EKONOMI
HÖGSKOLAN
Lunds universitet

Institutionen för informatik
Kandidatkurs våren 2006

Säkerhetstänkande integrerat i systemdesign via formaliserade metoder

Kandidatuppsats 10 poäng inom Systemvetenskapliga programmet

Framlagd: 2006-06-09

Författare: Johan Andersson
Amina Borafia

Handledare: Anders Svensson

Resumé

Systemutvecklingsmetoder speglar olika verksamhetsperspektiv, och alla metoder är inte formaliserade, men gemensamt för dem är att de har till syfte att strukturera upp och stödja systemutvecklingsprocesser. Vilken metod som passar bäst får avgöras mot bakgrund av den aktuella systemutvecklingskontexten eftersom varje kontext är unik. Information utgör en värdefull tillgång i dagens organisationer, och den behöver skyddas mot både interna och externa säkerhetshot. I vår uppsats strävade vi efter att finna utrymme för att väva in säkerhetstänkande redan på designstadiet utifrån formaliserade systemutvecklingsmetoder för att utforma system som står bättre rustade att möta vår tids utmaningar inom datasäkerhet.

Utifrån vår teoretiska bas och våra empiriska undersökningar ute på ett stort IT-företag fann vi att betydelsen av säkerhet ökar hela tiden, och att systemutvecklare gör klokt i att vara medvetna om den enorma vikten av att integrera säkerhetstänkande i sina system så tidigt som möjligt. Vi fann också att formaliserade systemutvecklingsmetoder går mycket bra att kombinera med utökade moment, i detta fall riskanalys och säkerhetsplanering. Att koppla säkerhetsplanering till formaliserade systemutvecklingsmetoder kan vara ett bra sätt att tillmötesgå ett växande behov av säkerhetsarbete redan från början i systemutvecklingsprojekt.

Nyckelord: systemutvecklingsmetoder, utvecklingskontext, säkerhet, information

Abstract

Systems development methods mirror different organizational perspectives, and not all methods are formalised, but what they have in common is the purpose of structuring and supporting systems development processes. Which method would be the most suitable may be determined by the systems development context at hand, because every systems development context is unique. Information is a valuable asset in today's organizations, and it needs to be protected against both internal and external security threats. In our essay we aspired to find and present suggestions as to how systems developers can include security in the very design based on formalised systems development methods to create systems that are better prepared to meet the security challenges of today.

Based on our theoretical foundation and our empirical studies at a major IT company, we found that the importance of security is constantly increasing, and that it is wise of systems developers to be aware of the tremendous importance of integrating security thinking into their systems as early as possible. We also found that formalised systems development methods could successfully be combined with added elements, in this case threat analysis and security planning. Connecting security planning to formalised methods for systems development could be a good way of accommodating the increasing need of security work right at the beginning of a systems development project.

Keywords: systems development methods, development context, security, information

Förord

Under vårterminen 2006 på systemvetenskapliga programmet vid Lunds Universitet författades denna C-uppsats i förhoppning att ta upp ett ämne som kan vara lika intressant för den säkerhetsintresserade lekmannen som för den praktiserande systemutvecklaren.

Vi vill varmt tacka alla de personer som gjort vårt examensarbete möjligt genom att ställa upp med sin dyrbara arbetstid under denna period, och som trots att de har hektiska scheman intresserat sig för vår studie och tagit sig tid att bidra med värdefulla uppgifter.

Vi tackar även Anders Svensson, vår handledare som gett oss tips och idéer då arbetet skulle påbörjas, samt bidragit med kommentarer, åsikter och stöd under arbetets gång.

Lund den 2006-06-01

Johan Andersson *Amina Borafia*

Innehållsförteckning

1 Inledning

I det moderna informationssamhället har just information blivit en speciellt värdefull tillgång inom organisationer, en tillgång som bara tycks bli av allt större strategisk och ekonomisk betydelse hela tiden (Glisson och Welland 2005). Att skydda denna mot intrång från obehöriga är en av vår tids kolossala utmaningar för de säkerhetsansvariga på företag eller organisationer. I och med att de potentiella hoten mot informationens integritet ständigt förändras krävs också ett innovativt tänkande från systemutvecklare för att bemöta och bekämpa detta (Lager 2006).

Om det inte funnits känslig information i några system, om våra datorer inte var anslutna till Internet eller om våra datorer inte var designade att utföra det som de idag kan så hade vi inte haft några säkerhetsproblem relaterade till IT (Sampson 2006). Ett helt säkert system skulle vara ett system som ingen kunnat läsa information ifrån eller föra in information i, tyvärr hade ett sådant system varit helt värdelöst och oanvändbart. Därför kommer det alltid att finnas vissa hot mot informationen, såsom misstag, olyckor och intrång (Lager 2006).

I och med detta har datasäkerhet utvecklats till ett brett begrepp som inte bara omfattar åtskilliga nivåer av skydd mot olika former av avsiktlig mer eller mindre professionell hackerverksamhet med syfte att stjäla, manipulera eller förstöra information i kommersiella syften eller för nöjes skull, utan även internt integritetsskydd för känsliga uppgifter som inte vem som helst ska ha fri tillgång till (Glisson och Welland 2005). Säkerhet idag är alltså mycket mer än att hantera sitt lösenord eller sin pinkod säkert så att ingen kommer åt den (Sampson 2006).

Ett av dagens stora säkerhetshot, främst för mindre firmor med begränsad budget, är att användare eller anställd personal tar med sig egna filer och lagringsenheter som utan deras vetskap innehåller skadlig kod. Sedan använder de sin egen utrustning och infekterar oavsiktligt organisationens nätverk eller datorer och utsätter därmed organisationen, sig själva, samt kunder för potentiella risker. För att förhindra detta krävs utbildning av användarna så de förstår riskerna de utsätter informationsintegriteten för då de gör detta (Lager 2006). Dessutom är det viktigt att hos personalen inskärpa betydelsen av var på Internet de surfar och att webbsidor de besöker kan innehålla material som skadar deras datorer (Stimpson 2006).

Detta interna informationsskydd kräver både kostsam och omfattande administration och ständig uppdatering av skilda behörighetsnivåer för olika kategorier av personal inom ett företag eller en hel koncern (Stimpson 2006). Idag finns det ett brett utbud av säkerhetsorienterade *business-to-business*-lösningar som kan skräddarsys av leverantören eller av den interna systemutvecklingsavdelningen för att integreras i organisationens system (Avison och Fitzgerald 2003).

Kraven på systemutvecklare har ökat eftersom även applikationer som inte primärt hanterar säkerhet i allt större utsträckning behöver skyddas med hjälp av inbyggda säkerhetsmekanismer, en utveckling som höjt komplexiteten i arbetet med datasäkerhet. Detta ökar också betydelsen av kontinuerlig vidareutbildning för att systemutvecklare ska kunna hålla sig uppdaterade om nya lösningar och arbetsmetoder som underlättar deras uppgifter. Det är viktigt att analysera sina säkerhetsbehov och att rekursivt bryta ner processen med att förverkliga dem så att man löser den huvudsakliga uppgiften genom att klara av delmål på vägen (Apvrille och Pourzandi 2005). Riskanalyser, där man fastställer hot och redan på tidigt stadium i utvecklingen förebygger dessa, är även att rekommendera för skydd av dagens IT-system (Dantu, Loper och Kolan, 2004).

1.1 Varför är frågan viktig att ta upp?

Vi tycker det är intressant att undersöka hur säkerhetstänkande kan byggas in direkt i systemet via bruket av metoder under utvecklingen av informationssystemen, av ett par olika anledningar. Först och främst är datasäkerhet ett friskt debatterat ämne i dagens IT-orienterade klimat eftersom information ständigt utvecklas till en allt viktigare konkurrensfördel (Glisson och Welland 2005). Att visa kunder att deras konfidentiella uppgifter är och förblir skyddade är en förutsättning för att de ska vilja anlita organisationen (Lager 2006).

God säkerhet betyder inte bara skydd mot externa angrepp från hackers, utan även mot insiderjobb och mot förlust eller förvrängning av information. Säkerhetsbrister som beror på designfel orsakar stora ekonomiska förluster för moderna organisationer (Glisson och Welland 2005). Detta kan leda till att drabbade organisationer hamnar i finansiellt och PR-mässigt underläge i förhållande till sina konkurrenter eftersom information är en mäktig drivkraft inom världsekonomin (Lager 2006).

Användare idag måste vara försiktiga varje gång de kommunicerar med eller via tekniska system som hanterar information, allt från mobiltelefoner, handdatorer, pc-maskiner till servrar kan drabbas av säkerhetshål som kan utnyttjas av obehöriga personer för att komma över personuppgifter, kontokortsnummer, personliga brev eller sekretessbelagd information. Gränsen mellan datasäkerhet på kontoret och hemma har blivit flytande eftersom ett stort antal människor världen över arbetar på distans via mobila IT-lösningar utöver det arbete de utför under kontorstimmarna. På dessa mobila enheter kan det finnas information som inte ska läcka ut till vem som helst, och därför krävs fungerande säkerhetslösningar som omfattar mobila enheter oberoende av var de befinner sig (Stimpson 2006).

IT finns inblandat i mer och mer av vår vardag, exempelvis ekonomi, läkarvård, underhållning och kommunikation, vilket är resultatet av de senaste 30 årens snabba utveckling inom området (Avison och Fitzgerald 2003), och även därför känns det viktigt att undersöka hur säkerhetsplanering kan införlivas med metoder i praktiken.

1.2 Syfte

Vårt syfte är göra en studie och föra ett resonemang om förebyggande säkerhetstänkande och koppla detta till formaliserade metoder för utveckling av informationssystem. Med stöd av den teoretiska litteraturstudien och vår empiri argumenterar vi för att säkerhetsplanering bör införlivas i design och systemutveckling på ett tidigt stadium, så att säkerhet blir en inbyggd aspekt av systemet och inte en tillsats i efterhand. Vi vill ta reda på hur organisationer kan skydda sin information, mjukvara och hårdvara genom att designa system som är skapade för att värna om dessa tillgångar, system som själva utgör en central del av säkerhetslösningarna.

Detta är intressant att undersöka eftersom datasäkerhet ständigt blir en alltmer central fråga, efterhand som både nya tekniska lösningar för att värna om information och metoder att bryta sig igenom eller kringgå skyddsåtgärder gör entré i IT-världen.

1.3 Avgränsning

Vårt empiriska material består av intervjuer med ett antal personer från en enda avdelning inom en stor organisation, vilket naturligtvis begränsar möjligheterna att göra allmängiltiga observationer. Vi strävar ändå efter att få fram material och utforma analyser och slutsatser som även andra kan få glädje av att ta del av. Frågorna vi ställt fokuserar på arbetet med och tänkandet bakom de säkerhetslösningar företaget valt utifrån sina kontextuella behov, och vi tänker inte gå djupare in på genomgångar av specifika tekniska komponenter i företagets skydd mot dataintrång mer än att presentera de hoten som kan ses som vanligast idag.

Säkerhetstänkandet står i centrum för intervjuerna, och specifika lösningar diskuteras enbart med intervjupersonernas uttryckliga medgivande. Analysen i kapitel fem genomför vi mot bakgrund av litteraturen och vårt empiriska material. Vi håller oss därför till att lyfta fram och diskutera behovet av tidig säkerhetsplanering i systemutveckling och koppla detta till analysfasen i formaliserade metoder. I och med att detta ämne förändras hela tiden så har vi i denna uppsats använt oss av högaktuell litteratur kring vårt ämne.

Den teoretiska diskussionen kring formaliserade systemutvecklingsmetoder hålls på en så generell nivå som möjligt eftersom avsikten med den är att presentera hur säkerhetsarbete behandlas i den litteratur vi funnit. Vi vill belysa de centrala tankegångarna bakom bruket av formaliserade systemutvecklingsmetoder och kombinera dem med ett utökat säkerhetstänkande. Anledningen till att vi huvudsakligen kommer att hålla oss till att diskutera säkerhetsplanering mot bakgrund av metodologier bakom formaliserade metoder är att dessa metodologier finns dokumenterade och beskrivs i litteraturen, och dessa är i sin tur sammanfattande för ett flertal ledande formaliserade systemutvecklingsmetoder.

1.4 Disposition

Efter denna inledande bakgrund och klargörande av vad vårt kandidatarbete kommer att handla om går vi in på metoden bakom vårt skrivande och vår vetenskapliga utgångspunkt i avsnitt två. Tredje avsnittet behandlar den teoretiska basen för vårt kandidatarbete och den litteratur vi tagit del av. Här går vi igenom vår tids vanligaste hot mot informationssäkerhet. I

avsnitt fyra redogör vi för det empiriska arbetet i form av intervjuer, som analyseras i avsnitt fem. I sjätte avsnittet lägger vi fram våra slutsatser, och sist kommer vår referenslista samt bilagor.

2 Metod

I vår metoddiskussion börjar vi med att redogöra för vår vetenskapliga utgångsposition för att förtydliga varför vi utformat vårt kandidatarbete på detta sätt. Sedan går vi igenom hur vi arbetat med teoretisk metod och hur vi valt ut vår referenslitteratur. Vi diskuterar också vad som ligger bakom vårt val av empirisk metod och hur vi gått tillväga med intervjuerna.

2.1 Vetenskapligt perspektiv

Eftersom vi inom ramen för vårt kandidatarbete strävade efter att skaffa oss en inblick i våra respondenters arbete med säkerhet samt systemutveckling och en utökad förståelse för hur de upplever de olika möjligheterna och utmaningarna i sina respektive yrkesroller blev det naturligt för oss att utgå ifrån ett hermeneutiskt forskningsperspektiv (Bryman 1997). Respondenternas uppfattningar har varit ytterst värdefulla för oss, och de har även gett oss tillfälle att reflektera över skillnader i hur de upplever och bedömer olika aspekter av säkerhetsarbete.

I vår undersökning strävade vi efter att lyfta fram respondenternas erfarenheter och uppfattningar om hur arbetet med säkerhet och systemutveckling kan finslipas. Vi ville inte bara studera hur saker och ting ser ut utan vi hoppas även kunna hjälpa till med att förbättra säkerhetsarbete i praktiken (ibid). Eftersom vi interagerat personligen med våra respondenter i syfte att förstå deras skilda perspektiv på säkerhetsarbete och systemutveckling har vi utfört vår studie i hermeneutisk anda, och vi har använt den personliga intervjun som kvalitativ metod (Ryen 2004).

Under våra år inom den systemvetenskapliga utbildningen Vid Lunds Universitet har vi även själva kommit i kontakt med metoder och deras användningsområden, exempelvis SAP, direktmodellen, Soft Systems Methodology och livscykelmodellen. Detta har gett oss en konkret bakgrundsbild att relatera till det metodbruk vi studerat under vårt examensarbete och en förståelse för att olika metoder är lämpliga vid olika tillfällen och i olika situationer (Fitzgerald et al., 2002). Vi är medvetna om att förkunskaper påverkar tolkningen av nya kunskaper i den hermeneutiska cirkeln, där förståelse leder till ny förståelse (Holme och Solvang 1997), och eftersom detta är en naturlig del av mänsklig inlärning anser vi inte att vi kunnat undvika att våra tidigare erfarenheter påverkade vår tolkning av det teoretiska och empiriska materialet, utan att vi enbart kan notera detta och vara uppmärksamma på det.

2.2 Teoretisk metod

Vi utgår ifrån befintlig forskning om säkerhetsaspekter på systemutveckling för att på ett så tidigt plan som möjligt kunna få med säkerhetsaspekterna i utvecklingen. Vi använder oss sedan av intervjuerna för att ta reda på var i utvecklingsarbetet det vore lämpligast att väga in denna säkerhetsaspekt i bruket av formaliserade metoder.

Ett examensarbete som listar och avhandlar samtliga nu kända tekniker som används för att stjäla eller förvanska data hade hunnit bli inaktuellt innan det presenteras. Därför använder vi istället den generaliserande termen skadlig kod, som syftar på kod som hotar att underminera säkerheten i informationssystem och de enheter som är anslutna till dem. Däremot nämner vi ett par kategorier av personer som ägnar sig åt dataintrång, eftersom vi anser att säkerhetsriskerna utgår från den mänskliga faktorn bakom de ständigt skiftande teknikerna.

Det kommer med största sannolikhet även att dyka upp nya namn på dem som bryter sig in i informationssystem, men oavsett vad de själva eller andra kallar dem och vad de har för motiv så lär de fortsätta att utgöra en utmaning för systemutvecklare världen över. Det var därför vi valde att ta med dem i vår teoretiska genomgång för att ge en bakgrundsbild till det säkerhetsklimat organisationer behöver ha i åtanke vid systemutveckling. Vi går inte heller närmare in på de skiftande motiv som ligger bakom dessa gruppers dataintrång. Vår avsikt är att lyfta fram hot mot informationssäkerhet, och att konfidentiella uppgifter måste skyddas mot obehöriga användare utgör ett centralt tema i vårt empiriska material.

2.3 Empirisk metod

Eftersom vi inte är ute efter att bevisa några definitiva samband utan snarare vill lägga fram exempel på säkerhetsarbete som komplement till vår teoretiska bas valde vi en kvalitativ ansats för att kunna gå på djupet. Att vi genomfört en kvalitativ undersökning innebär inte att vi på något sätt tagit ställning emot ett kvantitativt tillvägagångssätt. Vårt val beror helt och hållet på vad vi ansåg vara en lämplig empirisk metod för vår typ av arbete (Holme och Solvang 1997). Om vi strävat efter att forska på bredden för att erhålla statistiska resultat som kunde stödja eller motbevisa en eller flera hypoteser vi ställt upp vore en kvantitativ studie betydligt mer ändamålsenlig (Bryman 1997).

Istället för att genomföra en bred kvantitativ studie med ett så högt antal respondenter som möjligt för att kunna dra generella slutsatser har vi hållit oss till en kvalitativ undersökning där vi strävar efter en djupare analys och förståelse för hur våra respondenter arbetar och hur de upplever sitt arbete med säkerhet på olika nivåer. Vi tar också med en systemutvecklingsaspekt i vårt empiriska material eftersom vi ville koppla det vardagliga arbetet med metoder i praktiken till den teoretiska basen. Vi ansåg att ett kvalitativt perspektiv skulle ge oss mer utrymme att sätta oss in i respondenternas arbetsuppgifter, och att vi då dessutom skulle kunna vara mer flexibla i vår undersökning och till viss del variera våra frågor efter vem vi talade med i den aktuella intervjun (Holme och Solvang 1997).

Vi är högst medvetna om att vi har ett relativt litet antal respondenter som alla arbetar inom samma avdelning och att svaren vi fått kanske därför är mer representativa för just denna enhet, i och med att personalen där är specialiserade på arbete med och runt

dokumenthantering. Trots försök att få kontakt med folk inom bredare skikt av organisationen har vi fått mycket begränsad respons på den fronten, och därför valde vi att fokusera vår empiri på de personer som visade ett aktivt intresse av att medverka. Det märktes i samtalen att de var engagerade när vi diskuterade saker de var kunniga inom och djupt intresserade av, och vi anser att denna positiva attityd haft stor betydelse för det empiriska material de generöst bidrog med. Allt material vi sammanställt under empirin grundar sig direkt på respondenternas svar, och med deras medgivande har vi omsatt informationen i löpande text, så som den presenteras i kapitel fyra. De har också läst igenom vår text och gett oss sitt godkännande av den.

2.4 Intervjuteori

Vi har fokuserat våra frågor kring intervjupersonernas respektive tankar och uppfattningar om säkerhetsplanering och säkerhetshöjande åtgärder inom avdelningen utifrån deras olika erfarenheter vid intervjutillfället. För att kunna lyfta fram information ur olika perspektiv tillfrågade vi respondenter ur skilda yrkeskategorier, och det visade sig även att samtliga hade väldigt skilda bakgrunder i fråga om utbildning och tidigare arbetslivserfarenhet, vilket vi går närmare in på i det empiriska kapitlet.

Eftersom detta är en kvalitativ studie så har vi vägt in det faktum att våra frågor hade olika relevans för de olika respondenterna beroende på deras respektive yrkesroller. Detta har också medfört att vi fått varierande svar på samma fråga, vilket kändes värdefullt i och med att det gav oss ett bredare analysunderlag. Tre av våra respondenter arbetar med olika aspekter av datasäkerhet. Vi har även tagit med en intervju med en systemutvecklare i organisationen eftersom han är med och utvecklar och underhåller de system som säkerhetsfrågorna berör.

Själv är han inte direkt involverad i säkerhetsarbete, men eftersom vårt uppsatsämne handlar om att väva in säkerhet i systemdesign ansåg vi ändå att hans uppgifter var intressanta och kunde kombineras med de andra respondenternas. Att belysa denna uppdelning mellan ansvarsområdena datasäkerhet och systemutveckling kändes relevant för vår studie i och med att det ger exempel på ett sätt att arbeta, som vi sedan behandlar vidare i vår analys och slutsats.

Forskare använder ett flertal olika termer för sina intervjupersoner, ofta beroende på deras vetenskapliga perspektiv och hur de förhåller sig till personerna de inhämtat information ifrån, men att vi valt att kalla dem respondenter innebär inte att vi enbart betraktar dem som individer som besvarat en uppsättning frågor vi ställt (Ryen 2004). Visst utgick vi från en intervjumall vi ställt samman, men vi lät oss även vägledas av respondenternas olika kunskap och yrkeserfarenhet när vi formulerade följdfrågor, och det framkom information som vi inte uttryckligen frågade efter. För att få fram så mycket användbart empiriskt material som möjligt uppmuntrade vi dem att berätta på sitt eget sätt.

Följaktligen tog intervjuerna olika lång tid i anspråk. Väl medvetna om att vi tog upp våra respondenters arbetstid erbjöd vi oss att vara färdiga inom cirka tre kvart. Den snabbaste intervjun tog ungefär 35 minuter och den längsta över en timme. Vi noterar här att vi vid samtliga intervjuer oavsett tid fick utförliga svar på alla frågor som respondenterna upplevde

som relevanta för sina yrkesroller. Det som varierade var hur pass utförligt de berättade omkring ämnet som frågan gällde, och vi anser att vi fick fram många värdefulla uppgifter genom att låta respondenterna avgöra hur lång tid de ville ta på sig att informera oss. Varken organisationen eller respondenterna nämns vid namn i vårt arbete eftersom vi utlovat anonymitet till alla som så önskar.

Vid två av intervjuerna gjordes bandupptagningar av varierande kvalitet, och vid de sista två delade vi upp arbetet så att den ena av oss ställde frågorna och den andra koncentrerade sig på att nedteckna svaren. Vi beslöt att göra så eftersom den enda hjälpligt fungerande inspelningsutrustningen var mycket otymplig och inspelningarna visade sig vara av begränsad nytta. För att motverka risken att viktig information föll oss ur minnet behandlade vi det empiriska materialet och omsatte det i sammanhängande text så snart som möjligt under samma dag som intervjun genomförts.

Intervjuerna ägde rum på respondenternas kontor i Malmö, och avsikten med intervjuerna är att presentera en konkret verklighetsbakgrund som visar hur säkerhetstänkandet kan yttra sig i det vardagliga arbetet på ett stort IT-företag så att vi har något praktiskt att jämföra med och analysera utifrån referenslitteratur om säkerhetsplanering och formaliserade systemutvecklingsmetoder. Vårt syfte med analysen var att nå fram till en slutsats där vi diskuterar förslag om hur säkerhetstänkande kan vävas in i ett tidigt stadium av systemutveckling med hjälp av formaliserade metoder. Här strävar vi efter att komma med ett kunskapsbidrag som kan bli till både teoretisk nytta och praktisk användning.

2.5 Källkritik

Mycket av vårt material är hämtat från tidsskrifter och andra typer av publikationer riktade till IT-folk, då detta är det mest tidsaktuella material kring detta ämne som går att finna. Anledningen är att detta är ett så snabbt föränderligt ämne där relevanta saker snabbt blir irrelevanta och där nya möjligheter eller hot fort dyker upp eller blossar upp till kritiska situationer. Eftersom vi valt denna typ av material finns det risker i att vissa branscher och deras behov överprioriteras på bekostnad av andra, exempelvis att de frågor som diskuteras huvudsakligen gäller stora och inflytelserika organisationer, och att de mindre organisationernas säkerhetsbehov och de säkerhetslösningar de har råd med kommer i skymundan.

Vi är också medvetna om att det kan finnas en baksida med att använda tidsaktuellt material från artiklar i vår uppsats, att materialet snabbt kan bli inaktuellt igen just eftersom IT-branschen befinner sig i ständig och mycket snabb förändring. Detta skulle kunna medföra att delar av vår teoretiska grund får begränsad tidsrelevans. Båda dessa punkter är viktigt att bära i minnet när vi utvärderar våra källor.

3 Teori

I detta avsnitt diskuterar vi utifrån litteratur som tar upp behov av tidig säkerhetsplanering, samt litteratur som behandlar metodologier för systemutveckling. Anledningen till att vi dessutom diskuterar olika kategorier av personer som gör intrång i informationssystem är att vi vill lyfta lägga tonvikten på de mänskliga aktiviteterna bakom de varierande teknikerna.

3.1 Den mänskliga riskfaktorn

Dagens informationssystem är utsatta för en uppsjö av säkerhetsutmaningar som ständigt blir fler. Namnen på hoten och teknikerna bakom dem varierar, men gemensamt för dem är att de kan underminera informationssäkerheten i system. Innan Internet började användas av gemene man var det infekterade filer som medföljde disketter eller cd-skivor som var främsta distributionsformen för skadlig kod, och då var även spridningen mycket långsammare. Vissa av dessa destruktiva koder är utformade för att utnyttja mänskliga användarmönster genom att slå rot i ett annat körbart program på datorn och kan ställa till med olika slags problem när det infekterade värdprogrammet körs. I värsta fall går betydelsefulla data förlorade eller så sprids känslig information vidare till obehöriga personer (Riordan et al., 2005).

Andra former av skadlig kod sprids genom hela nätverk utan att användare behöver göra något särskilt för att medvetet eller omedvetet vidarebefordra dem. De är främst utformade för att kopiera sig själva till varje maskin de kommer i kontakt med som innehåller den eller de säkerhetsluckor de utnyttjar. De sprids ofta på Internet, och plötsliga dramatiska ökningar av nätverksaktivitet kan vara ett tecken på att en mask tagit sig in i organisationens nätverk, som riskerar att bli så överbelastat att kommunikationen mellan klienter och servrar kollapsar (Riordan et al., 2005). Alltså orsakar skadlig kod mycket omfattande, dyra och tidsödande systemfel.

Säkerhetsåtgärder är svar på en hotbild. Hot kan definieras som en isolerad händelse eller pågående situation som kan skada informationssystem genom att manipulera eller förstöra data, alternativt göra det tillgängligt för obehöriga parter. Intrång sker inte enbart utifrån. Även intern personal kan missbruka sina eller sina kollegors användaruppgifter för att ta del av information som ligger på högre åtkomstnivåer. Vissa är till och med så skickliga att de undgår upptäckt (Bace 2000).

Idag är kriminaliteten på Internet en växande säkerhetsrisk. Personer med omfattande datorkunskaper allierar sig med kriminella gäng för att exempelvis sälja känslig information, personuppgifter eller kreditkortsnummer som de kommer över till dessa och på så vis tjäna stora pengar på andra personers och organisationers bekostnad. De utnyttjar anonymiteten som de kan få på Internet till att hålla så låg profil att de nästan inte är spårbara, och de kan

sitta i hela olika delar av världen och arbeta tillsammans för att knäcka ett system eller på annat vis komma åt vad de är ute efter. Detta globala samarbete försvårar arbetet med att stoppa dessa kriminella element, och mjukvaruutvecklare måste därför kämpa för att motverka dessa kriminella gärningar redan på mjukvarunivå och via utbildning av användarna. Förr använde kriminella gäng som arbetade med Internetbedrägerier och datastölder endast hackers som ett verktyg, idag är dessa personer en del av den kriminella affärsidén och dessa personer används för att begå exempelvis kriminella brott med högteknologiska metoder (Tiller 2005).

I de kretsar som dessa personer umgås, både privat och via chat-rum eller nyhetsgrupper, så delas de ofta in i två huvudgrupper: *elite* och *kiddies*, där *kiddies* är en förkortning av *script kiddies*. Pfleeger (2003) kallar dessa istället a*mateurs* och *crackers* i sin bok, men det är samma sak, och vi kommer härefter kalla dem *elite* och *kiddies* i vår text då det är vad de kallas i nyare källor samt av personerna själv (Mollick 2005).

De personerna som ses som *elite* är oftast de som är uppfinningsrika och som sätter sig in i de tekniska detaljerna i systemen för att exempelvis hitta hål i dem eller utnyttja dem på ett sätt som det inte är tänkt. De som räknas som *kiddies* är de som använder sig utav kunskapen eller programmen som e*lite* tagit fram för att utnyttja för egna ändamål eller för att finna andra hål eller användningsområden för ett system eller någon teknisk applikation. Personerna som räknas som elit inom dessa kretsar utnyttjar sällan sin kunskap till direkt kriminella handlingar, vilket oftast kiddies gör, även om det finns undantag på båda sidorna (Mollick 2005).

Åsikterna om vilka grupper som står för den största brottsliga användningen av material de kommit över via dataintrång går isär, och eftersom vi endast diskuterar dessa personers aktiviteter med avsikt att presentera en bild av vilka säkerhetsutmaningar dagens informationssystem står inför får vi nöja oss med att konstatera att det finns personer med olika kunskapsnivåer och motiv som kan bryta sig in i ett system (Pfleeger 2003; Mollick 2005).

Oavsett om motivet tilldataintrånget är spänning eller ekonomisk vinning så innebär dessa aktiviteter en konstant risk. De som via intrång är ute efter att skaffa sig åtkomst till information som de inte har behörighet att läsa eller använda sätter en stolthet i att i så stor utsträckning som möjligt ligga steget före och kringgå de senaste säkerhetsåtgärderna på marknaden. Det pågår en kontinuerlig kapprustning mellan dem som gör intrång av olika skäl och dem som arbetar för att förhindra undermineringen av datasäkerhet i organisationer och i våra hem (Riordan et al., 2005).

Konsekvenserna av dessa typer av intrång kan vara allt ifrån att få återställa en backup, om sådan gjorts, till kostnader samt arbete för flera miljarder. Dessutom orsakar detta förlorat kundförtroende, som kan ta lång tid för en stor organisation att bygga upp igen. Detta nämns av Tiller (2005), och exemplifieras av Lager (2006) där han tar upp en massiv stöld av kreditkortsnummer som skedde i juli 2005 och då över 40 miljoner kreditkortsinnehavare drabbades. Stöld av användaruppgifter är ett ökande säkerhetshot, både i fråga om tillgång till finansiella konton och när det gäller missbruk av personuppgifter. Enligt Lager (2006) är de flesta av dagens kunder medvetna om de risker som finns, och därför är de väldigt försiktiga med att ge ut sina personuppgifter, mycket på grund av risken med identitetsstöld som finns då stora mängder personuppgifter kan finns lagrade inom en och samma organisation.

Uppfinningsrika personer har insett betydelsen av sekretess och de sekretesskrav dagens organisationer måste kunna uppfylla gentemot sina kunder. De organisationer som dessa personer startat upp kan genom säker lagring av data erbjuda andra organisationer att ta hand om deras lagring av känslig information. De erbjuder exempelvis hög kryptering och säkerhet som i praktiken inte ska kunna låta någon obehörig ha tillgång till någonting. Detta är tjänster som stora organisationer, där hantering av stora mängder känslig data sker dagligen i arbetet, har stor nytta av och som lättar den egna arbetsbördan. Marknaden för dessa tjänster har dessutom ökat sedan flera länder, däribland Japan med väldigt många IT-företag och IT-kunder, infört lagar som tvingar organisationer att hantera personuppgifter säkert. Japan gjorde detta genom att bland annat göra personuppgiftsläckor straffbart (Lager 2006).

En viktig aspekt av säkerhetshot är vardagligt användande av datorer och nätverk, och ett sätt att reducera riskerna är utbildning av personalen (Stimpson 2006). Denna interna säkerhetsutbildning, samt att det anställs pålitlig personal, är viktigt eftersom många stölder av personuppgifter sker inifrån organisationerna, upp till hälften av alla personuppgiftsstölder (Lager 2006). Vi borde alla bli mer medvetna om säkerhetsfrågor och hjälpa de organisationer vi arbetar i att med vår kunskap förbättra säkerheten efter bästa förmåga för att motverka förluster för organisationen och dess kunder om någon via säkerhetshål skulle ta sig in i organisationens system och komma över känslig information. Säkerhetsplanering bör finnas med och vävas in i alla delar av en organisations verksamhet, så att säkerhetstänkandet finns med från början och genom detta förhindra den elektroniska kriminaliteten så gott det går (Tiller 2005). Med elektronisk kriminalitet menas kriminalitet som på något vis involverar datoranvändning (Pfleeger 2003).

3.2 Säkerhet från början

Säkerhetstänkandet bör tas med i alla modeller och därför finnas med i samtliga av utvecklingens faser för att på så sätt skapa system med inbyggd väldigt hög säkerhet, och där brister, om eller när sådana upptäcks, lätt kan korrigeras. Allt ifrån analys, planering och design till själva kodknackningen ska vara säkert, och då ska även riskbedömningar göras på val av programmeringsspråk, för att på så sätt utveckla ett säkert system redan från grunden (Apvrille och Pourzandi 2005).

För systemutvecklare som utvecklar en mjukvara som ska hantera känslig information krävs det därför att de tidigt i sin utveckling försöker eliminera riskerna för spridning av informationen, som då i värsta fall kan användas på ett oetiskt eller olagligt sätt för att skada individer eller hela organisationer. Utvecklaren behöver även se till att informationen hålls säker från att eventuellt försvinna eller tas bort. Detta kan göras genom att tidigt i planeringen även planera in hur informationen ska lagras, hanteras och skickas, men även hur den ska säkras från att andra program eller användare ska kunna läsa den. (Glisson och Welland 2005).

En billig metod att skydda programvara är att utforma koden så att hackers får svårt att förstå hur den är utformad, vilket gör det mindre intressant ur ekonomiskt och tidsperspektiv att missbruka den. På så sätt blir det svårare för en angripare att identifiera kodningens svaga länkar, men liksom denna teknik kan användas för att skydda programvara kan den lika enkelt missbrukas för att dölja skadlig kod som en hacker kan ”baka in” i något som

användare laddar ner till sina datorer. Virusdetektorer kan bli förvirrade av kodens utformning och missa att den innehåller skadligt material. Trots att informationen kanske hålls lagrad och skickas krypterad så kan virusprogrammerare via dekompilering av originalprogramvaran ta reda på nycklarna som krävs för att öppna filerna, och på detta sätt läsa informationen, eller skriva om programvaran så den fungerar annorlunda, och då distribuera vidare den känsliga informationen till obehöriga personer (Udupa et al., 2005).

Förmodligen står en del av förklaringen till denna utveckling att finna i att dagens IT-system är så avancerade, så multifunktionella och så komplexa att utvecklarna har svårt att överblicka hela systemet och hitta alla hål, läckor eller säkerhetsbrister innan de måste släppa programvaran till konsumenterna av ekonomiska skäl och för att alls kunna konkurrera på marknaden. Problem med utveckling av säkerhetsaspekter i programvara kan också bero på att systemutvecklare översållas med mängder av teoretisk information som är svår att överblicka och tillämpa i den praktiska utvecklingsprocessen (Apvrille och Pourzandi 2005).

Dessutom finns det ännu inte så mycket vägledande forskning om integration av tekniska säkerhetslösningar i systemdesign (Glisson och Welland 2005). Det är också viktigt att vidta fungerande åtgärder för att skydda företagets information, så att tid och pengar inte spills på lösningar som invaggar användare i falsk säkerhet, medan utveckling av lämpligare lösningar underprioriteras (Udupa et al., 2005).

Säkerhetsbrister är mycket kostsamma för moderna organisationer varje dag, och oftast är det inte säkerhetsmekanismerna som misslyckas med att skydda informationen som systemet hanterar, utan problemet ligger ända nere på design-nivån. Säkerhetsaspekter har beaktats för sent i utvecklingsprocessen, och därför klarar de färdiga systemen inte av att hantera de säkerhetshot de utsätts för i daglig drift. För att få bukt med sådana problem är det viktigt att organisationer fokuserar på säkerhetstänkande redan när systemet designas och att utvecklarna följer upp detta genom hela utvecklingsprocessen (Glisson och Welland 2005).

Utan att gå in på direkt tekniska termer i denna uppsats, finns det åtgärder för att förhindra obehöriga från att göra intrång så de kan nå känslig data så finns lagrad i systemet. Det är flera saker organisationen bör tänka på vid utveckling, administration och hantering av ett system. Pfleeger (2003, sid. 22) listar saker de steg som bör vägas in för att förhindra skada:

- Förhindra åverkan, genom att blockera attacken
- Avskräck från attacker, genom att göra dom svårare utan att göra dom omöjliga
- Få andra mål mer attraktiva, eller gör ens egen datalagring mindre attraktiv.
- Upptäck det, oavsett om detta görs under attacken eller efteråt
- Återställ allt till sin ordning efter attacken.

Flera av dessa åtgärder bör ske samtidigt i både utveckling och administration av ett system för att det ska vara så säkert som möjligt samtidigt som man är medveten om problemen och hoten som kan finnas (Pfleeger 2003).

3.3 Metodologier bakom formaliserade metoder

Metodologier inom systemutveckling representerar olika sätt att tänka kring hur informationssystem bör utformas. Det finns ett antal metodologier med skilda inriktningar

som har kommit att forma några av de mest omtalade formaliserade systemutvecklingsmetoderna i litteraturen. För att lyfta fram de centrala tankegångarna bakom formaliserade metoder går vi kortfattat igenom olika metodologiska perspektiv. Eftersom vi strävar efter att hålla vår teoretiska diskussion på ett så generellt plan som möjligt fokuserar vi på att nå fram till en för metodologierna gemensam tidpunkt i utvecklingsarbetet där säkerhetsplanering kan inkluderas.

Avison och Fitzgerald (2003) presenterar följande kategorier med metodologier, där indelningen de gjort främst grundar sig på sättet att arbeta:

- Processorienterade metodologier
- Objektorienterade metodologier
- Snabbutvecklingsmetodologier
- Människoorienterade metodologier
- Organisationsorienterade metodologier
- Blandade/Övriga metodologier

De **processorienterade** metodologierna är oftast väldigt väldefinierade och varje arbetsmoment beskrivs noga i detalj. Metoderna som kan definieras som processorienterade är i de flesta fall skapade för att kunna utveckla alla typer av system, dock är de inte lika vanliga idag som de var förr. Idag har nyare metodologier tagit över, främst de objektorienterade, även om de processorienterade metodologierna fortfarande finns kvar.

Huvudmoment i de processorienterade metoderna är vanligtvis top-down-orienterade, eller så bygger de på en liknande struktur, där en generell analys över vad som ska utvecklas först görs, för att sedan arbeta sig framåt med mer detaljerade analyser och detaljerat arbete. I de tre modeller som Avison och Fitzgerald (2003) tar upp finns det en metod som inte har riktigt samma uppbyggnad som de två andra. Den största skillnaden ligger i att den inte använder sig utav eller följer livscykelmodellen, vilket de flesta andra formaliserade metoder idag gör.

Trots detta finns det stora likheter i upplägget då metoden är lika välstrukturerad som de övriga och uppdelad i faser där första faserna innebär analys av den verklighet som systemet kommer att beröra. Detta innebär även analyser av vad som kommer förändras efter införandet av systemet, med kostnadskalkyler och flödes-diagram som beskriver förändringarna enkelt, eller där det enkelt går att se vad som kommer påverkas. Efterkommande faser hanterar kortfattat utvecklingen och implementationen av systemet, och dessa moment kan ta längst tid, men huvudfokus ligger på analyserna som skapar den dokumentation som ligger till grund för hur systemet sedan kommer att se ut och fungera (ibid).

De **objektorienterade** metoderna har sedan introduktionen blivit väldigt populära, främst då de har ett standardiserat notations-språk (UML), men även eftersom de moderna programmeringsspråken idag bygger på objektorientering, så från planeringen går det direkt översätta vidare till notationsspråket, och utifrån detta går det sedan direkt överföra till programmering, vilket underlättar och förenklar hela utvecklingsprocessen och allt utvecklingsarbete som utförs i metoden (Avison och Fitzgerald 2003). I objektorientering är tanken att knyta data till de operationer som hanterar dem, och dessa operationer är sedan de punkter där data görs åtkomliga i systemet, inkapsling. Enligt Mathiassen är målet att bryta ner systemet i komponenter med minimala gränssnitt (Mathiassen et.al 2001). Objektorienterade modeller passar, tack vare uppbyggnaden och konceptet med

objektorientering, utmärkt till utveckling som har nära verklighetsanknytning, såsom utveckling av system till organisationer för hantering av exempelvis löner och kundorder (Avison och Fitzgerald 2003).

De objektorienterade metoderna är uppdelade i faser, och arbetet pågår iterativt, så utökningar, förändringar och förbättringar sker kontinuerligt under arbetets gång genom dessa faser. Förändras faktorer eller förutsättningar i den miljö där systemet ska implementeras så går det lätt att återgå till denna fas i arbetet och förändra den tack vare att strukturer, objekt och klasser redan i ett tidigt skede identifierats och definerats och då bara modifieras för att passa in (ibid).

Eftersom det krävs viss kunskap och medvetenhet om den miljö som systemet ska fungera i behövs analysfaser i början av utvecklingen innan övriga moment kan inledas. Därför får utvecklarna vara ute och studera miljön systemet ska implementeras i innan de påbörjar något annat. De kan då lättare få en uppfattning om organisationens struktur och sätt att arbeta och därefter smidigare anpassa systemet exakt efter de yttre förhållandena, istället för att organisationen ska anpassa sig efter systemet (ibid).

De objektorienterade modellerna följer livscykelmodellen, och tack vare deras struktur och planering samt dokumentation under utvecklingens gång så förenklas arbetet med att hålla systemen anpassade till organisationerna, även om den största och mest använda av dessa metoder, RUP, påstår sig vara arkitektur-centrerad. Då de första objektorienterade metoderna dök upp fanns inte UML, men skaparen av RUP skapade även UML, och detta var till stor glädje för många, varpå UML adopterades av övriga metoder med, trotts att den huvudsakligen skapades för att fungera tillsammans med RUP (ibid).

Då en normal utvecklingsprocess av ett system kan ta oerhört lång tid på sig i och med alla analyser och alla studier av omgivningen som systemet ska implementeras i, samt att all dokumentation ska skrivas och bearbetas så har det skapats **snabbutvecklingsmetodologier** för utveckling av system med minimal tidsförbrukning, dessa kallas gemensamt RAD, *Rapid Application Development*. RAD-metoderna lämpar sig bra i situationer där ett system kan behövas ganska omgående eller till en lite mindre budget, eller möjligtvis till en organisation som inte har tänkt hantera kritisk data via systemet. Stora system bör inte utvecklas med RAD-metoderna då dessa helt enkelt endast är skapade för att tillverka små eller medelstora system i små grupper där nära kontakt med kunden nästan är ett tvång (ibid).

Dessa metoder finns utformade på lite olika sätt. Vissa handlar om en utvecklingsfilosofi där kod ska genereras så fort som möjligt för att fungera så ändamålsenligt som möjligt, medan andra lägger tonvikt på en minimal analys. Gemensamheter har de en hel del, exempelvis så skapas program-delarna så fort som möjligt och testas kontinuerligt under utvecklingsarbetet för att på så vis hela tiden ha koll på att det är fungerande kod som skapas (ibid).

Eftersom dessa utvecklingsmetoder inte lägger någon större tonvikt vid analys innan framtagandet av de faktiska applikationerna så får kunden (eller de framtida användarna) kontinuerligt under arbetets gång testa koden för att se om programmet som skapas är det som han eller hon vill ha. Med detta inte sagt att ingen analys eller planering före arbetet genomförs, men det sker inte på samma nivå eller på samma sätt som i exempelvis objektorienterade metoder där själva programmeringsprocesserna inte är ett lika centralt moment. En annan gemensam nämnare hos de RAD-metoder som Avison och Fitzgerald presenterar är att skulle något vara fel så ska utvecklarna inte gå tillbaka och leta upp felet för

att korrigera, de ska då istället kassera den kod som inte fungerar och istället skapa ny kod för att ersätta den felaktiga (ibid).

En gemensam nämnare inom **människoorienterade** metodologier är att de som påverkas av systemet också bör få vara med och påverka utformningen av det. Behovet av förändring i organisationen utreds utifrån ett medarbetarperspektiv. Det uppfattas inte enbart som viktigt att användare medverkar i systemutvecklingen utan även att deras kunskap tas till vara när systemet utformas. Människan anses kommunicera med systemet, och denna kommunikation bör stödjas genom att göra berörda parter delaktiga i systemutvecklingsprocessen (Avison och Fitzgerald 2003).

I de **organisationsorienterade** metodologierna står strävan att se till helheten i centrum för systemtänkandet. Vid projektarbete gäller det att inte förlora perspektivet på den organisatoriska helheten som arbetet ingår i. System betraktas också som helheter som är större än summan av delarna som utgör dem. Att ta hänsyn till systemets intressenter anses mycket betydelsefullt för att utveckla väl fungerande system. Dessa metodologier betonar vikten av att i analysfasen reda ut vad problemet faktiskt är så att resurser inte går till spillo på att enbart bemöta symptomen på ett underliggande problem (ibid).

Till skillnad från ett hårt systemtänkande där problem anses vara tydligt definierade riktar organisationsorienterade metodologier uppmärksamhet mot mer luddiga och oklara problemsituationer där iblandade parter upplever att något bör göras men inte lyckas sätta fingret på vad detta är. Gränsen mellan metoder och metodologier är varken knivskarp eller odebatterad, och vissa metodologier tillhandahåller konkreta steg som systemutvecklare kan följa för att reda ut problemsituationen och strukturera upp projektarbetet (ibid).

Blandade metodologier utgör sammansättningar av inslag från andra metodologier, verktyg och tekniker för systemutveckling. De har kombinerats för att ge stöd åt organisationer med behov av heltäckande lösningar (Avison och Fitzgerald 2003).

Många systemutvecklingsmetoder innehåller faser som härstammar från livscykelmodellen, är en linjär modell som via ett par enkla definierade steg övergripande beskriver de moment som ska genomföras vid en systemutveckling. Avison och Fitzgerald (2003) och Beynon-Davies (2002) nämner även att det finns flera varianter och variationer i livscykelmodellen, men skillnaderna som finns mellan de olika presentationerna av livscykelmodellen, eller vattenfallsmodellen som den ibland kallas, är egentligen inte intressant i sig då modellerna har som avsikt att visa upplägget i en systemutveckling eller fungera som en mall vid skapandet av en egen utvecklingsmetod eller för att lägga upp ett sätt att arbeta (Avison 2003). Vid närmare granskning har vi upptäckt att även om modellerna vid första anblick såg ut att skilja sig så var skillnaderna minimala, skillnaderna handlade främst om att moment eller momentdelar var uppdelade eller sammanfogade, beroende på synvinkeln, men innehållet var detsamma.

De moment som beskrivs av Beynon-Davies är följande:

- Systems conception
- Systems analysis
- Systems design
- Systems construction
- Systems implementation

- Systems maintenance

Avison och Fitzgerald (2003) beskriver momenten i modellen såhär:

- Feasibility study
- System investigation
- Systems analysis
- Systems design
- Implementation
- Review and maintenance

Livscykelmodellen finns beskriven på flera sätt, men momenten är i huvudsak de samma. Modellen förklaras även som en iterativ variant där analys, design-, konstruktions- och implementationsdelarna utförs återkommande vid behov.

Livscykelmodellen är den modellen som de flesta systemutvecklingsmodeller bygger på (Beynon-Davies 2002; Avison och Fitzgerald 2003). Livscykelmodellen/vattenfallsmodellen skiljer sig kraftigt från vanliga systemutvecklingsmetoderna främst genom att den inte har den detaljnivå över de olika momenten som krävs. Detta gör att den som den är presenterad inte fungerar så bra som utvecklingsmetod i praktiken.

Modellen har därför haft sitt ursprung främst som mall för att skapa de systemutvecklingsmetoder som uppkommit med tiden eller som mall för hur ett upplägg av ett utvecklingsprojekt bör gå till om en färdig metod inte följs. Varför livscykelmodellen, trots sina indelningar i och presentation av moment, inte fungerar som systemutvecklingsmetod kan förklaras genom att ta upp den lista över moment som en metodologi ska innehålla enligt Avison och Fitzgerald (2003):

- En serie faser som beskriver utförandet, även innehållandes under-faser
- En serie tekniker som beskriver hur kostnad och annat ska räknas ut, samt hur själva utvecklingsprocessen av mjukvaran ska gå till
- En serie verktyg som hjälper till med exempelvis analys
- Ett tränings-schema, ev med uppsatta kurser och utbildning för de inblandade utvecklarna
- En filosofi

De för oss i denna uppsats, viktigaste momenten i livscykelmodellen är de som tas upp från och med "System Analys", vilket har olika placeringar i olika presentationer, men placeringen av detta moment sker i början på de livscykelmodeller vi tagit del av. Vi uppfattar dessa genomgångar av livscykelmodellen som innehållsmässigt likartade. Skillnaden ligger i olika rubriksättningar och att Beynon-Davies förklarar modellen mer kortfattat än Avison och Fitzgerald.

Vi kan sammanfattningsvis notera att metodologierna i princip har en del gemensamma moment. De är indelade i distinkta faser och i alla ingår någon form av analys. Vissa metodologier lägger större tonvikt vid analyser än andra, men det är ett gemensamt moment som de innehåller och som föregår övriga moment, även om det innebär iterativa processer där analys återkommer vid behov. Efter att ha tagit del av Avisons och Fitzgeralds (2003) översikt över metodologierna har vi kommit fram till att det vore lämpligt att i analysfasen lägga ytterligare tonvikt vid riskanalys och säkerhetsplanering.

3.4 Behov av formaliserade metoder

Bruket av formaliserade metoder utvecklades gradvis som svar på upplevda problem inom systemutveckling. Förutom att funktionaliteten hos många informationssystem uppfattades som undermålig tog de lång tid att utveckla, vilket ledde till kostnader som överskred budget. Formaliserade metoder började utformas för att möta behovet av mer strukturerat systemutvecklingsarbete och högre kvalitet på de utvecklade systemen. Från slutet av 1960-talet och framåt har det ökade intresset för strukturerad systemutveckling lett till att massor av olika metoder har utformats (Fitzgerald et al. 2002).

Under denna tidsperiod har kraven på informationssystem förändrats dramatiskt för att de ska kunna stödja informationsbehandling i ett världsklimat som ständigt blir mer komplext och dynamiskt. Parallellt med snabb teknologisk utveckling har ekonomin globaliserats, vilket har förändrat hela konkurrenssituationen. Arbete kan idag utföras av en billigare leverantör i ett annat land och överföras till en samarbetspartner omgående via Internet (Avison och Fitzgerald 2003). Så som vi exemplifierar med vårt empiriska material ställer sådan elektronisk överföring och lagring högra krav på skydd av information.

Formaliserade metoder för systemutveckling definieras av Fitzgerald et al. (2002) som alla metoder som formellt använts och dokumenterats hos en viss organisation, både de egenutvecklade och de kommersiellt tillgängliga metoderna. Formaliserade metoder följs inte alltid exakt så som de är nedskrivna och de föreskriver inte heller nödvändigtvis absoluta regler för hur systemutvecklingarbete ska gå till utan erbjuder snarare vägledning. Fitzgerald et al. delar upp metodernas roller i två skilda huvudkategorier som båda påverkar systemutvecklingsarbetet:

Rationella metodroller ligger på en intellektuell nivå och handlar om varför metoder överhuvudtaget behöver användas i systemutvecklingen. De rationella metodrollerna beskriver hur metoden används för att dela upp de större processerna under utvecklingsarbetet i mindre steg, där olika utvecklare kan ta tag i olika uppgifter och sedan förena sina resultat till en lösning, men även att ge projektledningen större kontroll över utvecklingsprocessen.

Till de rationella rollerna hör den kommunikativa aspekten av metodanvändning. Metoden blir ett gemensamt språk som alla de olika inblandande parterna kan förstå. Den ekonomiska roll en utvecklingsmetod spelar i projektet som den används i är också rationell. Denna underlättar för projektledningen att fördela sin arbetskraft och resurser dit det vid tillfället behövs bäst i processen. Dessa roller bildar tillsammans ett strukturellt ramverk för kunskapsutbyte och processdokumentation, och genom att standardisera processen främja utbytet mellan utvecklarna. (Fitzgerald et al. 2002.)

Politiska roller som metoder kan spela är mer dolda till sin natur än de rationella rollerna. De politiska rollerna manifesteras inte lika öppet eftersom de är mer relaterade till förtroende och processer som pågår mellan människor och grupper inom organisationen. Politiska metodroller kan förse metodförespråkare med en maktbas som de kan använda för att förbättra sin position i förhållande till andra grupper eller personer. Ett exempel på politisk metodroll är en upplevd trygghetsfaktor, att rätt praxis har använts under systemutvecklingsprocessen. Politiska metodroller strukturerar upp processen på ett mer professionellt sätt och hjälper dessutom att skydda systemutvecklare mot alldeles för snäva deadlines och orimliga krav användare kan ställa.

På liknande sätt finns det även en legitimitetsfaktor i politiska metodroller. En organisation kan påstå sig använda en viss metod för att vinna kontrakt eller marknadsfördelar, exempelvis kan detta ske vid ISO-certifiering. Om de som ansvarar för ISO-utvärderingen blir övertygade av dokumentationen och argumenten får organisationen en legitimitetshöjande ISO-certifiering (Fitzgerald et al., 2002).

3.5 Utvecklare och utvecklingskontext

Utvecklingskontext är enligt Fitzgerald et al. (2002) den mest komplexa komponenten i systemutvecklingsprocessen. Författarna anser även att denna komponent är den viktigaste då den kräver att utvecklarna analyserar den utförligt för att uppfylla kundernas krav och förväntningar på systemet. Med utvecklingskontext menas det användningsområde som ett system utvecklas för, samt det sammanhang det utvecklas i. Fitzgerald et al. (2002) förespråkar att det är främst utifrån kontexten man ska välja vilka delar ur metoderna som passar för det aktuella projektet.

Varje nytt projekt har en unik utvecklingskontext, och alla faktorer som ingår i kontexten påverkar hur systemet ska utvecklas, och i denna kontext innefattas bland annat teknik, organisationskultur, funktionalitet, effektivitet, etc. Fitzgerald et al. (2002) menar att det går att välja metod och utvecklare vid ett projekt, dessa faktorer kan alltså påverkas och varieras, men man kan inte välja en annan kontext. Åter menar de att det är utvecklarna som har möjlighet, och även ett visst ansvar, att genom informationssystemet/systemen skapa en bättre kontext.

Utvecklingskontexten har en allt viktigare extern aspekt också. Dagens komplexa och dynamiska informationssamhälle är starkt påverkat av globaliseringen, och moderna organisationer konkurrerar i allt större utsträckning på en världsarena, samtidigt som teknologin snabbt rör sig framåt. Tjänster kan erbjudas till betydligt lägre kostnad från samarbetspartners i framväxande ekonomier i Asien än i organisationers egna hemländer, vilket gör att informationssystem utvecklas i en mycket hårdare konkurrensmiljö än tidigare. Detta skärper ytterligare kundernas krav på funktionalitet och kvalitet (Avison och Fitzgerald 2003).

Vid systemutveckling finns det många faktorer som påverkar slutresultatet, bland annat påverkar utvecklarens eller utvecklarnas kompetens samt erfarenhet väldigt mycket av slutresultatet. Fitzgerald et al. menar också att det finns ett flertal undersökningar som visar att utvecklarens kompetens och erfarenhet är väldigt betydelsefulla faktorer. Mer erfarenhet resulterar i rutin samt bättre och snabbare slutresultat. Utvecklarna lär sig med tiden vilka lösningar som är bäst och vad som fungerar i vilket sammanhang (Fitzgerald et al., 2002).

Även kreativitet kan lyftas fram som en viktig faktor vid systemutvecklingen. Dock finns det åtskilliga metoder, främst formaliserade metoder, som är utformade för att utvecklaren inte ska distraheras för mycket av sin egen kreativitet under utvecklingsprocessen. Formaliserade metoder strukturerar upp arbetsgången för att uppgiften ska hamna i centrum och för att det ska bli lättare att uppfylla kundens kravspecifikationer. För mycket fokus på kreativitet kan

även ta lång tid så att utvecklingskostnaderna överskrider projektets budget, vilket är oerhört vanligt (ibid).

Utvecklare startar oftast sin karriär inom systemutveckling med att hålla sig starkt till metoderna som finns, för att sedan, med tiden lämna dem, för att efter detta upptäcka att detta inte är effektivt nog och därefter återgå till att följa någon metod. Fitzgerald et al.. (2002) illustrerar detta med en S-kurva och menar att detta är ett tecken på att utvecklarna med tiden känner sig säkrare på sina uppgifter, men upptäcker till slut att användningen av formaliserade metoder förbättrar deras produktivitet.

Det är inte alla systemutvecklare som är utbildade specialister. I viss utsträckning har användare själva utvecklat de system de arbetar med varje dag utifrån sin kunskap om sina respektive yrkesområden. Sådana system kan dock visa sig svåra att underhålla just eftersom de blir betydligt mer beroende av personen eller gruppen som skapat dem på grund av att dokumentation och formaliserade metoder saknats i systemutvecklingen (Avison och Fitzgerald 2003).

Ett system kan definieras som en uppsättning beståndsdelar som interagerar för att uppfylla ett gemensamt mål inom ramen för en avgränsning, det vill säga helheten som systemet utgör. Komponenterna har olika deluppgifter att klara av som ingår i systemets större uppgifter. Nyckelorden i systemdefinition är alltså interrelaterade beståndsdelar, avgränsning och gemensamt syfte. Elementen som ingår i ett system är beroende av varandra för att kunna bidra till systemets huvudsakliga uppgifter, och om något av dessa subsystem går sönder påverkas alla de andra också eftersom den gemensamma uppgiften då inte kan utföras. Ett fungerande system skapar syngergieffekter genom att producera ett resultat som subsystemen inte skulle ha kunnat åstadkomma separat. Helheten blir större än summan av delarna (Marakas 2003).

Vid systemutveckling ställs systemutvecklare inför många beslut som måste tas för att utvecklingsarbetet ska kunna fortsätta framåt. De måste ta hänsyn till om systemet ska kunna förändras med tiden, om ett standardsystem krävs eller om det krävs ett nytt system. Vid utveckling av helt nya system måste systemutvecklarna ta hänsyn till om uppgifterna som ska lösas är unika till sin karaktär eller om det finns tidigare lösningar på denna typ av problem som går att återanvända. Dessa faktorer påverkar alla valet och användningen av en metod (Mathiassen 2001).

3.6 Teorisyntes

Vid vår litteraturgenomgång upplevde vi en skillnad i fråga om hur stor vikt som läggs vid diskussion av säkerhetsaspekter. I böcker om systemutvecklingsmetoder behandlades säkerhet översiktligt och ytligt. Det tycktes falla utanför ramen för de aspekter av systemutveckling som författarna ville framhålla. Vi fann inga djupare diskussioner om säkerhetsutmaningar och åtgärder som systemutvecklare borde vidta med dem i åtanke. I de vetenskapliga artiklarna vi studerade framträdde en annan bild av säkerhetsarbete. Här betonades potentiella risker tydligare och vikten av att motverka dem poängterades. Säkerhetsplanering framhölls som en viktig del av systemutvecklingen och inte som en separat tillsats.

Vi tolkade denna skillnad som att litteraturen speglar en pågående process, att vikten av säkerhetsplanering vid systemutveckling ständigt ökar, och att ämnet behandlas olika eftersom artiklarna är mer högaktuella än böckerna och dessutom publiceras betydligt snabbare. Detta stödjer vår uppfattning att säkerhetsplanering bör kombineras med de formaliserade metoderna som kan ligga till grund för systemutveckling i en organisation, och att detta är en utmaning som även vi själva bör vara beredda på att möta som deltagare i framtida systemutvecklingsprojekt.

4 Empiri

Här tolkar och sammanställer vi det empiriska materialet från våra intervjuer med de olika respondenterna som medverkat i studien.

4.1 Intervju 1

Respondent nummer ett har titeln systemspecialist och är anställd som en av avdelningens systemutvecklare. I grund och botten är han utbildad till elkraftsingenjör och har senare byggt på med kurser med inriktning mot programmering och systemutveckling. Han har över 25 års praktisk erfarenhet och började programmera i Assembler i stordatormiljö i slutet av 1970-talet. Idag arbetar han huvudsakligen med inköpta lösningar som modifieras efter behov. Utvecklarna får tillgång till all källkod och kan anpassa programvaran precis som de vill. Den största fördelen vår respondent ser i detta är att det sparar enormt mycket tid och pengar att bygga vidare på en färdig grund och slippa skriva allt från början.

Främst arbetar han mot externa kunder men står även för utveckling och underhåll av systemen som behövs för avdelningens egen produktion. Han bekräftar uppgiften från respondent 1 om att metoder blivit viktigare idag. Enligt hans uppfattning har formella metoders betydelse ökat på grund av kraven på effektivitet i en konkurrensdriven bransch. Metoder ger struktur och vägledning i arbetet, och det blir exempelvis enklare att lägga fram offerter till kunder när man följer en metod som projektmodellen Promise.

Hans arbete är uppdelat i delprojekt, och han uppger att det är viktigt att som projektdeltagare hålla sig inom tidsramarna och ha en förståelse för helheten i uppgiften. Det räcker inte att vara skicklig inom sitt eget område eftersom man som systemutvecklare bara är en del av systemutvecklingsprocessen och därför behöver ha förståelse för samtliga delar av projektet och kunna sätta sig in i de olika parternas terminologi.

Formaliserade metoder i systemutveckling förenklar också underhållet av systemen, eftersom de som ska uppdatera koden inte alltid är samma personer som skrivit den, och då är det viktigt att ha en dokumenterad standard som alla systemutvecklare kan följa. Han efterlyser tydligare kravspecifikationer från kundsidan, både i fråga om säkerhet och i största allmänhet, eftersom dessa ofta inte är särskilt klart formulerade. Vissa kunder saknar förståelse för möjligheterna och begränsningarna hos en teknisk lösning, som kan visa sig kräva mycket intensiva arbetsinsatser fastän den låter enkel när den diskuteras vid möten mellan parterna.

Systemutvecklingsprojekt börjar med möte med kunden där riktlinjerna för projektet dras upp, och man förklarar vad kunderna kan vänta sig av produkten eller tjänsten. Så här arbetar man inom organisationens projekt för att samtliga parter ska kunna sätta sig in i situationen och för att bana väg för smidigare kommunikation. Vår respondent betonar att en stor fördel med att lägga upp arbetet så är att det blir mångsidigt eftersom flera olika yrkesgruppers

perspektiv representeras. Systemutvecklingsprojekt brukar omfatta projektledare, chefer, beslutsfattare och arbetsgrupper från skilda avdelningar inklusive kundrepresentanter

I ett mindre team blir det lättare att behålla fokus på huvuduppgiften så att arbetet inte splittras upp av för många viljor. Det finns en risk att olika yrkesgrupper kommunicerar förbi varandra eftersom de talar olika språk, och det är inte alltid lätt att sätta sig in i varandras perspektiv. Det är inte heller ovanligt att kunder behöver övertygas om vikten av styrning under projektets gång. Krav måste formaliseras från båda sidor så att det inte uppstår missförstånd som underminerar projektet.

En av de stora riskerna han framhåller när det gäller systemen är strömavbrott, eftersom databaser kan ta så stor skada av oväntade stopp att de måste rekonstrueras. Det finns vissa färdiga lösningar som kan hjälpa till med sådan databasrekonstruktion, och hur sårbar organisationen är inför plötsliga incidenter beror på backup, vilket han anser att man borde lägga ännu större tonvikt vid än i dagens läge.

4.2 Intervju 2

Vår andra respondent har åtta års erfarenhet som projektledare inom avdelningen. Hon är formellt utbildad till fritidspedagog och har även erfarenhet från sjukvård och barnomsorg. Rollen som projektledare har hon gradvis vuxit in i, och det är behoven på avdelningen som har format hennes arbetsuppgifter. Vid behov har hon tagit på sig nya ansvarsområden och utvidgat sin kunskapsbas. Hennes huvudsakliga ansvarsområde är att ta fram rutiner, hålla i aktivitetsplanering och delegera besked från centralkontoret. Hon håller kvalitetsmöten med teamleaders för de olika uppdragen och arbetar en hel del med säljsupport, offerter och frågor som gäller ISO-certifiering, vilket organisationen fick runt millennieskiftet.

Hon ansvarar för mindre bitar av säkerhetsområdet och har arbetat med detta sedan 2002. De viktigaste faserna inom säkerhetsplanering är enligt hennes uppfattning att ta fram backup-rutiner och krisplaner. Lyckligtvis har ännu inte någon allvarligare incident inträffat där betydande mängder data gått förlorade, men hon uppger att riskanalyser behöver genomföras och att avdelningen behöver en tydlig handlingsplan för en eventuell krissituation. En sådan plan är under utveckling, och det som då har högst prioritet är att kunna ersätta skadade eller förstörda maskiner så att produktionen kan återupptas snarast, samt att via en central backup-nyckel kunna återställa information som påverkats av incidenten.

De största omedelbara hoten hon kan tänka sig är inbrott, brand, och översvämning. Kontoret ligger nämligen på bottenplan och har tidigare varit i farozonen för vattenskador. Hackerangrepp uppger hon att organisationens system utsätts för kontinuerligt, men i denna fråga hänvisar hon vidare till en kollega som har mer direkt ansvar för att åtgärda sådana problem med hjälp av tekniska lösningar. Organisationens system skyddas enligt en central säkerhetspolicy.

Policies är formulerade och dokumenterade för ett antal säkerhetsrelaterade områden, exempelvis en policy för incident- och krishantering, där olika kategorier av störningar definieras. En incident är en händelse som stör organisationens ordinarie verksamhet eller hotar viktiga värden i verksamheten. Kris är ett allvarligare tillstånd där strategiska värden

hotas i ett förlopp som organisationen saknar eller riskerar att förlora kontrollen över. Vikten av att följa upp hantering av incidenter och kriser betonas, så att organisationen kan införa åtgärder som minskar risker och konsekvenser.

Syftet med policyn är att skydda information, förtroendekapital och varumärken och att hantera säkerhetsproblem på ett professionellt sätt. Att reagera snabbt på störningar av tjänster och leveranser är avgörande för att begränsa förlusterna för kunder och för den egna verksamheten. Vid riktigt allvarliga leveransförseningar riskerar organisationen att åläggas att betala vite till drabbade kunder. Policyn formulerar koncernens åtagande gentemot kunder, medarbetare och marknaden som organisationen är verksam inom.

Det finns också en informationssäkerhetspolicy som slår fast att kunderna måste erbjudas den säkerhetsnivå de förväntar sig, och att sekretess måste respekteras, inte bara när det gäller kunduppgifter utan även i fråga om intern information av ekonomiskt och strategiskt värde. Policyn betonar att verksamhetens framtid är beroende av att kunder har förtroende för den informationssäkerhet som erbjuds. Det måste kännas tryggt att anlita organisationen som samarbetspartner. Vid systemutveckling åt kund är det kundens ansvar att fastställa krav på säkerhetsskydd för både projektet och systemet som ska levereras, och den egna organisationen ska dokumentera dessa krav i avtalet mellan parterna. Har specifika säkerhetskrav inte ställts upp av kunden ska detta också uttryckligen dokumenteras för tydlighetens skull.

Enligt internationell standard är syftet med informationssäkerhet att värna om sekretess, riktighet och tillgänglighet hos informationen, som också ska vara spårbar. Det är informationens ägare, exempelvis kunden, som avgör vem som ska ha tillgång till uppgifterna. Likaså ska informationen inte kunna manipuleras av obehöriga användare. Det är bara de parter som enligt avtalet är behöriga som ska kunna ta fram uppgifterna och följa upp ändringar eller hantering av dem. Liknande regler gäller för företagshemlig information som bara ska kunna användas av dem som behöver den för att kunna utföra sina arbetsuppgifter.

Formella metoder spelar stor roll i arbetet eftersom dokumentation av rutiner hjälper till att klargöra för personalen vad som gäller i ett visst läge. Dokumenterade rutiner kan alla följa utan att behöva vara beroende av att ha tillgång till en person man brukar gå och fråga vid osäkerhet, men vår respondent betonar att detta också kräver mer intresse och engagemang hos gemene man. En av de viktigaste metoderna är projektmodellen Promise som innehåller milstolpar man måste klara av för att kunna gå vidare till nästa fas i projektarbetet. Detta är ett effektivt sätt att säkerställa att viktiga moment inte glöms bort och att projektplanerna godkänns på ett tidigt stadium. När projektdokument tagits fram ger beställaren hos kunden sitt godkännande och även en slutrapport formuleras, som vägledning till framtida projekt.

Rutinerna som är relaterade till ISO-certifieringen är framtagna av revisionsbolaget det Norske Veritas, och revisioner av de säkerhetsstandards som är ISO-relaterade genomförs på intern och extern nivå. Tidigare brukade kunder efterfråga ISO-certifiering vid förhandling om offerter, och enligt vår respondents uppfattning är det sannolikt att kunder nu snarast förutsätter att ett stort IT-företag lever upp till ISO-kraven. Hela organisationen är indelad efter processer, och denna arbetsmetod har tagits fram centralt. Olika branscher får olika certifieringar och det finns en ISO-certifiering för IT-säkerhet också.

När systemet drabbas av säkerhetsbrister kan det resultera i att enskilda PC inte fungerar eller att en hel server kraschar med produktionsbortfall som följd. Då blir det svårt att leverera till kund enligt avtal eftersom stora volymer elektroniska dokument läggs på hög, och produktionen kan släpa efter i flera dagar eller i värsta fall veckor. Vid ett tillfälle stängdes internnätet ner på grund av ett virushot, och då avbröts den elektroniska kommunikationen inom företaget, och det gick inte heller att koppla upp sig mot Internet.

Vid en säkerhetsbrist prioriteras felsökning, vilket kräver goda rutiner för omstart av maskinpark. Viktigast är att få igång produktionen igen, och detta kräver att maskinerna fungerar. Det har tidigare uppstått problem med mjukvara och överföring efter driftstopp. I sådana lägen är det viktigt att gå ut med så tydlig information som möjligt till kunderna om vad som inträffat och kontrollera att all deras information kommit med i överföringen. Kommunikation är förutsättningen för smidig återgång efter driftstopp. Vår respondent kunde inte erinra sig några specifika säkerhetskrav kunder brukar ställa på systemen, och det är huvudsakligen arbetet med fakturor som omges av strikta sekretesskrav på grund av hanteringen av konfidentiella kunduppgifter. Nyligen har en kund uttryckligen efterfrågat en krisplan, men ofta förutsätter kunder att arbetet med backup fungerar. Däremot är det vanligt att de efterfrågar tillgång till support.

Avdelningschefen har det lokala ansvaret för arbetet med datasäkerhet och skydd av information, och på central nivå skickar ledningen ut policies till IT-avdelningar som ser till att direktiven sprids vidare i ledet. Ledningens roll i säkerhetsarbetet är oerhört viktig eftersom det bara är de som kan höja kvaliteten på säkerheten och se till att deras policies följs på lokal nivå. Det finns officiella rutiner för hantering av säkerhetsincidenter. Backup finns men inte på alla uppgifter. Den stora utmaningen är att verkställa planerna, vilket kostar pengar.

Arbete med dokumenterade rutiner för återställning av skadad eller förlorad information pågår för fullt och är ett livligt omdiskuterat ämne. Det önskvärda målet är att produktionen ska vara igång igen inom max åtta timmar efter ett driftstopp men helst hälften. Organisationen har kommit en bra bit på väg och strävar efter att förenkla underhåll av backup-material. För att åstadkomma detta ser man över hela miljön på avdelningen. Någon helt ny produktion har aldrig behövt byggas upp eftersom avdelningen hittills varit förskonad från allvarligare incidenter.

Mindre övningar i krishantering har ägt rum i samband med serverkrascher, vilka ofta beror på att serverns minneskapacitet inte räcker till för all data den måste hantera. Varje ny kund innebär ett stort antal uppgifter, vilket kräver enormt lagringsutrymme. Arrangerade övningar i krishantering har inte hållits, utan dessa har varit övningar i praktiken, som svar på en uppkommen situation. System och backup-material ses över kontinuerligt, liksom servrarna. Tidsbrist har försenat arbetet med en krisrutin, men en sådan kommer att formuleras exakt. Ännu finns inga tillfälliga rutiner att använda i väntan på att produktionen ska återgå till det normala. Sådana rutiner är svåra att sätta upp eftersom man då måste ta hänsyn till ett stort antal faktorer i olika scenarion.

Personalen spelar också en viktig roll i det vardagliga arbetet med säkerhetsrutiner eftersom alla har tillgång till Internet via sin PC. Vår respondent har rekommenderat att alla inom avdelningen tänker sig för innan de öppnar mail och besöker webbsidor som de inte säkert kan lita på innehållet hos. Under en tidigare ägare fanns en säkerhetsplan, och det blir ofta teamleaders uppgift att sprida rekommendationerna vidare till den personal som arbetar inom

deras ansvarsområde. Vår respondent anser att det kan vara en god idé att ta upp sådana här vardagliga säkerhetsfrågor på avdelningens enhetsmöten, vilka brukar hållas en gång i månaden och där all personal inom avdelningen samlas för att ta del av aktuell information.

4.3 Intervju 3

Vår tredje respondent är enhetschef och har det övergripande ansvaret för avdelningen. Hon har arbetat inom organisationen sedan 1978 och var tidigare stansoperatris, arbetsledare och anställd på revisionsbyrå. Hon anser själv att hon borde vara mer involverad i säkerhetsarbetet än vad hon är i dagsläget. Organisationen har en plan för nödsituationer, men hon upplever att avdelningen bör vara bättre förberedd om en brand skulle uppstå eller om någon form av bombattentat drabbade byggnaden. De konkreta säkerhetsåtgärderna i ett sådant läge bör förtydligas så att alla vet vad de ska göra.

Att enhetschefen tog med bombattentat bland de tänkbara riskerna är inte enbart en teoretisk spekulation. Vid ett tidigare tillfälle har avdelningen drabbats av skadade vattenledningar på grund av en mindre bomb som exploderade i fastigheten. Ingen vattenskada uppstod i lokalen, men det tog ett antal timmar att få tillgång till kranvatten igen. Även stöld har förekommit i form av inbrott, då värdefulla maskiner gick förlorade.

Enhetschefens roll i säkerhetsarbete går huvudsakligen ut på att delegera uppgifter, sprida information vidare inom avdelningen och se till att säkerhetsföreskrifter efterlevs av personalen hon ansvarar för. Via organisationens nätverk har avdelningen full koll på sekretess, och brandväggarna motverkar intrång på servern. Hon uppger att säkerhetsarbete har blivit mer betydelsefullt med tiden. Att säkerställa leverans till kund har alltid varit en prioritet, men det är först under det senaste decenniet som hot om dataintrång har uppstått.

Betydelsen av metoder har ökat och stora summor har investerat i att bygga upp kvalitetscertifiering som motsvarar ISO-kraven. Hela arbetet är centrerat kring leveranser, och dokumentering av processer och historik är en viktig del av kvalitetscertifieringen, i och med att leverans till kund är det som verksamheten vilar på. Avdelningen arbetar så här eftersom ett koncernbeslut togs om detta under en tidigare ägare. En intern revision av säkerhetsstandards är på väg, och en extern genomfördes förra året. Då kan stickprov tas på dokumentering av vilket arbetsmoment som helst för att visa att kvaliteten håller måttet.

Vår respondent anser att ett bra mått på effekter av förbättrande åtgärder är att avdelningen så gott som alltid vinner förhandlingen om kunder vid en offertprocess eftersom organisationen inger förtroende och har ett gott namn i branschen. I grund och botten strävar organisationen efter ett kontinuerligt förbättringsarbete med säkerhetsrutiner. Vad som ska göras om säkerhetsbrister uppstår finns dokumenterat i en krisplan, som utgör underlag till en handlingsplan så att konsekvenserna av en eventuell kris kan begränsas.

Om säkerhetsproblem uppstår prioriteras kunden och leveranserna, och ansvaret för arbete med säkerhet och skydd av information ligger hos henne själv som enhetschef. Det finns också en säkerhetsansvarig på central nivå. De dokumenterade säkerhetsrutinerna är avstämda mot ISO-certifieringen. Koncernen har dessutom en handlingsplan, och

organisationen är tydliga med vad som tillämpas. Under en tidigare ägare fanns ännu mer detaljerade direktiv om säkerhetsföreskrifter.

Enligt vår respondents erfarenhet ställer kunder specifika säkerhetskrav på systemen, men nu för tiden tar de ofta för givet att organisationen är ISO-certifierad. Kunder efterfrågar ofta zipade filer med kryptering och lösenordsskydd. Skulle säkerhetsproblem uppstå får ingen information gå förlorad. Där är det nolltolerans som gäller, och vår respondens vet inte på rak arm inom hur lång tid normal produktion ska kunna återupptas men hon anser att det bör ordnas så snart som möjligt med minsta möjliga tjänsteförlust.

Rutiner för att återställa skadad eller fel överförd information efter säkerhetsproblem beror på incidentens art. Organisationen har investerat miljonbelopp i backup både lokalt och i Stockholm. Information som är av kritiskt värde för kunden lagras på speglade diskar. Efter säkerhetsincidenter och justerande åtgärder övervakas systemen extra, och backup görs på information från produktionskritisk server. Det finns tre kritiska servrar som kräver backup, och de förvaras i en datahall som utrustats med sprinklersystem till skydd mot brand, och maskinerna står på ett upphöjt golv så att de inte ska behöva stå i vattenpölar. Inga speciella övningar hålls för personal som ska medverka vid återgång till normal drift.

I nuläget diskuteras vilka tillfälliga rutiner som ska användas i väntan på att återgång till normal drift kan genomföras. Ny personal informeras om hur var och en kan bidra till säkerheten, men mail med opålitligt innehåll släpps inte igenom brandväggen. Nätet är utformat för att skydda organisationens informationsdepåer, och rutinerna är idag huvudsakligen automatiserade. Intranätet är omgärdat av säkerhetshöjande rutiner, och man behöver kontakta helpdesk och identifiera sig som behörig användare för att få tillgång. Nätet är lösenordsskyddat, och en användare har tre försök på sig att ange rätt lösenord. Sedan låses kontot. Ansvarsbeskrivningar för säkerhetsarbete finns, och dessa omfattar även befattningsbeskrivningar.

4.4 Intervju 4

Avdelningens tekniskt ansvarige är vår fjärde respondent. Han har arbetat fyra år i företaget, först som dataregistrerare under en prövoperiod, och sedan har han gradvis vuxit in i rollen som ansvarig för de tekniska aspekterna av datasäkerhet. Utöver sin gymnasieutbildning har han byggt på med certifikat och kurser i SQL och NT, som var baserade på Microsofts lösningar. Dessutom har han fått internutbildning i program för dokumenthantering, som är avdelningens huvudsakliga uppgift. Det är detta som menas med produktion. Idag är han ansvarig för all säkerhet inom avdelningen. Det är han som ser till att maskiner, servrar och nätverket i sin helhet fungerar som det ska. Han sköter backup, underhåll av brandvägg och antivirusprogram.

Lösningen som genererar backup på information heter Legato, och hur mycket backup som lagras varierar beroende på kundkrav. Informationen kan sparas lokalt eller hos en depå. All vital information överförs via VPN mellan avdelningen och kunden, och det krävs programvara och certifikat för att ansluta till organisationens nätverk, och informationen är både krypterad och lösenordsskyddad. All hårdvara hålls avskärmad från Internet. IP-adresser skyddas inom det interna nätet.

Säkerhet har han arbetat med professionellt de senaste tre åren, men han har alltid haft intresse av området och varit observant på de brister som system kan innehålla och som gör dem sårbara för intrång. Han ansvarar för säkerhetsfrågor både internt och ut mot kunder. Eftersom han inte är formellt utbildad skapar han mest sina egna arbetsmetoder genom att pröva sig fram till den mest effektiva lösningen i den aktuella situationen, vilket han själv anser gör honom mycket flexibel i sitt arbete.

Han anser att vilka metoder man än följer så är det viktiga att man har ett bollplank att utbyta idéer med hela tiden eftersom input hjälper en framåt. Om system behöver låsas vid uppdateringar och test arbetar han metodiskt i olika steg, som går ut på att avskärma de berörda maskinerna så att information inte läcker ut under processen. Han följer huvudsakligen interna arbetsmetoder och är inte inblandad i interna eller externa revisioner av säkerhetsstandards.

Inom avdelningen arbetar man ofta på ett sätt som skiljer sig från andra avdelningars eftersom uppgifterna är av en annorlunda natur. Dokumenthantering är bara en del av organisationens verksamhet, och både systemen och maskinhallen är annorlunda än andra filialers. Bland annat arbetar avdelningen mot en snabb Unixmaskin. Nätet är omgärdat och skyddat från direkt kontakt med Internet, och den tekniskt ansvarige håller sig uppdaterad via nyhetsgrupper om aktuella säkerhetsförbättringar på marknaden. Han säkerställer att rutinerna blir bättre efter uppgraderingar genom att testa lösningen i en avskärmad miljö och se om den fungerar innan den omsätts i praktiken.

Om en säkerhetsbrist uppstår dras nätverkskabeln ut till att börja med för att begränsa problemområdet så att ett eventuellt virus inte sprids mellan maskinerna. Ofta avskärmas alla maskiner som är anslutna till samma switch och de kontrolleras allihop med säkerhetsprogram och antivirusprogram. Leverans till kund har högsta prioritet i ett sådant läge. Deadlines ska hållas i så stor utsträckning som möjligt eftersom kunden står i centrum.

Ledningens roll i arbetet med datasäkerhet spelar in i början av en överenskommelse när offert skrivs och säkerhetsgarantier till kund formuleras. Ansvaret ligger hos de kvalitetsansvariga som meddelar vidare vad som utlovats till kunden. Beslut om säkerhetsnivå är upp till kunden att fatta, sedan är det organisationens uppgift att tillmötesgå kraven. Organisationen är ett tjänstebolag som erbjuder kunder vad de vill ha. Om detta av någon anledning är svårt att åstadkomma exakt formuleras alternativa lösningsförslag. Säkerhetsrutiner är avstämda mot ISO-certifieringen, exempelvis tystnadsplikt och vad personal får och inte får använda maskinerna till. Under en tidigare ägare tillämpades ISO-9000, och arbete måste utföras så att det stämmer med villkor för certifiering.

Kundernas prioritering brukar vara att vitala data måste skyddas och inte får hamna i fel händer. Information får bara hanteras av avdelningens personal som har skrivit på överenskommelser om sekretess. Vilka säkerhetskrav kunder ställer varierar. Vissa uppdrag omges av tyngre sekretesskrav än andra. Om en säkerhetsincident skulle inträffa för avdelningen stöd från servicedesk som skickar ut personal som hjälper till. Vår respondent hanterar då den tekniska sidan med underhåll av hård- och mjukvara, och en kollega till honom tar hand om kundspecifika data och ser till att informationen hålls intakt och överförs rätt.

Vissa uppdrag utförs under mer tidspress än andra, men generellt vore det oacceptabelt om information gick förlorad på grund av en säkerhetsincident. Det finns dokumenterade rutiner för att återställa skadad eller förlorad information och återgå till normal drift snarast möjligt. Unixmaskinen lagrar dokument 30 dagar, och äldre data finns hos bandstationen. Vår respondent påpekar att det är viktigt att ta hänsyn till att system kan vara extra känsliga efter säkerhetsproblem och justerande åtgärder. Därför testar han utförligt i avskärmad miljö innan nya eller reparerade maskiner sätts i drift. Maskiner är beroende av varandra i systemet, och brister det i ett steg så får det konsekvenser i nästa också. Därför måste problemområdet isoleras genom lokala test så att det framgår var ett eventuellt fel ligger och så att resurser kan sättas in för att lösa detta så snabbt som möjligt.

Det finns inga övningar för personal som ska medverka vid en återgång till normal drift efter en säkerhetsincident. Exempel på tillfälliga rutiner i ett nödläge är reservuppkopplingar för produktionen så att avdelningen kan fortsätta leverera till kund medan de ordinarie uppkopplingarna återställs. Dessutom finns det ett internt program som via distansåtkomst ser till att personal kan använda program som de inte har installerade på sina datorer, exempelvis om maskiner fått ersättas på grund av hårdvaruhaveri.

Information om säkerhetshöjande åtgärder ges till personal när de kommer till avdelningen, och om någon anställd orsakat säkerhetsproblem på sin PC mister de tillgång till Internet under en månad. Det har hänt att folk laddat ner och installerat program som skadat maskinens kapacitet genom överbelastning. Om en allvarlig säkerhetskris skulle uppstå skulle vår respondent hållas ansvarig inför ledningen, och även avdelningschefen skulle få kritik. Detta är dock ännu ett teoretiskt scenario eftersom allvarliga säkerhetsproblem hittills motverkats med framgång.

4.5 Sammanknytning av intervjuer

Arbetet inom organisationen är uppdelat i projekt och delprojekt, och det är viktigt att förstå olika yrkesgruppers terminologi för att kommunikationen mellan de inblandade parterna ska flyta så smidigt som möjligt. Specifika säkerhetskrav framförs sällan av kunderna. Tidigare efterfrågades ofta ISO-certifiering, men idag tycks kunder förutsätta att organisationen är certifierad och uppfyller ISO-kraven. Säkerhetspolicies har formulerats och dokumenterats centralt för att sedan spridas vidare till de lokala kontoren runt om i landet och i världen.

Erfarenheterna av att använda metoder skiljer sig åt mellan respondenterna. Projektledaren och systemutvecklaren lyfter fram den interna projektmodellen Promise. Den tekniskt ansvarige på avdelningen har utarbetat sina egna metoder som han anpassat efter situationens krav. Enhetschefen associerar närmast metoder till ISO-certifieringens krav, men de följer alla någon form av mer eller mindre formaliserade metoder i sina respektive yrkesroller, och de är överens om att betydelsen av att använda metoder har ökat under deras tid i organisationen. De är också överens om att metoder krävs för att effektivt kunna tillmötesgå kundernas krav och fullgöra leveranser.

På en punkt går emellertid uppfattningarna om bruket av metoder isär. Projektledaren förespråkar de formella dokumenterade metoderna som hon själv följer i sitt arbete eftersom hon upplever att dokumentation av formaliserade metoder gör arbetet mer oberoende av att

någon viss person finns till hands för att hjälpa till. Vem som helst kan ta del av dokumentationen och utföra arbetsuppgifterna genom att följa metoderna steg för steg. Den tekniskt ansvarige tycker att han upplever större flexibilitet i att utforma egna situationsanpassade metoder allt efterhand som behovet av lösningar uppstår, åtminstone när det gäller hans eget arbete. Formaliserade metoder hade han ingen speciell erfarenhet av att använda.

Respondenterna är överens om att leverans till kund är avgörande för den egna verksamheten. Om säkerhetsproblem uppstår får ingen information gå förlorad, och det är viktigt att följa upp överföringar så att kunden tagit emot all data. En förutsättning för att kunna fullgöra sina leveranser och sitt avtal med kunderna är att se till att maskinerna och programvaran fungerar. Vid en säkerhetsincident prioriteras felsökning, och maskiner avskärmas i mindre grupper för att begränsa omfattningen av ett problem och kunna åtgärda det så att produktionen uppnår normal nivå så snart som möjligt.

I fråga om kundernas krav på säkerhet i systemen hade respondenterna olika erfarenheter utifrån sina respektive yrkesroller. Systemutvecklaren ansåg att kundkrav borde formuleras tydligare, och han upplevde att kunder ofta inte har någon klar bild av vad de vill ha. Han menade att specificerade kundkrav är en viktig förutsättning för förbättrad systemutveckling. Den tekniskt ansvarige upplevde att den största prioriteringen från kunderna är att deras sekretessbelagda information inte får hamna i orätta händer och enbart ska hanteras av organisationens personal som skrivit på överenskommelser om tystnadsplikt.

Projektledaren kunde inte erinra sig att hon kommit i kontakt med kunders krav på säkerhet i system som de beställt eller som organisationen använde, men däremot var hon överens med enhetschefen i att kunder tigigare begärde ISO-certifiering men att de i dagsläget tycks förutsätta att organisationen lever upp till dessa föreskrifter. Enligt enhetschefens erfarenhet var uttalade säkerhetskrav från kunder vanligt förekommande, främst i fråga om att den information som flödar mellan dem och organisationen ska skyddas mot intrång från obehöriga. Hon framhöll också att kunder speciellt efterfrågade kryptering och lösenordsskydd.

Systemutvecklaren ansåg att det fanns utrymme för att ytterligare förbättra arbetet med backup, men generellt var respondenterna av uppfattningen att informationssäkerheten var god och att nätet är utformat för att hålla obehöriga ute ur systemet så att känsliga uppgifter inte läcker ut. Den fysiska säkerheten såg de fler brister i. De framhöll risker som brand, översvämning, strömavbrott och bombhot. Systemutvecklaren påpekade att strömavbrott kan skada databaser så att omfattande rekonstruktion måste utföras, och enhetschefen ansåg att beredskapen hos gemene man att utrymma lokalen och skydda maskinerna om brand uppstod borde bli bättre. Detta ansåg hon att avdelningen idag inte var så väl förberedd inför.

5 Analys

Utifrån det teoretiska och empiriska material vi presenterat i de båda närmast föregående kapitlen kommer vi här att redovisa den analys vi gjort, samt föra en diskussion kring det analyserade materialet.

5.1 Metodanvändning

Denna uppsats skrevs med syfte att undersöka ett behov av säkerhetstänkande redan tidigt i utvecklingsarbetet och utifrån detta föreslå lösningar som tillmötesgår de behov som framkommit utifrån det material vi använt samt de fakta vi fått från de intervjuer vi utfört. Vi hittade under början av arbetet ett par vetenskapliga artiklar som talade för att säkerhetsaspekter ska beaktas redan så tidigt som i metoderna som följs vid systemutveckling, och vi kom fram till att de intervjuade personerna i sitt arbete följde metoder och policies som inkluderade säkerhetsföreskrifter och åtgärder. Dock var inte samtliga metoder formaliserade.

Vi fann varierande exempel på metoder när vi talade med våra respondenter. Den tekniskt ansvarige hade utvecklat sina egna situationsanpassade metoder genom att prova sig fram till de bäst fungerande lösningarna efterhand som han växte in i sin yrkesroll. Det tycktes inte råda något konfliktförhållande mellan hans egenhändigt utformade metoder och de formaliserade metoder som avdelningen använde sig av. Hans metoder verkade snarare ha en kompletterande funktion eftersom han utvecklat dem för att täcka upp områden som det tidigare inte funnits tillräckliga lösningar för. De andra metoderna som följdes i organisationen var betydligt mer formaliserade, projektmodellen Promise och dokumenterade säkerhetspolicies som gäller koncernen i sin helhet. Inom ramarna för dessa officiella direktiv som täcker stora områden av verksamheten har avdelningens personal hittat sätt att arbeta som uppfyller kraven i ISO-certifieringen.

Gemensamt för våra respondenter oavsett om de följer egna eller formaliserade metoder var att de uppgav att de arbetar så som de gör för att på bästa sätt kunna leverera till kunderna enligt avtal och ge dem vad de förväntar sig av organisationen. Metoderna har alltså utformats mot bakgrund av att avdelningen är en kundcentrerad servicebyrå med huvuduppgift att behandla dokument med mer eller mindre känsliga uppgifter på ett så professionellt sätt som möjligt och garantera säker överföring av data mellan sig och kunderna.

5.2 Uppfyllande av säkerhetskrav

I våra intervjuer lyftes olika aspekter av säkerhet fram. Den fysiska biten handlade om att sätta personal och maskiner i säkerhet vid omedelbar fara som brand, bombhot och översvämning. Att sätta maskinerna i säkerhet vid en incident och hålla så många som möjligt fungerande samt att snabbt ersätta skadade eller förstörda är en förutsättning för att kunna hålla produktionen igång, detta poängterades av flera av respondenterna. För att garantera att produktionen återupptas så snart nya maskiner anskaffats är det teoretiskt möjligt att arbeta via distansåtkomst och använda terminaler som ännu inte har den nödvändiga programvaran installerad. Detta är emellertid inte prövat i praktiken eftersom en så allvarlig kris inte drabbat avdelningen vid något tillfälle.

Det finns också en reservförbindelse till kunderna om den ordinarie av någon anledning skulle ligga nere. Skydd av information fokuserar på åtkomst, hantering, lagring och överföring. Den generella överenskommelsen med kunder betonar att information enbart får hanteras av personal som omfattas av organisationens sekretesspolicies. Information måste också överföras på ett sätt som skyddar den mot bortfall av data i processen, och den ska lagras hos organisationen, i Unixmaskinen eller på en bandstation, under en viss tid så att man kan gå tillbaka och ta fram den vid behov eller på begäran av kunden.

Det rent tekniska informationsskyddet tycks vila på organisationens nätlösning. Projektledaren kommenterade att hackerangrepp förekommer i stor utsträckning, men enhetschefen framhöll att nätet är utformat för att hålla alla obehöriga parter utanför. Tillgång till intranätet förutsätter kontakt med helpdesk där man måste identifiera sig som behörig användare för att få tillgång till företagsintern information, och även som behörig användare får man bara tre försök på sig att ange korrekta inloggningsuppgifter. Enligt enhetschefen ska det inte vara möjligt för någon utanför organisationen att göra intrång och missbruka uppgifter som kunder överlämnat i god tro.

Vårt empiriska material knyter an till den teoretiska bakgrunden på ett antal punkter. Av litteraturen vi läste in oss på framgick att ett flertal organisationer drabbats av säkerhetsproblem efter att personalen öppnat mail som innehöll farligt material och surfat på webbsidor med skadligt innehåll. Flera av våra respondenter bekräftar att användare spelar en roll i datasäkerhet genom sitt vardagliga bruk av systemet. Enligt enhetschefen passerar inga mail med opålitligt innehåll genom brandväggen, men personalen får ändå information om säkerhetshöjande åtgärder som de själva kan bidra med. Den tekniskt ansvarige framhöll att ett antal personer laddat ner material som drog ner kapaciteten i deras maskiner, och att de därför mist tillgång till Internet under en månad som straff.

Stöld av användaruppgifter har organisationen satsat stort på att motverka. Enligt vår referenslitteratur är detta ett ökande problem i dag, och stulna uppgifter missbrukas ofta för att stjäla pengar från konton eller att olovandes ta reda på personuppgifter (Lager 2006). Nätet som vår organisation använder är utformat med sådana intrång i åtanke, för att ge maximalt skydd åt kundernas och personalens konfidentiella uppgifter. Här är det viktigt att skilja mellan subjektiva förväntningar på vad systemet bör klara och vilka angrepp det faktiskt klarar av i praktiken. Som intervjuare måste vi också vara medvetna om att säkerhetsfrågor är ett känsligt område, och att detta kan påverka svaren vi får fram i samtalen, speciellt eftersom organisationens framgång är beroende av kundernas förtroende, vilket framgick tydligt av intervjuerna.

Projektledaren bekräftade att försök till intrång är vanligt förekommande, men enligt enhetschefen håller systemet effektivt angriparna ute. Så som vi argumenterade i vår litteraturstudie som ligger till grund för kapitel tre dyker nya typer av tekniker och angripare upp hela tiden, och dagens fungerande skyddsåtgärd kan visa sig vara morgondagens potentiella säkerhetsbrist. Detta gäller inte enbart våra respondenters organisation utan organisationer i allmänhet som påverkas av dagens snabba tekniska utveckling. Det är också viktigt att vara medveten om att säkerhetshål inte behöver vara synliga för den egna organisationen men att de ändå kan upptäckas och utnyttjas av personer som är så skickliga i dataintrång att de inte lämnar spår efter sig (Mollick 2005). Uppfattningen att den egna beredskapen mot dataintrång är fullgod kan alltså utvecklas till en potentiell säkerhetsrisk i sig själv.

Ännu en beröringspunkt med litteraturstudien som vi noterade när vi granskade vårt empiriska material är att ur organisationens synvinkel är skadan skedd redan när ett dataintrång genomförs. Våra respondenter betonade att en central del av överenskommelsen med kunden är just löftet om att skydda information som överlämnas i förtroende, och om detta förtroende bryts förlorar organisationen sitt anseende i branschen. Både kunden och organisationen tar alltså skada av att ett dataintrång inträffar och blir känt oavsett om uppgifterna används olagligt eller om någon bröt sig in i systemet för att utmana sin egen skicklighetsnivå.

5.3 Riskanalys och krisplanering i förebyggande syfte

I textmaterialet vi hittat och använt oss av i detta arbete har vi återkommande noterat att organisationer gjort riskanalyser kring datorsäkerhet och informationssäkerhet. Detta var inget vi uttryckligen fick bekräftat hos personerna vi intervjuade, dock hade de en väl utarbetad krishanteringsplan som involverade allt kring datorsäkerhet och säkerhet kring leverans om något skulle hända deras tekniska utrustning vilket i sin tur kunde drabba informationshanteringen i datorsystemen. Riskerna kring informationshantering idag är så stora på grund av alla hot, både inifrån och utanför organisationen att antingen riskanalyser eller krishanteringsplaner är en nödvändig del av säkerhetstänkande för att allt ska fungera även om en allvarlig incident inträffar.

Riskanalys anser vi bör finnas med redan inför och under systemutvecklingsprocessen. Det framkom i en intervju att dokumentation för hantering av kriser eller avvärjning av risker inte funnits så länge i organisationen, och att det krävts lite extraarbete för att få igenom detta. Efter att ha läst de artiklar vi funnit som tagit upp detta ämne, samt mot bakgrund av intervjumaterialet, är vi av uppfattningen att detta är ett viktigt inslag i förebyggande systemutveckling.

En förutsättning för ett sådant arbete med dokumentation som redogör exakt för vilka åtgärder som ska vidtas, är att organisationen har en klar bild över vilka risker som kan finnas (Dantu, Loper och Kolan, 2004). Oavsett om det handlar om hårdvara som måste återställas eller mjukvara som måste omprogrammeras eller omkonfigureras, bör planer finnas för att återställa leveranskapacitet och informationshantering till det normala inom minimal tid så varken kund eller organisation blir lidande, vilket framkom i våra intervjuer var de viktigaste faktorerna att ta hänsyn till vid en incident av något slag. Förebyggande riskanalys och snabb

krishantering förespråkades av våra respondenter, och vi uppfattar detta som en god och flexibel strategi för att bevara sin informationssäkerhet och hantera situationer som kan utgöra hot mot den.

5.4 Säkerhetstänkande inom ramen för formaliserade metoder

Uppgiften vi tog på oss när vi började planera vårt examensarbete var att undersöka möjligheten att använda existerande systemutvecklingsmetoder för att bygga in säkerhetsaspekter i systemutvecklingen redan på designstadiet. Med detta menar vi inte att utvecklingsteamet ska binda sig vid specifika säkerhetslösningar som de sedan håller fast vid under hela systemets livscykel, utan att själva säkerhetsplaneringen bör beaktas från första början.

Här är det också viktigt att ställa upp alternativ för vilka specifika lösningar systemet kommer att kräva och vara öppen för möjligheten att det kan behövas olika lösningar under systemets livscykel. Denna flexibilitet är en viktig faktor i en tid av oerhört snabb teknisk utveckling. De tillägg vi gjort i den modifierade version av modellen som syns nedan är enbart för att åskådliggöra hur vi resonerat. Vår avsikt är inte att ändra på existerande metoder utan att visa hur vårt resonemang passar in i dem. Riskanalys och säkerhetsplanering vill vi väva in tidigt i utvecklingsprocessen, gärna i analysfasen eftersom detta är ett gemensamt steg i de ledande metodologierna som de formaliserade metoderna utfår ifrån. Där kan utvecklare lyfta fram och utvärdera riskerna som utgör en del av den miljö som organisationen är verksam inom. Det är också viktigt att designa systemet på ett sådant sätt att det går att modifiera och uppdatera så att det klarar att hålla jämna steg med interna och externa säkerhetsrisker.

Precis som Fitzgerald et al. (2002) klargör att val av systemutvecklingsmetoder måste anpassas till den aktuella utvecklingskontexten så menar vi att riskanalys och säkerhetsplanering också bör utföras med hänsyn till detta. Dessutom är det viktigt att väga in vilken typ av system som ska utvecklas, vad det ska användas till och hur länge organisationen planerar att använda det. Därför argumenterar vi inte för något specifikt sätt att analysera risker eller planera in säkerhet i systemdesignen.

5.4.1 Riskanalys

Riskanalys bör genomföras i planeringen kring det framtida systemet. Vi anser att det är viktigt att börja redan tidigt i utvecklingen och kontinuerligt stämma av resultatet mot analysen för att säkerställa att produkten lever upp till de fastställda kraven. Detta är egentligen tyngdpunkten i resultatet av vår studie eftersom organisationer här bör göra omfattande satsningar och tillhandahålla nödvändiga resurser för att den slutgiltiga produkten ska bli så säker som det bara är möjligt.

Utifrån riskanalysen inför varje projekt kan organisationen avgöra vilka hot som kan finnas och vad som kan drabba informationsbehandlingen om något inte skulle gå enligt planerna, eller om en informationsstöld skulle ske. Utifrån denna analys går det sedan att beräkna vilka förebyggande åtgärder som bör inkluderas, vilka åtgärder som bör utföras i händelse av en

informationsstöld eller informationsläcka samt beräkna kostnader för sådana incidenter och utifrån detta ha avsätta nödvändiga resurser. Riskanalysen kan visa på hot som kan finnas mot organisationens informationssäkerhet, och de ansvariga kan eventuellt även förutse vilka typer av individer som skulle ha nytta av denna, och utifrån detta sätta upp olika spärrar för åtkomst och bruk av informationen.

5.4.2 Säkerhetsplanering för informationssystem

Denna punkt avser det faktiska arbetet som resultatet av riskanalys medför, hur informationen som genererats av analysen ska omsättas i praktiken. Vid säkerhetsplanering bör organisationen utgå från de tidigare analyserna som gjorts och utifrån detta sätta upp planer, samt bör dokument kring hantering av en eventuell incident eller kris upprättas. Ett sådant dokument kan exempelvis beskriva vad ansvarig personal ska göra för att åtgärda incidenten samt uppgifter som beskriver varje medarbetares uppgifter tills arbetet kan återgå till det normala.

5.4.3 Kontinuerlig uppdatering

Då de punkter vi nämnt ovan är saker som hela tiden förändras krävs det att de ständigt hålls aktuella. Hot som kanske inte längre är relevanta bör omvärderas för att passa in i den hotbild som är aktuell vid tidpunkten eftersom det hela tiden upptäcks nya hot och risker som utnyttjas av obehöriga personer som vill komma över information. Uppdatering bör ske med vad som kan anses vara rimliga tidsintervaller. Om direkta nya hot uppstår bör det finnas utrymme för att hantera dem omgående. Saknas utrymme, hårdvara, kapital, tid eller annat till att hela tiden hålla organisationens säkerhetsplanering och riskanalyser uppdaterade kommer kanske systemen snabbt bli inaktuella och detta kan innebära stora risker för både kunder och organisation, samt för eventuella samarbetspartners.

6 Slutsats

I detta avslutande kapitel presenterar vi vad vi kommit fram till under arbetets gång, vilka tankar som väckts hos oss angående vårt arbete och vad vi fått för uppslag till framtida forskningsansatser.

6.1 Slutsatser

De formaliserade metoder som exemplifieras i vår referenslitteratur användes inte i organisationen vi hållit kontakt med under vårt examensarbete. Däremot kan deras interna projektmodell ha påverkats av dessa eller andra formaliserade metoder, vilket inte framgår av vår studie. Oavsett namn på metoderna går metodanvändningen som en röd tråd genom både vårt teoretiska och empiriska underlag, både metoder för säkerhet och för systemutveckling. Så som framgick av intervjuerna använder organisationen sin interna projektmodell för båda dessa områden.

Vi upplevde att våra respondenter tog mycket allvarligt på sin egen och kundernas säkerhet i dagens läge, och vi har kommit fram till att tänkandet på denna avdelning går bra ihop med vårt ämne, tidig säkerhetsplanering i systemdesign via metoder. Systemutvecklaren betonade att han inte arbetade med säkerhetsfrågor men däremot att han ofta kom i kontakt med kundkrav, vilka han ansåg kunde bli mycket tydligare, och här i dessa inledande möten ser vi ett gott tillfälle att diskutera säkerhetsaspekter med kunderna som beställer systemen. Samma princip gäller också för intern systemutveckling, innan man börjar skriva eller modifiera kod skulle interna möten om säkerhetsplanering kunna hållas. Detta kan kompletteras med uppföljningsmöten inför varje säkerhetshöjande uppdatering av systemet.

Utifrån vår litteraturstudie och våra empiriska undersökningar har vi kommit fram till att det finns ett behov av säkerhetsarbete redan tidigt i utvecklingen av ett system, och vi anser även, utifrån de fakta vi tagit del av under arbetets gång, att säkerhetsarbete är något som krävs kontinuerligt under hela tiden som ett system är i drift då det finns risker och utmaningar i alla steg där information hanteras, lagras eller transporteras. Vi finner det mycket svårt att ge konkreta och allmängiltiga råd om vilken typ av förebyggande säkerhetsarbete som krävs, utan detta får anpassas efter situationen och beroende på vilken typ av data det aktuella systemet ska hantera, samt vilket slags hantering det handlar om, exempelvis om systemet ska lagra datamängder under en period eller behandla dem och omgående skicka dem vidare till ett annat system.

Detta är ännu en viktig punkt att väga in vid riskanalys och säkerhetsplanering inför systemutveckling. Organisationer har olika stora resurser, och säkerhetsfrågor liksom övriga frågor behöver lösas på ett praktiskt och ändamålsenligt sätt. I fråga om både säkerhetstänkande och konkreta lösningar anser vi att det är oerhört viktigt att vara flexibel och lyhörd inför skeenden och förändringar inom den miljö som omger organisationen.

6.2 Reflektioner i efterhand

Medan vi skrev detta arbete föddes idén att skicka ut enkäter till personer på annan ort med anknytning till säkerhetsarbete inom organisationen. Anledningen till att vi inte planerade in detta från början var att vi hade förhoppning om att få tag i fler respondenter inom avdelningen. Under arbetets gång upptäckte vi emellertid att det endast var ett fåtal personer som arbetade med säkerhetsfrågor. Detta tog vi som en nyttig lärdom inför framtida studier.

Responsen från dem vi kontaktade via mail var skiftande, några hänvisade vidare till varandra, andra sade sig ha ont om tid, och från resten hörde vi ingenting alls. Inför framtida examensarbeten tar vi med oss insikten om att det kan ta lång tid att väcka intresse för enkäter, de är lättare att avfärda än personlig kontakt med hänvisning till den egna tidsbristen. Vi har också upplevt en mycket positiv respons från dem som bidragit med empiriskt material till vår studie, och under arbetets gång har vi känt av vikten av att vara ute i god tid när många punkter står på dagordningen.

6.3 Vidare forskning i ämnet

Till sist vill vi gärna återknyta till vad vi sade i metodkapitlet, där vi förklarade vårt val av empirisk metod. Något vi blev intresserade av under arbetets gång är eventuella samband mellan tidpunkten då säkerhetsplanering tas med i systemutvecklingen och vilka säkerhetsproblem systemet drabbas av under sin livscykel. Det vore i så fall relevant att studera omfattningen av dessa säkerhetsincidenter, organisationens beredskap inför dem, och vilka konsekvenser problemen fick på kortare och längre sikt. En hypotes som forskarna, vi eller andra, då kunde utgå ifrån är att det kan finnas en korrelation mellan tidig säkerhetsplanering och förebyggande hantering av säkerhetsbrister.

En kvantitativ forskningsmetod med ett stort antal respondenter från olika typer av organisationer skulle lämpa sig för detta ämne. För att resultatet skulle få så allmängiltig karaktär som möjligt krävs naturligtvis ett representativt urval av respondenter. Vårt examensarbete skulle i så fall kunna utgöra ett slags kvalitativ upptakt till ett betydligt bredare kvantitativt forskningsprojekt. Redan idag skrivs stora mängder litteratur om behovet av tidig säkerhetsplanering, och då vi läst in oss på en del av denna under arbetets gång har vi noterat att detta tycks vara ett framväxande forskningsområde.

Bilaga 1

Intervjuguide om säkerhetsarbete

A	Name of the interviewer	
B	Date of interview	
C	Duration of interview	
D	Type of interview (personal, phone, e-mail, chat)	
E	Location of interview	
F	Language used during the interview	
G	How did you get in touch with the interviewee	

A	Title	
B	Name (keep confidential)	
C	Year of birth	
D	Female/male	
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	

I	Career:	
J	Number of years with organisation	
K	Previous positions (in organisation – elsewhere)	

Hur involverad är du i arbetet med säkerhet?

Hur vill du beskriva din roll/ansvarsområden?

Hur ser ert arbete med säkerhetsplanering ut? Beskriv era viktigaste faser?

Inledande fas:

- Riskanalys
- Identifiera möjligheter
- Identifiera potentiella hot

- Hur lång erfarenhet av säkerhetsarbete?
- Vilka områden ansvarar du för?

- Hur skulle du beskriva din roll inom säkerhetsarbete?

- Vad har format den?

- Hur stor roll spelar formella metoder i arbetet? Varför?

- Har betydelsen av metoder ökat eller minskat sedan du började arbeta med det?

- Vilka metoder följs i arbetet?

- Varför valdes just de?

- Hur har ni kommit fram till ert sätt att arbeta (revisionsbyrå, konsultbolag mm.)

- Varför har ni valt just detta sätt?

- Har ni interna revisioner av säkerhetsstandards? Externa?

- Hur förbättrar ni arbetet med datasäkerhet? Mäts effekter av åtgärder?

- Hur säkerställer ni att rutinerna blir bättre efter en uppdatering?

- Vill du beskriva hur ditt arbete ser ut när systemet drabbas av säkerhetsbrister?

- Vad händer? Vad prioriteras?

- Vilken roll spelar ledningen i arbetet med datasäkerhet och skydd av information?

- Vem tar vilka beslut? Var ligger det övergripande ansvaret?

- Är säkerhetsrutinerna avstämda mot en policy? Vilken?

- Hur förhåller sig säkerhetsarbetet till kundernas kravspecifikationer?

- Brukar kunder ställa specifika säkerhetskrav på systemen, och vad brukar de i så fall prioritera?

- Hantering av säkerhetsincidenter
    - Identifiera vem/vilka som skall utföra vilken åtgärd
    - Fastställa var en accepterbar nivå för informations- och tjänsteförlust ligger
    - rutiner (dokumenterade?) som behövs för att återställa skadad eller förlorad information och återuppta normal drift inom den tid som innan har identifierats
    - hänsyn tas till att system kan vara extra känsliga efter säkerhetsproblem och justerande åtgärder
    - övningar för den personal som skall medverka vid en återgång

- testning och uppdatering av system och back-up

- nödrutiner som beskriver åtgärderna som skall vidtas efter en allvarlig incident

- de tillfälliga rutiner som används i väntan på att återgång till normalläge skall göras

- de rutiner som skall användas för en återgång till normalläge

- de åtgärder som har till syfte att öka förståelsen och medvetenheten om säkerhetsrisker hos de anställda

- ansvarsbeskrivningar

- de tillgångar och resurser som krävs för att återgång till normalläge skall vara genomförbart

Bilaga 2

Intervjuguide om systemutveckling

A	Name of the interviewer	
B	Date of interview	
C	Duration of interview	
D	Type of interview (personal, phone, e-mail, chat)	
E	Location of interview	
F	Language used during the interview	
G	How did you get in touch with the interviewee	

A	Title	
B	Name (keep confidential)	
C	Year of birth	
D	Female/male	
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	

I	Career:	
J	Number of years with organisation	
K	Previous positions (in organisation – elsewhere)	

- Hur lång erfarenhet har Du inom systemutveckling?
- Vilka sorters system brukar Du arbeta med?
- Utvecklar Du från ruta 1 eller använder verktyg eller inköpta lösningar som modifieras?
- Varför arbetar Du just så? På vilket sätt är det fördelaktigt?
- Hur skulle Du beskriva Din roll inom systemutveckling?
- Vad har format den?

A) Formaliserade metoder

- Hur stor nytta har Du haft av metoder Du lärde Dig under utbildningen? På vilket sätt?

- Var utbildningen en bra förberedelse inför det verkliga arbetslivet eller fanns det ett stort glapp att överbrygga?

- Brukar Du arbeta utifrån någon speciell metod eller kombination av metoder?

- Varför valdes just den/de?

B) Metodroller

- Hur stor roll spelar formella metoder i arbetet? Varför?

- Är metoder mer eller mindre betydelsefulla idag än när Du började med systemutveckling?

- Hur ser arbetet med kravspecifikationer ut? Fungerar det bra? Varför/Varför inte?

C) Utvecklingskontext

- Hur brukar ett systemutvecklingsprojekt se ut? Varför ser det ut just så?

- Hur stor frihet har Du att använda Din personliga kreativitet i utvecklingsprocessen?

D) Utvecklare

- Vilka parter brukar vara inblandade i ett systemutvecklingsprojekt?

- Arbetar ni i stora eller små team?

- Varför? Vilka är fördelarna med att lägga upp arbetet så?

- Utnyttjar Du breda skikt av Din kunskap eller blir det mest ett begränsat antal rutinuppgifter?

E) Perspektiv på informationsbehandlingssystem

- Vilken syn har Du på informationssystem? Vilken roll spelar Din utbildning?

- Har synen påverkats av erfarenhet och i så fall hur?

- Vilken erfarenhet har du av säkerhetsarbete i systemutveckling?

Bilaga 3

Intervjuprotokoll för respondent 1

A	Name of the interviewer	Amina Borafia
B	Date of interview	2006-02-15
C	Duration of interview	40 minuter
D	Type of interview (personal, phone, e-mail, chat)	personlig intervju
E	Location of interview	kontor
F	Language used during the interview	svenska
G	How did you get in touch with the interviewee	arbetskamrat

A	Title	Systemspecialist
B	Name (keep confidential)	
C	Year of birth	1948
D	Female/male	Male
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	Elkraftsingenjör, Västerviks Tekniska Högskola

I	Career:	
J	Number of years with organisation	11
K	Previous positions (in organisation – elsewhere)	Systemprogrammerare

- **Hur lång erfarenhet har Du inom systemutveckling?**

Började arbeta med systemutveckling 1978, stordatordrift och programmering i Assembler.

- **Vilka sorters system brukar Du arbeta med?**
- **Utvecklar Du från ruta 1 eller använder verktyg eller inköpta lösningar som modifieras?**

Stor skillnad mot dagens arbete med inköpta lösningar som modifieras, t.ex Front Collector och Forms Rec.

- **Varför arbetar Du just så? På vilket sätt är det fördelaktigt?**

Det är mångsidigt och vi har tillgång till all källkod så vi kan anpassa programvaran efter önskemål.
Man slipper uppfinna hjulet igen.

- **Hur skulle Du beskriva Din roll inom systemutveckling?**
- **Vad har format den?**

Kundkrav har utformat arbetet och rollen inom systemutveckling. Man arbetar tillsammans med projektledare och hur nära kundkontakt man har varierar mellan projekt. Arbetar huvudsakligen mot externa kunder och ger dem förslag till lösningar. Det är inga större skillnader jämfört med att arbeta mot interna kunder.

- **Hur stor nytta har Du haft av metoder Du lärde Dig under utbildningen? På vilket sätt?**
- **Var utbildningen en bra förberedelse inför det verkliga arbetslivet eller fanns det ett stort glapp att överbrygga?**

Har byggt på med kurser efter utbildningen vid Västerviks Tekniska Högskola. I utbildningen ingick en hel del moment som sedan inte användes i det praktiska arbetslivet Det utgjorde mest en grundutbildning att sedan bygga vidare på.

- **Brukar Du arbeta utifrån någon speciell metod eller kombination av metoder?**
- **Varför valdes just den/de?**

Inom företaget arbetar vi med delprojekt. Tidsramar och förståelse för helheten är viktigt. Vi använder den interna projektmodellen Promise.

- **Hur stor roll spelar formella metoder i arbetet? Varför?**

Metoder erbjuder vägledning att följa och ger struktur. Modeller byggs upp, steg ska godkännas, begrepp ska klargöras och genomföras.

- **Är metoder mer eller mindre betydelsefulla idag än när Du började med systemutveckling?**

Metoder spelar större roll idag på grund av krav på effektivitet inom en konkurrensdriven bransch. Offerter till kund underlättas av metoder.

- **Hur ser arbetet med kravspecifikationer ut? Fungerar det bra? Varför/Varför inte?**

Det kunde bli bättre eftersom riktiga kravspecifikationer ofta saknas. Kunder vet ofta inte vad de vill ha och saknar riktig förståelse för vad en teknisk lösning kan och inte kan göra för dem. De tror att lösningen är enkel och inser inte vilken arbetsinsats som krävs. Ofta talar olika yrkesgrupper olika språk och kommunicerar förbi varandra. Alla har olika utgångspunkter och har svårt att sätta sig in i varandras.

- **Hur brukar ett systemutvecklingsprojekt se ut? Varför ser det ut just så?**

Det börjar med möte med kunden, där man drar upp riktlinjer för projektet och skapar datafångstrutiner. Kunden får en bild av vad de kan förvänta sig. Vi arbetar så här för att alla parter ska förstå situationen och för att underlätta kommunikation mellan alla som ingår i samarbetet. Det behövs styrgrupper och arbetsgrupper, men ofta är det svårt att få kunder att förstå behovet av styrning. Krav måste formaliseras från båda sidor för att undvika missförstånd.

- **Hur stor frihet har Du att använda Din personliga kreativitet i utvecklingsprocessen?**

Vi försöker följa vissa standarder för att kunna underhålla systemen efterhand, speciellt när de som skrivit koden och de som ska uppdatera den inte är samma personer, då är det viktigt att hålla sig till en gemensam standard som alla kan förstå och arbeta med. Levande system som förändras kontinuerligt kräver sådana arbetsmetoder.

- **Vilka parter brukar vara inblandade i ett systemutvecklingsprojekt?**
- **Arbetar ni i stora eller små team?**

Systemutvecklingsprojekt brukar omfatta projektledare, olika chefer, beslutsfattare, arbetsgrupper från olika avdelningar inklusive kundrepresentanter. Vi försöker hålla teamen små för att undvika flum och för att det är lättare att samordna arbetet i mindre grupper. För många viljor kan göra projektet ofokuserat.

- **Varför? Vilka är fördelarna med att lägga upp arbetet så?**

Det blir mångsidigt eftersom olika yrkesgruppers perspektiv representeras. Kommunikationen mellan olika yrkeskategorier underlättas.

- **Utnyttjar Du breda skikt av Din kunskap eller blir det mest ett begränsat antal rutinuppgifter?**

Det varierar utifrån vad projektet går ut på. Man måste ha förståelse för sammanhanget och delarna som ingår i det. Man måste ha insikt om helheten. Det räcker inte att kunna sitt eget område eftersom man är en pusselbit och behöver ha förståelse för samtliga delar. Det är viktigt att kunna sätta sig in i olika yrkesgruppers terminologi. Ofta har vi stor kontakt med ekonomifolk i fråga om utveckling av system för behandling av leverantörsfakturor.

- **Vilken syn har Du på informationssystem? Vilken roll spelar Din utbildning?**
- **Har synen påverkats av erfarenhet och i så fall hur?**

Man har glädje av informationssystem men blir också mycket beroende av dem. Strömavbrott är riskabla eftersom de kan förstöra databaser som måste rekonstrueras, och det finns system som hjälper till med att fixa detta, vissa är färdiga lösningar. Hur sårbar organisationen är beror på backup, vilket vi borde arbeta mer med. Däremot är det inte lika viktigt när det

gäller material som passerar våra system flyktigt och som vi inte längre har ansvar för när vi skickat utfilen vidare till nästa part.

- Vilken erfarenhet har du av säkerhetsarbete i systemutveckling?

Jag arbetar inte med säkerhetsfrågor. Det är bättre att ta upp det med projektledaren och med vår tekniskt ansvarige eftersom de är direkt involverade i säkerhetsfrågor.

Bilaga 4

Intervjuprotokoll för respondent 2

A	Name of the interviewer	Amina Borafia
B	Date of interview	2006-05-11
C	Duration of interview	1 timme 15 minuter
D	Type of interview (personal, phone, e-mail, chat)	Personlig
E	Location of interview	Kontor
F	Language used during the interview	Svenska
G	How did you get in touch with the interviewee	Arbetskamrat

A	Title	Projektledare
B	Name (keep confidential)	
C	Year of birth	1958
D	Female/male	Female
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	Fritidspedagog

I	Career:	
J	Number of years with organisation	8
K	Previous positions (in organisation – elsewhere)	Barnomsorg, sjukvård, telefonförsäljare

Hur involverad är du i arbetet med säkerhet?

Arbetar med ISO-certifiering och tar fram rutiner för backup.

Hur vill du beskriva din roll/ansvarsområden?

Är just nu involverad i projekt, säljsupport och offerter. Tar fram uppdaterade rutiner och håller kvalitetsmöten med teamleaders.

Hur ser ert arbete med säkerhetsplanering ut? Beskriv era viktigaste faser?

Det viktigaste är att ta fram backup-rutiner och krisplaner.

Inledande fas:

- Riskanalys

Finns inte ännu men det borde definitivt göras. Det behövs en handlingsplan för en eventuell krissituation.

- Identifiera möjligheter

En sådan handlingsplan är på väg att utvecklas. Främst måste vi få tag i maskiner som kan ersätta de som skadats eller förstörts om något allvarligt inträffar.

- Identifiera potentiella hot

Brand, översvämning och inbrott är det som ligger närmast till hands att planera inför. Hackerangrepp förekommer, men vi skyddas av koncernens centrala säkerhetspolicy.

- Hur lång erfarenhet av säkerhetsarbete?

Ansvarar huvudsakligen för de mindre bitarna inom säkerhetsarbete och har gjort det sedan 2002.

- Vilka områden ansvarar du för?

Delegerar besked från centralkontoret, håller i aktivitetsplanering och tar fram rutiner för informationshantering.

- Hur skulle du beskriva din roll inom säkerhetsarbete? (redan besvarat)

- Vad har format den?

Är inte formellt utbildad för den yrkesroll jag har idag. Istället har jag lärt mig efterhand beroende på vad situationen har krävt.

- Hur stor roll spelar formella metoder i arbetet? Varför?

De spelar mycket stor roll, och jag förespråkar dokumentation. Rutiner behöver dokumenteras för att alla ska veta vad som gäller. Alla kan jobba efter det och är då inte beroende av att kunna gå till en viss person och fråga. Dokumentation av formella metoder behöver bli mer lättillgänglig, och det behövs mer intresse hos gemene man att ta del av den.

- Har betydelsen av metoder ökat eller minskat sedan du började arbeta med det?

Den ökar hela tiden och vi ser en tendens att utveckla väldigt detaljerade rutiner, vilket är oerhört viktigt inom stora uppdrag.

- Vilka metoder följs i arbetet?

Vi arbetar efter projektmodellen Promise, som är mycket viktig för oss. Den innehåller milstolpar som måste klaras av innan projektdeltagarna kan gå vidare till nästa fas i arbetet. Detta behövs för att säkerställa att vi inte missat något på vägen. Driften av organisationens verksamhet är uppdelad i processer, och detta är en arbetsmetod som tagits fram på central nivå. Produktion kräver omfattande protokollföring.

- Varför valdes just de?

De ger god vägledning i projektarbete. Projektdokument tas fram, projektplaner ska godkännas, och det krävs också godkännande av leverans från beställaren hos kunden. Sedan upprättas en slutrapport som vi kan gå tillbaka till vid behov.

- Hur har ni kommit fram till ert sätt att arbeta (revisionsbyrå, konsultbolag mm.)

Rutinerna är ISO-relaterade och har tagits fram av ett revisionsbolag. Det finns olika certifieringar för olika branscher, och IT-säkerhet har sin egen ISO-certifiering.

- Varför har ni valt just detta sätt?

Vi arbetar så här för att uppfylla kraven för ISO-certifiering. Kunder brukade efterfråga certifiering tidigare, speciellt i samband med upprättande av offerter.

- Har ni interna revisioner av säkerhetsstandards? Externa?

Ja, interna och externa revisioner av ISO-standards.

- Hur förbättrar ni arbetet med datasäkerhet? Mäts effekter av åtgärder? (hänvisar till respondent 4)
- Hur säkerställer ni att rutinerna blir bättre efter en uppdatering? (hänvisar till respondent 4)

- Vill du beskriva hur ditt arbete ser ut när systemet drabbas av säkerhetsbrister?

Om vi har otur fungerar inte våra PC, vid ett tillfälle stängdes internnätet ner på grund av virushot. Om en server kraschar går produktionen ner och vi får svårt att leverera till kund. Volymen av obehandlade dokument backas på och vi kan ligga efter i dagar eller veckor efter det.

- Vad händer? Vad prioriteras?

Vi börjar med felsökning, vilket kräver goda rutiner för omstart. Produktionen har högsta prioritet. Maskinparken måste fungera. Det har tidigare uppstått mjukvaru- och överföringsproblem efter driftstopp.

- Vilken roll spelar ledningen i arbetet med datasäkerhet och skydd av information?

Ledningens roll är viktig, de måste vara tydliga och se till att deras policies följs.

- Vem tar vilka beslut? Var ligger det övergripande ansvaret?

På vår avdelning är det enhetschefen som är ytterst ansvarig. På central nivå skickar ledningen ut policies till servicedesk på IT-avdelningar som sprider informationen vidare.

- Är säkerhetsrutinerna avstämda mot en policy? Vilken?

Jag är inte säker på vilken, men någon borde de absolut sortera under. Vi har en allmän säkerhetspolicy.

- Hur förhåller sig säkerhetsarbetet till kundernas kravspecifikationer?

En kund har nyligen efterfrågat en krisplan, och det skulle verkligen behövas en tydlig sådan. Kunder tar för givet att arbetet med backup fungerar helt och hållet. Däremot frågar de efter support.

- Brukar kunder ställa specifika säkerhetskrav på systemen, och vad brukar de i så fall prioritera?

Kunder som vi hanterar fakturor åt ställer höga sekretesskrav.

- Hantering av säkerhetsincidenter
    - Identifiera vem/vilka som skall utföra vilken åtgärd

      Det är vår tekniskt ansvarige som ska felanmäla. Vem som ska göra vad finns fastställt i våra officiella rutiner.

    - Fastställa var en accepterbar nivå för informations- och tjänsteförlust ligger

      Inom åtta timmar bör produktionen vara igång igen.

- rutiner (dokumenterade?) som behövs för att återställa skadad eller förlorad information och återuppta normal drift inom den tid som innan har identifierats

Detta är hett diskuterat. Backup finns men inte på allt. Det tuffa är att verkställa planerna, vilket kostar. Vi har kommit långt och ser över hela miljön för att förenkla underhåll av backup-material.

- hänsyn tas till att system kan vara extra känsliga efter säkerhetsproblem och justerande åtgärder

Detta kräver att vi håller tätare kontakt med kunderna för att se till att information inte gått förlorad. Information till kunden om vad som händer är avgörande. Som leverantör måste vi hantera kommunikationen väl.

- övningar för den personal som skall medverka vid en återgång

Vi har inte hållit några sådana övningar för en helt ny produktion. Mindre övningar har vi fått i samband med serverkrascher och detta har varit spontana övningar i praktiken. Det har hänt att en server haft för litet minne.

- testning och uppdatering av system och back-up

Detta ser vi över kontinuerligt precis som arbetet med servrarna. Nya kunder kommer in hela tiden och detta kräver stora mängder lagringsutrymme för alla relaterade uppgifter.

- nödrutiner som beskriver åtgärderna som skall vidtas efter en allvarlig incident

En krisrutin håller på att utformas, men den har försenats på grund av tidsbrist. Den kommer att formuleras i exakta ordalag.

- de tillfälliga rutiner som används i väntan på att återgång till normalläge skall göras

Vi har inga ännu. Det är svårt att sätta upp eftersom man då måste ta hänsyn till ett stort antal olika scenarion.

- de rutiner som skall användas för en återgång till normalläge

Något så allvarligt har ännu inte hänt.

- de åtgärder som har till syfte att öka förståelsen och medvetenheten om säkerhetsrisker hos de anställda

Jag har rekommenderat att alla i personalen tänker sig för innan vi öppnar mail och besöker webbsidor vi inte kan lita på. Under en tidigare ägare fanns det en säkerhetsplan för detta. Detta kan vara bra att ta upp på enhetsmöten.

- ansvarsbeskrivningar

Det är teamleaders uppgift att sprida informationen vidare bland den personal som arbetar inom deras ansvars område.

- de tillgångar och resurser som krävs för att återgång till normalläge skall vara genomförbart

Jag vet inte eftersom detta sorterar under ekonomin.

Bilaga 5

Intervjuprotokoll för respondent 3

A	Name of the interviewer	Johan Andersson
B	Date of interview	2006-05-17
C	Duration of interview	1 timme
D	Type of interview (personal, phone, e-mail, chat)	Personlig
E	Location of interview	Kontor
F	Language used during the interview	Svenska
G	How did you get in touch with the interviewee	Kontakter

A	Title	Enhetschef
B	Name (keep confidential)	
C	Year of birth	1949
D	Female/male	Female
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	Gymnasieutbildning

I	Career:	
J	Number of years with organisation	28
K	Previous positions (in organisation – elsewhere)	Stansoperatris, arbetsledare

Hur involverad är du i arbetet med säkerhet?

Jag är ansvarig för att det fungerar men själv inte direkt involverad, det borde jag vara.

Hur vill du beskriva din roll/ansvarsområden?

Jag delegerar och sprider information uppifrån vidare.

Hur ser ert arbete med säkerhetsplanering ut? Beskriv era viktigaste faser?

Inledande fas:

- Riskanalys

Via koncernens tekniska lösningar har vi full kontroll över sekretessen kring informationen vi hanterar. Nätet ger säkerhet och brandväggar motverkar intrång på servern. Koncernen har en säkerhetsplan, och här skulle vi behöva en egen åtgärdsplan för nödsituationer, exempelvis brand eller bombhot.

- Identifiera möjligheter

Vår ISO-certifiering gör oss väl rustade att motverka säkerhetsrisker.

- Identifiera potentiella hot

- Hur lång erfarenhet av säkerhetsarbete?

Jag har arbetat med det sedan 1978, och under den tidsperioden har säkerhetsarbete blivit mer betydelsefullt. Det har alltid varit viktigt att säkerställa leveranser till kund men hot från intrång har uppstått efterhand som de tekniska lösningarna har utvecklats. De nya hoten uppstod i takt med distansåtkomst till information.

- Vilka områden ansvarar du för?

Att sprida information inom avdelningen som jag är ansvarig för.

- Hur skulle du beskriva din roll inom säkerhetsarbete?

Jag delegerar uppgifter, ger personalen får information som gäller vår organisation och ser till att säkerhetsföreskrifter följs inom avdelningen.

- Vad har format den?

Har vidareutvecklat min kunskap kontinuerligt när situationen har krävt det.

- Hur stor roll spelar formella metoder i arbetet? Varför?

De är viktiga eftersom hela arbetet är centrerat kring leveranser och kvalitetscertifiering med processer och historik som gör informationen spårbar.

- Har betydelsen av metoder ökat eller minskat sedan du började arbeta med det?

Den har ökat och vi investerar mycket i att bygga upp vår kvalitetscertifiering.

- Vilka metoder följs i arbetet?

Vi arbetar mycket med projektmodell och kvalitetscertifiering.

- Varför valdes just de?

För att leverans till kund är det som verksamheten vilar på.

- Hur har ni kommit fram till ert sätt att arbeta (revisionsbyrå, konsultbolag mm.)

Det var ett koncernbeslut under en tidigare ägare.

- Varför har ni valt just detta sätt?

(se ovan)

- Har ni interna revisioner av säkerhetsstandards? Externa?

Vi ska snart ha en intern, och förra året genomfördes en extern. Stickprov tas för att dokumentera kvalitén.

- Hur förbättrar ni arbetet med datasäkerhet? Mäts effekter av åtgärder?

Vi får jobbet av kunden när valet står mellan oss och konkurrenter eftersom vi inger förtroende, det är det bästa betyg vi kan få.

- Hur säkerställer ni att rutinerna blir bättre efter en uppdatering?

Vi strävar efter kontinuerligt förbättringsarbete.

- Vill du beskriva hur ditt arbete ser ut när systemet drabbas av säkerhetsbrister?

Det finns dokumenterat i en krisplan som utgör underlag till handlingsplan, för att minska konsekvenserna av en eventuell kris.

- Vad händer? Vad prioriteras?

Kunden prioriteras.

- Vilken roll spelar ledningen i arbetet med datasäkerhet och skydd av information?

Ansvaret ligger hos mig.

- Vem tar vilka beslut? Var ligger det övergripande ansvaret?

Vi har en säkerhetsansvarig inom koncernen.

- Är säkerhetsrutinerna avstämda mot en policy? Vilken?

Ja, de är avstämda mot ISO-certifieringen.

- Hur förhåller sig säkerhetsarbetet till kundernas kravspecifikationer?

(se nedan)

- Brukar kunder ställa specifika säkerhetskrav på systemen, och vad brukar de i så fall prioritera?

Ja, de ställer krav men tar certifiering för givet. Kunder efterfrågar zipade filer med kryptering och lösenordsskydd.

- Hantering av säkerhetsincidenter
    - Identifiera vem/vilka som skall utföra vilken åtgärd

      Detta var bättre formulerat med tydligare direktiv under en tidigare ägare. Då hade vi mer detaljerade säkerhetsföreskrifter.

    - Fastställa var en accepterbar nivå för informations- och tjänsteförlust ligger

      Jag vet inte de exakta siffrorna på rak arm, men egentligen borde det råda nolltolerans för tjänsteförlust. Informationsförlust ska inte inträffa, vi måste se till att allt överförs.

    - rutiner (dokumenterade?) som behövs för att återställa skadad eller förlorad information och återuppta normal drift inom den tid som innan har identifierats

      Det beror på incidentens art, vi har investerat miljonbelopp i backup här och i Stockholm. Vi kör med speglade diskar.

    - hänsyn tas till att system kan vara extra känsliga efter säkerhetsproblem och justerande åtgärder

      Ja, systemen övervakas extra då, backup görs på produktionskritisk server. Servern förvaras i en datahall med upphöjt golv och sprinklersystem.

    - övningar för den personal som skall medverka vid en återgång

      Nej, vi har inget speciellt i den vägen.

- testning och uppdatering av system och back-up

(se ovan)

- nödrutiner som beskriver åtgärderna som skall vidtas efter en allvarlig incident

Ja. (se ovan). *Det finns tre kritiska servrar som kräver backup.*

- de tillfälliga rutiner som används i väntan på att återgång till normalläge skall göras

Detta diskuteras nu.

- de rutiner som skall användas för en återgång till normalläge

(se tidigare svar)

- de åtgärder som har till syfte att öka förståelsen och medvetenheten om säkerhetsrisker hos de anställda

Vi informerar personalen om att vara ansvarsfulla när de surfar på nätet, men mailservern håller farliga mail utanför systemet, nätet skyddar oss. Vi har automatiserade rutiner för detta. Intranätet är omgärdat av säkerhetshöjande rutiner, och man behöver kontakta helpdesk för att komma in. Skriver man in fel lösenord tre gånger nekas man åtkomst till kontot och kan inte göra fler försök.

- Ansvarsbeskrivningar

Ja, det finns, och de omfattar befattningsbeskrivningar.

- de tillgångar och resurser som krävs för att återgång till normalläge skall vara genomförbart

Detta innefattas av backup-rutinerna.

Bilaga 6

Intervjuprotokoll för respondent 4

A	Name of the interviewer	Johan Andersson
B	Date of interview	2006-05-17
C	Duration of interview	35 minuter
D	Type of interview (personal, phone, e-mail, chat)	Personlig
E	Location of interview	Kontor
F	Language used during the interview	Svenska
G	How did you get in touch with the interviewee	Kontakter

A	Title	Tekniskt ansvarig
B	Name (keep confidential)	
C	Year of birth	1983
D	Female/male	Male
E	Position (keep confidential)	
F	Organisation (keep confidential)	
G	Division (department, unit or group) (keep confidential)	

H	Education and training	Kurser och certifikat

I	Career:	
J	Number of years with organisation	4
K	Previous positions (in organisation – elsewhere)	Dataregistrerare

Hur involverad är du i arbetet med säkerhet?

Jag är ansvarig för all säkerhet på avdelningen underhåll av brandvägg, nätsystem och antivirus. Vi har en lösning som kallas Legato som drar backuper beroende på kundkrav, informationen sparas här eller i en depå.

Hur vill du beskriva din roll/ansvarsområden?

Ser till så att allt fungerar som det ska. Tar hand om allt tekniskt, maskiner, server och switches till exempel. Vid behov delegerar jag vidare till kollegor.

Hur ser ert arbete med säkerhetsplanering ut? Beskriv era viktigaste faser?

Inledande fas:

- Riskanalys

All vital information överförs via VPN mellan oss och kunden. Det krävs program och certifikat för att ansluta till vårt nät. Information krypteras. All hårdvara är avskärmad från Internet. Uppdatering sköts hos oss, och vi använder mörkade IP-adresser inom nätet.

- Identifiera möjligheter
- Identifiera potentiella hot

- Hur lång erfarenhet av säkerhetsarbete?

Tre och ett halvt år har jag arbetat med det professionellt, men jag har alltid haft intresse av säkerhetsfrågor och brister i system.

- Vilka områden ansvarar du för?

Jag är ansvarig för säkerhet både inom avdelningen och ut mot externa kunder.

- Hur skulle du beskriva din roll inom säkerhetsarbete? (se ovan)

- Vad har format den?

Har vuxit in i rollen efterhand och lärt nytt när situationen har krävt det. Har byggt på min kompetens med internutbildning, kurser i SQL och NT.

- Hur stor roll spelar formella metoder i arbetet? Varför?

Det viktigaste är att ha ett bollplank, man måste ha folk att utbyta idéer med.

- Har betydelsen av metoder ökat eller minskat sedan du började arbeta med det?

Input har alltid varit viktigt.

- Vilka metoder följs i arbetet?

Det finns en systematisk process med olika steg för att låsa informationssystemen. Maskiner avskärmas så information inte läcker ut under processen. Detta är interna arbetsmetoder.

- Varför valdes just de?

De har visat sig vara mest effektiva, jag har provat mig fram till vad som fungerar bäst, jag gör ofta egna lösningar på situationer och det känns flexibelt att kunna arbeta så här.

- Hur har ni kommit fram till ert sätt att arbeta (revisionsbyrå, konsultbolag mm.)

(se ovan)

- Varför har ni valt just detta sätt?

(se ovan)

- Har ni interna revisioner av säkerhetsstandards? Externa?

Jag är inte inblandad i den delen av verksamheten. Vår avdelning är olik de andra i fråga om system och maskinhall, vi arbetar mot en snabb Unix-maskin. Vi har ett eget sätt att arbeta.

- Hur förbättrar ni arbetet med datasäkerhet? Mäts effekter av åtgärder?

Vi har ett instängt och skyddat nät, och håller oss uppdaterade via nyhetsgrupper om aktuella förbättringar.

- Hur säkerställer ni att rutinerna blir bättre efter en uppdatering?

Vi testar och ser om det fungerar avskärmat innan uppdateringen omsätts i praktiken.

- Vill du beskriva hur ditt arbete ser ut när systemet drabbas av säkerhetsbrister?

Generellt drar man ut nätverkskabeln för att avskärma problemområdet så det inte sprider sig mellan maskinerna. Ofta avskärmas en hel switch och alla maskiner under den kollas med säkerhetsprogram och antivirusprogram.

- Vad händer? Vad prioriteras?

Leverans till kund är det viktigaste, deadlines ska hållas i så stor utsträckning som möjligt. Kunden står i centrum.

- Vilken roll spelar ledningen i arbetet med datasäkerhet och skydd av information?

De påverkar processen i början när de skriver offert och lovar kunden säkerhetsgarantier.

- Vem tar vilka beslut? Var ligger det övergripande ansvaret?

De som är kvalitetsansvariga, till exempel projektledaren inom avdelningen. De meddelar vad som utlovats till kunden och lämnar sedan över till oss, men det är kunden som styr.

- Är säkerhetsrutinerna avstämda mot en policy? Vilken?

Ja, mot ISO-policyn. Under en tidigare ägare hade vi ISO-9000 som till exempel inkluderar tystnadsplikt och vad personal får och inte får använda maskinerna till.

- Hur förhåller sig säkerhetsarbetet till kundernas kravspecifikationer?

Det varierar, men allt måste stämma med villkoren för ISO-certifieringen. Vi är ett tjänstebolag som erbjuder kunder vad de vill ha och utformar alternativa lösningar om det behövs.

- Brukar kunder ställa specifika säkerhetskrav på systemen, och vad brukar de i så fall prioritera?

Vitala data ska inte hamna i fel händer. Information ska endast hanteras av vår egen personal som omfattas av överenskommelsen med kunden.

- Hantering av säkerhetsincidenter

Vi får stöd från servicedesk, och de skickar ut folk som hjälper till.

  - Identifiera vem/vilka som skall utföra vilken åtgärd

    Jag hanterar den tekniska biten med mjukvara och hårdvara, en kollega hanterar det kundspecifika.

  - Fastställa var en accepterbar nivå för informations- och tjänsteförlust ligger

    Det är oacceptabelt, ingen information får försvinna, och vissa jobb har mer tidspress än andra.

  - rutiner (dokumenterade?) som behövs för att återställa skadad eller förlorad information och återuppta normal drift inom den tid som innan har identifierats

    Ja, rutinerna går igenom olika steg, information ligger kvar 30 dagar i Unix, äldre data finns på bandstationen.

  - hänsyn tas till att system kan vara extra känsliga efter säkerhetsproblem och justerande åtgärder

    Vi testar utförligt i avskärmad miljö innan reparerade och nya maskiner sätts i drift. Maskiner är beroende av varandra i systemet, och det är viktigt att isolera ett problemområde via lokala test.

- övningar för den personal som skall medverka vid en återgång

Nej, inget.

- testning och uppdatering av system och back-up

Ja. (se ovan)

- nödrutiner som beskriver åtgärderna som skall vidtas efter en allvarlig incident

Vi har mycket förebyggande arbete med detta. (se tidigare svar)

- de tillfälliga rutiner som används i väntan på att återgång till normalläge skall göras
-

Vi har reservuppkopplingar till produktion och distansprogram för att kunna använda programvara man ännu inte har hunnit installera på ersättningsmaskinerna.

- de rutiner som skall användas för en återgång till normalläge

(se ovan)

- de åtgärder som har till syfte att öka förståelsen och medvetenheten om säkerhetsrisker hos de anställda

Om någon orsakat säkerhetsproblem på sin PC mister de tillgång till Internet under en månad. Det har hänt att personal installerat förbjudna program som ställt till problem genom att överbelasta maskinens resurser. Detta får man information om när man anställs.

- Ansvarsbeskrivningar

Jag har ansvaret inför ledningen, men om allvarliga problem skulle uppstå skulle även avdelningschefen få kritik uppifrån.

- de tillgångar och resurser som krävs för att återgång till normalläge skall vara genomförbart

7 Referenser

Böcker

Avison, D., Fitzgerald, G. (2003) *Information Systems Development: Methodologies, Techniques and Tools*. New York, McGraw-Hill

Bace, R.G., (2000) *Intrusion Detection*, Macmillan Technical Publishing, Indianapolis

Beynon-Davies, P. (2002) *Information Systems - An Introduction to Informatics in Organisations*. Hampshire, Palgrave

Fitzgerald, B., Russo, N.L., Stolterman, E. (2002) *Information Systems Development: Methods in Action.* New York, McGraw-Hill.

Holme, I.M., Solvang, B.K., *Forskningsmetodik – Om kvalitativa och kvantitativa metoder*, Lund, Studentlitteratur

Marakas, G.M. (2003) *Decision Support Systems: In the 21st Century*. New Jersey, Prentice Hall

Mathiassen, L., Munk-Madsen, A., Nielsen, P.A., Stage, Jan. (2001*). Objektorienterad analys och design*, Lund, Studentlitteratur

Pfleeger, Ch. P., Pfleeger, Sh. L., *Security in Computing – Third Edition*, 2003, New Jersey, Pearson Education inc.

Ryen, A. (2004) *Kvalitativ intervju – från vetenskapsteori till fältstudier*, Malmö, Liber

Artiklar

Apvrille, A, Pourzandi, M. "Secure Software Development by Example", July/August 2005 *IEEE Security & Privacy*

Dantu, R., Loper, K., Kolan, P. "Risk Management using Behavior based Attack Graphs", 2004, *IEEE Computer Society*

Glisson, W.B., Welland, R., "Web Development Evolution: The Assimilation of Web Engineering Security", *2005 IEEE*

Lager, M. "Customer Relationship Management", Jan 2006, 10, 1; *ABI/INFORM Global* (*IEEE Spectrum* January 2006, NA)

Mollick, E. "Tapping into the Underground", Summer 2005, vol. 46 no. 4,

MIT Sloan Management Review

Riordan, J., Wespi, A., Zamboni, D. May 2005, *IEEE Spectrum, NA*

Sampson, F. "A Penny for Your Thoughts, a Latte for Your Password", Jan/Feb 2006, *Interactions*

Stimpson, J., "The Practical Accountant"; Jan 2006; 39, 1; *ABI/INFORM Global*

Tiller, J. "Taming the New Wild West", May/June 2005, *Information Systems Security*

Udupa, S.K, Debray, S.K, Madou, M., "Deobfuscation – Reverse Engineering Obfuscated Code", *2005 IEEE*