktyg och metoder för riskanalys det finns kunna besvaras med en kvantitativ undersökning, men det skulle bli svårt att gå vidare med de andra frågorna. Därför väljer jag att använda en kvalitativ forskningsansats. På så sätt hoppas jag få en djupare insikt i min problematik. Nackdelen med kvalitativ ansats blir att undersökningen sker i ett mer begränsat sammanhang, och resultaten blir därmed inte lika generaliserbara som om en kvantitativ metod använts. Dock anser jag som sagt att kvantitativ ansats inte lämpar sig för mina delfrågor.

4.3.2 Induktion

Jag kommer inte att använda mig av befintliga teorier för att pröva om dessa kan appliceras på mitt problemområde, utan jag kommer att försöka undersöka den verklighet som existerar idag. Därmed blir min undersökning i det närmaste induktiv. Anledningen till detta är att jag inte funnit några lämpliga teorier som skulle kunna appliceras på min problematik.

4.3.3 Triangulering

Jag kommer att använda mig av *triangulering* när jag undersöker mina problemställningar. Triangulering innebär att undersökningen sker ur två eller flera olika vinklar. Det finns, enligt Kjaer (1995), fyra olika trianguleringsformer:

Metodtriangulering: undersöker samma situation med olika undersökningsmetoder.

Datatriangulering: samlar data från olika källor och eventuellt olika situationer.

Forskartriangulering: mer än en forskare samlar information till undersökningen.

Teoretisk triangulering: flera teoretiska perspektiv används vid analysen av undersökningen.

Jag kommer att använda mig av metodtriangulering för att på så sätt få en mer nyanserad bild av vilka metoder och verktyg för riskanalys det finns. Genom att använda flera olika undersökningsmetoder minskar risken att någon specifik undersökningsmetods bias påverkar undersökningen. Av samma anledning kommer jag även i största möjliga utsträckning använda mig av datatriangulering. Genom att se på hur en metod eller ett verktyg för riskanalys beskrivs av olika källor hoppas jag kunna bilda mig en mer objektiv syn på dem, än om bara en källa använts.

4.3.4 Besöksintervju och dokumentstudie

Besöksintervju och dokumentstudie är de undersökningsmetoder som jag anser lämpar sig bäst för att besvara mina frågeställningar. Med intervjuer kan jag relatera mina frågeställningar till den faktiska användningen av verktyg och metoder för riskanalys, d.v.s. till empirin. Med intervjuer ges därtill möjlighet att följa upp och förklara frågor, samt att använda probes. Detta går ej med enkäter. Därför anser jag att enkäter inte är lämpliga för kvalitativa undersökningar. Med en studie av olika dokument, främst litteratur, hoppas jag få tillgång till information som inte kan fås vid intervjuer. Det finns tyvärr inte så mycket litteratur om ämnet. Jag har dock funnit en del beskrivningar av olika metoder och verktyg för riskanalys, som det vore synd att inte beakta. Exempel på dessa är:

- *Computer Security Products Byers Guide.* Bok skriven av Computer Security Institute (1997), vilken listar olika IT-säkerhetsprodukter.

- *Guide to BS 7799 Risk Assessment and Risk Analysis.* Författarna Humphreys et al (1998) beskriver sin metod som kallas för C:Cure.
- *Http://www.dfs.se.* Dataföreningens hemsida, vilken beskriver deras riskanalysprodukter.

Det finns alltid en risk att dokumenten inte är objektiva. Detta kommer jag försöka undvika med hjälp av källkritik, där de punkter som nämns i kapitel 4.1.3 kommer att beaktas. Dessutom kommer undersökningens resultat främst att bygga på intervjusvaren. Dokumenten blir snarare ett komplement till intervjuresultaten. För att finna lämpliga dokument kommer jag söka via olika medier. Först och främst kommer jag söka efter litteratur på olika bibliotek. De bibliotek jag avser att söka på är Högskolan i Skövdes bibliotek, Göteborgs Universitetsbibliotek (UB) och Arthur Andersens företagsinterna bibliotek. Som komplement till detta kommer jag även att söka dokument på Internet. *Metacrawler*[3] kommer då att användas som sökmotor eftersom den, enligt mig, är den bästa sökmotorn som finns på Internet. I många fall finns det, som sagt, en stor anledning till att vara kritisk till det som står i dokumenten. Speciellt när det gäller källor hämtade från Internet. Ofta är informationen på Internet av marknadsföringskaraktär. Jag kommer att i största möjliga utsträckning inte använda mig av sådana källor för att försöka värdera hur "bra" ett verktyg eller en metod är. Dock anser jag att de kan vara värdefulla för att visa hur metoden/verktyget är uppbyggd, vilket resultat den producerar o.s.v.

Intervjuerna kommer att utföras med låg grad av standardisering och strukturering. Detta är faktorer som enligt Holme och Solvang (1991) utmärker en kvalitativ intervju. Vid låg grad av standardisering och strukturering bör problemställningens alla delområden täckas, men eftersom det i detta fall ges större utrymme vid själva frågandet behöver inte de enskilda frågorna formuleras i förväg, menar Patel och Davidsson (1994). Det kan räcka med att ha med sig en uppställning av frågeområden som intervjuaren håller sig till. Det är vad jag tänker göra.

Anledningen till att jag inte vill genomföra intervjuerna per telefon är att det kan vara svårt att ställa krångliga och känsliga frågor via detta medium. Dessutom ökar risken att respondenten svarar mindre genomtänkt på telefon än vid ett besök. Även respondentens omgivande miljö kan ge en störande effekt på intervjun om den utförs på detta sätt. Dessutom behöver intervjuerna förmodligen vara tidsmässigt långa, för att jag skall kunna få den information jag vill. Därmed lämpar sig besöksintervjuer bättre, anser jag.

Jag kommer använda ostrukturerade frågor vid intervjuerna eftersom det är svårt att förutsäga vad respondenten kommer att svara. En ostrukturerad intervju har den fördelen att följdfrågor kan ställas och diskussioner kring problem kan genomföras. Nackdelen är att det tar mycket tid i anspråk, men det tycker jag uppvägs av att kvaliteten på svaren förmodligen blir bättre, eftersom respondenten får stort svarsutrymme.

Vid intervjuer kan man, enligt Patel och Davidsson (1994), sekvensera frågorna med så kallad *”tratt-teknik”*. Detta innebär att intervjuaren börjar med stora och öppna frågor, för att senare gå över till mer specifika. Denna teknik anses vara motiverande och aktiverande i och med att respondenten till att börja med får verbalisera sig som

[3] Metacrawler finns på adressen: http://www.metacrawler.com

han/hon vill. Detta tänker även jag göra genom att i början fråga intervjupersonen exempelvis vilka olika metoder och verktyg för riskanalys han/hon känner till. Därefter kommer jag gå in på mer detaljerade frågor angående respektive verktyg eller metod.

Vid intervjuerna kommer jag att försöka att använda mig av *probes*. De tekniker som jag nämnde i kapitel 4.2.2 är de som kan bli aktuella. Vilka tekniker jag kommer att nyttja får improviseras fram vid varje intervjutillfälle. Det är omöjligt att bestämma i förväg.

För att registrera intervjusvaren kommer jag använda mig av en kombination av anteckningar och ljudbandsinspelning. På detta sätt minskar risken för att någon data förloras. För att öka reliabiliteten hos intervjuerna ytterliggare kommer jag använda mig av en extra observatör vid intervjuerna. Överensstämmelsen mellan registreringen av informationen mellan de två observatörerna kan då, enligt Patel och Davidsson (1994), utgöra ett mått på reliabiliteten. Dessutom kommer jag att skicka ut min redogörelse för respektive intervju till varje respondent i efterhand. På så sätt får respondenterna möjlighet att korrigera uppgifter som jag kan ha missuppfattat.

4.3.5 Urval

Jag kommer, som framgår i min avgränsning, enbart undersöka medelstora och stora företag i Sverige. Men vilket urval av respondenter skall jag göra? Holme och Solvang (1991) menar att syftet med kvalitativa intervjuer är att öka informationsvärdet och skapa en grund för djupare och mer fullständiga uppfattningar om det fenomen man undersöker. Detta mål kan uppnås på flera sätt. För det första bör man uppnå en så stor variationsbredd som möjligt i urvalet. Denna variation tänker jag få genom att välja respondenter med erfarenhet från olika branscher, t.ex. från statliga, kommunala och privata bolag. För det andra, fortsätter Holme och Solvang (1991), kan man öka informationsvärdet genom att använda sig av respondenter som på goda grunder kan antas ha riklig kunskap om de företeelser man undersöker. Detta tänker jag uppnå genom att enbart intervjua personer med stor erfarenhet av arbete med informationssäkerhet och riskanalyser. Störst erfarenhet av detta har förmodligen den som är informationssäkerhetsansvarig i en organisation. Därför är det personer med denna befattning jag i första hand kommer att försöka finna. Om jag finner en person med en annan befattning, men som har de önskvärda egenskaperna, kommer inte detta att vara något hinder.

4.3.6 Konfidentiella respondenter

Respondenterna kommer att vara anonyma. Detta tror jag ger större sannolikhet att svaren blir korrekta. Då kan *prestigebias* undvikas som, enligt Dahmström (1996), kan uppstå när vissa ämnesområden innehåller prestigeladdade frågor. Det finns en stor risk, tror jag, att de personer jag kommer intervjua kan uppfatta vissa frågor som prestigefyllda. Det är förmodligen så att en informationssäkerhetsansvarig inte vill framhäva brister som finns i det egna systemet, eller i de metoder och verktyg för riskanalys som han/hon använder.

5 Genomförande

I detta kapitel kommer jag att beskriva det praktiska förfarandet med vilken jag anbringade mina valda undersökningsmetoder, d.v.s. intervjuer och dokumentstudie, på problemet.

5.1 Intervjuer

För att hitta lämpliga respondenter ringde jag till olika organisationer och frågade om de hade någon ansvarig för informationssäkerheten. Eftersom Håkan Stålstad i DEP3 sökte ett liknande urval ringde vi tillsammans. För att uppnå den spridning vi ville ha på respondenternas bakgrund, med avseende på bransch, ringde vi till olika sorters verksamheter. Vi försökte finna minst en respondent från respektive grupp: statliga verk, kommunala bolag och privata bolag. De privata bolagen försökte vi sprida med avseende på verksamhetstyp, exempelvis tillverkande företag, banker, högteknologiska företag, försäkringsbolag, konsultbolag osv. Vi ville även få geografisk spridning på organisationerna, helst ville vi undersöka organisationer från både västra, östra, norra och södra Sverige. Det skulle kunna vara så att ett verktyg, eller en metod har lokal förankring, därför ansåg jag att en geografisk spridning på respondenterna skulle vara givande.

Efter en tids rundringning ansåg jag att ett lämpligt urval hittats. Med tanke på intervjuernas art (kvalitativa) begränsade jag antalet till fem stycken. Fler ansåg jag inte skulle vara resursmässigt genomförbart.

Med tanke på att intervjuerna skulle utföras med låg grad av standardisering och strukturering, ansåg jag det inte vara lämpligt att utforma ett frågeformulär med precisa och strukturerade frågor. Jag utformade istället ett dokument, med de områden jag ville behandla under intervjuerna, utifrån mina frågeställningar. Detta dokument finns att se i bilaga 2. Ämnesområden skickades till respondenterna ca en vecka före varje intervju för att ge respondenterna möjlighet att tänka igenom sina svar i förväg. Intervjuerna utfördes på respondenternas arbetsplats. Tyvärr fick jag aldrig möjlighet att intervjua någon från norra Sverige. Detta berodde på att jag först hittade en respondent som verkade lämplig, men han avböjde i sista stund, efter att ha läst mina intervjufrågor. Han ansåg sig inte vara lämplig att besvara dem. Vid denna tidpunkt var det för sent att hitta någon ny.

Nedan följer en beskrivning av det som framkom vid intervjuerna. Allt som beskrivs är respondenternas åsikter och inte mina egna. Jag kommer, för att underlätta för läsaren, inte återge intervjuerna ordagrant, utan sammanfattar i stället det som jag anser vara viktigt.

5.1.1 Intervju 1

Intervju 1[4] gjordes med den ADB-säkerhetssansvarige på en kommunal förvaltning i västra Sverige. Fortsättningsvis kallar jag honom Sven[5]. Sven har jobbat med informationssäkerhet i 12 år, men har jobbat med IT ända sedan 1961. Nu ansvarar

[4] Tyvärr glömde jag bandspelaren vid denna intervju. Beskrivningen bygger enbart på anteckningar från mig och en extra observatör.

[5] Alla namn på respondenterna kommer i fortsättningen, av anonymitetsskäl, vara fingerade.

han för den aktuella kommunens informationssäkerhet. Den förvaltning han arbetar på har ca 250 anställda, som alla arbetar med IT-frågor. I den aktuella kommunens säkerhetspolicy står det följande:

> För system i drift vilar ansvaret på de verksamhetsansvariga att risk-bedömningar genomförs regelmässigt. Den ADB-säkerhetsansvarige skall aktivt verka för att riskbedömningar genomförs samt bistå de verksamhetsansvariga med bl.a. metodval i detta arbete.

Det är alltså Sven som är kommunens "riskanalysexpert". Han menar att de största hoten mot kommunens informationssystem är:

- *Dålig tillgänglighet*. Systemens prestanda måste vara så goda att det går att använda dem utan problem.
- *Bristfällig sekretess*. Kommunen får ej bryta mot sekretesslagarna, samtidigt som offentlighetsprincipen inte får hotas.
- *Skandaler*. Det värsta som användarna av systemen tycker kan hända är att exempelvis offentliga handlingar kommer på drift eller att andra händelser, som kan skapa tidningsrubriker, inträffar.

På sikt kommer förvaltningen ta ställning till om man skall certifiera sig mot BS 7799. Sven tror att det kan komma att dröja 1-2 år innan detta ställningstagande görs.

De metoder för riskanalys som Sven känner till är de olika SBA-metoderna[6]. Han har själv varit med och utvecklat SBA Scenario, SBA Projekt och SBA Check. Vad gäller verktyg känner han, förutom SBA Analys, till ett norskt sådant vid namn ISAP, men han har inte använt någon av dessa själv.

I kommunens IT-säkerhetsarbete används enbart SBA Scenario som riskanalysmetod. Något datoriserat verktyg för riskanalys används inte. Anledningen till att man valt SBA Scenario var att det i princip var den enda som fanns att välja på när de började göra riskanalyser. Valet stod då mellan SBA Scenario och en metod som IBM utvecklat på 1970-talet. Dock var IBM:s metod för invecklad för att vara praktisk användbar, menar Sven. Att det finns få etablerade metoder för riskanalys är ett stort problem även idag, fortsätter han. Många företag utvecklar egna metoder som blir företagsspecifika, samtidigt som de vill hålla dem för sig själva.

Anledningen till att Sven fortfarande använder SBA Scenario, trots att det nu finns en datoriserad variant vid namn SBA Analys, är att han anser att gruppdynamiken går förlorad när datorstöd används. Detta tror dock Sven kanske kommer att ändra sig i framtiden, när alla ändå bär med sig handdatorer överallt. Anledningen till att Sven inte enbart använder sig av en stor checklista, som exempelvis SBA Check, är att checklistor oftast är för generella. Detta innebär att de måste anpassas till den aktuella verksamheten, och det är enligt Sven "ett hästjobb". Däremot använder Sven en egen checklista som är baserad på hans samlade erfarenheter. Denna checklista använder han som ett komplement till SBA Scenario.

SBA Scenario går, enligt Sven, till på följande sätt:

---

[6] SBA är en akronym för *sårbarhetsanalys*, och är namnet på Dataföreningens riskanalysprodukter (egen anm.).

1. Man samlar 8-10 personer med olika bakgrund. De olika aktörerna i analysen kan exempelvis vara: användare, IT-experter, verksamhetsansvariga och scenarioledaren (som oftast är Sven).
2. Tydliga avgränsningar görs över vad man skall analysera. Detta steg är mycket viktigt anser Sven. Om man inte tydligt avgränsar sig finns risken att man börjar analysera ett för stort område, vilket medför att man inte hinner bli färdiga på utsatt tid.
3. Aktörerna får sedan tillsammans hitta på olika scenarior över vilka hot som skulle kunna inträffa och hur detta i så fall skulle kunna ske. Man kan exempelvis börja med att varje person får fylla i meningen: "Det värsta som skulle kunna hända är att…", för att hitta lämpliga scenarion.
4. Konsekvenserna av varje scenario bestäms sedan. Till hjälp finns ett antal checklistor. Det finns en checklista för områdena: *Lagar, Avtal, Dåligt rykte, Personal, På sikt* och *Ekonomi*. När alla konsekvenser bestämts summeras dessa i en matris.
5. Sannolikheten för att respektive scenario skall inträffa bedöms. Detta görs på årsbasis, t.ex. scenario 1 inträffar sannolikt en gång vart femte år o.s.v.
6. En bristbeskrivning görs. Här analyserar man vad det är som gör att scenariorna kan inträffa.
7. Skyddsåtgärder föreslås.

Det resultat som SBA Scenario ger är alltså en lista med åtgärdsförslag.

Hela SBA Scenario skall enligt metodens föreskrivningar ta 2 arbetsdagar att genomföra. Detta räcker inte har Svens erfarenhet visat. En så kort analys får aldrig acceptans hos användarna. För att få en riktigt bra analys krävs, enligt Sven, 3 veckors arbete av scenarioledaren. Men detta gör inte Sven allt för ofta. Det som tar längst tid är efterarbetet, d.v.s. att sammanställa resultatet. Normalt ägnas 1 dag till scenariorna, och 2 dagar till sammanställning av resultatet. Men detta arbete tar förmodligen längre tid för en oerfaren analysledare, menar Sven. Kvaliteten på resultatet beror helt på hur många scenarior som görs. Desto fler scenarior, desto bättre resultat.

Den svåraste steget i metoden är, enligt Sven, att bedöma sannolikheter. Att finna hoten är inte så svårt, men sannolikhetsbedömningen blir alltid en gissning. Sven menar att hot som redan inträffat övervärderas nästan alltid vad gäller dess sannolikhet att inträffa igen.

Vid intervjun påpekade jag att metoden inte innehåller något steg för att identifiera de tillgångar som finns. Detta tyckte Sven inte var nödvändigt. Om seminariegruppen är rätt sammansatt så representeras alla tillgångar, menar han. Den person som är ansvarig för något som har ett värde för organisationen vet alltid om vilka dessa är, menar Sven.

På frågan om hur användbart resultatet från SBA Scenario är svarar Sven att hans erfarenhet visat att ca 70% av bristerna kan upptäckas med metoden. De sista 30% återfinns med hjälp av Svens egna checklistor, menar han.

Fördelar med SBA Scenario

En fördel med SBA Scenario är att olika aktörer medverkar. Det är ofta, enligt Sven, en vanlig tjänsteman som föreslår de bästa lösningsförslagen, och inte någon av IT-experterna.

Färdigtryckta analysblanketter medverkar till att risken för att någon detalj glöms bort minskar, exempelvis hålls för vem konsekvenserna är hela tiden åtskilt. Detta ger en stringent behandling av informationen, menar Sven.

En annan fördel med SBA Scenario är, enligt Sven, att den ej kräver lång utbildning eftersom det är en enkel metod. Den är enkel att använda eftersom den ger en steg för steg-beskrivning över vad man skall göra. Det räcker att scenariohandledaren kan metoden bra. Cirka 1 timmes introduktion är allt som behövs för att alla aktörerna skall komma igång. Det som kräver lite mer utbildning är att utvärdera och sammanställa resultatet från analysen. För detta krävs det, enligt Sven, att man kan informationssäkerhet bra.

SBA Scenario är mycket generellt utformad, den kan därmed användas i många olika situationer och branscher. Det behöver inte ens handla om IT-relaterad säkerhet, menar Sven. Dessutom är den billig i inköp, den kostar ca 2500 kr. Då ingår ett häfte som beskriver metoden, samt ett antal analysblanketter.

En annan fördel med SBA Scenario är, anser Sven, att den är en pedagogiskt bra metod. Säkerhetsmedvetenheten ökas hos alla som medverkar seminariet. Man kan säga att man får en säkerhetsutbildning på köpet.

Nackdelar med SBA Scenario

Sven saknar förslag på scenarior i SBA Scenario. Om det fanns skulle det bli lättare för deltagarna i seminariet att komma igång. Det tar alltid en stund innan deltagarna blir "varma i kläderna" och kommer på egna scenarior, säger han. Det vore viktigt att dessa scenarioförslag uppdaterades med jämna mellanrum. Med förlegade förslag riskerar man att leda deltagarna på fel spår. Dessa förslag skulle kunna bygga på verkliga händelser som andra organisationer har råkat ut för, säger Sven.

En annan nackdel, som också bygger på att det är svårt för deltagarna att komma på egna scenarior, är att scenarioledaren måste vara kreativ och lyhörd för att analysen skall lyckas. Metodens utfall hänger därmed mycket på scenarioledarens förmåga. Detta gör att det är svårt att förutsäga analysens kvalitet i förväg, om man inte vet att scenarioledaren har de rätta egenskaperna, menar Sven.

Det tar, som redan sagts, lång tid att sammanställa resultatet av analysen. Detta kan ses som en nackdel. Sven säger att det tar ca 2 dagar för en rutinerad person, och kanske 3 till 4 dagar för en orutinerad. Detta, föreslog jag, skulle kanske kunna avhjälpas med att använda den datoriserade varianten av SBA Scenario; SBA Analys. Sven höll med om detta, med SBA Analys skulle man slippa en del efterarbete. Nackdelen med detta skulle dock vara att rapporterna blev dåliga. Enligt Sven måste rapporten skrivas så att ledningen förstår den. Därför skulle rapporterna som det datoriserade verktyget genererade ändå behöva omarbetas.

När Sven utbildade en grupp kommunala tjänstemän i SBA Scenario, gav han dem i uppgift att göra en analys av sina egna verksamheters informationssäkerhet. Det framkom sedan vid en utvärdering av hur det hade gått, att strukturen på den rapport som metoden framställde inte passade för kommunal verksamhet. Detta ansåg Sven vara en nackdel. För att passa bättre för kommunal verksamhet kanske den skulle behöva modifieras något, menar han.

Till sist påpekar Sven att han tycker SBA Scenario är en mycket bra metod för riskanalys. Strax efter vår intervju skulle Sven kalla samman ett informationssäkerhetsråd

för att diskutera kommunal informationssäkerhet. De kommer vid detta möte göra ett "år 2000"-scenario på låg nivå i verksamheten. Då kommer SBA Scenario användas, avslutar Sven.

5.1.2 Intervju 2

Intervju 2 gjordes med en IT-säkerhetskonsult, som vid tidpunkten för min intervju var inhyrd på deltid av ett stort internationellt tillverkande företag. Fortsättningsvis kallar jag honom Nisse. Nisse har jobbat med informationssäkerhet i 13 år. Han har under denna tid varit informationssäkerhetschef på två stora tillverkande, bland annat på det företag där han nu har sitt konsultuppdrag. Han arbetar enbart med IT-säkerhet[7].

Det hot som är störst mot det aktuella företaget riktas mot tillgängligheten. Om exempelvis ett virusangrepp gjorde att systemen inte blev tillgängliga, skulle detta få stora konsekvenser om detta fick en längre varaktighet. Det skulle kunna bli en katastrof, eftersom det inte finns några manuella rutiner kvar som kan ta över om systemen går ner. Hot mot sekretessen är något mindre besvärande, eftersom informationen som behandlas till största delen inte är känslig för obehörig insyn.

Nisse berättar att riskanalysen bedöms som en av de viktigaste preventiva delarna av informationssäkerhetsarbetet i företaget.

De metoder och verktyg för riskanalys som Nisse känner till är SBA-sviten och en metod vid namn SARA. SARA är en akronym för *Simple to Apply Risk Analysis*, och Nisse var med och utvecklade den i början på 1990-talet. Metoden ägs av en förening vid namn *European Security Forum* (ESF) som har ca 200 stora internationella företag som medlemmar. För att få använda SARA måste man vara medlem i ESF, vilket kostar ca 200.000 kr per år. När man är medlem i ESF är SARA fri att använda. Dessutom får man tillgång till ett stort antal publikationer och nyhetsbrev rörande informationssäkerhet.

SARA har även en "lillebror" vid namn SPRINT. Denna metod är mindre omfattande än SARA. För att avgöra vilken metod (SARA, SPRINT, eller ingen alls) som skall användas finns det en tillhörande metametod, d.v.s. en metod för att välja rätt metod. Det finns en illustration över den i bilaga 3. Metametodens arbetssteg är:

1. *Sorting Procedure*. Först bedöms vilka system i verksamheten som bör analyseras, och i vilken prioritetsordning detta skall ske. Detta är en ren skrivbordsanalys, och tar enligt Nisse ca 3 minuter att genomföra för en kunnig person. En fråga ställs per system och per respektive område: tillgänglighet, integritet och sekretess (CIA)[8]. Exempelvis ställs frågan: *vad händer om systemets tillgänglighet hotas?* Konsekvensen av respektive område bedöms sedan på en femgradig skala. Resultatet av detta steg blir en grovsortering av verksamhetens olika system, med avseende på skattad hög, medium, eller liten påverkan på den verksamhet som betjänas av respektive system/applikation. Utifrån denna lista väljer man vilka system det är viktigast att gå vidare med.

[7] Nisse arbetar således inte med hela informationssäkerhetsproblematiken.

[8] I fortsättningen kommer jag att referera till dessa tre begrepp som *CIA*, vilket är den akronym som verkar vara gängse norm i den litteratur jag läst. Förkortningen kommer från engelskans *Confidentiality, Integrity and Availability.*

2. *Preliminary Business Impact Analysis*. En preliminär analys gör sedan av det valda systemet (vilken också är början av SPRINT). Denna analys blir lite mer detaljerad än den föregående. 6-7 frågor ställs för varje CIA-område. Konsekvenserna bedöms enligt samma 5 -gradiga skala som i föregående steg. Varje konsekvens bedöms alltid som s.k. *worst-case*, d.v.s. den påverkan det skulle få om det allra värsta inträffade. Tillgänglighetsaspekten bedöms med en tidsfaktor, t.ex. hur många timmar eller dagar som systemet maximalt får vara nere. Resultatet summeras sedan på en blankett. Detta steg tar ca 1-4 timmar att utföra, med ungefär 3 personer involverade.
3. *Tool Selection*. Den preliminära analysen ligger till grund för vilken metod som skall användas; SARA eller SPRINT. Beslutet tas av de som har ansvaret för systemet. Anses systemet vara ett *Business Critical System* (BCS) väljs SARA, och anses det vara ett *Business Important System* (BIS) väljs SPRINT. Om systemet inte anses ha någon nämnvärd risk görs ingen mer ingående riskanalys. *Sorting Procedure* blir därmed den enda riskanalys som görs för de system som väljs bort, säger Nisse.

SARA

SARA är, enligt Nisse, en riskanalysmetod som fokuserar på konsekvenser, medan hoten har en underordnad roll. Den utförs i form av ett seminarie där ca 7-10 personer medverkar. Huvuddelen av de deltagande skall vara personer från verksamheten med verksamhetskunskap, personer från *Business Management* som Nisse uttrycker det. Det är dessa som kan fastställa vilka krav verksamheten har på informationen, samt vilka konsekvenser olika typer av störningar kan få. Därtill bör det medverka personer med IT-kunskap, som tekniskt kan applikationen i fråga. De skall stödja *Business Management* i riskanalysprocessen. Till sist skall en seminarieledare samt en assistent vilka kan SARA-metoden medverka.

SARA tar ca 2 dagar att genomföra, säger Nisse. Metodens olika arbetssteg är:

1. *Introduktion*. Ca 1 timmes utbildning av seminariedeltagarna i hur metoden används.
2. *Avgränsning*. Bakgrundsmaterial, beskrivningar, flödesscheman, etc. analyseras.
3. *Scenarior*. Olika scenarior arbetas fram. För varje scenario gör sedan steg 4-7.
4. *CIA grundfrågor*. Ett antal frågor ställs för respektive CIA. Dessa frågor är av *worst-case* karaktär. Frågorna handlar exempelvis om: Typ av *disclosure* för varje viktig informationsresurs; Konsekvenser beroende till vem som informationen kan spridas till o.s.v.
5. *Konsekvensen bedöms*. Detta görs både kvalitativt och kvantitativt. Man försöker att värdera konsekvenserna i pengar, vilket dock inte alltid är så enkelt eller ens möjligt. Dessutom görs en kvalitativ bedömning med en 5-gradig skala, där A är högst och E är lägst.
6. *Sannolikheten bedöms*. Sannolikheten bedöms av deltagarna. Detta görs med en 5-gradig skala från *probable* (A) till *impossible* (E).
7. *Brister bedöms*. Vad som bör åtgärdas i systemet rekommenderas av deltagarna. Konsekvensen och sannolikheten vägs samman. Om exempelvis ett scenario får

två A, d.v.s. både högsta frekvens och tyngsta påverkan, ger detta en indikation på att bristen bör åtgärdas omedelbart.

Dessa steg behöver inte följas exakt. Resultatet av SARA blir en lista med vad som behöver åtgärdas och i vilken ordning detta bör göras. Hur det skall åtgärdas berör dock inte metoden.

Det som ofta tar lång tid, och som är svårt är, enligt Nisse, att kvantitativt (i pengar) bedöma konsekvenser.

Fördelar

Den största fördelen med SARA är, enligt Nisse, att den ger ett bra och användbart resultat. Man får dokumenterat vilka sårbarheter som finns i systemen och man får klara indikationer på vad som behöver åtgärdas, och i vilken prioritetsordning detta bör ske. På köpet marknadsförs behovet av informationssäkerhet bland deltagarna. Nisse menar att efter en genomförd SARA-analys höjs den allmänna säkerhets-medvetenheten hos de som medverkade vid analysen.

En annan fördel är, enligt Nisse, att SARA inte är detaljstyrd utan anpassningsbar. Detta medför att seminarieledaren har frihet att anpassa metodens steg utifrån de aktuella förutsättningarna. Dessutom är den generell till sitt användningsområde. Den passar de flesta branscher, menar Nisse. Man kan i princip analysera vilka risktyper som helst med den.

SARA är också mycket enkel att använda, menar Nisse. Det krävs ingen speciell utbildning i förväg av deltagarna. Det räcker med 1 timmes introduktion.

Nackdelar

En risk med SARA är att seminarieledaren måste kunna metoden och informations-säkerhet bra, eftersom det inte finns några checklistor att stödja sig mot. Därför hänger det slutliga resultatet mycket på seminarieledarens förmåga, menar Nisse. En annan risk som föreligger är att fel avgränsningar görs vid början av seminariet. Om ett för stort område analyseras ökar chansen att man inte hinner bli färdig på utsatt tid, vilket kan medföra att kvaliteten på analysen försämras. T.ex. om man stressar för att hinna klart.

På min fråga om det kan vara svårt för deltagarna att "komma igång" och hitta på egna scenarier, svarar Nisse att så inte är fallet. Han har istället upplevt att det ibland kan vara svårt att få stopp på deltagarna när de har kommit igång. Annars upplever inte Nisse att det finns någon direkt nackdel med SARA, eller att något saknas. När jag påpekade att det inte finns något steg där tillgångarna identifieras, svarar Nisse att detta i princip görs i *Sorting Procedure*, samt i avgränsningarna. Där bestäms vad som är viktigt att analysera.

SPRINT

Om SPRINT väljs har de första frågorna redan ställts i *Sorting Procedure*. SPRINT består enbart av checklistor, vilka systemet kontrolleras mot. Det tar, enligt Nisse, upp till en halv dag att genomföra en SPRINT-analys. Att genomföra denna analys är, enligt Nisse, ett mer rutinmässigt arbete. Checklistan som SPRINT består av är framtagen utifrån resultat som framkommit vid tidigare SARA-analyser, gjorda av medlemmar i ESF.

Även vid en SPRINT-analys skall personer med olika bakgrund medverka. Både IT-experter och personer med verksamhetskunskap bör således vara med, säger Nisse. Det räcker ofta med 3 deltagare. Enligt Nisses erfarenhet ger SPRINT upp till 75% av det resultat som SARA ger, med mindre än 25% av den arbetsinsats som SARA kräver. Resultatet av SPRINT blir, enligt Nisse, annars det samma som från SARA.

OSCAR

OSCAR är ett dokumentations- och rapportverktyg framtaget för att stödja SARA. Verktyget följer strikt SARA-metodens olika steg. Nisse säger att han använt detta verktyg 2 gånger. Ett lämpligt förfarande är, enligt Nisse, att man är 2 personer som leder ett SARA-seminarium. En som leder seminariet, och en som följer upp och noterar kommentarer, värderingar och annan viktig information i en dator med hjälp av OSCAR.

OSCAR ger, enligt Nisse, färdiga rapporter som resultat, samt en mycket bra dokumentation över vad som sagts på seminariet. Om man inte dokumenterar detta omedelbart försvinner mycket av den information som seminariet gav. Resonemangen som leder fram till ett beslut, ett resultat, eller en kommentar innehåller ofta lika mycket viktig information som det som man kom fram till, menar Nisse.

5.1.3 Intervju 3

Intervju 3 gjordes med den informationssäkerhetsansvarige på en stor bank med huvudkontor i östra Sverige. Fortsättningsvis kallar jag honom Olle. Olle har jobbat med informationssäkerhet i 10 år. I den aktuella koncernen har varje linjechef ansvaret för informationssäkerheten. Olles roll består av att ansvara för det regelverk som gäller för hela koncernen, samt att agera som rådgivare och revisor av linjechefernas säkerhetsarbete.

De största hoten mot bankens informationssäkerhet är, enligt Olle, hot mot tillgängligheten. Eftersom bankens kärnverksamhet består av ekonomiska transaktioner, kan bristfällig tillgänglighet i informationssystemen hota hela verksamhetens existens. Ett specifikt tillgänglighetshot är virus, vilket banken ser allvarligt på. Ett annat hot är intrång. Flest intrångsförsök sker från den egna personalen, men det har även förekommit försök till externa angrepp. Inget intrång har enligt Olles kännedom lyckats.

Riskanalyser är, enligt Olle, basen i bankens säkerhetsarbete. Varje verksamhetsområde mäter själva sin informationssäkerhet med en *self-assessment*, d.v.s. självutvärderingar. Dessa utvärderingar ger ett betyg på säkerheten i systemen och åtgärdslistor, vilka sedan är revisionsbara.

De metoder och verktyg för riskanalys som Olle känner till är: SBA Scenario, SBA Analys, SBA Projekt, ISAP, ZERGO och KALLE[9]. De metoder som Olle har använt är ZERGO, KALLE och SBA Projekt. Han har även deltagit vid SBA Scenario seminarier.

[9] KALLE heter egentligen något annat, men pga anonymiteten kan inte rätt namn användas.

KALLE

KALLE är en metod som den aktuella banken tagit fram tillsammans med ett konsultbolag. Den är konfidentiell och Olle kan därför bara beskriva den generellt.

Metoden används för att värdera operationella risker i en verksamhet eller ett projekt. Den består av en checklista som är indelad i olika områden där risker skall värderas. Exempel på områden är katastrofplanering, IT och kriminalitet. Alla verksamheter inom banken måste utföra KALLE. KALLE är mycket konkret säger Olle. Allt bedöms i pengar.

Metoden går till så att man samlar ca 10 personer från den verksamhet som skall utvärderas. KALLE kräver kunskap om verksamheten. Under ledning av en seminarieledare som kan metoden diskuteras sedan varje punkt i checklistan. Detta tar ca 1 dag. Stegen i metoden är:

1. Först tittar man på vilka hot som finns (med hjälp av checklistan).
2. Man fastställer konsekvenserna uttryckt i pengar.
3. Sannolikheten att hotet inträffar bedöms.
4. Vilka åtgärder har redan satts in?
5. Lista över vad som behöver åtgärdas tas fram.

Efter att man analyserat de risker som finns med i checklistan, får man som resultat en lista med vad som behöver åtgärdas och ett betyg (uttryckt i pengar) på hur säker verksamheten/resultatet från det aktuella projektet är för tillfället. Betyget säger i princip hur mycket pengar det kommer att kosta om man inte täcker upp de risker som finns.

Det svåraste med KALLE är att bestämma vad det kostar om hoten inträffar. Hur mycket kostar det egentligen exempelvis om bankens rykte försämras? Men det måste göras eftersom KALLE är helt kvantitativ.

Fördelar

Den största fördelen med KALLE är, enligt Olle, att verksamheterna verkligen värderar sina operationella risker. Man måste räkna med kostnaden för att något kan gå snett, säger han. Dessutom ser man om skyddsåtgärderna är kostnadseffektiva. Det är ju ingen mening att betala mer för skyddsåtgärderna än vad själva konsekvensen kostar, menar Olle.

KALLE är enkel. Det räcker med en 1/2-timmes introduktion av ledaren. Resultatet går dessutom, enligt Olle, snabbt att sammanställa. Det tar ca 1 timme att dokumentera det i Microsoft Excel, säger han.

Nackdelar

KALLE fångar inte upp de tekniska riskerna som kan uppkomma med ny teknik, menar Olle. Metoden ger enbart ett test mot det regelverk som redan existerar (d.v.s. checklistan). Det finns en risk att nya hot, som inte finns med i checklistan, kan missas.

Metoden passar bäst för finansiell verksamhet, menar Olle. Den mäter allt kvantitativt och den handlar mycket om avkastning och värde för företaget. Därför kanske den inte passar andra branscher, tror Olle.

ZERGO

ZERGO är en metod som är framtagen av den engelska firman Zergo. Den består av en metod och en dokumentationsmall som används för analys av de tekniska delarna av IT-projekt och system. ZERGO är en kvalitativ metod som bedömer risker med en 3-gradig skala:

Low risk - Acceptabelt att sätta igång.

Medium risk - Kan sätta igång men de viktigaste åtgärderna måste genomföras först.

High risk - Då får man inte sätta igång.

Metoden kräver IT-experter som kan identifiera alla hot och bedöma riskerna. Detta är ingen metod att sätta i händerna på verksamhetsfolk, menar Olle. Metoden utförs med ett seminarie där 3-4 IT-experter gör följande steg iterativt tills det är klart:

1. Identifiera hot.
2. Bedöma konsekvensen.
3. Bedöma sannolikheten.
4. Vilka skyddsåtgärder finns för tillfället?
5. Den kvarvarande risken bedöms.
6. Slutbetyg sätts

Om det finns några *High risk* kvar måste dessa åtgärdas, och steg 1-6 göras om igen. Det tar ca 3 dagar att utföra en ZERGO-analys. Resultatet av ZERGO blir, enligt Olle svaret på frågan: Hur stora hot finns det om vi implementerar detta system?

SBA Projekt

SBA Projekt är, enligt Olle, ett verktyg som bedömer ett projekts sårbarhet. Verktyget svarar på frågan om projektets organisation är av sådan art att det kan klara de uppställda målen, d.v.s. om projektet går att genomföra?

Verktyget används så att man svarar på ett antal frågor. Därefter bedömer verktyget om projektet är genomförbart, och beskriver varför. Olle säger att frågorna kring själva tekniken är uråldriga, men frågorna om ansvarsförhållande inom projektet och om projektets organisation är mycket användbara. Verktyget är inriktat enbart mot systemutvecklingsprojekt. Således passar den för de flesta branscher, bara det är ett systemutvecklingsprojekt, menar Olle.

Det tar ca 2 timmar att genomföra en analys, och då närvarar projektledaren och beställaren. Verktyget är så enkelt att ingen handledare behövs för att det skall fungera. SBA Projekt är, enligt Olle, en mycket billig försäkring mot att ett projekt skall gå snett utan att man varnats om det.

Verktyget ger, enligt Olle, ett mycket användbart resultat. Hur sannolikt det är att projektet skall lyckas anges i procent, och vilka brister som finns beskrivs.

SBA Scenario

Olle har medverkat vid ett SBA Scenario-seminarie. Han upplevde då att det var en ganska tung metod att jobba med, och att den tog lång tid. Metoden är demokratisk, och det gillade inte Olle. Han anser att det är de som jobbar med informationssäkerhet

som vet bäst vilka skyddsåtgärder som är bäst lämpade vid olika situationer, inte verksamhetsfolk.

Avslutningsvis påpekade Olle att det absolut svåraste steget i alla metoder för riskanalys som han använt är att hitta rätt människor som skall medverka. Kvaliteten på analysen hänger helt på att rätt människor medverkar, menar han.

5.1.4 Intervju 4

Intervju 4 gjordes med en konsult som arbetar med IT-juridik och informationssäkerhet på ett konsultbolag med ca 25 anställda. Företaget ligger i västra Sverige. Fortsättningsvis kallar jag honom Bo. Bo har jobbat med informationssäkerhet i 7 år, och har haft sin nuvarande befattning i 1,5 år.

De verktyg och metoder för riskanalys som Bo känner till är SBA Analys, SBA Safer, IAD (*Interactive Application Development*) och PROPS. Han har använt SBA Analys, SBA Check och SBA Safer. SBA Analys har Bo varit med och påverkat, genom att han skickat kritik till Dataföreningen som utvecklar SBA Analys. Bo använder SBA Analys som standardverktyg vid alla riskanalyser han genomför ute hos kunder.

SBA Analys

SBA Analys är, enligt Bo, ett datoriserat verktyg som bygger på metoden SBA Scenario. De blanketter som ingår i SBA Scenario är inlagda i SBA Analys som formulär. Verktyget är, enligt Bo, byggt med applikationen Microsoft Access som grund, och anpassat med Visual Basic 5 som programmeringsspråk. I bilaga 4 finns skärmbilder som visar hur de olika menyerna och formulären i SBA Analys ser ut.

Totalt brukar de analyser Bo genomför bestå av ungefär 10-12 scenarior, som arbetas fram av en grupp med ca 7-10 personer. De steg som utförs är:

1. *Vad händer?* Först definierar gruppen ett antal tänkbara hot i form av scenarior. Ett antal formulär skall fyllas i verktyget, men detta brukar Bo vänta med tills alla scenarior identifierats. Vad som orsakar varje scenario, och vilka följdverkningar varje scenario får bedöms sedan av gruppen. För varje enskilt scenario görs sedan steg 2-5.
2. *Vad blir konsekvensen?* Konsekvensen av scenariot bedöms utifrån 6 områden: *Lagar, Avtal, Dåligt rykte, På sikt, Personal* och *Ekonomi*. Dessa områden beskrivs var för sig på ett konsekvensblad. På varje konsekvensblad kan man kryssa i rutor för de konsekvenser som stämmer in på det aktuella scenariot. Även egna konsekvenser kan läggas in. Man kan i verktyget välja om man vill jobba kvalitativt eller kvantitativt. Bo arbetar alltid kvantitativt. Det ger bättre resultat anser han. Dock är det, enligt Bo, för omständigt att värdera olika konsekvenser i exakta pengar. Därför använder han något han kallar "leksakspengar", där konsekvenserna bedöms på en skala mellan 1-100. Detta blir som en kompromiss mellan kvalitativ och kvantitativ bedömning. I detta steg bedöms även sannolikheten för att scenariot skall inträffa. Sannolikheten bedöms antingen i frekvens per år, eller kvalitativt med en 4-gradig skala. Om scenariot inträffat tidigare noteras detta.
3. *Slutsumma*. Verktyget räknar fram en slutsumma över scenariots årliga kostnad. Delsummor för varje konsekvensområde redovisas.

4. *Bristbeskrivning*. Deltagarna i seminariet bedömer sedan vilka brister som finns i informationssystemet som gör att scenariot blir möjligt. Bristernas prioritet att åtgärdas bedöms med en 5-gradig skala. Verktyget räknar ut bristernas totala kostnad.
5. *Vilka skyddsåtgärder bör genomföras?* Gruppen föreslår vilka olika skyddsåtgärder som skulle kunna vara möjliga. Varje skyddsåtgärds effektivitet för att förhindra scenariot bedöms med en 4-gradig skala från *Mycket hög* till *Låg*. Varje åtgärd klassificeras som förebyggande, upptäckande, begränsande eller återställande skydd. Man listar även vilka brister som åtgärden skyddar mot. Kostnaden för skyddsåtgärden bedöms också.
6. *Handlingsplaner*. Verktyget redovisar sedan utifrån en kostnadsnyttoanalys vilken skyddsåtgärd som är bäst för varje scenario. När alla scenarior gjorts konsoliderar verktyget alla scenariorna, och redovisar vilka skyddsåtgärder som är bäst totalt. En skyddsåtgärd kan ju åtgärda flera scenarior o.s.v.

Bo brukar inte följa programmet strikt. Det är lättare, anser han, att sätta upp pappers-lappar på en vägg som beskriver scenariorna. Då kan alla deltagarna hela tiden se vad det är man diskuterar, och alla kan se vad alla tycker. Alla deltagare får skriva ner scenarior, sedan tar man bort de som är lika. Bo brukar föra in resultatet från diskussionerna i verktyget under pauserna. Han tycker att man tappar fart om man för in data i verktyget under diskussionens gång. Ett alternativ är att man har en person som enbart för in data i verktyget, men Bo menar att kvaliteten på datan då kan bli sämre. Han tycker det är bäst att föra in datan själv.

Det tar, enligt Bo, ca 1 dag att genomföra en analys med SBA Analys. Det första scenariot brukar ta 1 timme, men sedan går det snabbare när deltagarna blir "varma i kläderna". Det tar sedan 3-4 dagar att sammanställa rapporten. Verktyget genererar, efter en normal analys, en rapport på ca 50 sidor. Då är varje scenario beskrivet.

Bo säger att det inte brukar vara svårt att få deltagarna att hitta på egna scenarior. Det är dock ofta svårt för dem att bestämma det första värdet. Det som alltid är svårast är att bedöma konsekvensen. Därför är det, enligt Bo, viktigt att gruppen innehåller både tekniker, som kan tekniken, och ekonomer som är vana att kvantifiera saker i pengar.

Själva metoden (d.v.s. SBA Scenario) är mycket lätt att använda, tycker Bo. Han har inte upplevt att det har varit svårt att få deltagarna att "komma igång". Dock kräver den att seminarieledaren har förmågan att få folk att prata och att kunna avbryta när diskussionerna skenar iväg. Metoden kräver också att det finns personer med informationssäkerhetskunskap bland deltagarna för att det skall bli ett bra resultat, menar Bo. Det är svårt för oinsatta att föreslå skyddsåtgärder o.s.v. Den kritiska faktorn för om analysen skall bli bra är därmed att få dit rätt folk. Bo anser att det är viktigt att även beslutsfattare medverkar vid seminarierna. På så sätt framgår det tydligare för deltagarna att riskanalysen är ett viktigt arbete, samtidigt som resultaten får större "tyngd".

SBA Analys kostar, enligt Bo, 9.000 kr i inköp och 1.000 kr/år för att få uppdateringar.

Fördelar

Bo tycker att det är bra att man kan välja om man vill arbeta kvalitativt eller kvantitativt. Om man väljer att göra den kvalitativa varianten som kallas för Tio-

Analys, får man, enligt Bo, ett mer grovhugget resultat. Men då brukar man hinna med både seminariet och sammanställa rapporten på en dag. En annan sak Bo uppskattar är att det går att jobba i flera grupper och sedan sammanställa resultatet. Om en grupp är för stor är det effektivt att dela upp gruppen och arbeta åtskilt.

Verktyget och metoden är, enligt Bo, mycket lätt att använda. Det räcker med ca 10 minuters utbildning innan man sätter igång.

Det resultat som verktyget ger är mycket användbart, säger Bo. Dock är det dåligt presenterat. Den automatgenererade rapporten är ändå en bra grund att arbeta vidare på. Det sparar tid gentemot om det skulle gjorts för hand, samtidigt som rapporterna får samma struktur varje gång vilket medför att de blir lättare att läsa, speciellt för beslutsfattarna. Verktyget genererar även grafer som exempelvis illustrerar de olika skyddsåtgärdernas effektivitet. Detta är bra ur läsbarhetssynpunkt, menar Bo.

Verktyget är, enligt Bo, mycket generellt. Han har använt det till allt från riskanalys av informationssäkerhet till problemlösning. Det kan t.ex. användas i systemutvecklingsprocessen för att få fram krav på tänkta system, menar han. Dock kräver det anpassning av verktyget eftersom frågorna ibland blir fel.

Verktyget kan ge historikrapporter, d.v.s. vad som ändrat sig mellan olika analyser. Denna funktion har Bo inte använt men han tror att det kan vara bra för verksamheter som gör upprepade riskanalyser. På så sätt kan man se om säkerheten blivit bättre eller sämre mellan analyserna.

En fördel med SBA Analys gentemot SBA Scenario är, enligt Bo, att man sparar tid på att använda SBA Analys. Alla blanketter finns samlade på ett ställe (d.v.s. i datorn) och rapporten automatgenereras, vilket sparar tid.

I stort tycker Bo att det är en mycket bra metod. vars styrka ligger i att identifiera hot. Det är också lätt att få folk att säga vad de tycker, menar han.

Nackdelar

Det är ofta svårt att få personer att deltaga vid analysen. Det tar en arbetsdag i anspråk och det är inte många som vill avsätta så mycket tid. Bo brukar förlägga analyserna till ett hotell eller liknande. Annars händer det att folk "bara skall gå till sitt rum" och försvinner.

Rapporterna som verktyget skapar kräver, enligt Bo, mycket anpassning för att vara användbara. Rapporterna är inte snygga säger han, men de genereras i en RTF-fil vilket gör att de är lätta att anpassa. Dock tar detta lång tid.

Problemet med att arbeta i olika grupper är att de olika grupperna sätter olika summor på samma saker. Gruppernas bedömningar är alltid konsekventa inom grupperna, men inte mellan grupperna. Därför blir det ofta fel när flera gruppers analyser förs samman. Exempelvis så kanske den ena gruppen sätter 10% högre värden än vad den andra gruppen gör. Därför skulle det vara bra om man kunde gå in och sänka eller höja de olika gruppernas bedömningar överlag, t.ex. om man vill höja alla värden från en grupp med 10%.

Det finns, enligt Bo, ett antal saker som behöver åtgärdas i SBA Analys:

- Programmet slutar att fungera om man förminskar storleken på fönstren. Då måste användaren starta om programmet.

- Ibland försvinner konsekvenser. Det är mycket pinsamt när det händer säger Bo. Han brukar låtsas som om inget har hänt, och hoppas att ingen skall märka det.
- Man kan bara ha ett fönster uppe samtidigt. Detta tycker Bo är dåligt eftersom man exempelvis ofta vill jämföra olika scenarion med varandra.
- Det finns ingen ångra-funktion, vilket gör att om man av misstag trycker på OK-knappen så går det inte att få det ogjort. Programmet sparar arbetet varje gång OK-knappen nedtrycks.
- Verktyget borde vara lättare att anpassa. Det vore bra om det kunde göras med dialogrutor, i stället för att som nu behöva modifiera direkt i databasen.
- Snyggare rapporter. Exempelvis står ordet "Titel" överst på varje sida vilket är oestetiskt och onödigt. Verktyget är dessutom designat för 50 scenarion. Detta innebär att det ibland i rapporten skrivs ut X tomma rader, där X = 50 - (aktuellt antal scenarion).
- Varje scenario är åtskilt. Det vore bättre om man kunde arbeta med flera scenarior parallellt, eftersom många scenarior har många liknande egenskaper. Det blir onödigt dubbelarbete att skriva in samma sak flera gånger, menar Bo.

SBA Check

SBA Check består, enligt Bo, av en stor checklista med frågor riktade mot verksamheten. Man kan även analysera hur en grupp fungerar. Verktyget består av ca 100 frågor som bedöms med en skala från 0-10.

Detta är också ett bra verktyg tycker Bo. Man kan ställa samma frågor till olika personer och sedan väga samman resultatet.

SBA Safer

SBA Safer är, enligt Bo, ett verktyg som försöker väga in alla aspekter av informationssäkerheten på en gång. Detta medför att verktyget blir tungt att använda och kräver en stor arbetsinsats. Det kostar miljoner att genomföra en analys med SBA Safer. Dock ger det ett gediget resultat, menar Bo.

Bo tror inte att SBA Safer kommer att finnas kvar på marknaden så länge till, eftersom det har en för liten målgrupp. Bo har förstått via samtal med Dataföreningen att SBA Safer inte kommer att vidareutvecklas i sin nuvarande form.

5.1.5 Intervju 5

Intervju 5 gjordes med den informationssäkerhetsansvarige på ett statligt verk, med huvudkontor i östra Sverige. Fortsättningsvis kallar jag honom Bengt. Det aktuella verket har sammanlagt 14.000 anställda fördelade på 21 olika myndigheter. Bengt har arbetat med informationssäkerhet i totalt 15 år. Sin nuvarande befattning har han haft i 11 år. Bengts formella titel är huvudman för informationssäkerhet. Denna befattning delar han tillsammans med en annan person. Varje myndighet som verket förfogar över har en egen säkerhetschef. Dessa chefer har ansvaret för varje myndighets informationssäkerhet. Bengts uppgift är att ställa kraven på säkerheten som myndigheterna måste uppfylla, samt att ge metodstöd. Han har även ansvaret för att hålla verkets hotbild uppdaterad. Målet är att alla myndigheter skall jobba mot samma hotbild. Det finns även lokala hotbilder, som inte Bengt kan överblicka.

De största hoten mot verkets informationssäkerhet är, enligt Bengt:

- Insiderbrott
- Yttre angrepp
- Ekonomisk brottslighet
- Strömavbrott

De verktyg och metoder för riskanalys som Bengt känner till är SBA Scenario, SBA Analys och ISAP. SBA Scenario har han använt många gånger, och han har då varit seminarieledare. SBA Analys har han provat några gånger, och ISAP har han funderat på att använda. Dock anser han att ISAP är för komplicerad för att vara praktiskt användbar. Den kräver enligt hans vetskap att man har en heltidstjänst som enbart arbetar med ISAP. Han vet dock att Stockholms Stad och SJ använder ISAP.

På frågan varför han valde just SBA Scenario som riskanalysmetod svarar Bengt att det är den mest välkända och beprövade metoden som han känner till. Några andra anledningar hade han ej.

SBA Scenario

Förr i tiden brukade Bengt genomföra 2 dagars seminarie för varje analys. Nu för tiden får det oftast räcka med 1 dag. Det är bara om det behövs som 1 extra dag utnyttjas. Före varje seminarie brukar Bengt skicka ut en broschyr som beskriver metoden. Detta medför att deltagarna blir bättre förberedda, och mindre tid till utbildning krävs.

Under seminarierna brukar ca 5-7 scenarior per dag hinnas med, säger Bengt. Det tar sedan ungefär 1,5 dag att sammanställa resultatet i en rapport.

Det som är svårast är att bedöma scenariornas sannolikhet, menar Bengt. Ofta brukar Bengt inte lägga så mycket tid på detta. Om ett scenario har hög konsekvenskostnad måste detta åtgärdas oavsett hur sannolikt det är, anser han. Det är även svårt att bedöma konsekvensernas kostnad. Vad kostar det t.ex. om viss information kommer i orätta händer?

Bengt menar att det är viktigt att inte ha för stora seminariegrupper. Då finns risken att någon person kommer i skymundan. Det är bättre att dela upp gruppen om man är fler än 12 deltagare, anser han.

Det resultat som metoden ger är, enligt Bengt, en rapport som föreslår olika skyddsåtgärder. Dessa listas med prioriteter, d.v.s. vilka behöver implementeras direkt och vilka är det inte lika bråttom med. Resultatet är användbart till fortsatt arbete. Metoden ger ej en fullständig analys, anser Bengt. För att definitivt bestämma skyddsåtgärder krävs det en längre detaljstudie.

Det har även hänt att resultatet från analysen inte gått att använda alls, men detta är ovanligt, säger Bengt.

Fördelar

En fördel med metoden är, menar Bengt, att den är generell. Den passar i princip alla typer av verksamheter, det behöver inte ens vara IT-relaterat. Metoden går att vinkla åt det håll man vill, anser han.

Metoden är billig i inköp. Den kostar ca 3000 kr, säger Bengt. Den är också mycket lätt att använda. Det går fort att komma igång. Metoden är dessutom mycket bra på att finna de risker som finns, fortsätter Bengt. Han rekommenderar därför SBA Scenario som metod för riskanalys till sina myndigheter.

Nackdelar

En brist med metoden är, enligt Bengt, att den inte föreskriver hur resultatet skall sammanställas. Detta medför att det tar lång tid, speciellt om man inte är van vid detta arbete sedan tidigare.

Han tycker inte det är så lämpligt att deltagarna diskuterar lösningar, d.v.s. skyddsåtgärder. Det är svårt att bestämma direkt, och det kräver en stor teknisk kompetens, menar Bengt. Han upplever också att deltagarna ofta fastnar i diskussioner kring lösningar, istället för att rikta sin uppmärksamhet mot vilka risker som finns. Därför brukar Bengt styra bort detta moment vid tidsbrist.

Bengt upplever att det ofta svårt att få igång deltagarna att hitta på egna scenarior. Metoden kräver mycket av seminarieledaren, menar han. Ledaren måste ha engagemang och förmåga att avgränsa scenariorna till rimliga storlekar, för att resultatet skall bli bra.

En annan nackdel är, enligt Bengt, att det är så mycket blanketter att fylla i. Det kan ibland bromsa gruppens kreativitet.

5.2 Dokumentstudie

I detta kapitel kommer jag gå igenom de metoder och verktyg för riskanalys jag funnit i olika dokument. För att finna lämpliga dokument använde jag mig av de sökmetoder som jag redogjorde för i metodkapitlet. För de metoder som även innehåller ett verktyg så kommer dessa att beskrivas tillsammans med metoden. Jag tror att det blir mer lättläst på så sätt.

5.2.1 Metoder för riskanalys

MARION

MARION är en fransk metod för riskanalys som *Department of Computer Science* på Rand Afrikaans University i Sydafrika beskriver på sin hemsida.

MARION är, enligt Rand Afrikaans University (1999), en kommersiell metod med tillhörande datorverktyg. Metoden utvecklades 1984 av en fransk organisation vid namn APSAIRD. Sedan 1985 har APSAIRD underhållit två statistiska databaser som innehåller empiriska data angående incidenter och kostnader för informationssäkerhet. Dessa databaser används i metoden som referens för att räkna fram sannolikheter och kostnader för hot. Resultatet av metoden blir en handlingsplan, vilken kallas för ISMP (*Information Security Master Plan*).

Stegen i MARION är enligt Rand Afrikaans University (1999):

1. *Risk Environment*. Denna fas skall motivera för ledningen att det behövs ett fortsatt arbete. Avgränsningar görs och information om organisationen samlas in. Som en del av undersökningen görs en bedömning av vilka organisatoriska begränsningar som kan påverka analysen, och i slutändan påverka ISMP. Exempel

på begränsningar kan vara moral, förmåga att förändras, informationsflöden, beslutsfattande, mål o.s.v.

2. *Impact Analysis*. I denna fas görs scenarion över möjliga händelser som kan hota organisationens informationssystem. Konsekvensen av varje scenario bestäms i relation till respektive CIA-område. Verktyget innehåller en stor mängd scenarion som kan användas till hjälp. Bedömningar kan göras antingen kvalitativt eller kvantitativt.
3. *Risk Audit*. En säkerhetsrevision utförs med hjälp av checklistor för att bedöma den totala säkerhetsnivån i organisationen. Med detta steg får man också en uppfattning om hur mycket resurser som läggs på informationssäkerheten för tillfället.
4. *Risk Resolution*. I detta steg tas ISMP fram, som genereras av verktyget. ISMP innehåller tre delar: budget, planering och ansvar. Verktyget genererar grafik som åskådliggör resultatet. Dessutom innehåller verktyget en ordbehandlingsdel, vilket medger att ISMP modifieras efter organisationens behov. ISMP innehåller exempelvis: beskrivning av scenarior, nuvarande kostnad för säkerheten, beskrivning av begränsningar, detaljerad handlingsplan över vilka skyddsåtgärder som behöver implementeras, samt budget med direkta kostnader och marginalkostnader.

MARION är, enligt Caelli et al (1996), en av de få metoder för riskanalys som har stöd i historiska data.

C:Cure

En förening vid namn DISC har, enligt Humphreys et al (1998), på uppdrag av British Standards Institution tagit fram en skrift där författarna rekommenderar hur en riskanalys bör genomföras för att ett företag skall kunna certifiera sig mot BS 7799. Metoden kallar författarna för C:Cure.

C:Cure består, enligt Humphreys et al (1998), av två processer:

- *Risk Assessment Process*
- *Risk Management Process*

Risk Assessment Process består, enligt Humphreys et al (1998), av följande steg:

- *Asset identification and valuation.* I detta steg identifieras alla tillgångar (inom det avgränsade området som analyseras). Detta görs genom att allting listas som har ett värde för organisationen. Ett värde sätts sedan på varje tillgång som representerar tillgångens betydelse för verksamheten. Informationen som hämtas i detta steg bör komma från de som "äger" tillgångarna, d.v.s. de som verkligen vet tillgångens värde, föreskriver metoden.
- *Threat Assessment.* Här identifieras vilka hot som finns mot tillgångarna. Detta rekommenderas att göras med både intervjuer med anställda, IT-specialister och säkerhetspersonal, samt med hotlistor. Med metoden medföljer checklistor med exempel på vanliga hot och sårbarheter. För varje hot identifieras: 1. Vem eller vad skapar hotet. 2. Vilka tillgångar hotas. 3. Sannolikheten för att hotet skall inträffa.

- *Vulnerability Assessment.* De sårbarheter som finns i det existerande systemet identifieras. Sannolikheten för att ett hot utnyttjar sårbarheten bedöms. Sårbarhetslistor finns till hjälp i detta arbete.
- *Identification of Existing and Planned Security Controls.* De skyddsåtgärder som redan finns implementerade identifieras. Detta görs för att inte onödiga skyddsåtgärder skall implementeras, samt för att undersöka att existerande skyddsåtgärder är berättigade med avseende på systemets nuvarande risker. Dessutom är det viktigt att veta vilka skyddsåtgärder som existerar när nya skall införskaffas, exempelvis med tanke på kompabilitet.
- *Risk Assessment.* Riskerna bedöms utifrån informationen som insamlades i de tidigare stegen. Metoden ger förslag på tre tekniker detta kan göras på. Resultatet blir en lista med riskerna för varje tillgång som identifierats.

Risk Management Process består, enligt Humphreys et al (1998), av följande steg:

- *Identification and Selection of Security Controls.* Utifrån resultatet från Risk Assessment Process ser man vilka risker som måste eller bör reduceras. Riskerna skall reduceras till den nivå som är acceptabel för verksamheten. Detta görs genom att implementera lämpliga skyddsåtgärder. Kostnaden för skyddsåtgärden får inte överstiga konsekvensen av hotet eller sårbarheten. De existerande skyddsåtgärderna tas också i åtanke vid valet av nya skyddsåtgärder. Det medföljer listor med skyddsåtgärder som lämpar sig för olika hot i metoden.
- *Reducing the Risks.* Risker kan reduceras på många olika sätt. Dessa övervägs i detta steg. Exempel på sätt kan vara att undvika risken, flytta risken (t.ex. med en försäkring), reducera hotet, reducera sårbarheten, eller reducera skadan.
- *Risk Acceptance.* Efter att skyddsåtgärderna implementerats återstår alltid risker. Detta beror, enligt Humphreys et al (1998), på att en organisations informationssystem aldrig kan vara helt säkra. Dessutom är det möjligt att vissa tillgångar medvetet lämnats oskyddade. I detta steg identifieras den återstående risken.

C:Cure kan utföras i två versioner. Antingen som *Basic Risk Assessment* eller *Detailed Risk Assessment*. Vilken version man väljer beror, enligt Humphreys et al (1998), på vilket krav på informationssäkerhet som organisationen har. Beroende på vilken version man väljer att göra utförs varje steg mer eller mindre detaljerat. Metoden beskriver vad som skall göras och hur detta skall göras olika beroende på vilken version man väljer. De två olika beskrivningarna finns i bilaga 6. Man kan även välja att kombinera olika delar från de två versionerna, om detta anses vara givande.

Vilka tekniker för riskanalysen som skall användas anger C:Cure inte. Metoden ger dock ett antal förslag på tekniker som användaren kan välja om han/hon vill. Det är dessutom upp till användaren om bedömningarna skall göras kvalitativt eller kvantitativt.

C:Cure kostar £27.50 och finns att köpa på http://www.c-cure.org.

SBA Analys

SBA Analys är, enligt Dataföreningen (1999a), en metod med tillhörande programvara för att finna och analysera brister i informationssäkerheten och ta fram förslag till skyddsåtgärder. SBA Analys är en generell metod och ger möjlighet till såväl val av analysområden (t.ex. ekonomi, kvalitet) som val av hotbilder (t.ex. virus, hacking).

Den baseras på arbetsmetoden SBA Scenario vilken försetts med ett datorstöd för insamling, analys och lagring av data. SBA Analys har dessutom byggts på med funktioner från SBA Safer vilka ger möjlighet att beräkna risker och ta fram rapporter. SBA Analys kan användas för analys av såväl befintlig som planerad verksamhet och datorstöd.

SBA Analys ger, enligt Dataföreningen (1999a), två alternativ över hur analysen kan utföras:

- HuvudAnalys
- TioAnalys

HuvudAnalys ger en analys med sannolikheter och kostnader i numeriska tal. Riskkostnaden kan beräknas med olika valutor. Detta är således den kvantitativa varianten av SBA Analys. TioAnalysen ger, enligt Dataföreningen (1999a), en snabbare analys eftersom sannolikheter och kostnader anges i värden mellan 1 och 10, vilket ger möjligheter till breda och översiktliga analyser. Riskkostnaderna beräknas som ett grovt värde i skalan 1-10. Detta är således den kvalitativa varianten av SBA Analys.

SBA Analys rapportmodul ger, fortsätter Dataföreningen (1999a), direkt vid analysens slut en preliminär rapport separat för varje grupp, samt gemensamt för grupper som arbetar parallellt. Grafiska bilder ingår i rapporterna. Standardrapporten ger bl.a.:

- Dokumentation av deltagare per grupp samt analysobjekt
- Beskrivning och prioritering av scenariorna efter dessas konsekvenser
- Beskrivning och prioritering av bristerna efter dessas bristkostnad
- Beskrivning och prioritering av åtgärderna efter dessas effektivitet mot prioriterade brister

Analysledaren har sedan, enligt Dataföreningen (1999a), möjlighet att redigera rapporten, göra en sammanfattning och skriva in sina rekommendationer.

Pris: *9.500 kr*

Plattform: *Windows 95/98 och Windows NT*

Tillverkas av:

Dataföreningen i Sverige

Box 45153

10430 Stockholm

SBA Check

SBA Check är, enligt Dataföreningen (1999b), en metod med tillhörande verktyg för att identifiera brister i en verksamhet eller brister i ett utvecklingsprojekt. För att en säkerhetsnivå ska kunna upprätthållas krävs, enligt Dataföreningen (1999b), att den ständigt följs upp och aktualiseras. Uppföljning är en aktivitet som ofta upplevs som tråkig och besvärlig att genomföra. Detta faktum leder ofta till att den inte alls genomförs eller inte genomförs på ett systematiskt sätt, menar Dataföreningen (1999b).

SBA Check är, fortsätter Dataföreningen (1999b), en metod för att i första hand möjliggöra en datoriserad uppföljning av en installerad IT-säkerhetsnivå i en löpande verksamhet. Metoden syftar till att besvara följande frågor:

- Fungerar beslutad säkerhetsnivå?
- Finns områden där säkerheten inte fungerar?
- Finns för hög säkerhet inom något område?
- Saknas kunskap om säkerheten inom något område?

Huvudsyftet med SBA Check är, enligt Dataföreningen (1999b), att värdera hur säkerheten fungerar. SBA Check tar inte ställning till om det är rätt säkerhetsteknik som installerats, utan anger endast om vald teknik fungerar. SBA Check kan även användas till att bedöma om ett utvecklingsprojekt innehåller de skyddsåtgärder som krävs enligt verksamhetens policy och riktlinjer.

Som resultat av en genomgång med SBA Check erhålls, enligt Dataföreningen (1999b), ett underlag för beslut om eventuella ändringar i resurstilldelning, bemanning, val av teknologi m.m., för att uppnå önskad säkerhetsnivå.

Vid leverans innehåller SBA Check en stor frågedatabas, fortsätter Dataföreningen (1999b). Användaren bestämmer vilka objekt (delar av verksamheten) som ska analyseras och vilka områden (delar av säkerhetssystemet) som ska prövas. De objekt och områden som ingår i SBA Check finns i bilaga 5.

Användaren kan också, enligt Dataföreningen (1999b), välja vilka hotområden som skall undersökas. För varje hotområde väljer man sedan vilken säkerhetsnivå som ska gälla. Man kan välja mellan hotområdena: *sekretess, tillgänglighet och riktighet.*

Med hjälp av användarens val tar, enligt Dataföreningen (1999b), SBA Check fram ett antal frågor. Efter att frågorna besvarats får användaren svar på om det som granskades verkligen håller den beslutade säkerhetsnivån.

Enligt Larsson (1999) kommer en ny version av SBA Check att komma ut till hösten 1999.

Pris: *3.295 kr*

Plattform: *Windows 95/98 och Windows NT*

Tillverkas av:

Dataföreningen i Sverige

Box 45153

10430 Stockholm

SBA Nyckel

SBA Nyckel är, enligt Dataföreningen (1999c), en analysmodell som gör det möjligt för en verksamhet att analysera vilka nyckelfunktioner och nyckelpersoner det finns inom verksamheten.

Inom alla verksamheter finns en eller flera resurser som har större betydelse för verksamhetens funktion än övriga resurser, menar Dataföreningen (1999c). Om denna resurs inte fungerar kan det innebära att stora svårigheter uppstår för verksamheten. Resurserna kan vara både maskinella och personella.

SBA Nyckel ger, enligt Dataföreningen (1999c), möjlighet att dokumentera och redovisa olika samband, samt att kartlägga ansvarsförhållanden, funktions-uppdelningar och andra problemområden.

Som resultat av en genomgång med SBA Nyckel erhålls ett underlag för beslut för eventuella ändringar i resurstilldelning, bemanning, val av teknik m.m. för att uppnå önskad säkerhetsnivå.

SBA Nyckel är, enligt Dataföreningen (1999c), en generell metod där endast användarens kreativitet begränsar användningsområdena. I handboken ges ett antal beskrivande exempel. Avsikten är att användaren med hjälp av Microsoft Excel (eller annat kalkylprogram) skall bygga sina egna matriser för att redovisa olika samband för t.ex. nyckelpersonal och/eller nyckelfunktioner. Enligt Larsson (1999) medföljer ett färdiggjort Microsoft Excel-kalkylblad vid köp av SBA Nyckel.

Pris: *385 kr*

Tillverkas av:

Dataföreningen i Sverige

Box 45153

10430 Stockholm

5.2.2 Verktyg för riskanalys

SBA Projekt

SBA Projekt är, enligt Dataföreningen (1999d), ett datoriserat hjälpmedel för att tidigt upptäcka tänkbara risker inom ett projekt. SBA Projekt ger också förslag på skydds-åtgärder som kan motverka riskerna. För att ett projekt skall fungera är det, enligt Dataföreningen (1999d), viktigt att på ett tidigt stadium identifiera riskerna i projektet. Utgångspunkten för verktygets riskanalys är de synpunkter och kunskaper som deltagarna i det aktuella projektet har.

Syftet med SBA Projekt är, enligt Dataföreningen (1999d), att identifiera vilka problem som kan komma att uppstå i projektet, och att ge förslag på hur dessa problem kan undvikas eller begränsas. SBA Projekt kan däremot inte användas för att sätta betyg på hur bra projektet bedrivs.

SBA Projekt är, enligt Dataföreningen (1999d), utformat för att användas av projekt-ledare, säkerhetsansvariga, beställare, leverantörer, verksamhetsansvariga och revisorer.

SBA Projekt analyserar, enligt Dataföreningen (1999d), risker inom följande områden:

1. *Projektets storlek.* Har projektet en rimlig storlek i förhållande till tidigare projekt-erfarenhet.
2. *Verksamhetens förutsättningar.* Vilka förutsättningar i form av tidigare erfarenhet och kunskap finns i verksamheten.
3. *Teknologi.* Hur väl förtrogen är den egna organisationen och leverantörerna med den teknologi man väljer för det nya systemet.
4. *Projektorganisation.* Hur organiseras och bemannas projektet.

5. *Projektets förutsättningar.* Vilken är projektets yttre och inre miljö.
6. *Beställarpåverkan.* Vilka problem kan uppstå i relationen med beställaren.
7. *Leverantörens uppdragsbedömning.* Vilka risker kan uppstå för leverantören om man lämnar en offert.
8. *Intern förankring.* Hur väl är den lämnade offerten och ambitionen att "ta ordern" förankrad i den egna verksamheten.
9. *Beställarens uppdragsbedömning.* Finns det några speciella risker med just den här leverantören och hur ser egentligen leverantörsbilden ut.

Vid arbete med SBA Projekt kan man, enligt Dataföreningen (1999d), välja mellan fyra olika typer av sammanställningar avsedda för olika behov:

- *Att genomföra ett projekt.* Denna typ av analys används vid utvalda tillfällen under projektets genomförande för att tidigt upptäcka risker. Den omfattar fråge-områdena 1-5.
- *Att starta ett projekt.* Denna typ av analys används för att i ett tidigt skede upptäcka risker i projektet och risker i relationen till beställare och omfattar fråge-områdena 1-6.
- *Att lämna offert.* Denna typ av analys används i samband med att en offert ska lämnas och den omfattar frågeområdena 1-8.
- *Att utvärdera en offert.* Denna typ av analys används av en beställare som vill utvärdera lämnade offerter och den omfattar frågeområdena 1-5 och 9.

För att genomföra en analys med SBA Projekt samlar man, enligt Dataföreningen (1999d), en grupp där de berörda aktörerna finns representerade. Erfarenheter visar att en insats på högst fyra timmar för en genomgång av SBA Projekt kan bli mycket lönsam. Man får hjälp att tidigt identifiera och åtgärda risker. Därigenom ökar förutsättningarna för att projektet lyckas, menar Dataföreningen (1999d).

SBA Projekt ger även förslag på tänkbara skyddsåtgärder för att lösa identifierade problem, fortsätter Dataföreningen (1999d). Åtgärdsförslagen bygger på erfarenhet. Ett svar med hög riskfaktor leder alltid till att åtgärdsförslag presenteras på bild-skärmen. Åtgärdsförslagen består av en lista ur vilken man kan välja den skyddsåtgärd som passar bäst i den aktuella situationen.

Som resultat av en genomgång med SBA Projekt erhålls, enligt Dataföreningen (1999d), underlag för beslut om eventuella ändringar i projektets resurstilldelning, bemanning, teknologival etc. Resultatet presenteras i form av olika rapporter. Man kan få ut rapporter på alla frågor som besvarats med "Vet ej", en rapport som redovisar en bedömning av risknivån för hela projektet, en rapport som redovisar en riskbedömning för de olika delområdena, rapporter som redovisar speciella risk-områden med åtgärdsförslag m.m. Alla rapporter kan visas på skärm, skrivas ut eller sparas som fil för fortsatt bearbetning i ett ordbehandlingsprogram.

Pris: *4.900 kr*

Plattform: *Windows 95/98 och Windows NT*

Tillverkas av:

Dataföreningen i Sverige

Box 45153

10430 Stockholm

SBA Safer

SBA Safer är, enligt Dataföreningen (1999e), ett verktyg för IT-säkerhetsarbete. Med SBA Safer kopplas riskerna till verksamhetsnära konsekvenser och nyckeltal vilket gör det lättare för beslutsfattare att förstå hur den operativa verksamheten påverkas av negativa händelser inom IT-området.

SBA Safer ger, enligt Dataföreningen (1999e), möjlighet att bedriva säkerhetsarbetet på ett lönsamt sätt genom att kostnaderna för säkerheten vägs mot vinsterna för verksamheten. SBA Safer innehåller stöd för presentation av resultat och rekommendationer samt förslag till handlingsplaner med text och grafik med termer och begrepp som normalt används av beslutsfattarna.

Informationen från en analys med SBA Safer kan, enligt Dataföreningen (1999e), användas som ingångsvärden vid nästa analys. Analysledarens kompetens ökar därmed och nya analyser kan genomföras snabbare och effektivare. Det går även att dela upp en analys i tiden eftersom verktyget lagrar delresultaten. Analysarbetet kan enkelt delas upp i så korta arbetspass att analysdeltagarna endast behöver samlas under kort tid. Det innebär att även mycket komplexa IT-system kan analyseras på ett effektivt sätt, menar Dataföreningen (1999e).

Med programvaran följer, enligt Dataföreningen (1999e), en bristdatabas och en åtgärdsdatabas. Databaserna innehåller vid leverans cirka 1.200 generella brister och åtgärder. Dessa är framtagna och bearbetade av erfarna säkerhetsanalytiker. Avsikten är att användaren skall anpassa och komplettera databaserna med brister och åtgärder som berör den egna verksamheten.

Pris: *14.900 kr*

Plattform: *Windows 95/98 och Windows NT*

Tillverkas av:

Dataföreningen i Sverige

Box 45153

10430 Stockholm

ISAP

Verktyget ISAP nämndes vid ett antal av mina intervjuer. Dock var det ingen av respondenterna som hade någon erfarenhet av detta verktyg. Den enda information jag funnit rörande detta verktyg är från dess hemsida på Internet, vilken drivs av företaget Security Group International, som tillverkar ISAP.

ISAP står för *Information Security Analysis Program* och är, enligt Security Group International (1996), ett PC-baserat verktyg för riskhantering.

ISAP består, enligt Security Group International (1996), av tre moduler:

- Revision
- Riskanalys

- Incidentrapportering

ISAP bygger, enligt Security Group International (1996), på en checklista med 1.592 frågor. Om användaren tycker att det fattas frågor i databasen, går det att lägga in egna. När riskanalysmodulen används ställs frågor uppdelade på CIA-områdena. Dessa frågor skall besvaras med hjälp av strukturerade intervjuer av de anställda. När alla frågor besvarats genererar verktyget en rapport över verksamhetens riskprofil. Rapporten innehåller både text och diagram.

Plattform: *Windows*

Svensk Distributör:

BerNet AB

Svärdsysslevägen 25

18435 Åkersberga

RiscPAC

I boken *Computer Security Products Byers Guide* som utges av CSI fann jag en beskrivning över vilka verktyg för riskanalys det finns på marknaden. Det första verktyget som beskrivs heter RiscPAC.

RiscPAC är, enligt Computer Security Institute (1997), ett verktyg som standardiserar och automatiserar periodiska riskanalyser. Analysen utförs med hjälp av en checklista som presenteras för användaren. Användaren svarar på frågorna och verktyget skapar en fil med svaren i. Denna fil analyseras sedan av verktyget, och rapporter genereras som beskriver verksamhetens riskprofil och föreslagna skyddsåtgärder.

Verktyget innehåller, enligt Computer Security Institute (1997), 18 olika standard-checklistor för olika behov. Checklistorna kan modifieras efter användarens behov. Analysen kan genomföras både kvalitativt och kvantitativt. Vid kvantitativ analys används en traditionell kostnadsnyttoanalys.

Plattform: *DOS, Windows*

Tillverkas av:

Computer Security Consultants, Inc.

590 Danbury Rd.

Ridgefield, CT 06877

U.K.

CORA

CORA står för *Cost of Risk Analysis* och är, enligt Computer Security Institute (1997), ett verktyg för riskanalys som lämpar sig bäst för organisationer med många liknande system. CORA beräknar en kostnadsnyttoanalys för varje system. Sedan tar CORA fram förslag på skyddsåtgärder och räknar ut vilka som ger bäst avkastning. Resultatet exporteras till ett Microsoft Excel kalkylblad.

Plattform: *Windows*

Tillverkas av:

International Security Technology, Inc.

99 Park Ave., 11th F1.

New York, NY 10016-1503

U.S.

The BUDDY SYSTEM

The BUDDY SYSTEM är, enligt Computer Security Institute (1997), ett verktyg som gör det möjligt att utföra riskanalyser för antingen enskilda datorer eller nätverk. Användaren får skapa egna "vad händer om…"-scenarion, för att se vad effekten blir av planerade skyddsåtgärder. Detta bedöms kvalitativt. Computer Security Institute (1997) anser att detta är ett av marknadens mest flexibla och kraftfulla verktyg för riskanalys.

Plattform: *DOS, Windows*

Tillverkas av:

Norman Data Defense Systems, Inc.

3040 Williams Dr., 6th F1.

Fairfax, VA 22031-0461

U.S.

BDSS

BDSS står för *Bayesian Decision Support System* och är, enligt Computer Security Institute (1997), ett verktyg för riskanalys som använder avancerade statistiska algoritmer för att bedöma risken. Verktyget kan dock användas både kvalitativt och kvantitativt. En riskmodell byggs upp som representerar relationen mellan sannolikheter och kostnader, för tillgångar, hot och sårbarheter. Till sist utför verktyget en kostnadsnyttoanalys av användarens föreslagna skyddsåtgärder.

Pris: *$18.000*

Plattform: *DOS, Windows*

Tillverkas av:

OPA, Inc.

765 Baywood Dr., Ste. 327

Petaluma, CA 94954

U.S.

COMPUSEC

COMPUSEC är, enligt Computer Security Institute (1997), ett verktyg som baserar sig på den europeiska standarden INFOSEC. Verktyget identifierar processer, hot m.m. Risker kalkyleras och simuleras med hjälp av trädanalys. Resultatet presenteras grafiskt.

Plattform: *Windows*

Tillverkas av:

Penta 3/P3K

Caleruega 67, 3A

Madrid, 28033

Spain

RiskWatch for Information Systems

RiskWatch for Information Systems är, enligt Computer Security Institute (1997), ett verktyg för riskanalys av informationssystem, som analyserar nätverk, stordatorer och applikationer. Det kan anpassas av användaren. Verktyget är kvantitativt och ger resultaten i grafiska presentationer. Verktyget finns också i en version som enbart rör fysisk säkerhet.

Pris: *$7.500*

Plattform: *DOS, Windows*

Tillverkas av:

RiskWatch, Inc.

900 Bestgate Rd., Ste. 210

Annapolis, MD 21401

U.S.

NetRISK

NetRISK är, enligt Computer Security Institute (1997), ett verktyg som hjälper användaren att identifiera och värdera verksamhetens informationstillgångar, definiera och gradera hoten som finns mot nätverket, samt att rekommendera lämpliga skyddsåtgärder. Verktyget är kvantitativt och gör en kostnadsnyttoanalys.

Pris: *$38.000*

Plattform: *Windows*

Tillverkas av:

Trident Data Systems

5933 W. Century Blvd., Ste. 700

Los Angeles, Ca 90045

U.S.

6 Analys

Utgående från mina frågeställningar kommer jag i detta kapitel analysera den information som samlades in i mitt genomförande.

Jag anser att min huvudfråga inte kräver någon djupare analys. För att svara på den kommer jag att lista alla de olika verktyg och metoder för riskanalys som jag stött på i min undersökning. Detta görs i kapitel 6.22. Det som dock kräver analys är hur bra mitt svar på denna fråga blir. Eftersom jag valt att genomföra en kvalitativ studie, blir svaret på denna fråga ej så generaliserbart att det går att säga att de verktyg och metoder jag funnit är alla som finns. Däremot anser jag mig kunna påstå att det är dessa verktyg och metoder som 5 experter inom svensk informationssäkerhet idag känner till. Som komplement till detta har jag även utfört en dokumentstudie för att finna andra verktyg och metoder för riskanalys, som finns beskrivna i litteratur och på Internet. Syntesen av dessa två undersökningar anser jag bör ge ett bra svar på frågan.

Delfrågorna är de frågor som, enligt mig, bäst besvaras genom mitt metodval. För att analysera vilka fördelar och nackdelar respektive verktyg och metod har, kommer jag att sammanställa det som jag anser kan sägas om varje verktyg och metod utifrån intervjusvaren. Detta kommer att ske i efterföljande underkapitel. Enbart metoder och verktyg som behandlats under intervjuerna kommer att utvärderas. Jag anser inte att det finns någon möjlighet att utvärdera de verktyg och metoder som enbart hittats via dokumentstudien. Det är endast erfarenhet från användande som, enligt mig, kan säga hur bra eller dålig en metod eller ett verktyg verkligen är. För att bedöma vilket resultat de olika verktygen och metoderna ger, anser jag dock att dokumentstudien är användbar.

6.1 SBA Scenario

SBA Scenario är en metod för riskanalys som alla respondenter kände till och hade erfarenhet av. Metoden är, enligt både Sven och Bengt, generell och passar för de flesta branscher. Det behöver inte ens vara IT-relaterad säkerhet som analyseras. Metoden är baserad på scenarior.

SBA Scenario tar ungefär 3 dagar att utföra framkom det vid intervjuerna. Det normala är att 1 dag ägnas åt seminariet, och att 2 dagar ägnas åt att sammanställa resultatet. Enligt Bengt brukar 5-7 scenarior hinnas med per dag. Kvaliteten på resultatet beror på hur många scenarior som görs, menar Sven.

Fördelar

Det allmänna omdömet om SBA Scenario var, hos de flesta respondenterna, att det är en bra metod, som ger ett gott resultat. Den används regelbundet och rekommenderas av både Bengt och Sven.

SBA Scenario upplevdes som enkel att använda. Sven menade att det beror på att den har en steg-för-steg beskrivning över vad som skall göras. Detta medför att risken för att något steg glöms bort minskar, samt att det inte krävs någon större utbildning av användarna. Detta medför att det går snabbt att komma igång. Även Bengt ansåg att den var mycket enkel att använda. Att metoden är lätt anser jag är en stor fördel.

Sven tog upp en annan sak som han ansåg vara bra med metoden, nämligen att olika sorters aktörer medverkar i analysen. Enligt Svens erfarenhet är det ofta en vanlig

tjänsteman som föreslår de bästa lösningsförslagen, och inte IT-experterna. Det tror jag beror på att tjänstemännen har bättre domänkännedom, och därmed större förståelse för verksamhetens processer. Även om en IT-expert kan säga vad som ger det bästa skyddet i teorin, finns det förmodligen verksamhetsspecifika variabler som kan spela in, vilka IT-experten inte har kännedom om. Det kanske t.ex. inte är så stor mening att investera i en dyr brandvägg om de mest kostsamma angreppen sker från den egna personalen.

En annan fördel är, anser Sven, att metoden är pedagogiskt bra. Man får en säkerhetsutbildning av de som deltar i analysen på köpet. Detta är bra, men det gäller för de flesta scenariometoder tror jag. Det är inget som är specifikt för SBA Scenario.

Det är enligt min mening bra att det finns checklistor till hjälp som föreslår konsekvenser, eftersom det kan underlätta för deltagarna att komma på konsekvenser av scenariorna.

Bengt menar att metodens styrka ligger i att finna de risker som finns, därför rekommenderar han den till sina verksamheter. Detta sade Bo också. Bo menar även att metoden är bra för den får människor att säga vad de tycker.

Nackdelar

Både Bengt och Sven har upplevt att det är svårt att få seminariedeltagarna att komma igång att hitta på egna scenarior. Detta tyckte dock inte Bo. Jag tror att problemet hänger på vilka som deltager i seminariet och vem som leder det. Hur som helst vore det nog fördelaktigt med förslag på scenarior, som Sven ville ha. På så sätt skulle det finnas hjälp till hands om det skulle behövas.

Bengt ansåg att en nackdel med SBA Scenario är att det är många blanketter att fylla i. Detta kan ibland bromsa gruppens kreativitet, menar han. Jag kan förstå att detta kan upplevas som ett problem, men det som sägs på seminariet bör dokumenteras. En lösning på detta problem skulle kanske kunna vara att utse en "sekreterare" som sköter all dokumentation.

Sven tycker att det är en nackdel att strukturen på rapporten ej passar för kommunal verksamhet. Jag anser dock att det är praktiskt omöjligt för en metod att passa perfekt för alla typer av verksamheter. Ju mer specifik en metod är, desto mindre blir målgruppen som metoden passar för. Då är det bättre att varje verksamhet anpassar metoden efter sitt eget behov.

Både Sven och Bengt säger att det svåraste i metoden är att bestämma sannolikheterna. SBA-scenario har inga empiriska sannolikheter, detta tycker jag är en svaghet. Om det hade medföljt en lista med vanliga hot och dess ungefärliga sannolikhet, skulle det bli lättare för deltagarna att bedöma sannolikheterna.

En annan svaghet är, tycker jag, att metoden inte har något steg där tillgångar identifieras. Detta medför att en tillgång bör representeras av den person som är ansvarig för tillgången, annars finns risken att den glöms bort. Därför blir det oerhört viktigt att rätt personer deltager i analysen. Analysens resultat hänger även mycket på seminarieledarens förmåga. Detta är något som både Sven och Bengt framhåller.

Både Olle och Bengt anser att det är en nackdel att personer från verksamheten skall föreslå skyddsåtgärder. Det är lätt att fastna i dessa diskussioner, samtidigt som det kräver teknisk kompetens, menar de. Detta håller jag inte med om. Den tekniska kompetensen skall medverka ändå, och om deltagarna fastnar i meningslösa

diskussioner är det ledarens roll att ingripa. Det kan, som tidigare sagts, vara verksamhetspersoner som finner de bästa lösningarna. Därför anser jag att det är bra att skyddsåtgärder diskuteras.

Sven tycker att det tar förhållandevis lång tid att sammanställa resultatet (2-4 dagar beroende på erfarenhet). Nackdelen med SBA Scenario ligger i att den inte föreskriver hur resultatet skall sammanställas, som Bengt påpekar. Detta bidrar till att det kan ta lång tid att sammanställa resultatet, speciellt om man inte har erfarenhet av detta arbete.

Metoden kan också upplevas som tung att arbeta med. Olle hade medverkat vid en analys med SBA Scenario, och han uppskattade inte att metoden var så demokratisk. Han ansåg att det är bättre att IT-experterna sköter valet av skyddsåtgärder. Men det håller jag, som sagt, inte med om.

Bo ansåg att det var en nackdel med metoden att det är svårt att få folk att deltaga. Analysen tar ju en dag i anspråk. Detta tycker jag inte är metodens fel. Det är, enligt mig, den som genomför analysen som har till uppgift att motivera varför det är ett viktigt arbete.

Resultat

Resultatet av SBA Scenario blir en lista med skyddsåtgärder, som seminariedeltagarna föreslagit. Skyddsåtgärderna listas med prioriteter. Enligt Sven hittar SBA Scenario ca 70% av bristerna i systemen. Bengt menar att metoden ej ger en fullständig analys. För att definitivt bestämma skyddsåtgärder krävs en längre detaljstudie, anser han. Men om detta behövs eller ej beror, enligt mig, på kontexten, d.v.s. hur viktigt det är för verksamheten att verkligen finna *alla* risker, skyddsåtgärder o.s.v.

6.2 SBA Analys

SBA Analys är en metod och ett verktyg som bygger på SBA Scenario. Det var enbart Bo som hade erfarenhet av SBA Analys av respondenterna. Bo använder SBA Analys till alla riskanalyser han genomför ute hos kunder.

SBA Analys är ett generellt verktyg och passar, enligt Bo, de flesta branscher. Det tar enligt honom 4-5 dagar att genomföra en analys med SBA Analys. 1 dag för seminariet och 3-4 dagar för att sammanställa resultatet.

Eftersom SBA Analys bygger helt på SBA Scenarios metod, kan man säga att SBA Analys i princip har samma fördelar och nackdelar som SBA Scenario. Därför kommer jag bara ta upp de fördelar och nackdelar som är specifika för SBA Analys i min analys.

Fördelar

SBA Analys är enligt Bo mycket lätt att använda. Det räcker med 10 minuters utbildning för att komma igång. Detta är självklart en fördel.

Man kan välja om bedömningarna skall göras kvalitativt eller kvantitativt i SBA Analys. Detta tycker jag är bra eftersom det ger flexibilitet. Analysen kan göras snabbt och översiktligt, eller mer ingående, beroende på vad som passar det aktuella fallet.

Man kan dela in sig i grupper och sedan konsolidera resultatet, vilket enligt mig är en stor fördel. Bo menar att arbetet blir ineffektivt om gruppen är för stor. Det tror jag

också. Enligt min erfarenhet blir ofta någon person tyst och/eller åsidosatt när grupper är för stora. Detta kan i värsta fall innebära att viktig information inte kommer fram.

SBA Analys automatgenererar rapporten. Detta kan, enligt Bo, spara tid och gör att rapporterna får ett enhetligt utseende, vilket medför att de blir lättare att läsa. Dessutom genereras grafer, som enligt Bo, gör rapporten mer lättläst. Det tycker jag är bra. Det ligger enligt mig mycket i uttrycket "en bild säger mer än tusen ord". Det är intressant att notera att det tar lika lång tid att sammanställa resultatet med SBA Scenario som med SBA Analys, trots att rapporten genereras. Detta tycker jag tyder på att rapporten kanske kräver lite väl mycket anpassning för att vara bra. Dock kan detta bero på individuella olikheter.

Med hjälp av funktionen historik kan man få uppföljning av säkerhetsnivån i verksamheten, om upprepade riskanalyser genomförs. Detta tycker jag är mycket bra. Utan uppföljning är det svårt att veta om rätt skyddsåtgärder implementerats. Dessutom kan man se vilka nya risker som tillkommit, sedan tidpunkten för den senaste analysen.

Alla blanketter finns samlade på ett ställe (i datorn). Detta tycker Bo är bra. På så sätt minskar risken för att någon blankett kommer på avvägar.

Nackdelar

Sven menar att gruppdynamiken går förlorad med ett datorverktyg, men det håller jag inte med om. Om en dator används och bildskärmen projiceras med en projektor, anser jag inte att detta borde innebära något problem.

Det är, enligt Bo, svårt att sammanställa flera grupper eftersom de ofta gör olika bedömningar. Det skulle behövas en funktion där en grupps bedömningar överlag kunde sänkas eller höjas, som Bo påpekar.

En annan nackdel är att det finns ett antal brister i applikationen. Det verkar inte som om utvecklaren (Dataföreningen) lagt ner så mycket resurser på tester av programvaran. Dock tycker jag inte att de brister som Bo påpekade gör att applikationen är oanvändbar. Den största bristen är att konsekvenser ibland kan försvinna. Detta bör åtgärdas omedelbart anser jag. De andra bristerna är av sådan art att de gör arbetet med verktyget onödigt omständigt, t.ex. kan man inte ha flera fönster uppe samtidigt.

Resultat

Resultatet av SBA Analys blir en automatgenererad rapport som beskriver alla scenarior, och redovisar vilka skyddsåtgärder som är bäst. Resultatet baserar sig på en kostnadsnyttoanalys av analysdeltagarnas bedömningar. Grafiska bilder ingår i rapporten.

6.3 SBA Projekt

SBA Projekt är ett verktyg som bedömer ett projekts sårbarhet. Verktyget är baserat på en checklista. SBA Projekt passar, enligt Olle, de flesta branscher så länge det gäller systemutvecklingsprojekt.

Det tar, enligt Olle, ca 2 timmar att genomföra en analys med SBA Projekt. Enligt Dataföreningen (1999d) skall högst 4 timmar behöva läggas på analysen.

Fördelar

SBA Projekt är, enligt Olle, så enkel att använda att ingen handledare behöver vara närvarande vid analysen.

Den stora fördelen med SBA Projekt är, enligt Olle, att ansvarsförhållanden och brister i projektets organisationen bedöms på ett bra sätt. Detta tror jag kan vara mycket lönsamt. Om brister upptäcks på ett tidigt stadium blir konsekvenserna inte lika stora som om de upptäcks för sent, tror jag. Olle menar att SBA Projekt är en billig försäkring mot att ett projekt skall misslyckas. Dessutom går analysen snabbt att genomföra. Det tror jag kan minska motståndet mot att använda verktyget.

Nackdelar

Enligt Olle är frågorna som rör teknik uråldriga, och därmed inaktuella.

Resultat

Verktyget bedömer utifrån svaren på frågorna om projektet är av sådan art att det kan klara de uppställda målen. Det slutliga resultatet blir, enligt Olle, svaret på frågan: går projektet att genomföra med nuvarande resurser? Dessutom bedöms hur sannolikt det är att projektet skall lyckas i procent, och de brister som finns beskrivs. SBA Projekt ger, enligt Dataföreningen (1999d), även förslag på skyddsåtgärder.

6.4 SBA Check

SBA Check är en metod med tillhörande verktyg vars syfte är att identifiera brister i en verksamhets informationssäkerhet. SBA Check baserar sig på en checklista.

Fördelar

Bo anser att SBA Check är ett bra verktyg. Genom att ställa samma frågor till olika personer kan resultatet sammanvägas och ge en bra bild av säkerhetsnivån i verksamheten. Detta tycker jag är bra, men det gäller i princip för alla verktyg och metoder som baseras på checklistor.

Nackdelar

Sven tycker att SBA Check är för generell och kräver mycket anpassning för att passa den egna verksamheten. Risken med checklistor är alltid, anser jag, att de inte ställer för verksamheten rätt frågor. Därför bör man nog alltid räkna med att egen anpassning behöver göras.

Resultat

Som resultat ges, enligt Dataföreningen (1999b), svar på om det granskade systemet håller den beslutade säkerhetsnivån. SBA Check tar inte ställning till om det är rätt skyddsåtgärder som installerats, utan anger endast om vald teknik fungerar.

6.5 SBA Safer

SBA Safer är ett kvantitativt verktyg för riskanalys. Det innehåller, enligt Data-föreningen (1999e), en databas med ca 1.200 brister och åtgärder.

Fördelar

SBA Safer ger, enligt Bo, ett mycket gediget resultat.

Nackdelar

Enligt Bo försöker SBA Safer att väga in alla aspekter av informationssäkerheten på en gång. Det medför att verktyget blir tungt att använda och kräver en mycket stor arbetsinsats, eftersom allt skall kvantifieras i pengar.

Bo tror inte att detta verktyg kommer att finnas kvar på marknaden länge till. Därför är detta verktyg inget jag rekommenderar.

Resultat

Som resultat presenteras, enligt Dataföreningen (1999e), verksamhetens risker kopplade till olika nyckeltal, och handlingsplaner tas fram. Analysen baseras på en djupgående kostnadsnyttoanalys.

6.6 SBA Nyckel

SBA Nyckel är en metod och ett verktyg som analyserar vilka nyckelpersoner och nyckelfunktioner som finns inom en verksamhet. Bedömningarna görs, enligt Data-föreningen (1999c), kvantitativt.

Ingen av respondenterna hade erfarenhet av SBA Nyckel. Därför gör jag inte någon bedömning av dess fördelar och nackdelar.

Resultat

Som resultat av en genomgång med SBA Nyckel erhålls, enligt Dataföreningen (1999c), ett underlag för beslut om eventuella ändringar i resurstilldelning, val av teknik, bemanning o.s.v., för att nå upp till den önskade säkerhetsnivån med avseende på nyckelresurser. Som jag beskrev i kapitel 2.3.4 är nyckelresurser viktiga att skydda. SBA Nyckel verkar vara användbar i detta arbete.

6.7 SARA

SARA är en metod för riskanalys som utvecklats av ESF. För att få använda SARA måste man vara medlem i ESF, vilket kostar 200.000 kr per år. SARA har även, enligt Nisse, en "lillebror" vid namn SPRINT. Denna metod är inte lika omfattande som SARA. För att avgöra vilken metod (SARA, SPRINT, eller ingen alls) som skall användas finns det en tillhörande metametod, d.v.s. en metod för att välja rätt metod. Nisse var med och utvecklade SARA på början av 1990-talet. Därför finns det en viss risk att Nisse inte är objektiv i sina bedömningar om metoden. Tyvärr är Nisse den enda av respondenterna som använt SARA, därför bygger min analys av SARA helt på hans uppgifter.

SARA fokuserar, enligt Nisse, på konsekvenser och inte på hot. Metoden bygger på scenarior. Det tar ca 2 dagar att genomföra analysen.

Fördelar

Den största fördelen med SARA är, enligt Nisse, att den ger ett bra och användbart resultat. Man får ett kvitto på vilka sårbarheter som finns i systemen och man får klara indikationer på vad som behöver åtgärdas, och i vilken prioritetsordning detta skall

ske. Detta är dock ingen egenskap som jag tror är specifik för SARA, det gäller för många metoder för riskanalys.

En annan fördel som Nisse tar upp är att behovet av informationssäkerhet marknadsförs ute i organisationen "på köpet". Nisse menar att efter en genomförd SARA-analys höjs den allmänna säkerhetsmedvetenheten, speciellt hos de som medverkade vid analysen. Detta är inte heller någon egenskap som är specifik för SARA, anser jag.

SARA är inte rigid utan anpassningsbar, menar Nisse. Detta medför att seminarieledaren har full frihet att anpassa metodens steg utifrån de aktuella förutsättningarna. Dessutom är SARA generell till sitt användningsområde. Den passar de flesta branscher, fortsätter Nisse. Man kan i princip analysera vad som helst med den, säger han. Att metoden är anpassningsbar tycker jag är bra. Om en metod är strikt tror jag risken finns att den inte används alls, eftersom den då upplevs som omständlig och tidskrävande.

SARA är också mycket enkel att använda, menar Nisse. Det krävs ingen speciell utbildning i förväg av deltagarna. Det räcker med 1 timmes introduktion.

Det är mycket bra med en metametod tycker jag. På så sätt kan rätt metod/verktyg väljas till varje system. Det är inte kostnadseffektivt att genomföra en stor och tidskrävande analys på ett system som inte är viktigt.

Nackdelar

En risk med SARA är att seminarieledaren måste kunna metoden och informationssäkerhet bra, eftersom det inte finns några checklistor att stödja sig mot. Därför hänger det slutliga resultatet mycket på seminarieledarens förmåga, menar Nisse. En annan risk som föreligger är att fel avgränsningar görs vid början av seminariet. Om för stort område analyseras ökar chansen att man inte hinner bli färdig på utsatt tid, vilket kan medföra att kvaliteten på analysen försämras. Dessa två nackdelar är dock något som jag tror gäller för de flesta scenariometoder.

Några andra nackdelar ser inte Nisse med metoden. Dock tror jag att denna åsikt kan vara färgad av prestigebias, eftersom Nisse själv varit med och utvecklat SARA.

Resultat

SARA ger ej förslag på skyddsåtgärder. Resultatet blir en lista över vilka brister som behöver åtgärdas och i vilken prioritetsordning detta bör göras.

6.8 SPRINT

SPRINT är en metod för riskanalys som består av en checklista, vilken systemet kontrolleras mot. Det tar, enligt Nisse, ca en halv dag att genomföra en SPRINT-analys. Att genomföra denna analys är, enligt Nisse, ett mekaniskt arbete. Checklistan som SPRINT består av är framtagen utifrån resultat som framkommit vid tidigare SARA-analyser, gjorda av medlemmar i ESF.

Enligt Nisses erfarenhet ger SPRINT 75% av det resultat som SARA ger, fast med 25% av den arbetsinsats som SARA kräver. Detta kan ses både som en nackdel och som en fördel anser jag, beroende på vad som är viktigast: att analysen skall gå snabbt eller att den skall hitta alla brister.

Resultat

Resultatet av SPRINT blir, enligt Nisse, detsamma som från SARA: en lista över vilka brister som behöver åtgärdas och i vilken prioritetsordning detta bör göras.

6.9 OSCAR

OSCAR är ett verktyg framtaget för att stödja SARA. Verktyget följer strikt SARA:s steg. Ett lämpligt förfarande är, enligt Nisse, att 2 personer handhaver seminariet. En som leder seminariet, och en som följer upp och noterar resultatet med hjälp av OSCAR.

Resultat

OSCAR ger, enligt Nisse, färdiga rapporter som resultat, samt en bra dokumentation över vad som sagts på seminariet. Om man inte dokumenterar detta omedelbart försvinner mycket av den information som seminariet gav. Resonemangen som leder fram till ett beslut, ett resultat, eller en kommentar innehåller ofta lika mycket viktig information som det som man kom fram till, menar Nisse.

6.10 ZERGO

ZERGO består, enligt Olle, av en metod och en dokumentationsmall som används för analys av de tekniska delarna av IT-projekt och system. ZERGO är en kvalitativ metod. Det tar ca 3 dagar att utföra en ZERGO-analys.

Olle kunde inte säga några fördelar eller nackdelar med ZERGO. Det är intressant att notera att ZERGO:s arbetssteg utförs iterativt. ZERGO är den enda iterativa metoden jag funnit i min undersökning. Om det är en fördel eller nackdel att den är iterativ kan jag ej bedöma.

Resultat

Resultatet av ZERGO blir, enligt Olle svaret på frågan: Hur stora hot finns det om vi implementerar detta system?

6.11 ISAP

ISAP är, enligt Security Group International (1996), ett verktyg för riskanalys som bygger på en checklista.

Ingen av respondenterna hade erfarenhet av ISAP. Därför kan jag inte göra någon bedömning om dess fördelar och nackdelar. Dock hade Bengt valt bort detta verktyg eftersom det verkade för komplicerat att använda. Så det kan man kanske se som en nackdel med verktyget; att det är komplicerat.

Resultat

När riskanalysmodulen används ställs, enligt Security Group International (1996), frågor uppdelade på CIA-områdena. Dessa frågor besvaras med hjälp av strukturerade intervjuer av de anställda. När alla frågor besvarats genererar verktyget en rapport över verksamhetens riskprofil. Rapporten innehåller både text och diagram.

6.12 MARION

MARION är, enligt Rand Afrikaans University (1999), en kommersiell metod med tillhörande datorverktyg. Metoden utvecklades 1984 av en fransk organisation vid namn APSAIRD. Sedan 1985 har APSAIRD underhållit två statistiska databaser som innehåller empiriska data angående incidenter och kostnader för informationssäkerhet. Dessa databaser används i metoden som referens för att räkna fram sannolikheter och kostnader för hot. Bedömningarna kan göras antingen kvalitativt eller kvantitativt. Både scenarion och checklistor används.

Jag kan ej bedöma MARION:s specifika fördelar och nackdelar, men generellt tror jag det är bra med empiriska data. Det visade sig ju i intervjuerna med Sven, Bengt och Nisse att det som var svårast att bedöma är sannolikheter och konsekvenser. Att få stöd av empiriska data i detta arbete tror jag kan underlätta.

Resultat

Resultatet av metoden blir, enligt Rand Afrikaans University (1999), en handlingsplan som automatgenereras av verktyget. Handlingsplanen innehåller tre delar: budget, planering och ansvar. Verktyget genererar grafik som åskådliggör resultatet. Dessutom innehåller verktyget en ordbehandlingsdel, vilket medger att handlingsplanen modifieras efter organisationens behov. Handlingsplanen innehåller exempelvis: beskrivning av scenarior, nuvarande kostnad för säkerheten, beskrivning av begränsningar, detaljerad handlingsplan över vilka skyddsåtgärder som behövs implementeras, budget med direkta kostnader och marginalkostnader.

6.13 C:Cure

En förening vid namn DISC har, enligt Humphreys et al (1998), på uppdrag av British Standards Institution, tagit fram en skrift där författarna rekommenderar hur en risk-analys bör genomföras för att en organisation skall kunna certifiera sig mot BS 7799. Metoden kallas C:Cure.

C:Cure kan utföras i två versioner. Antingen som *Basic Risk Assessment* eller *Detailed Risk Assessment*. Vilken version man väljer beror, enligt Humphreys et al (1998), på vilket krav på informationssäkerhet organisationen har. Beroende på vilken version man väljer att göra utförs varje steg mer eller mindre detaljerat. Vilka tekniker för riskanalysen som skall användas anger C:Cure inte. Metoden ger dock ett antal förslag på tekniker som användaren kan välja om han/hon vill. Det är dessutom upp till användaren om bedömningarna skall göras kvalitativt eller kvantitativt.

Jag kan ej bedöma C:Cure:s specifika fördelar och nackdelar, men generellt tror jag det är bra att man beaktar existerande skyddsåtgärder, vilket görs i C:Cure. Det är onödigt att skydda sig mot sådant som det redan finns fungerande skydd mot. Den återstående risken identifieras i C:Cure. Det finns alltid risker kvar, anser jag. Inga skyddsåtgärder är perfekta och vissa risker lämnas kanske medvetet oskyddade. Därför är det bra att identifiera de återstående riskerna så att de inte glöms bort.

C:Cure är mycket generellt beskriven, anser jag. Den är på gränsen till att vara en modell och inte en metod. C:Cure ger förslag på vilka tekniker som kan användas, men det är upp till varje användare att bestämma detta själv. Om en metod är generell medför det att den förmodligen är svår att använda om man inte har erfarenhet av tidigare arbete med riskanalyser, eftersom det ges så lite stöd i teknikvalet.

Resultat

Resultatet av C:Cure blir att skyddsåtgärder väljs och att riskerna reduceras. Den risk som återstår efter att skyddsåtgärderna implementerats identifieras.

6.14 RiscPAC

RiscPAC är, enligt Computer Security Institute (1997), ett verktyg för riskanalys. Analysen utförs med hjälp av en checklista. Analysen kan genomföras både kvalitativt och kvantitativt. Vid kvantitativ analys används en traditionell kostnadsnyttoanalys.

Resultat

Användaren svarar på frågorna och verktyget skapar en fil med svaren i. Denna fil analyseras sedan av verktyget, och rapporter genereras som beskriver den aktuella riskprofilen. Dessutom föreslås skyddsåtgärder.

6.15 CORA

CORA är, enligt Computer Security Institute (1997), ett verktyg för riskanalys som lämpar sig bäst för organisationer med många liknande system.

Resultat

CORA beräknar en kostnadsnyttoanalys per varje system. Sedan tar CORA fram förslag på skyddsåtgärder och vilka som ger bäst avkastning. Resultatet exporteras till ett Microsoft Excel kalkylblad.

6.16 The BUDDY SYSTEM

The BUDDY SYSTEM är, enligt Computer Security Institute (1997), ett verktyg för riskanalyser av antingen enskilda datorer eller nätverk. Verktyget bygger på scenarior som bedöms kvalitativt. Computer Security Institute (1997) anser att detta är ett av marknadens mest flexibla och kraftfulla verktyg för riskanalys.

Resultat

Vilket resultat The BUDDY SYSTEM ger har jag ej funnit i min dokumentstudie.

6.17 BDSS

BDSS är, enligt Computer Security Institute (1997), ett verktyg för riskanalys som använder avancerade statistiska algoritmer för att bedöma risken. Verktyget kan dock användas både kvalitativt och kvantitativt. En riskmodell byggs upp som representerar relationen mellan sannolikheter och kostnader, för tillgångar, hot och sårbarheter.

Resultat

Verktyget gör en kostnadsnyttoanalys av användarens föreslagna skyddsåtgärder.

6.18 COMPUSEC

COMPUSEC är, enligt Computer Security Institute (1997), ett verktyg som baserar sig på den europeiska standarden INFOSEC.

Resultat

Risker kalkyleras och simuleras med hjälp av trädanalys. Resultatet presenteras grafiskt.

6.19 RiskWatch for Information Systems

RiskWatch for Information Systems är, enligt Computer Security Institute (1997), ett verktyg för riskanalys av informationssystem, som analyserar nätverk, stordatorer och applikationer. Verktyget är kvantitativt.

Resultat

Vilket resultat som verktyget ger har jag ej funnit i in dokumentstudie, dock menar Computer Security Institute (1997) att det presenteras grafisk.

6.20 NetRISK

NetRISK är, enligt Computer Security Institute (1997), ett verktyg som hjälper användaren att identifiera och värdera verksamhetens informationstillgångar, definiera och gradera hoten som finns mot nätverket, samt att rekommendera lämpliga skydds-åtgärder. Verktyget är kvantitativt. Jag tolkar det som att NetRISK används för att göra riskanalys av nätverk, d.v.s. av kommunikationssäkerheten.

Resultat

Verktyget gör en kostnadsnyttoanalys av skyddsåtgärderna.

6.21 Företagsinterna metoder

De företagsinterna metoder för riskanalys som jag stött på i min undersökning är:

- *IAD*. Detta är Cap Geminis metod och den är inte offentlig.
- *PROPS*. Detta är Ericssons metod och den är inte offentlig.
- *KALLE*. Denna metod är företagsintern för den bank där jag var och gjorde intervju 3.
- *Arthur Andersen Risk Assessment Methodology*. Denna metod är företagsintern för Arthur Andersen.

Dessa metoder tar jag inte med i svaret på mina frågeställningar, eftersom de är företagsspecifika, och inte kan användas av någon annan.

6.22 Sammanfattande tabell

I denna tabell listar jag de verktyg och metoder för riskanalys som jag funnit i min undersökning.

Namn	Art	Typ	Kommentar	Pris
SBA Scenario	Metod	Kvalitativ	Använder scenarior.	3.000 kr
SBA Analys	Metod och Verktyg	Kvalitativ och Kvantitativ	Samma metod som SBA Scenario, fast datoriserad.	9.500 kr
SBA Safer	Verktyg	Kvantitativ	Utförlig analys. Kräver stor arbets-insatts.	14.900 kr
SBA Projekt	Verktyg	Kvalitativ	Bedömer ett projekts sårbarhet.	4.900 kr
SBA Nyckel	Metod och Verktyg	Kvalitativ	Analyserar vilka nyckelresurser som finns i verksamheten.	385 kr
SBA Check	Metod och Verktyg	Kvalitativ	Checklista för att finna brister i informationssäkerheten.	3.295 kr
SARA	Metod	Kvalitativ och Kvantitativ	Använder scenarior. Fokus på konsekvenser och inte på hot.	200.000 kr
SPRINT	Metod	Kvalitativ	Checklista.	Ingår i SARA
OSCAR	Verktyg	Kvalitativ och Kvantitativ	Följer SARA strikt.	Ingår i SARA
ISAP	Verktyg	N/A	Strukturerade intervjuer av de anställda m.h.a. checklista.	N/A
MARION	Metod och verktyg	Kvalitativ och Kvantitativ	Använder både scenarion och checklistor. Har stöd av historiska data.	N/A
C:Cure	Metod	Kvalitativ och Kvantitativ	Baserar sig på BS 7799. Mycket generell.	£27.50
RiscPAC	Verktyg	Kvalitativ och Kvantitativ	Checklista.	N/A

CORA	Verktyg	Kvantitativ	Kostnadsnyttoanalys. Lämpar sig bäst för organisationer med många liknande system.	N/A
The BUDDY SYSTEM	Verktyg	Kvalitativ	Använder scenarior.	N/A
BDSS	Verktyg	Kvalitativ och Kvantitativ	Använder statistiska algoritmer för att bedöma risken.	$18.000
COMPUSEC	Verktyg	N/A	Baserar sig på den europeiska standarden INFOSEC. Risker kalkyleras och simuleras m.h.a. trädanalys.	N/A
RiskWatch for Information Systems	Verktyg	Kvantitativ	N/A	$7.500
NetRISK	Verktyg	Kvantitativ	Kostnadsnyttoanalys av kommunikationssäkerheten.	$38.000
ZERGO	Metod	Kvalitativ	Används för analys av de tekniska delarna av IT-projekt och system. Iterativ.	N/A

7 Slutsats

I detta kapitel kommer jag att sammanfatta resultatet av min undersökning. Frågeställningen som jag i denna undersökning ville få svar på var:

- Vilka verktyg och metoder för riskanalys av en verksamhets informationssäkerhet finns det?

Delfrågorna till huvudfrågeställningen var:

- Vilka fördelar och nackdelar har dessa verktyg och metoder?
- Vilket resultat ger de olika verktygen och metoderna?

Jag fann sammanlagt 20 olika verktyg och metoder för riskanalys av en verksamhets informationssäkerhet. Jag kommer inte att räkna upp dessa ännu en gång, utan läsaren hänvisas till tabellen i kapitel 6.22, för det fullständiga svaret på min huvudfråga.

De olika verktygens och metodernas fördelar och nackdelar, samt deras resultat, kommer jag inte heller upprepa i detta kapitel. Läsaren hänvisas till respektive verktygs eller metods underkapitel i kapitel 6 för svaret på delfrågorna. Dock kommer jag nu presentera de generella slutsatser som jag dragit av min undersökning.

De metoder för riskanalys som jag fann bestod nästan alla av i princip samma grundsteg. Det som skiljer dem åt är var fokus ligger, hur risker bedöms och om de är baserade på checklistor och/eller seminarier. Vilken typ av metod som bör väljas beror, menar jag, på hur viktigt det är för verksamheten att informationssäkerheten är hög.

Checklistor går snabbare än scenarior, men ger sämre resultat. Fördelen med checklistor visade sig vara att samma frågor kan ställas till olika personer, och därefter kan resultatet sammanvägas. Risken finns dock att fel frågor ställs, därför behöver checklistor ofta anpassas till den aktuella verksamhetens behov.

Scenariometoderna tar längre tid att utföra, men ger ett mer gediget resultat. Det är bra att olika sorters aktörer medverkar i riskanalysen. Det kan ofta vara tjänstemän, och inte IT-experter, som finner de bästa lösningarna. Dessutom får deltagarna en säkerhetsutbildning på köpet.

Även om det kan tyckas tungt att arbeta med en kvantitativ metod, så anser jag att det inte behöver vara något problem. Även om en metod eller ett verktyg är kvantitativt går det att använda dem kvalitativt. Detta visade sig i intervju 4 där Sven beskriver hur han i SBA Analys hittat på en egen skala, hans "leksakspengar, från 1-100. Detta blir en kompromiss mellan SBA Analys kvantitativa *HuvudAnalys* och den kvalitativa *TioAnalys*.

Det som upplevdes svårast i arbetet med riskanalyserna var att bedöma sannolikheter och konsekvenser. Det visade sig också vara viktigt att göra rätt avgränsningar.

Ett problem är att många företag har egenutvecklade metoder som de inte vill sprida. Ett exempel på detta är metoden "KALLE" som den bank jag intervjuade hade egenutvecklat. Förmodligen finns det många bra metoder och verktyg som inte är tillgängliga på marknaden.

Slutligen vill jag säga att resultatet av de olika metoderna beror mer på vilka som utför dem, än på själva metodernas uppbyggnad. I princip alla mina respondenter har

sagt att det är analysgruppens sammansättning, och analysledarens förmåga och erfarenhet som avgör det slutliga resultatet.

8 Diskussion

I detta kapitel kommer jag diskutera resultatet av min undersökning. Jag tar även upp de erfarenheter jag fått under arbetets gång. Dessutom ger jag förslag på fortsatt arbete.

Jag anser att riskanalyser är en viktig del av informationssäkerhetsarbetet. Två av undersökningens respondenter (Nisse och Olle) menade att riskanalysen är det viktigaste av alla steg i säkerhetsprocessen. Trots detta har det varit mycket svårt att finna vetenskapligt material som behandlar verktyg och metoder för riskanalys. Det tycker jag påvisar att det behövs mer forskning inom området, eftersom det onekligen finns problem i de existerande verktygen och metoderna. I och med att hoten mot informationssäkerheten hela tiden växer, är det viktigt att säkerhetsmedvetenheten i organisationerna höjs. En standard för informationssäkerhet är något jag tror kan medföra att denna medvetenhet ökar. BS 7799 är den standard som verkar få störst genomslag, både i Sverige och internationellt. Tyvärr föreskriver BS 7799 inte hur riskanalysen kan eller bör genomföras. Undersökningens frågeställningar var därmed mycket relevanta, anser jag.

Hur väl jag lyckades att besvara frågeställningarna är svårt för mig att säga. Jag anser själv att mitt förväntade resultat uppfylldes. Dock var det svårt att ge en rekommendation över vilka verktyg och metoder som bör väljas i olika situationer. Därför blev min rekommendation mycket generell. Förmodligen skulle mina frågeställningar besvarats bättre, om mer resurser funnits tillgängliga. En kvantitativ undersökning, exempelvis med enkäter, skulle förmodligen gett ett bättre svar på frågan om vilka verktyg och metoder det finns. Då hade resultatet blivit mer generaliserbart.

Mitt urval av respondenter kunde gjorts på ett bättre sätt. Om fler personer intervjuats som enbart deltagit vid riskanalyser och inte varit analysledare, kanske ett annat resultat erhållits. Det är möjligt att analysdeltagare upplever andra problem med verktyg och metoder för riskanalys än vad analysledare upplever. Det optimala hade varit om jag hade intervjuat personer från båda "lägren".

8.1 Erfarenheter

En lärdom jag drog när jag utförde intervjuerna var att det ibland var svårt att avgöra hur objektiv respondenten var. Trots att intervjuerna genomfördes konfidentiellt upplevde jag ibland prestigebias hos respondenterna. Speciellt när respondenten själv varit med och utvecklat en viss metod eller ett visst verktyg. Dock vet jag inte hur detta skulle kunnat undvikas. Kanske skulle dessa respondenters svar valts bort ur undersökningen, men jag ansåg att viktig information då skulle gått förlorad.

Det visade sig vara svårt att finna dokument rörande verktyg och metoder för riskanalys på Internet. Det tog mycket tid, och gav inte så mycket användbar information. Det visade sig också att det inte fanns speciellt mycket litteratur rörande ämnet.

Rent intervjutekniskt visade det sig vara bra att det närvarade två observatörer vid varje intervju. Det hände vid ett flertal tillfällen att jag kontaktade den extra observatören, när jag var osäker på något svar. Användningen av probes var svår och kräver, tror jag, stor erfarenhet av intervjuer för att fungera bra. Dock tycker jag att "uh-huh"-proben fungerade ypperligt. Den medförde att intervjuerna flöt på bättre,

eftersom respondenten visste när han kunde fortsätta, och att jag förstod vad han hade sagt.

Jag tycker att det var bra att intervjuerna var ostrukturerade. Det medförde att samtalet flöt på ett naturligt sätt, eftersom jag kunde anpassa frågorna efter varje respondent. Det hade i princip varit omöjligt för mig att i förväg bestämma lämpliga frågor, eftersom jag inte visste vad respektive respondent hade erfarenhet av.

8.2 Förslag till fortsatt arbete

Som jag tidigare nämnde var det svårt att finna vetenskapligt material som rörde mitt problemområde. Detta tyder på att mer forskning behövs. Det som, enligt undersökningens respondenter, är svårast i riskanalyser är att bedöma sannolikheter och konsekvenser. Om detta arbete kunde underlättas och/eller förbättras, tror jag mycket skulle vara vunnet. Ett möjligt sätt att åstadkomma detta skulle kunna vara att använda en teknik vid namn *Fuzzy Logic*, som jag stötte på när jag gick en kurs i Objektorienterad Modellering.

Tag en hög med grus, och tag bort ett korn. Är det fortfarande en grushög? Om svaret är ja, tag bort ytterligare ett korn. Om det nu bara finns ett korn kvar, är det då en grushög? När slutar det att bli en grushög? Verkligheten som vi så ofta modellerar är, enligt Penker (1999), full av situationer som liknar grushögen, ändå fortsätter vi att envisas med trubbiga verktyg som endast ger svaren ja/nej, sant/falskt, 1/0 osv. 1964 utvecklade, fortsätter Penker (1999), professor Lotfi Zadeh Fuzzy Logic. Fuzzy Logic är kontinuerlig logik, d.v.s. den fungerar precis som vanlig logik i filosofin eller matematiken men med undantaget att svaren är inte är sant eller falskt, utan svaren ges med sanningshalten noll procent till 100 procent. Påståendet, "han är 50 år och medelålders", är ett påstående som de flesta skulle betrakta som sant, men om det vore en man på 40 år, är det då sant, eller en man på 35 år, var går gränsen? Det finns ingen skarp gräns mellan medelålders eller inte, utan gränsen är vad de flesta skulle kalla "flytande". En "flytande" gräns kan lätt åstadkommas med Fuzzy Logic (se figur 5 i bilaga 1), och användas vid modellering av en verklig företeelse.

Med Fuzzy Logic kan man, enligt Penker (1999), bygga upp ett antal utsagor med bedömningskurvor som kombineras med de logiska operatorerna och, eller, inte. Till Fuzzy Logic finns också en metod samt olika tekniker för att bedöma resultatet (så kallad *defuzzification*). Det vore intressant att undersöka om detta går att applicera på riskanalys. Spontant känns det som att det skulle kunna vara fruktbart. Var går t.ex. gränsen mellan hög och medelstor risk? Fuzzy Logic kanske skulle kunna förbättra skärpan, och underlätta bedömningarna, i de kvalitativa verktygen och metoderna.

Ett annat område som skulle vara intressant att studera närmare är traditionell Risk Management. I min undersökning stötte jag på ett antal metoder för riskanalys som inte var ämnade för analyser av informationssäkerhet. Dessa traditionella metoder kanske skulle kunna användas även till analyser av informationssäkerhet. En studie som kopplade samman traditionell Risk Management med riskanalyser av informationssäkerhet skulle förmodligen vara givande.

8.3 Avslutning

Jag tycker inte att man bör avskräckas av alla potentiella hot, utan i stället se på hoten som en möjlighet till att skapa en positiv förändring. Det visade sig, när jag gjorde mina intervjuer, att säkerhetsarbetet ofta ses som ett nödvändigt ont ute i

organisationerna. Jag menar att det är viktigt att ha en positiv inställning till informationssäkerheten. Det kinesiska tecknet för risk tycker jag är en bra symbol för detta. Det kinesiska språket har, enligt Hamilton (1996), samma symbol för risk som för möjlighet[10]. Symbolen tycker jag kan tolkas som att risker inte ensidigt behöver vara något negativt, utan kan också leda till något positivt. Detta tycker jag man bör ta till vara på genom att noggrant analysera de risker som finns, för att på så sätt se hur riskerna kan åtgärdas eller till och med utnyttjas. Det kan mycket väl vara så att vissa av de existerande skyddsåtgärderna är redundanta, eller skyddar mot hot som inte är någon stor risk längre. Dessutom sätts hela organisationen under "luppen" vid en risk-analys. Detta kan medföra att verksamhetens processer kan förbättras, eftersom miss-förhållanden kan upptäckas när en noggrann granskning av system och processer görs.

Till sist vill jag säga att jag inte tycker att man skall se på säkerhetsarbetet som en kostnad utan som en besparing, vilket det med stor sannolikhet blir om korrekta bedömningar görs i riskanalysen. Om en sådan attitydförändring skulle komma till stånd, tror jag mycket skulle vara vunnet.

[10] Se bild på försättsbladet.

Referenser

Bell, J. (1993) *Introduktion till forskningsmetodik*. Lund: Studentlitteratur.

Bernard, R. (1995) *Research Methods in Anthropology – Qualitative and Quantitative Approaches*. London: AltaMira Press.

Borg, T. Lozano, A. Löfgren, T. Malmgren, S. Palicki, J. (1997) *IT-säkerhet för ditt företag*. Stockholm: Bonnier DataMedia.

British Standards Institution. (1995) *Code of Practice for Information Security Management; BS7799*. London: British Standards Institution.

Broder, J. (1984) *Risk Analysis and the Security Survey*. Boston: Butterworth-Heinemann.

Börjesson, L. (1998) Föreläsning 1998-11-03 på kursen *Informationssamhället, 3p* vid Högskolan i Skövde.

Caelli, W., Longley, D., Shain, M. (1996 [1994]) *Information Security Handbook*. London: Macmillan Press LTD.

Cohen, F. (1995) *Protection and Security on the Information Superhighway*. New York: John Wiley & Sons.

Computer Security Institute. (1997) *Computer Security Products Byers Guide*. San Fransisco: Computer Security Institute.

Computer Security Institute. (1998) *1998 CSI/FBI Computer Crime and Security Survey*. San Fransisco: Computer Security Institute.

Computer Sweden. (1998) *Nr 104*. Stockholm: IDG Communications.

Computer Sweden. (1999) *Nr 17*. Stockholm: IDG Communications.

Dahmström, K. (1996) *Från datainsamling till rapport – att göra en statistisk undersökning*. Lund: Studentlitteratur.

Dataföreningen. (1999a) *SBA Analys*. As is 1999-04-15 http://www.dfs.se/sba_analys.htm

Dataföreningen. (1999b) *SBA Check*. As is 1999-04-15. http://www.dfs.se/sba_check.htm

Dataföreningen. (1999c) *SBA Nyckel*. As is 1999-04-15 http://www.dfs.se/nyckel.htm

Dataföreningen. (1999d) *SBA Projekt 3.0*. As is 1999-04-15 http://www.dfs.se/sba_proj2.htm

Dataföreningen. (1999e) *SBA Safer*. As is 1999-04-15 http://www.dfs.se/safer.htm

Ernst & Young. (1997) *Information Security Survey*. As is 1999-03-01 http://www.dsv.su.se/~fred/survey97.pdf

Gilbert, I. (1995) Guide for Selecting Automated Risk Analysis Tools. I Hutt, A.E., Bosworth, S., Hoyt, D.B. (eds) (1995) *Computer Security Handbook*. New York: John Wiley & Sons.

Hamilton, G. (1996 [1985]) *Risk Management 2000*. Lund: Studentlitteratur.

Hemeren, P. (1999) Föreläsning 1999-01-26 på kursen *Examensarbete i ADB, 20p* vid Högskolan i Skövde.

Holme, I.M., Solvang, B.K. (1991) *Forskningsmetodik - Om kvalitativa och kvantitativa metoder*. Lund: Studentlitteratur.

Humphreys, E. Moses, R. Plate, A. (1998) *Guide to BS 7799 Risk Assessment and Risk Analysis.* London: British Standards Institution.

Hutt, A.E., Bosworth, S., Hoyt, D.B. (eds) (1995) *Computer Security Handbook*. New York: John Wiley & Sons.

Hutt, A.E. (1995) Management´s Role in Computer Security. I Hutt, A.E. et al. *Computer Security Handbook.* New York: John Wiley & Sons.

ITSEC. (1991) *Harmonized Criteria version 1.2*. London: Department of Trade and Industry.

Informationstekniska standardiseringen. (1994) *Terminologi för Informationssäkerhet – Rapport ITS 6.* Stockholm: Informationstekniska standardiseringen.

Johansson, M. (1998) Säkerhetsmekanismer. I SIG Security. (1998) *Säkerhets-arkitekturer*. Lund: Studentlitteratur.

Kjaer, M. (1995) *Kvalitativa metoder – för samhälls- och beteendevetare*. Lund: Studentlitteratur.

Larsson, O. (1999) Telefonintervju 1999-05-11 med Orvar Larsson som är ansvarig för SBA-sviten på Dataföreningen.

Olovsson, T. (1998) Introduktion till Säkerhet. I SIG Security. (1998) *Säkerhets-arkitekturer*. Lund: Studentlitteratur.

Patel, R. Davidson, B. (1994) *Forskningsmetodikens grunder – Att planera, genomföra och rapportera en undersökning*. Lund: Studentlitteratur.

Penker, M. (1999) *Fokus på Fuzzy Logic*. As is 1999-05-12 http://www.astrakan.se/utbild/html/artiklar.htm

Pfleeger, C. (1989) *Security in Computing*. New Jersey: Prentice-Hall.

PricewaterhouseCoopers. (1998) *Technology Forecast: 1999.* California: Pricewater-houseCoopers Technology Centre.

Rand Afrikaans University. (1999) *MARION*. As is 1999-04-15 http://www.pix.za/irc/marion.htm

Repstad, P. (1993) *Närhet och distans – kvalitativa metoder i samhällsvetenskap*. Lund: Studentlitteratur.

Security Group International. (1996) *Information Security Analysis Program*. As is 1999-04-30 http://www.isapc.com/isapc.htm

SIG Security. (1997) *Riktlinjer För God Informationssäkerhet – SSR97ETT*. Lund: Studentlitteratur.

Silberschatz, A. Galvin, P. (1998) *Operating System Concepts*. Reading: Addison Wesley Longman Inc.

Statskontoret. (1998a) *Sammanhållen strategi för samhällets IT-säkerhet*. As is 1999-01-01 http://194.251.183.23:81/sakerhet/sakerhet.htm

Statskontoret. (1998b) *Bilaga 10 – Certifiering av IT-verksamheter*. As is 1999-01-01 http://194.251.183.23:81/sakerhet/sakerbil.htm

STG – Allmänna Standardiseringsgruppen. (1998) *Företagsledningen och informationssäkerhet*. Stockholm: STG – Allmänna Standardiseringsgruppen.

Överstyrelsen för civil beredskap. (1999) *År 2000-omställningen*. As is 1999-03-04 http://www.ocb.se/detaljerad/millennieskiftet/Y2K.html

Förkortningar

CIA ……...……..Confidentiality, Integrity, Availability
CSI ……..…….Computer Security Institute
ESF …….European Security Forum
IT……..……...Informationsteknik
ITS…….Informationstekniska standardiseringen
ITSEC……..……Information Technology Security Evaluation Criteria
N/A……..Not available
STG …….Allmänna standardiseringen

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

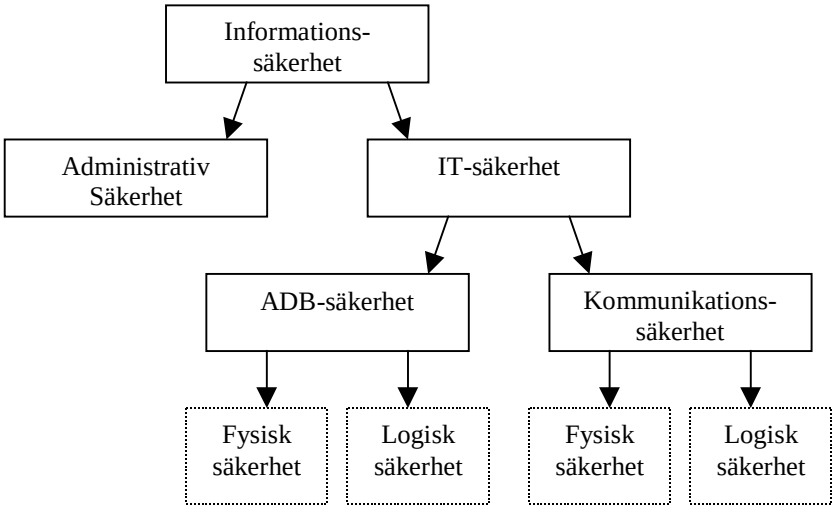
U

V

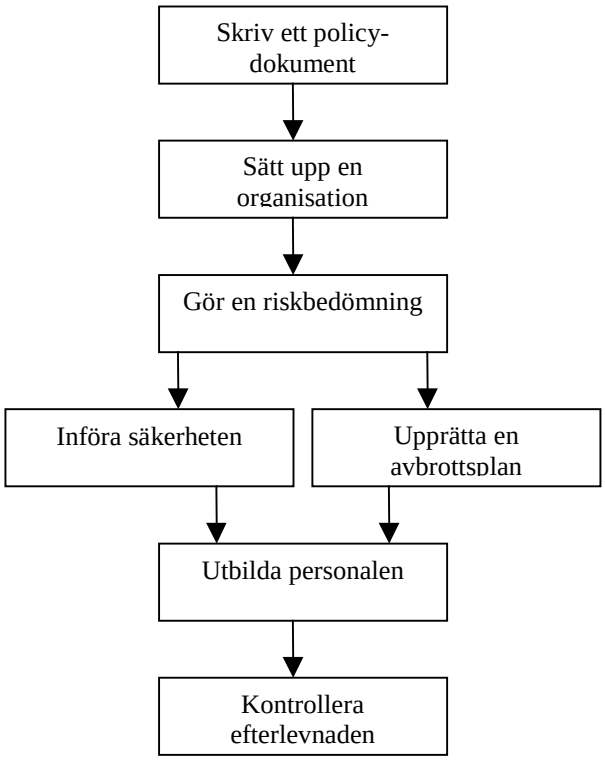
Z

Å

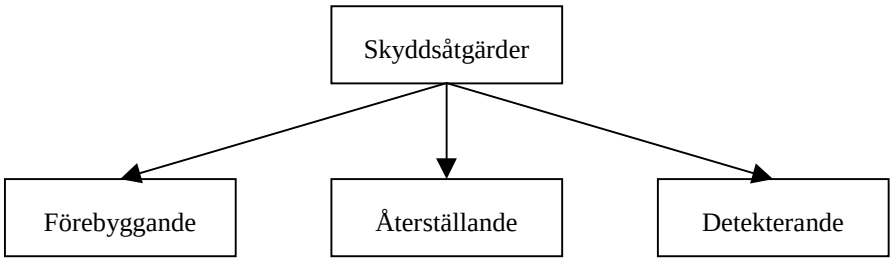
Bilaga 1 Illustrationer



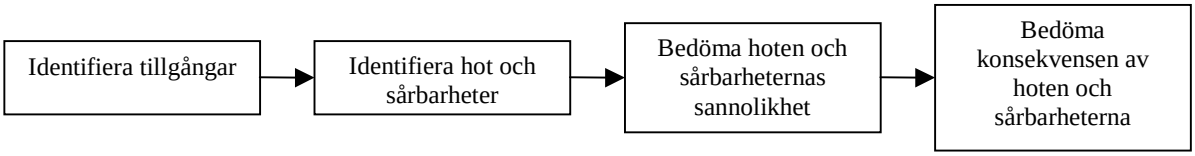
Figur 1: Inbördes förhållande mellan de begrepp som ingår i informationssäkerhet (SIG Security, 1997:xiii).



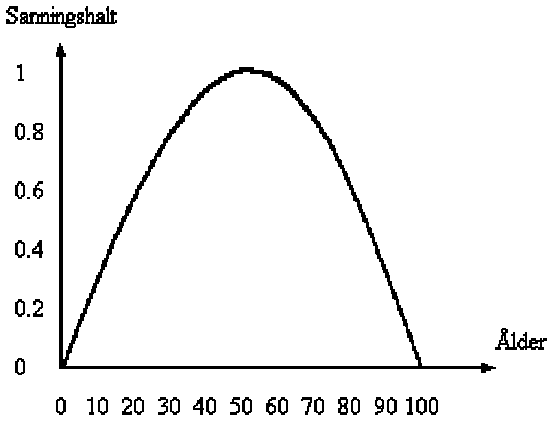
Figur 2: Process för god informationssäkerhet (STG – Allmäna standardiseringsgruppen, 1998:7).



Figur 3: Klassificering av skyddsåtgärder.



Figur 4:Grundläggande moment i riskanalys.



Figur 5: Diagrammet visar hur sant det är att en viss person är medelålders vid en viss ålder. Exempelvis är det 0.9 sant att en person som är 40 är medelålders. Ett diagram som visar sanningshalten för ett påstående kallas för ett fuzzy set. Dessa kan kombineras till avancerade utsagor (Penker, 1999).

Bilaga 2 Intervjufrågor

- Vilka olika verktyg och metoder för riskanalys känner Ni till?
- Vilka olika verktyg och metoder för riskanalys har Ni använt Er av?
- Varför valde Ni just dessa metoder eller verktyg?
- Kan Ni beskriva hur metoden är uppbyggd och vilka olika moment som ingår i den, alternativt hur verktyget används.
- Hur använde Ni verktyget eller metoden?
- Vilket resultat ger verktyget eller metoden?
- Vilka fördelar och nackdelar har dessa verktyg och metoder? Exempelvis med avseende på:

  Hur lång tid tar de att utföra?

  Är de komplicerade att använda, och krävs det mycket utbildning?

  Är de generella eller specifika - (strikt bestämda arbetssteg, eller göra hur man vill)?

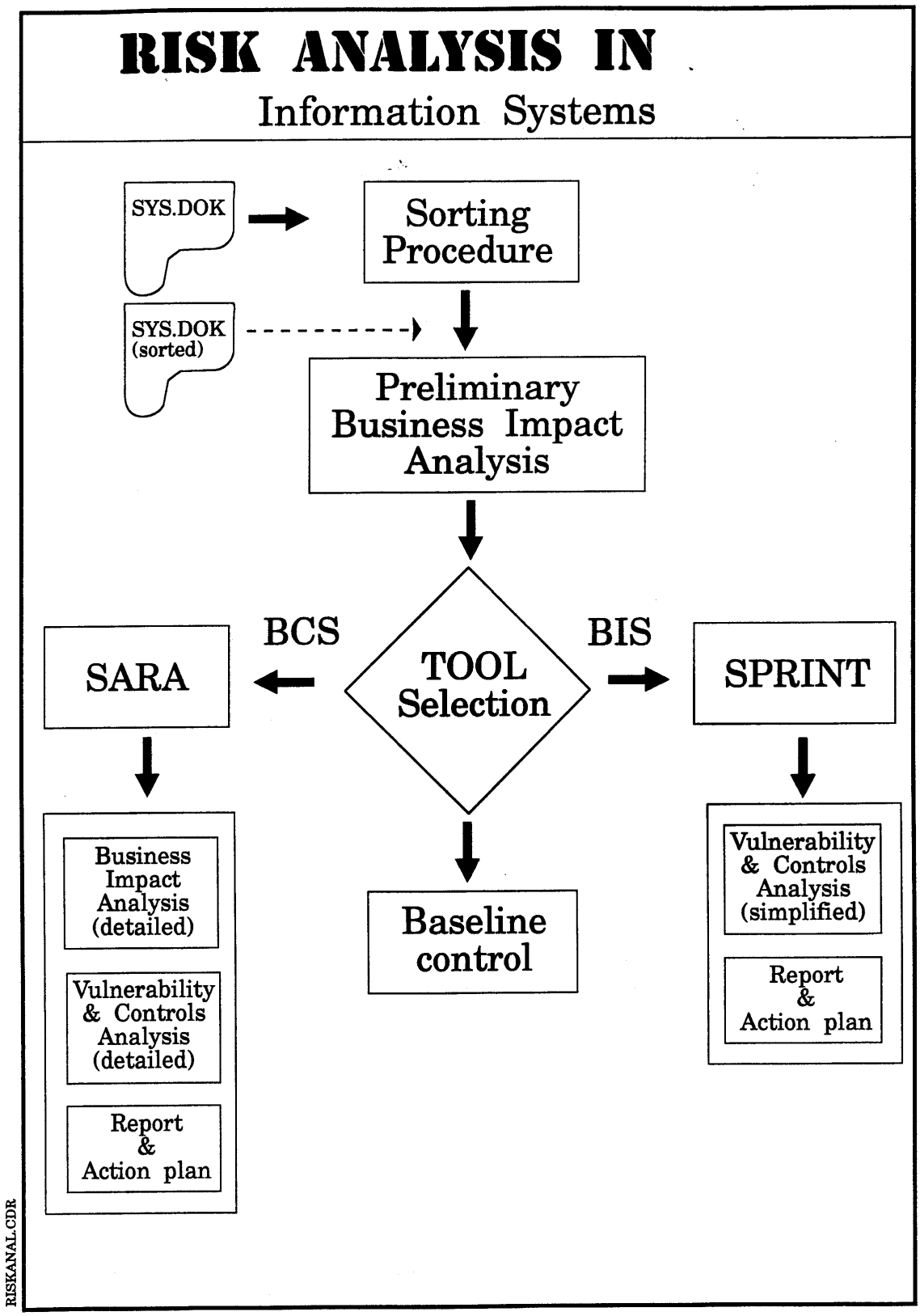
  Vad kostar den i inköp?

  Hur användbart är det resultat som verktyget eller metoden ger?

  Gav verktyget eller metoden det resultat som Ni förväntat Er?

  Om inte - vad saknades?
- Passar de olika verktygen och metoderna för någon speciell typ av bransch eller verksamhet?

Bilaga 3 SARA:s metametod



Bilaga 4 SBA Analys

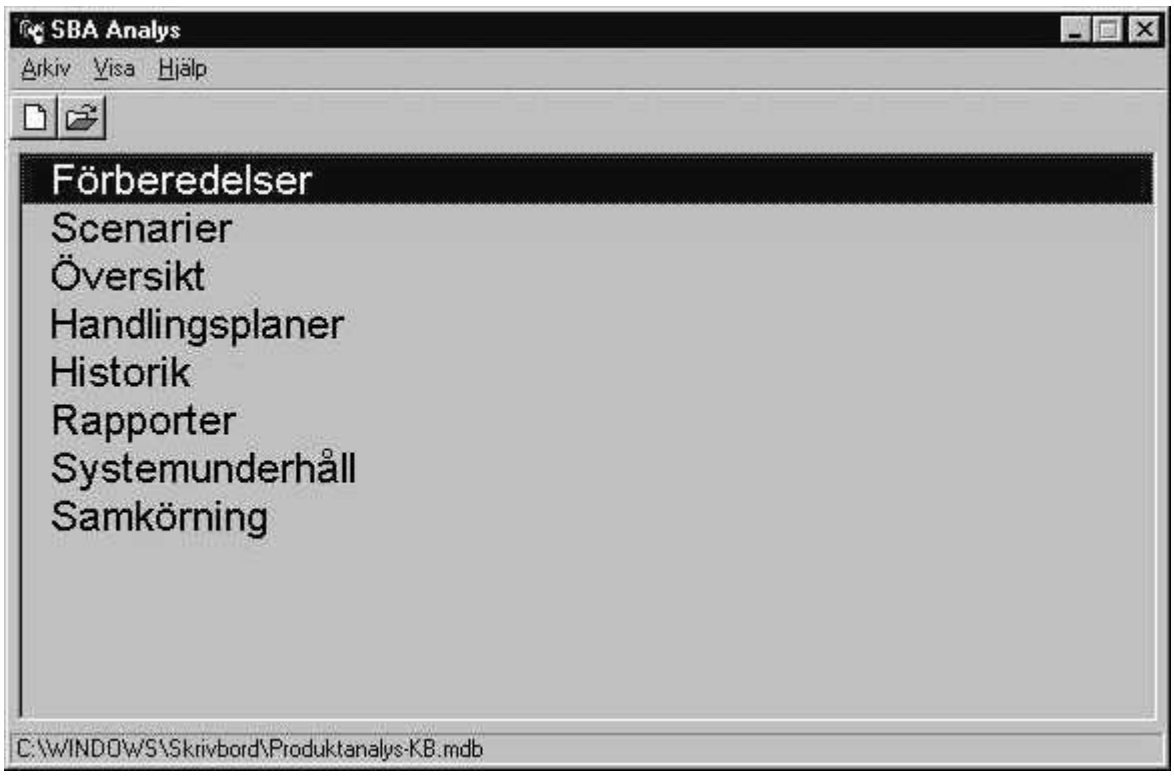


Bild 1: Startmenyn.

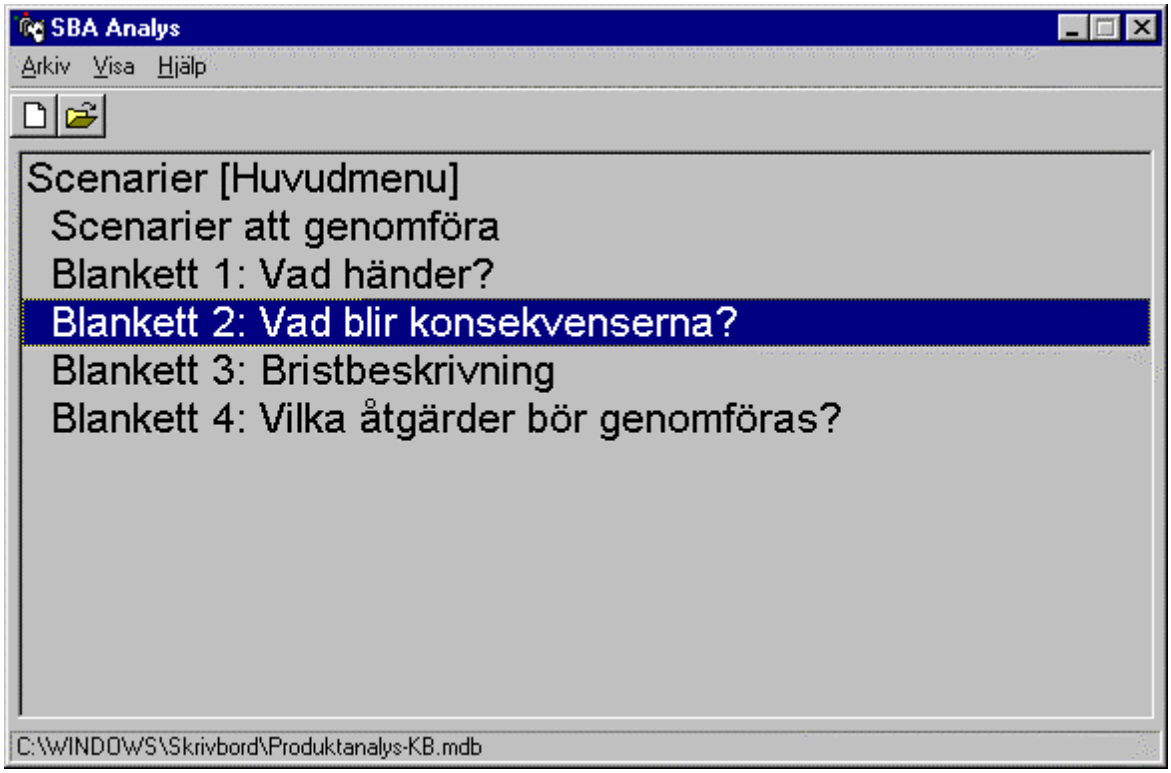


Bild 2: Huvudmenyn för scenarierna.

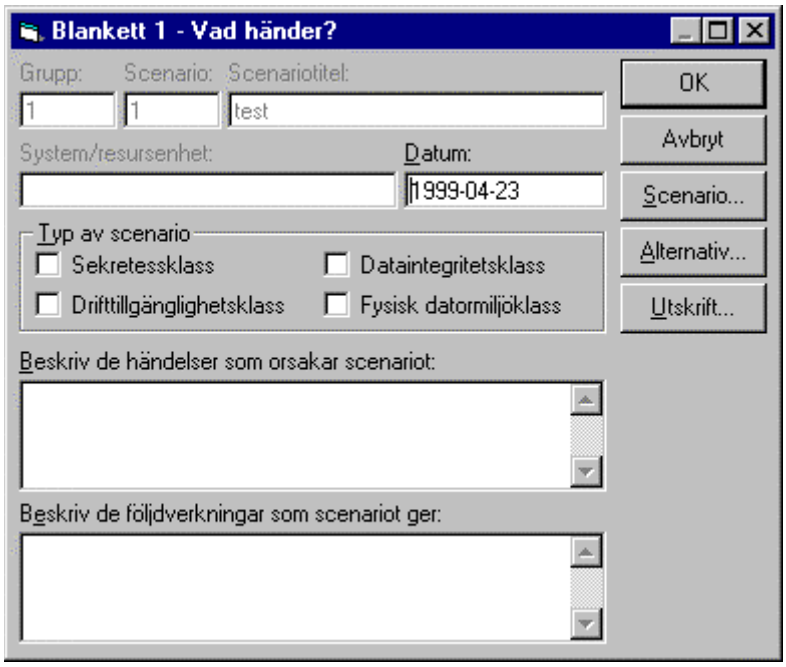


Bild 3: Scenariot definieras.

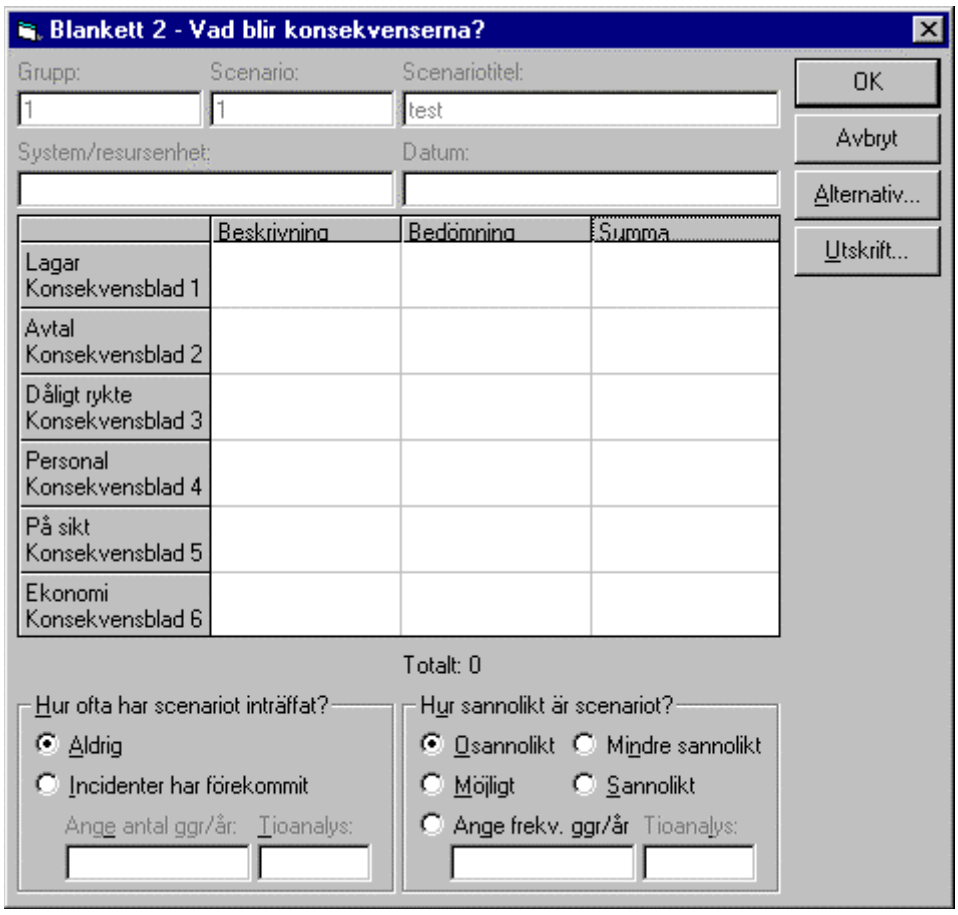


Bild 4: Konsekvensen av scenariot bedöms.

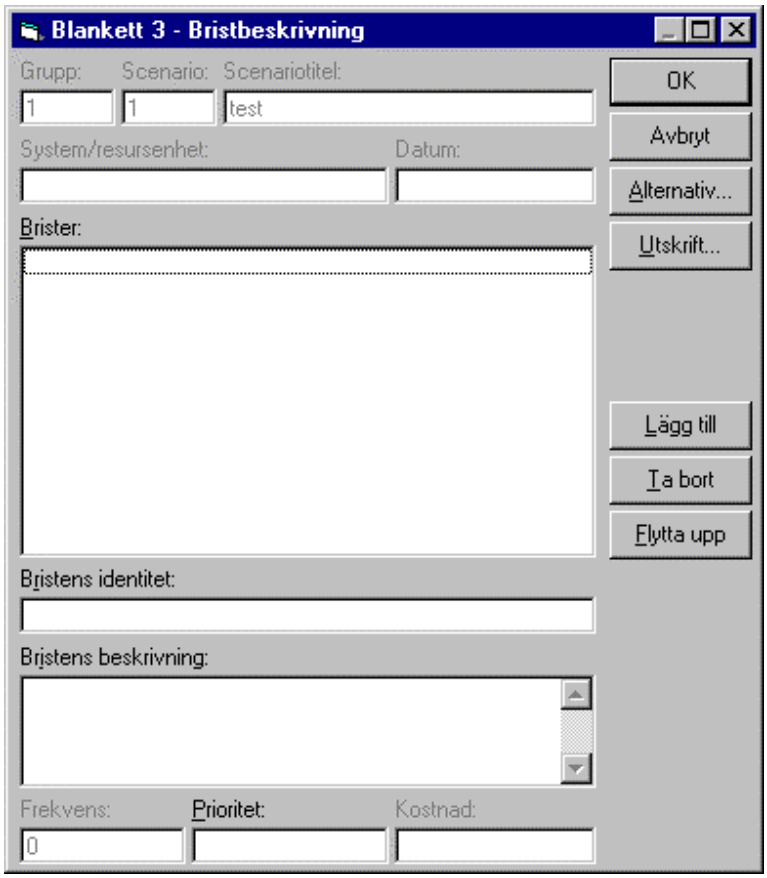


Bild 5: Bristerna i systemet beskrivs.

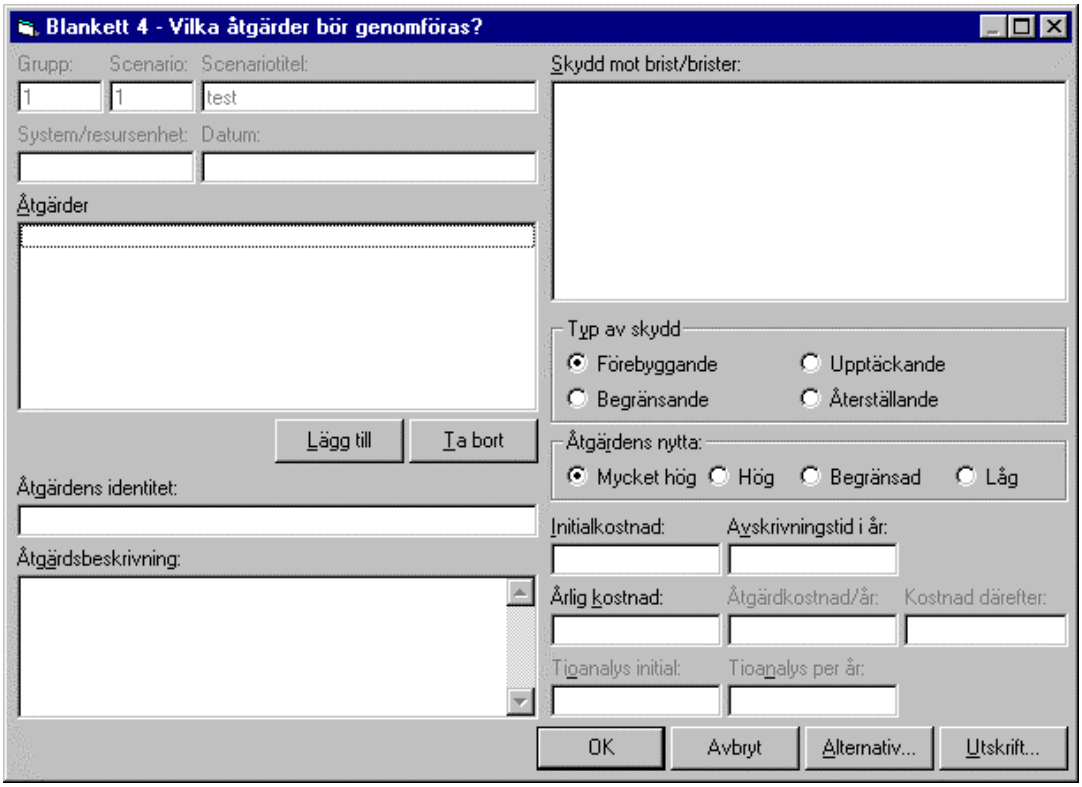


Bild 6: Tänkbara skyddsåtgärder listas.

Bilaga 5 Objekt och områden i SBA Projekt

Maskinvara:

Nät

LAN-server

Lokaldator

Stordator

Arbetsplats

PC-standalone

Bärbar dator

Programvara:

Operativsystem

Basprogramvara

Tillämpning

Data

Lokaler:

Arkiv

Datorhall

Serverrum

Skrivarrum

Organisation:

Utvecklingsorganisation

Driftsorganisation

Förvaltningsorganisation

Användarorganisation

Fysiskt skydd:

Tillträdesskydd

Elskydd

Brandskydd

Vätskeskydd
Klimatskydd

Förvaltning/Drift:
Datamedia
Inregistrering
Drift
Säkerhetskopiering
Återstart
Utskriftshantering
Felhantering
Ändringshantering
Test
Driftsättning
Dokumentation

Åtkomstskydd:
Identifiering
Åtkomstkontroll
Logg
Administration

Övrig säkerhet:
Säkerhetsorganisation
Avbrottsplanering
Datavirusskydd
Kryptering
Förändringsskydd
Personberoende
Datalag
RÖS (Röjande Signaler)

Bilaga 6 C:Cure

Risk Assessment and Management Tasks	Basic Risk Assessment Activities
Asset Identification and Valuation (4.1.2)	List those assets associated with the business environment, operations and information being assessed within the scope of the ISMS.
Threat Assessment (4.1.3)	List those threats associated with the list of assets using checklists of generalised or commonly known threats.
Vulnerability Assessment (4.1.4)	List those vulnerabilities associated with the list of assets using checklists of generalised or commonly known vulnerabilities.
Identification of Existing and Planned Security Controls (4.1.5)	Identify and document all existing/planned controls associated with the list of assets in accordance with previous security reviews.
Risk Assessment (4.1.6)	Collect together the information on assets, threats and vulnerabilities resulting from the above assessments to enable a pragmatic, simple, view of the measures of risks.
Identification and Selection of Security Controls (4.2.1) and Reducing the Risks (4.2.2)	For each of the assets listed identify the control objectives in BS 7799 that are relevant. Use the threats and vulnerabilities related to each of these assets to identify those controls associated with the relevant control objectives in BS 7799 to achieve these objectives.
Risk Acceptance (4.2.3)	There may be a need to consider a further reduction of risks by selecting additional controls, on a pragmatic basis.

Figur 1: Basic Risk Assessment

Risk Assessment and Management Tasks	Detailed Risk Assessment Activities
Asset Identification and Valuation (4.1.2)	Identify and list all those assets associated with the business environment, operations and information being assessed within the scope of the ISMS, define a value scale and for each asset assign values from this scale (values for confidentiality, integrity and availability).
Threat Assessment (4.1.3)	Identify all those threats associated with the list of assets and assign a value to them according to their likelihood of occurrence and severity.
Vulnerability Assessment (4.1.4)	Identify all those vulnerabilities associated with the list of assets and assign a value to them according to how easily they might be exploited by the threats.
Identification of Existing and Planned Security Controls (4.1.5)	Identify and document all existing/planned security controls associated with the list of assets in accordance with previous security reviews.
Risk Assessment (4.1.6)	Assess the risk as a function of the assets, threats and vulnerabilities resulting from the above assessments using, for example, one of the risk assessment methods outlined in Annex B, or any variant or similar type of method.
Identification and Selection of Security Controls (4.2.1) and Reducing the Risks (4.2.2)	According to the risks identified from the above assessment, suitable security controls need to be identified that will counter these risks. For each of the assets listed identify the control objectives in BS 7799 that are relevant to each assessed risk. Use the threats and vulnerabilities related to each of these assets to identify those controls associated with the relevant control objectives in BS 7799 to achieve these objectives. Finally assess how much the controls selected reduce the identified risks.
Risk Acceptance (4.2.3)	Categorise the residual risks as being either 'acceptable' or 'unacceptable'. For each of those identified as being 'unacceptable' decide whether further controls should be selected or whether to accept the level of residual risk.

Figur 2: Detailed Risk Assessment