Behovsanalys avseende värdering av IT-säkerhet

JONAS HALLBERG, NIKLAS HALLBERG, AMUND HUNSTAD

FOI-R--1820--SE Vetenskaplig rapport **Ledningssystem**
ISSN 1650-1942 December 2005

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1350 anställda varav ungefär 950 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömningen av olika typer av hot, system för ledning och hantering av kriser, skydd mot hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

Jonas Hallberg, Niklas Hallberg, Amund Hunstad

Behovsanalys avseende värdering av IT-säkerhet

FOI-R--1820--SE
ISSN 1650-1942

Ledningssystem
Vetenskaplig rapport

December 2005

Utgivare	Rapportnummer, ISRN	Klassificering
FOI - Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 Linköping	FOI-R--1820--SE	Vetenskaplig rapport
	Forskningsområde 4. Ledning, informationsteknik och sensorer	
	Månad, år December 2005	**Projektnummer** E7046
	Delområde 41 Ledning med samband och telekom och IT-system	
	Delområde 2	

Författare/redaktör	Projektledare
Jonas Hallberg Niklas Hallberg Amund Hunstad	**Godkänd av**
	Uppdragsgivare/kundbeteckning
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Behovsanalys avseende värdering av IT-säkerhet

Sammanfattning

Nätverksorienterade organisationer är beroende av tillförlitliga informationssystem. Graden av känsligheten hos information som hanteras inom Försvarsmakten innebär att IT-säkerhet är centralt för realiseringen av det nätverkbaserade försvaret (NBF). För att kunna säkerställa erforderlig IT-säkerhet krävs förmåga att värdera vilken nivå av IT-säkerhet olika system har. Arbetet som redovisas i denna rapport syftar till att identifiera behov avseende värdering av IT-säkerhet. Dessa behov kommer att utgöra grund för vidare arbete med att skapa metodiker och verktyg för värdering av IT-säkerhet i komplexa informationssystem.

Arbetet har genomförts i fyra steg: (1) insamling av data, (2) identifiering av utsagor, (3) analys av utsagor och identifiering av behov samt (4) analys och strukturering av behov. 6 intervjuer genomfördes och 13 relevanta dokument sammanställdes. Analysen av de transkriberade intervjuerna och dokumenten resulterade i att 110 respektive 105, dvs. totalt 215, utsagor identifierades. Analysen av utsagorna resulterade i 525 behov. Efter vidare analys och strukturering erhölls den resulterande behovsstrukturen som består av 13 övergripande kategorier och innehåller totalt 419 behov. Exempel på behov som identifierats är stöd för kravhantering, riskhantering, flexibel anpassning av säkerhetsnivåer under drift, värdera säkerhetsfunktioners förmåga att hantera olika säkerhetsaspekter, värdering av säkerhet hos tjänster och framtagande av beslutsunderlag.

Nyckelord

Behovsanalys, informationssäkerhet, IT-säkerhet

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 41 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization FOI – Swedish Defence Research Agency Ledningssystem Box 1165 581 11 Linköping	**Report number, ISRN** FOI-R--1820--SE	**Report type** Scientific report
	Programme Areas 4. C4ISTAR	
	Month year December 2005	**Project no.** E7046
	Subcategories 41 C4I	
	Subcategories 2	
Author/s (editor/s) Jonas Hallberg Niklas Hallberg Amund Hunstad	**Project manager**	
	Approved by	
	Sponsoring agency	
	Scientifically and technically responsible	

Report title (In translation)

Needs analysis regarding system security assessment

Abstract

Network-centric organizations depend on reliable information systems. The sensitivity of information handled by the Swedish armed forces results in IT security being critical for the implementation of the network-based defense (NBD). To ensure adequate IT security, the ability to assess security levels of systems is required. This report descibes an effort to identify needs regarding IT security assessment. These needs constitute important input to further development, including requirements engineering, of methods and tools for IT security assessment in complex information systems.

The effort descibed in this report consists of four main tasks: (1) data collection, (2) identification of statements, (3) analysis of statements, and (4) analysis and structuring of needs. During the data collection, six interviews were conducted and 13 relevant documents were collected. The analysis of the transcribed interviews and the documents resulted in the identification of 215 statements. The analysis of the statements resulted in 525 needs. The outcome of further analysis and structuring was 13 main categories with 419 needs, in total. Examples of identified needs are: requirements engineering, risk management, ability to adapt the security posture of systems during operation, knowledge of to what extent security functions address different aspects of security, and input to decision-making processes.

Keywords

Needs analysis, information security, IT security

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 41 p.
	Price acc. to pricelist

Innehåll

1. Inledning

Försvarsmakten genomför för närvarande ett omfattande utvecklingsarbete. Syftet är att omvandla den tidigare hierarkiska och försvarsgrensorienterade organisationsstrukturen hos invasionsförsvaret till ett nätverksbaserat försvar där internationella insatser ses som en central aktivitet. Nätverksbaserade organisationer är beroende av att kunna skapa förmågor som realiseras av system som består av andra system, dvs. enligt principen *system av system*. Detta ställer krav på möjligheten att kunna integrera system där de resulterande systemen har tillfredsställande säkerhetsnivåer.

Nätverksbaserade organisationer förutsätter en hög nyttjandegrad av modern informationsteknik (IT). De är starkt beroende av tillförlitliga informationssystem och graden av känsligheten hos information som hanteras inom Försvarsmakten innebär att IT-säkerhet är centralt för realiseringen av det nätverkbaserade försvaret (NBF). En allmänt vedertagen definition är att IT-säkerhet omfattar förmågan att bevara egenskaperna sekretess, riktighet och tillgänglighet (SIS, 2003) för data och system. För att kunna säkerställa erforderlig IT-säkerhet krävs förmåga att värdera vilken nivå av IT-säkerhet olika system har. Informationssäkerhet definieras som ”säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet” (SIS, 2003, s.8). Därmed är IT-säkerhet en del av informationssäkerhet.

Projektet *Värdering av IT-säkerhetsnivå hos system inom NBF* syftar till att understödja Försvarsmaktens arbete med att ta fram system med adekvat säkerhet. Detta genom att utveckla kunskap, metodik och verktyg för bedömning av IT-säkerhetsnivåer hos informationssystem inom NBF.

Arbetet i projektet har under 2005 bedrivits i form av ett antal delstudier.

1. Framtagande av scenarion (Hallberg m.fl., 2005b), vilka kan nyttjas som
   - illustration av situationer där IT-säkerhetsvärdering är nödvändigt,
   - utgångspunkt för resonemang kring behov av IT-säkerhetsvärdering och
   - underlag för behovsanalys avseende IT-säkerhetsvärdering.

2. Olika metodansatser för att identifiera behov avseende IT-säkerhetsvärdering studerades. Beierholm och Mattsson (2005) studerade

möjligheten att använda Grundad teori (Glaser & Strauss, 1967) i kombination med aktivitetsteori (Engeström, 1990) för att identifiera behov. Jonsson och Karlsson (2005) studerade möjligheten att använda verksamhetsmodellering tillsammans med aktivitetsteori för att identifiera behov. Hallberg, Hallberg och Hunstad (2005c) studerade användningen av kvalitetsdriven kravhantering (Hallberg m.fl., 2005a) för att identifiera behov.

3. Behovsanalys för att specificera en uppsättning behov avseende IT-säkerhetsvärdering, som senare kan användas som grund för framtagande av metodik och verktyg. Behovsanalysen baserades på metoden MedBeVIS (Hallberg m.fl., 2005c).

4. Utveckling av metod för värdering av säkerhet i informationssystem. Metoden, *Method for Assessment of System Security*, MASS, (Andersson, 2005) baserar sig på modellering av systementiteters säkerhetsegenskaper och relationer mellan entiteterna. Ett programvaruverktyg, ROME2, för denna typ av utvärdering har framtagits

5. En scenariobaserad utvärdering av MASS[1] har genomförts med utgångspunkt i tre enkla scenarion (nätverk med låg, medel respektive hög säkerhetsnivå). Utvärderingen fokuserade på huruvida utfall från MASS överensstämmer med initiala förväntningar och bedömningar.

6. En vidareutveckling av ramverket för värdering av säkerhet i system har genomförts[2].
   - Ramverket möjliggör kategorisering av olika metoder för utvärdering av säkerhet i system i relation till en uppsättning kriterier.
   - Ramverket underlättar identifiering och utvärdering av olika metoders styrkor och svagheter och vidare metodutveckling.
   - Ramverket belyser viktiga delproblem som måste beaktas vid värdering av säkerhet i system och tydliggör därmed områdets komplexitet.

[1] Examensarbete som är på väg att avslutas. Framläggning av rapport beräknas ske tidigt under 2006.
[2] Examensarbete som är på väg att avslutas. Framläggning av rapport beräknas ske tidigt under 2006.

Under arbetet med att ta fram en metod för behovsanalys visade det sig att det inte var lämpligt att utgå från scenarion, vilket initial var tanken. Istället baserades arbetet på intervjuer och analyser av relevanta dokument (Hallberg m.fl., 2005c). En behovsanalys baserad på scenarion ställer stora krav på precision i de scenariobeskrivningar som ligger till grund för behovsanalysen samt god domänkunskap hos de som deltar i arbetet med att omvandla scenario-beskrivningarna till behov. Det bedömdes även vara ovisst huruvida de scenarion som togs fram skulle spänna upp hela problemområdet så att inga väsentliga behov skulle missas.

Denna rapport presenterar resultatet av behovsanalysen, dvs. delstudie tre i listan ovan, i form av en övergripande struktur av identifierade behov.

1.1 Syfte

Syftet med arbetet som redovisas i denna rapport är att studera vilka behov av värdering av IT-säkerhet som kan identifieras. Dessa behov skall ligga till grund för vidare arbete avseende metodik och verktyg för värdering av IT-säkerhet i komplexa informationssystem.

1.2 Problemformulering

Det finns en stor brist i förmågan att påvisa att säkerheten i informationssystem är tillräcklig. Detta leder till ett övergripande behov av nya metoder och verktyg för värdering av IT-säkerhet. Vilka behov som skall ligga till grund för dessa är dock ännu ej identifierat. För att kunna ställa adekvata krav måste behovet av värdering specificeras. Dessa krav används sedan för att utveckla nya metoder och verktyg som uppfyller behoven bättre än de gamla.

2. Bakgrund

I följande avsnitt beskrivs områdena IT-säkerhetsvärdering och scenarioteknik samt forskningsprojektet *Värdering av IT-säkerhetsnivå hos system inom NBF* som detta arbete har utförts inom. Motsvarande beskrivningar avseende IT-säkerhetsvärdering, behovsanalys, Quality Function Deployment, kvalitetsdriven kravhantering och forskningsprojektet återfinns i arbetsdokumentet (Hallberg m.fl., 2005c).

2.1 IT-säkerhetsvärdering

IT-säkerhetsvärdering är ett omfattande forskningsområde utan entydig definition och generellt accepterad begreppsapparat (ACSA, 2002). Området syftar bland annat till att utveckla metoder och verktyg för värdering av IT-säkerhet, som skall fånga de egenskaper som är viktiga för säkerheten och ge relevant underlag till krav- och riskhanteringsprocesser (Hallberg m.fl., 2005b). Med detta avses hantering av IT-säkerhetskrav samt riskhantering i vid bemärkelse rörande hur IT-säkerhet skall hanteras samt vid beslut baserade på information vars kvalité beror av IT-säkerheten. Denna riskhantering inkluderar avvägningar som görs strategiskt, operativt och vid systemutveckling. IT-säkerhet behöver alltså kunna värderas olika beroende på situationer och förutsättningar. Detta medför att värderingens omfattning kan variera kraftigt, exempelvis från underförstådda antaganden om att IT-säkerheten är tillräcklig till omfattande evalueringar inför ackrediteringsbeslut.

Det finns grundläggande behov av metoder och tekniker för analys och värdering av IT-säkerhet hos system. Utan förmågan att kunna värdera dessa är det inte heller möjligt att bedöma:

- säkerhetsnivån hos system,
- vinster med investeringar i förbättringsåtgärder avseende säkerhet samt
- omfattning av risker vid systemmodifieringar.

För att kunna värdera IT-säkerhet måste först dess betydelse specificeras. Vidare måste omfattningen hos system som skall värderas bestämmas. Detta avser såväl rumslig utsträckning som vilka systemaspekter (organisation, human, teknik och drift) som skall beaktas. Även värderingens omfattning måste specificeras, till exempel avseende detaljgrad. Eftersom säkerhet inte kan mätas direkt, måste andra egenskaper hos system mätas. Dessa egenskaper kan vara faktorer som påverkar säkerheten (exempelvis säkerhetsfunktioner) eller konsekvenser av

aktuell säkerhet (exempelvis sårbarheter). Valet av vilka egenskaper som skall beaktas leder till olika angreppssätt, vilka kan vara:

- observerande, exempelvis baserat på uppsättningar av mätetal (eng. security metrics programs) (Swanson m.fl., 2003; Payne, 2001),
- testande, exempelvis baserat på arbetsinsats för motståndare (eng. adversary work-factor) (Schudel & Wood, 2000; Wood & Bouchard, 2001),
- granskande, exempelvis baserat på sammanvägning av flera systemegenskaper (Alves-Foss & Barbosa, 1995; Wang & Wulf, 1997) eller komponenter Common Criteria (CC, 1999) eller
- strukturbaserade, exempelvis baserat på olika komponenter och relationer mellan dessa (Clark m.fl., 2004; Oman m.fl., 2004; Blobel & Roger-France, 2001; Hallberg m.fl., 2004).

Omfattande dynamiska informationssystem kräver metoder baserade på granskning och systemstrukturen. Granskning är nödvändig eftersom det inte är möjligt att invänta resultat av observation och tester på färdiga system. Strukturen måste beaktas för att kunna hantera beroenden mellan system och delar av system samt att kunna värdera säkerhetsnivåer i delar med särskilda säkerhetskrav, såsom informationszoner (Fahs & Wiseman, 1999; Försvarsmakten, 2004) eller varierande användningsmiljö.

2.2 Systemutveckling

Systemutveckling är en process vars syfte är att skapa helt nya och/eller förändra befintliga system. Generellt kan dessa system baseras på teknik, verksamhet eller en blandning av dessa. Under utveckling av större rent tekniska informationssystem måste det tekniska systemet harmonieras med övriga delar i den verksamhet det är avsett att stödja för att det tekniska systemet skall fungera väl och motsvara de behov som finns i den verksamhet som avses stödjas. Den komplexa verksamhet som utveckling av system av denna typ innebär kräver kompetens från vitt skilda kunskapsområden, såväl tekniskt som beteendevetenskapligt orienterade. Jungert m.fl. (2004)

Av vikt vid systemutveckling är att beakta användarnas och verksamhetens behov och de olika krav dessa leder fram till. Säkerhetsrelevanta behov är särskilt komplicerande då dessa i allmänhet är icke-funktionella behov, behov som fokuserar på sådant man avser inte skall hända. Detta komplicerar naturligt nog även systemutvecklingsarbetet. För att beakta användares och verksamhetsrepresentanters säkerhetsrelevanta behov krävs det att en dialog förs mellan dessa och systemutvecklare.

2.3 Behovsanalys

Behovsanalys innebär undersökningar och studier med syfte att identifiera och analysera behov. I denna studie är syftet med behovsanalysen att påvisa behov avseende värdering av IT-säkerhet.

Behov är ett begrepp som de flesta har en intuitiv förståelse för, men som är svårt att exakt förklara. Vid utveckling av informationssystem är det viktigt att utgå från användarnas och verksamhetens behov, då begreppet behov ofta används i betydelserna brist eller problem (Witkin & Altschuld, 1995). Behov kan vara antingen medvetna eller omedvetna, samt verkliga eller upplevda. Påtalade behov är ofta relaterade till någon form av inneboende krav på åtgärd. Denna form av behov kallas för förändringsbehov.

Behov behöver dock inte vara otillfredsställda, vilket gör dem betydligt svårare att identifiera. Detta är fallet eftersom ett tillfredsställt behov ofta är ett omedvetet behov vars uppfyllelse känns självklar. Tillfredsställda behov kan dock bli väldigt tydliga efter en förändring, då det som tidigare tillfredsställde vissa behov inte längre gör det; exempelvis kan detta inträffa efter införande av nya IT-system. Trots att uppfyllda behov inte uttrycks explicit så väcker förändringar som leder till att de inte längre uppfylls ofta till stort missnöje.

I denna rapport avses behov vara tillstånd som kräver stöd eller åtgärder, oavsett om behovet redan är tillfredsställt eller ej.

2.4 Quality Function Deployment

Quality Function Deployment (QFD) är ett kvalitetssystem som syftar till att uppnå en hög grad av kundtillfredsställelse för utvecklade produkter och tjänster genom metodiskt arbete (Cohen, 1995). QFD utvecklades i Japan under senare delen av 1960-talet och har sedan dess spridits globalt.

Grunden i QFD är att erhålla förståelse för kunders behov och därefter omvandla dessa till egenskaper hos produkter och tjänster. Därmed skapas produkter och tjänster med hög grad av nytta för kunderna. QFD baseras på samma filosofiska grundsyn som TQM (eng. Total Quality Management), att sätta kundens behov i centrum och att inte utveckla produktegenskaper som inte ger kundnytta (Bergman & Klefsjö, 1994). QFD delar även TQMs kvalitetsverktyg som t ex relationsdiagram, tabeller och matriser.

2.5 Kvalitetsdriven kravhantering

Kvalitetsdriven kravhantering baseras på några av de kvalitetsverktyg som finns i QFD och genomförs i sex steg: (1) insamling av data, (2) identifiering av utsagor, (3) identifiering av behov, (4) analys av behov, (5) identifiering av krav och (6) analys av krav (Hallberg m.fl., 2005). Av intresse för denna studie är huruvida de fyra första stegen kan användas för att analysera behov avseende värdering av IT-säkerhet. Nedan beskrivs dock samtliga sex steg, vilka resulterar i en strukturerad kravmängd för det aktuella systemet.

2.5.1 Insamling av data

Under den första aktiviteten samlas information in som är av intresse för att kravställa det system som skall utvecklas. Insamling av data kan ske med ett flertal olika metoder och tekniker, exempelvis intervjuer, observationer, workshops och enkäter. Ett effektivt sätt att samla in relevant information är att efterfråga upplevda problem, något som indikerar situationer som upplevs otillfredsställande i något avseende. Otillfredsställande situationer avviker från det förväntande eller det önskade. Problem kan vara existerande eller tänkbara i framtida situationer. Ytterligare ett sätt att få intressant information är att samla in mål som beskriver vad som önskas uppnås med en förändring. Mål anger resultatet, dvs. ett önskat läge/tillstånd som skall uppnås. Ett tredje sätt är att efterfråga vilka återgärder som tros kunna tillfredsställa de brister som finns.

Utdata från detta steg skall vara i textformat. Detta innebär bland annat att intervjuer och diskussioner under workshops och andra typer av möten måste transkriberas eller på annat sätt dokumenteras i form av text.

2.5.2 Identifiering av utsagor

Under den andra aktiviteten analyseras texten för att identifiera utsagor, text som innehåller information vilken kan nyttjas för att bestämma behov. En utsaga skall inte vara för omfattande eller innehållsrik, utan bör bestå av en eller ett par meningar, men måste ändå ge en förståelse för vad texten beskriver.

2.5.3 Identifiering av behov

Under den tredje aktiviteten genomförs en analys av utsagorna. Analysen syftar till att ur utsagorna identifiera behov. För detta ändamål används kundrösttabeller (Shillto, 2001), där utsagorna analyseras ur olika perspektiv; (1) *vem* som berörs, (2) *vad* de anser sig behöva, (3) *när* de behöver det, (4) *var* det behöver användas, (5) *varför* behovet finns och (6) *hur* de vill att det skall

fungera. Varje utsaga kan innehålla ett eller flera behov, men det kan också vara så att utsagan är så innehållsfattig att inget behov alls kan extraheras. Resultatet av denna aktivitet utgörs av ett antal ostrukturerade behov.

2.5.4 Analys av identifierade behov

Under den fjärde aktiviteten genomförs en analys av de identifierade behoven. I ett första steg genomförs detta med relationsdiagram, där behov grupperas med likartade behov, så att kategorier skapas. Dessa kategorier grupperas sedan med liknande kategorier. De behov som erhålls från föregående steg är ibland enkla och kan inte delas upp i flera behov, och ibland sammansatta av flera olika behov. I det senare fallet kan behovet ses som en kategori innehållande andra kategorier och behov. Med fördel kan post-it-lappar användas för denna analys, som bör genomföras i samverkan med representanter vilka väl känner verksamhetsdomänen. Under analysen sorteras även dubbletter av behov bort och formuleringar ensas. Viktigt är också att spårbarheten från behoven till de utsagor som behoven kommer ifrån dokumenteras.

När relationsdiagrammen anses vara färdiga, genomförs det andra steget i denna aktivitet. Relationsdiagrammen överförs till hierarkiska diagram eftersom dessa ger en bättre översikt. Dessa diagram analyseras vidare, framförallt i syfte att upptäcka om några behov saknas. Om det finns luckor bland behoven, måste dessa bekräftas av representanter för verksamheten, eller med stöd av information som samlats in under den första aktiviteten. Även under denna analys är det möjligt att förändra behovsstrukturen.

2.5.5 Identifiering av krav

Under den femte aktiviteten analyseras de behov som har identifierats och strukturerats i syfte att identifiera de krav som skall ställas på ett framtida system. Kraven skall uppfylla svaret på frågan ”Hur kan detta behov tillfredsställas?” och formuleras på formen ”Systemet skall …” utan att specificera *hur* det skall realiseras. Resultatet av denna aktivitet utgörs av ett antal ostrukturerade krav.

2.5.6 Analys av identifierade krav

Under den sjätte aktiviteten genomförs en analys av de krav som har identifierats. Detta sker genom att använda samma typ av diagram och arbetssätt som under analysen av behov i den fjärde aktiviteten.

2.6 Forskningsprojektet

Syftet med projektet *Värdering av IT-säkerhetsnivå hos system inom NBF* är att understödja Försvarsmaktens arbete med att ta fram system med adekvat säkerhet. Detta genom att stärka kompetens och förmåga gällande värdering av IT-säkerhetsnivåer hos system. Förväntat resultat av projektet innefattar metoder för bedömning av IT-säkerhetsnivåer hos system inom NBF. Följande frågeställningar är centrala för projektet:

1. Vilka behov gällande värdering av IT-säkerhetsnivåer hos informationssystem påkallas av NBF?
2. Vilka metoder för värdering av IT-säkerhet svarar bäst upp mot de identifierande behoven?
3. Hur kan systemutvecklare och driftspersonal bäst nyttja de framtagna metoderna?

Det övergripande målet under 2005 är att besvara den första av frågorna ovan. Delmål för att besvara denna fråga är att ta fram:

1. Scenarion vilka tydliggör nyttan med och behoven av metoder för värdering av IT-säkerhetsnivåer inom NBF.
2. En kartläggning av relevanta metoder för behovsanalys inom området.
3. En sammanställning av behov gällande värdering av IT-säkerhetsnivåer.

3. Metod

Behovsanalysen som presenteras i denna rapport baseras på *Metod för behovsanalys avseende värdering av IT-säkerhet* (MedBeVIS), Figur 1, som tagits fram i projektet under året (Hallberg m.fl., 2005c). Grunderna i denna version av MedBeVIS härstammar i huvudsak från de fyra första aktiviteterna i Kvalitets-driven kravhantering (Hallberg m.fl., 2005a), användningsfall från *Unified Modeling Language*, UML, (OMG, 1999) samt felanvändningsfall (Sindre & Opdahl, 2000). MedBeVIS baseras på fem steg: (1) insamling av data, (2) identifiering av utsagor, (3) analys av utsagor och identifiering av behov, (4) analys och strukturering av behov och (5) modellering av behov avseende värdering av IT-säkerhet.

I föreliggande behovsanalys har de fyra första stegen i MedBeVIS använts. Under behovsanalysen hölls en öppen attityd mot identifierade behov, så att inte relevanta behov skulle sorteras bort av misstag. Detta då syftet med behovsanalysen är att tydliggöra behov relaterade till frågeställningen. Det är bättre med en något för omfattade mängd behov som indata till kravarbetet än att relevanta behov saknas. Många av behoven som identifierats kan upplevas som självklara, men det finns en vinst med att bekräfta detta genom empiriska studier. Dessutom ger de mindre självklara behoven som identifierats som viktiga störst effekt för de framtida användarna. Syftet med behovsanalyser är inte enbart att påvisa vilka funktioner och egenskaper som skall realiseras, utan också att tydliggöra vad som **inte** skall realiseras.

3.1 Insamling av data

Under den första aktiviteten sker insamling av data, som direkt eller indirekt innehåller information som påvisar relevanta behov. Insamlingen kan ske genom ett flertal olika metoder och tekniker, exempelvis intervjuer, scenarion, analys av verksamhetsmodeller och enkäter. I denna studie genomfördes intervjuer med personer som representerar utvecklare och domänexpert (Bilaga 1). Dessutom inhämtades dokument av relevans för problemfrågeställningen (Bilaga 1). Vid intervjuerna utgick frågeställarna ifrån ett antal på förhand givna relativt öppna frågor (Bilaga 2), samtidigt gavs respondenterna stor frihet att göra utvikningar kring frågeställningarna. Intervjuerna spelades in och transkriberades i sin helhet. Respondenterna gavs därefter möjlighet att senare korrigera och komplettera intervjutranskriptionerna. Utdata från detta steg är text, vilken i den

aktuella studien bestod av intervjutranskriptioner och andra relevanta dokument.

3.2 Identifiering av utsagor

I den andra aktiviteten analyseras texten i syfte att identifiera utsagor. Under genomläsningen markerades, för problemfrågeställningen relevanta, utsagor. Det vill säga utsagor innehållande en avgränsad information som på något sätt berör värdering av IT-säkerhet. Utsagorna kan med fördel vara delvis överlappande så att de inte blir alltför kortfattade och svåra att tolka. I denna studie analyserades varje intervjutranskription av två personer och varje dokument av en person.

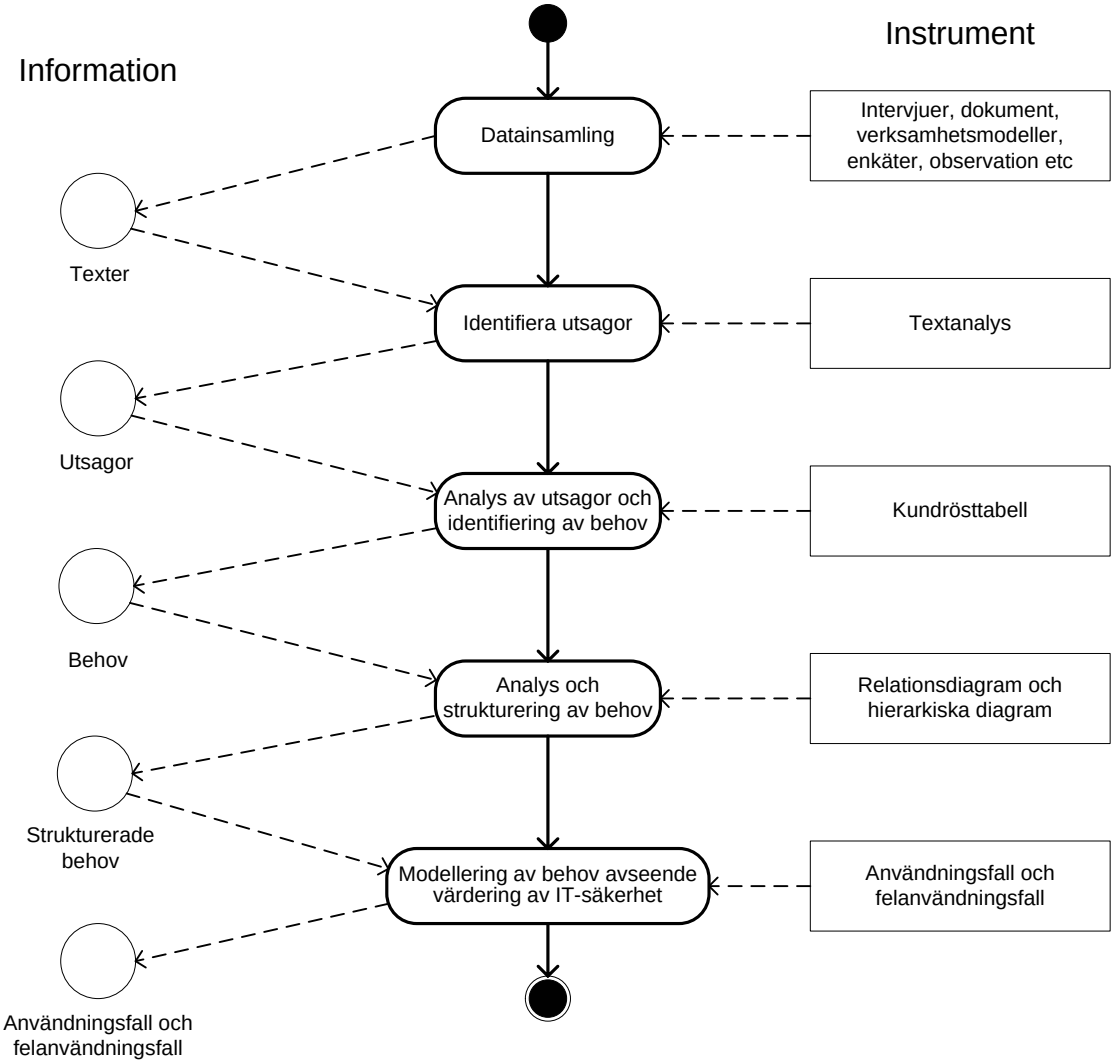
3.3 Analys av utsagor och identifiering av behov

I den tredje aktiviteten genomförs en analys av de identifierade utsagorna med hjälp av kundrösttabeller (Shillto, 2001). Syftet är att ur utsagorna identifiera behov som påvisar situationer där stöd för värdering av IT-säkerhet skulle vara önskvärda. Detta oavsett om behovet redan idag är tillfredsställt eller ej inom det system som utsagan avser. Kundrösttabeller stödjer arbetet med analysen genom sin struktur, vilken underlättar identifieringen av relevanta attribut i utsagorna. Resultatet av denna aktivitet utgörs av en samling ostrukturerade behov. I denna studie genomfördes först en grov sortering av utsagorna så att liknade utsagor kom att analyseras i relation till varandra. Detta för att underlätta själva analysen som genomfördes av en person. Analysresultatet granskades och korrigerades därefter av en annan person.

3.4 Analys och strukturering av behov

I den fjärde aktiviteten analyseras de identifierade behoven. Först genom att sortera och gruppera behoven med liknande behov i kategorier. Därefter grupperas kategorier till abstrakta kategorier, tills dess att ett antal övergripande toppkategori erhålls. Under denna analys tas dubbletter bort och behovens formuleringar bearbetas. Vissa behov delas upp i flera, andra behov med principiellt samma betydelse slås ihop. Det är viktigt för spårbarheten att dokumentera relationen mellan utsagor och behov. Denna första analys resulterar i en struktur över behoven och deras kategorier. Strukturen analyseras sedan, varvid behoven, kategorierna och deras relationer bearbetas ytterligare, för att förfina resultatet. I denna studie gjordes först en grov sortering och gruppering av behoven gemensamt av tre personer. Därefter gjordes en djupare

analys av de 13 övergripande kategorierna av enskilda personer. Vid behov interagerade dessa personer om flyttning av enskilda behov eller grupper av behov mellan de övergripande kategorierna. Slutligen granskades resultatet av två personer.



Figur 1: Diagram som beskriver *Metod för behovsanalys avseende värdering av IT-säkerhet* (MedBeVIS). Informationsobjekten (cirklar) visar vilken information som skapas respektive nyttjas i aktiviteterna. Vidare återfinns de instrument (rektanglar) som används i respektive aktivitet. I föreliggande behovsanalys har de fyra första stegen använts.

4. Resultat

Under behovsanalysen genomfördes 6 intervjuer, med sammanlagt 9 personer, och 13 dokument som bedömdes vara relevanta sammanställdes. Analysen av de transkriberade intervjuerna resulterade i 110 identifierade utsagor och dokumentanalysen resulterade i 105 identifierade utsagor, dvs. totalt 215 utsagor identifierades. Varje intervju analyserades av två personer och varje dokument av en person varvid utsagor markerades i den analyserade texten. Tre personer validerade gemensamt de identifierade utsagorna och samlade dem i ett dokument. De validerade utsagorna strukturerades och utgjorde grunden för skapandet av kundrösttabeller. Kundrösttabellerna analyserades av en person för att identifiera behov och analysen validerades av ytterligare en person. Detta resulterade i att 525 behov identifierades. Därefter analyserades, grupperades och strukturerades behoven. Under analysen togs dubbletter bort, formuleringar ensades och vagheter tydliggjordes. Den resulterande behovsstrukturen består av 13 övergripande kategorier, som totalt innehåller 419 behov.

4.1 Behov av att värdera IT-säkerhet

I detta avsnitt redovisas den struktur av behov som blev resultatet av behovsanalysen. I Tabell 1 sammanfattas strukturen på kategorinivå. Därefter följer en beskrivning av de olika kategorierna. Kategorierna beskrivs på en övergripande nivå baserat på de behov som återfinns inom respektive kategori.

Tabell 1: Strukturen av behovskategorier.

- B.1 Stöd vid utveckling
  - B.1.1 Säkerhet och utveckling
  - B.1.2 Kravhantering
    - B.1.2.1 Kravställa säkerhet
      - B.1.2.1.1 Kravställa IT-säkerhet
      - B.1.2.1.2 Kravställa informationssäkerhet
  - B.1.3 Ta fram säkerhetslösningar
- B.2 Stöd vid drift
  - B.2.1 Incidenthantering
    - B.2.1.1 Detektion
- B.3 Värdering
  - B.3.1 Värderingsomfång
  - B.3.2 Värdera faktorer
    - B.3.2.1 Värdera säkerhetslösningar
      - B.3.2.1.1 Värdera säkerhetslösningars påverkan

B.1 Stöd vid utveckling

Det finns ett antal generella behov av stöd avseende utvecklingsprocesser. En del av dessa pekar på att det behövs (1) en förståelse för systemkontexten vid utveckling av system, (2) kortare utvecklingstider samt att (3) utvecklingsprocessen skall ge stöd för ackreditering av det färdiga systemet. Vidare finns det behov av utvecklingsprocesser som redan under de tidiga faserna beaktar användbarhets- och säkerhetsaspekter samtidigt. Kategorin *Stöd vid utveckling* innehåller tre underkategorier med behov. Dessa är *Säkerhet och utveckling*, *Kravhantering* och *Ta fram säkerhetslösningar*.

B.1.1 Säkerhet och utveckling

Kategorin *Säkerhet och utveckling* innefattar behov av säkerhetsarbete relaterat till utvecklingsarbete. Det finns behov av att kunna beakta säkerhet redan från början av utvecklingsprocessen, exempelvis med avseende på stöd för att identifiera kravställare för verksamheters säkerhetskrav, hitta säkra lösningar som får användas och att dokumentera avvikelser från standarder gjorda under utveckling samt motiveringar till detta. Vidare finns det behov av att kunna integrera säkra kom-

ponenter till säkra system samt att byta säkerhetslösningar i ett system utan att påverka andra säkerhetslösningar.

B.1.2 Kravhantering

Inom kategorin *Kravhantering* fokuseras det på stöd för behovsanalys samt att kravställa såväl tekniska system som verksamhet. Det finns behov av att identifiera verksamheters mål och baserat på dessa identifiera vilken teknik som krävs för att verksamheter skall nå sina mål. Vidare finns det behov av att enhetligt formulera krav, och att kravspecifikationer integrerar verksamhetskrav med säkerhetskrav. *Kravhantering* innehåller underkategorin *Kravställa säkerhet*.

B.1.2.1 Kravställa säkerhet

När det gäller kravhantering avseende säkerhet, så finns det behov av att kunna identifiera säkerhetsbehov, att identifiera tidigt i utveckling vad som bör skyddas och mot vad. Säkerhetskrav måste baseras på och balanseras mot verksamhetsbehov och funktionella krav. Säkerhetskrav måste formuleras så att det möjliggör verifiering av lösningar mot dessa.

Krav på säkerhet måste kunna baseras på:

- verksamheters behov och riskbenägenhet,
- hotbild,
- lagar och direktiv fastställda av nationella och internationella organisationer,
- önskade förmågor att detektera och reagera på incidenter,
- informationsklassning och
- infrastrukturers säkerhetstjänster och tillämpningars specifika krav.

Säkerhetskrav måste vara mätbara och spårbarhet mellan aktiviteter, funktionella krav och säkerhetskrav måste finnas. Det finns behov av att kravställa en basnivå för säkerhet i system.

Kategorin *Kravställa säkerhet* innehåller underkategorierna *Kravställa IT-säkerhet* och *Kravställa informationssäkerhet*.

B.1.2.1.1 Kravställa IT-säkerhet

Det finns behov av att kunna kravställa IT-säkerhet baserat på:

- verksamheters behov,
- externa krav på verksamheter och
- hotbild, innefattande externa såväl som interna hot.

I kravställandet av IT-säkerhet måste hänsyn kunna tas till systems driftmiljö och livslängden på information. Vidare behöver säkerhetsnivån i nätverks åtkomstkontroll kravställas.

B.1.2.1.2 Kravställa informationssäkerhet

Tillräcklig informationssäkerhet måste kunna kravställas. Styrning av användares ansvar och åtkomsträttigheter samt styrning av övervakning behöver kunna kravställas. Det finns behov av att kravställa informationssäkerhet vid upphandling och inom:

- samhällsviktiga system,
- företag,
- statlig förvaltning och
- kontakter mellan statlig förvaltning och övriga samhället.

B.1.3 Ta fram säkerhetslösningar

Det finns behov av säkerhetslösningar baserade på mer användarvänlig teknik och bättre användargränssnitt samt att stödja framtagande av säkerhetsrutiner.
Olika säkerhetsmekanismer måste kunna integreras som skydd mot olika hot.
Det finns behov av att kunna identifiera säkerhetslösningar som:

- är baserade på säkerhetskrav och fungerar i verksamheten,
- uppfyller såväl säkerhetskrav som verksamheters krav,
- fungerar för SCADA[3]-system,
- kan hantera flera sekretessnivåer i samma nät och noder och
- medför att rätt balans nås mellan att förebygga incidenter, detektera incidenter och agera vid incidenter

B.2 Stöd vid drift

Det finns behov av att under drift anpassa systems säkerhet och funktionalitet till aktuell hotbild, kända svagheter och verksamhet. Säkerhetslösningar måste via öppna gränssnitt och protokoll kunna anslutas till system. Vidare finns det behov av att hantera olika aktörers åtkomstkrav och åtkomstkontrollbehov samt rättigheter och behörigheter. Det finns även behov av att göra uppföljning av säkerhet under drift.

Kategorin *Stöd vid drift* har underkategorin *Incidenthantering*.

[3] SCADA (eng. Supervisory Control And Data Acquisition) avser styr- och reglersystem som används för distribuerade processer, exempelvis inom infrastruktur för distribution av vatten och el. (Christiansson, 2004)

B.2.1 Incidenthantering

Det finns behov av att identifiera, värdera och hantera säkerhetsrelaterade incidenter, vilket innefattar att säkerställa att information inte förvanskas utan att det upptäcks. Det finns behov av att identifiera och värdera säkerhetsrelevanta händelser, för att initiera insatser innan incidenter uppträder. Åtgärder mot incidenter måste kunna sättas in tillräckligt snabbt.

Kategorin *Incidenthantering vid drift* har underkategorin *Detektion*.

B.2.1.1 Detektion

Det finns behov av att kunna detektera och samla indata om säkerhetsincidenter avseende:

- säkerhetspåverkande händelser,
- attacker mot och incidenter i nätverk,
- försök till informationsoperationer,
- intrång,
- manipulation av information,
- säkerhetsbrister och
- kritiska fel.

B.3 Värdering

De behov som direkt pekar på olika former av värdering har delats in i underkategorierna *Värderingsomfång*, *Värdera faktorer*, *Värdera säkerhetslösningar*, *Värdera säkerhetslösningars påverkan, Värderingsmekanismer* och *Värdera information*.

B.3.1 Värderingsomfång

Behov av generell värdering av förmågan inom informationssäkerhetsområdet har identifierats. Därutöver har följande aspekter av informationssäkerhet identifierats vara av vikt:

- IT-säkerhet,
- IT-säkerhet i relation till övrig säkerhet i organisationen,
- överlevnadsförmåga hos system och
- fysiska och logiska skydd.

Följande domäner har identifierats vara av vikt att värdera informationssäkerhet inom:

- verksamhet,

- den nationella IT-infrastrukturen,
- system av system,
- informationssystem,
- tjänstebaserade koalitioner av system,
- nätverk,
- systemlösningar,
- tjänster i informationssystem,
- system med informationszoner,
- e-handel rörande känslig och personlig information,
- SCADA-system,
- webbplatser,
- systemkomponenter,
- externa komponenter och
- filterfunktioner i nätverk.

B.3.2 Värdera faktorer

Denna kategori pekar på behoven av att kunna värdera hur säkerhet påverkas av olika faktorer, såsom:

- standarder,
- den mänskliga faktorn,
- psykologiska operationer och vilseledning,
- medvetenhet hos användarna,
- användbarhet,
- beroenden mellan IT-system,
- gränssnitt mellan komponenter,
- informationsutbyte mellan komponenter,
- sammankopplade infrastrukturer,
- lättillgänglig information om säkerhetsbrister och utnyttjande av sådana,
- skadlig kod,
- drift av systemet,
- informationsflöde,
- beroenden i säkerhetsarkitekturen och

- produkt- och tjänsteuppdateringar.

Kategorin *Värdera faktorer* innehåller underkategorin *Värdera säkerhetslösningar*.

B.3.2.1 Värdera säkerhetslösningar

En central faktor är de lösningar som används för att höja säkerheten. Säkerhetslösningar kan realiseras med teknik, metoder, organisation och regelverk. Såväl införda som planerade lösningar behöver kunna modelleras och värderas avseende exempelvis:

- säkerhetsnivå,
- förmåga att begränsa psykologiska operationer och vilseledningsmedels påverkan på IT-säkerheten,
- integration med andra säkerhetslösningar,
- uppfyllande av standarder,
- rimlighet,
- fullständighet,
- tillräcklighet och
- förmåga att hantera säkerhetsaspekter såsom:
  - åtkomstkontroll,
  - flera sekretessnivåer i samma nät och noder,
  - e-legitimation,
  - skydd mot attacker och
  - insiderproblematik.

Kategorin *Värdera säkerhetslösningar* innehåller underkategorin *Värdera säkerhetslösningars påverkan*.

B.3.2.1.1 Värdera säkerhetslösningars påverkan

Säkerhetslösningar har ofta andra effekter än de rent säkerhetsmässiga. Därmed finns behov av att såväl i förväg värdera som följa upp säkerhetslösningars konsekvenser avseende exempelvis verksamhet och användbarhet. Detta innefattar designval, konfiguration, uppdateringar och dynamiska förändringar av tekniska och organisatoriska system för att uppnå adekvat säkerhet.

B.3.3 Värderingsmekanismer

Kvantifiering av informations- och IT-säkerhet är nödvändig för att möjliggöra metoder och tekniker för värdering av säkerhet. Då säkerhet är ett komplext område med många skilda aspekter, finns behov av att väga samman resultat från fle-

ra olika metoder och tekniker. Det finns också behov av kontinuerlig uppföljning av säkerheten.

B.3.4 Värdera information

Information, eller strikt taget data, behöver värderas avseende:

- nytta,
- informationsvärde,
- säkerhetsrelevans,
- skyddsvärde,
- trovärdighet,
- ursprung,
- rimlighet och
- korrekthet.

Ytterligare behov som framträder i samband med informationsklassning avser hänsyn till faktorerna tid, rum och miljö samt klassning vilken medger anpassning av säkerhetsnivå.

B.4 Beslutsunderlag

Verksamhetsledningen behöver beslutsunderlag för att driva igenom förändring av säkerhetsfunktioner. Ledningen behöver även underlag för att kunna avdela resurser för IT-säkerhetsarbete.

B.5 Kommunicera kring säkerhet

Det finns behov av att kommunicera IT-säkerhetsfrågor inom organisationer ur verksamhets- och säkerhetsperspektiv, samt vid incidenter. Det finns behov av att kunna informera om säkerhet, säkerhetslösningar och konsekvenser av säkerhetsrelaterade händelser samt presentera säkerhetskrav och restriktioner.

Kategorin *Kommunicera kring säkerhet* innehåller underkategorierna *Kommunikation med ledningen* och *Kommunikation med anställda*.

B.5.1 Kommunikation med ledningen

Det finns behov av att kommunicera med ledningen kring IT-säkerhet, för att uppnå förståelse hos ledningen kring behovet av informationssäkerhet och behovet av insatser avseende säkerhet. Det är viktigt att säkerhetsansvariga har ledningens förtroende att genomföra säkerhetsarbete och att ledningen får information om säkerhetsfrågor och aktuellt läge. Säkerhetsansvariga måste kontinuerligt

kunna ge för verksamheten relevant återkoppling från säkerhetsarbetet och säkerhetsfunktioner till systemdriftsledningen.

B.5.2 Kommunikation med anställda

Det finns behov av att kommunicera med anställda kring IT-säkerhet. Detta inkluderar att informera om vikten av att använda befintliga IT-säkerhetslösningar.

B.6 Riskhantering

Det finns behov av att kunna genomföra riskhantering, där avvägning görs mellan sekretess, riktighet, tillgänglighet och de konsekvenser detta får för verksamheten. Verksamheters riskbenägenhet behöver också identifieras. Riskhantering måste ge underlag för att prioritera IT-säkerhetsåtgärder. Riskhantering måste också kunna genomföras under drift. Sårbarhets- och riskanalyser måste genomföras för kritisk infrastruktur. Det finns behov av att kunna analysera kostnaden för säkerheten i förhållande till nyttan. Ägare av tjänster i tjänstebaserade informationssystem måste kunna genomföra riskhantering. Vid riskhantering måste miljön där IT-system verkar beaktas utifrån den hotbild som finns och åtgärder måste utformas baserat på detta.

Kategorin *Riskhantering* innehåller kategorin *Riskanalys*.

B.6.1 Riskanalys

Det finns behov av att agera preventivt innan säkerhetsproblem uppstår. Riskanalyser behövs för att klargöra tänkbara hot, miljöer och situationer där någon form av risk uppkommer. Vidare skall riskanalyser innefatta konsekvensanalys och sannolikhetsbedömning. Det är viktigt att kunna dokumentera resultat av riskanalyser så att de kan ligga tillgrund för utformning av åtgärdsplaner.

Det finns behov av att kunna genomföra riskanalys

- i system av system,
- avseende infrastruktur och
- avseende kravställande faktorer.

Risker skall kunna analyseras:

- relativt hur värdefull informationen är,
- kvantitativt och i termer av pengar,
- avseende säkerhetseffekter av sammankopplade nät mellan organisationer och sammankopplade samhällsviktiga infrastrukturer,

- avseende ökat användande av nätbaserad funktionalitet och nätbaserade tjänster,
- avseende systemanvändning i nya miljöer och
- avseende nyttjande av andra aktörers infrastruktur.

Riskanalyser behöver kunna göras regelbundet, för att ge tillgång till uppdaterad information som underlag för säkerhetsarbetet. Det finns även behov av att genomföra riskanalyser för att säkerställa att tekniken inte medför att information sprids till icke-behöriga. Det finns behov av att få personal engagerad i riskanalys.

Kategorin *Riskanalys* innehåller underkategorierna *Hotanalys*, *Sårbarhetsanalys* och *Konsekvensanalys*.

B.6.1.1 Hotanalys

Det finns behov av att kunna genomföra hotanalys för att:

- identifiera aktörer och aktörsgrupper, deras drivkrafter och medel,
- väga externa och interna hot mot varandra,
- identifiera hot från andra nationer avseende psykologiska operationer och vilseledning,
- beakta de oväntade och överraskande hoten,
- värdera hur olika samverkande förmågor kan utgöra hot,
- bevaka hoten mot Internet-infrastrukturen i Sverige,
- identifiera IT-säkerhetshot, såväl avsiktliga som oavsiktliga, inom och i anslutning till systemet och
- identifiera tänkbara hot, miljöer och situationer där någon form av risk uppträder.

B.6.1.2 Sårbarhetsanalys

Det finns behov av att kunna genomföra sårbarhetsanalys avseende:

- kontinuerlig identifiering av brister,
- identifiering av sårbarheter i IT-infrastrukturen,
- samhällets sårbarhet för störningar i relation till utvecklingen inom IT-säkerhetsområdet,
- robusthet i Internet-infrastrukturen i Sverige,
- säkerhetsbrister inom den egna organisationen,
- identifiering av sårbarheter i nuvarande och framtida kritiska infrastrukturer,

- tekniska brister i den teknik som verksamheten behöver för att nå sina mål och
- uppskattningar av sårbarheter och beroendeförhållanden inom SCADA-system, speciellt relaterat till fjärrstyrning av sådana.

Det finns behov av att dokumentera resultatet av sårbarhetsanalyser, bland annat för att underlätta identifieringen av lösningar.

B.6.1.3 Konsekvensanalys

Det finns behov av att kunna genomföra konsekvensanalys avseende:

- hur skadlig kod drabbar organisationer och samhällsviktig infrastruktur,
- säkerhetseffekter och kostnader när känslig information ur eller känslig funktionalitet i system röjs,
- effekter på IT-säkerhetseffekter av vilseledande verksamhet,
- effekter av informationsoperationer och intrång på korrekthet hos data/information,
- påverkan av informationsoperationer på beslutsfattare,
- ökad funktionalitets inverkan på säkerheten och
- mått på effekter av skadlig kod.

B.7 Säkerhetslösningar

Säkerhetslösningar behövs för att minska samhällets sårbarhet av störningar i IT-system och konsekvenserna detta medför. Det finns behov av ökad automatisering av säkerhetsfunktionalitet, vilket kan genomföras med hjälp av regler för att automatisera konfiguration av säkerhetsfunktioner.

Det finns behov av att finna säkerhetslösningar som ger skydd:

- av infrastruktur,
- av skyddsvärd information,
- mot insiderattacker,
- mot skadlig kod,
- mot oavsiktlig felanvändning,
- mot icke-sanktionerad nätverkstrafik,
- mot informationsöverbelastning,
- vid anslutningar av externa komponenter och

- av infrastrukturer genom övervakning för att tillräckligt snabbt kunna agera vid avbrottssituationer och vikande prestanda.

Säkerhetslösningar behövs för att säkerställa:

- adekvat säkerhet i samhällsviktiga system,
- hög tillgänglighet och riktighet hos information, samt hög funktionalitet och användbarhet,
- motpartens identitet (identitetsverifiering),
- säkerheten på Internet, så att organisationer kan tillhandahålla tjänster där,
- adekvat och säker rättighetshantering samt
- spårbarhet avseende källa och transaktioner.

B.8 Verifiering och validering

Det finns behov av att verifiera:

- olika typer av system, exempelvis tjänstebaserade system,
- system mot ställda säkerhetskrav,
- säkerhetsarkitektur mot ställda säkerhetskrav,
- säkerhetslösningar och
- säkerhetsnivå hos komponenter.

För att kunna verifiera ställda säkerhetskrav måste dessa kunna kopplas till mätbara egenskaper. Det finns behov av att verifiera och validera säkerhetslösningar som hanterar flera sekretessnivåer i samma nät och noder, samt av att integrera verifierings- och valideringsmetoder på olika nivåer. Det finns behov av att validera modellbaserade lösningsförslag och kravställning för system.

B.9 Ledning och säkerhetsarbete

Det finns behov av stöd för ledningen att genomföra säkerhetsarbete. Ledningen skall:

- definiera mål och inriktning för säkerhetsarbete, skapa samsyn avseende vilken nivå av säkerhet som är tillräcklig,
- tydliggöra vem som skall kravställa säkerhet,
- fatta beslut om åtgärder,
- ta fram säkerhetspolicy som kan anpassas efter verksamhet, hotbild och risker,

- ta fram systemsäkerhetsplaner för viktiga IT-system och
- ta fram IT-säkerhetsinstruktioner.

Det måste finnas en tydlig koppling mellan säkerhetspolicy samt säkerhetsarbete och säkerhetsfunktioner.

B.10 Kompetens kring informationssäkerhet

Det finns behov av att minska säkerhetsriskerna genom ökad kompetens, förbättrade rutiner och ökat säkerhetsmedvetande. Det finns specifika behov av ökad kompetens kring informationssäkerhet avseende:

- allmän informationssäkerhet,
- säkerhetsrisker, inklusive risker för intrång av skadlig kod,
- hur man ökar skyddet,
- sårbarheter i IT-miljön och
- möjligheter att förbättra IT-säkerheten.

Det finns behov av ökad medvetenhet avseende säkerhetsaspekter och insikt om att säkerhet är en tillgång istället för ett hinder.

Det är viktigt att de som medverkar i utveckling av system, förstår nödvändigheten i att beakta säkerhetsaspekter tidigt under utvecklingsarbetet. Det är också viktigt att förstå vilka säkerhetskrav som ställs och hur de relaterar till säkerhetsfunktioner och säkerhetsmekanismer.

Kategorin *Kompetens kring informationssäkerhet* innehåller kategorierna *Kompetens hos IT-säkerhetspersonal* och *Kompetensen hos användare/anställda*.

B.10.1 Kompetens hos IT-säkerhetspersonal

Det finns behov av att öka kompetensen hos personer som arbetar med IT-säkerhet avseende:

- incidenthantering,
- rättighetsadministration,
- säkerhetskonfiguration i nät av nät,
- informationsklassning,
- riskbedömning,
- förmåga att sälja in och förankra beslut om säkerhetsåtgärder hos ledningen samt

- kravställning av säkerhetsåtgärder.

B.10.2 Kompetens hos användare/anställda

Det finns behov av att öka kompetensen hos användare/anställda avseende:

- informationssäkerhet och IT-säkerheten i allmänhet,
- skydd mot skadlig kod,
- konsekvenserna och riskerna med IT och
- koppling mellan handlingar och säkerhetskonsekvenser.

B.11 Tillit

Det finns behov av att öka användares tillit till informationstjänster och e- handelstjänster, vilka kräver att de är villiga att meddela personliga uppgifter till sådana tjänster. Ökad tillit till elektroniska tjänster bygger bland annat på att säkra tillgängligheten. Det finns ett behov hos organisationer att påvisa att de är värdiga tillit och förmår att förvalta och utveckla den. Det finns behov av att mäta hur individers oro påverkar utveckling och användande av informationstjänster. Därav finns behov av att mäta relationen mellan tillit som subjektivt mått och teknisk säkerhet.

B.12 Beskriva säkerhet och säkerhetskonsekvenser

Det finns behov av att kunna tydliggöra sambandet mellan hög grad av IT-nyttjande, informationssäkerhet och verksamhetsplanering. Det finns behov av att kunna beskriva:

- hur säkerhetshantering fungerar i verksamheter,
- relationen mellan säkerhet och användbarhet/användning,
- säkerhetsfunktioner som egenskaper hos ett IT-system,
- vilka verksamhetsaktiviteter och funktionella krav som får konsekvenser för säkerheten,
- ändrad hotbild vid ökat användande av nätbaserad funktionalitet och nätbaserade tjänster samt
- ändrad hotbild vid systemanvändning i nya miljöer.

B.13 Övriga

Det finns behov av att fånga tyst kunskap om säkerhet och att tillvarata anställdas erfarenheter i risk- och sårbarhetsanalyser. Det behövs en gemensam terminologi inom informationssäkerhetsområdet. Det finns behov av att ackreditera system, komponenter och tjänster för specifika tillämpningar.

5. Diskussion

Det finns påtagliga behov av att kunna påvisa huruvida säkerheten i informationssystem är tillräcklig (ACSA, 2002). Detta behov ökar i takt med att informationssystem integreras alltmer i alla former av verksamheter och med andra informationssystem. Behovet blir också större eftersom hotbilden förändras, då antagonister kan åstadkomma allt större verkan genom angrepp mot IT-system. Komplexiteten hos dessa system medför även att omedveten felanvändning såväl som medvetet missbruk kan få stora konsekvenser som är oöverblickbara för användaren.

Många organisationer, inklusive Försvarsmakten, omstrukturerar tidigare hierarkiska eller processorienterade organisationer till nätverksbaserade organisationer. Detta ställer ytterligare ökade krav på möjligheter att kunna skapa system genom att integrera andra system, med en tillfredsställande säkerhetsnivå hos det resulterande systemet . Dessa nätverksbaserade organisationer förutsätter också en hög nyttjandegrad av modern informationsteknik (IT). I många organisationer hanteras känslig information av system sammankopplade med öppna nät, vilket ställer krav på erforderlig IT-säkerhet. För att kunna bedöma nivån på IT-säkerhet hos olika system krävs metoder och verktyg för värdering.

Om metoder och verktyg för värdering beaktas som system, kan principer och erfarenheter från systemutvecklingsområdet nyttjas vid utvecklingen av dessa. Det finns två fundamentalt skilda ansatser för att utveckla system. Enligt den första ansatsen tas systemet fram först, varefter möjliga tillämpningar för systemet identifieras. Det är en riskfylld ansats som ofta leder till misslyckanden då tänkta användare inte erhåller någon större nytta av systemet. I vissa lyckosamma fall kan dock system konstruerade enligt denna ansats visa sig vara mycket gångbara och efterfrågade. Enligt den andra ansatsen söks först en förståelse för en möjlig användning av systemet, därefter skapas ett system som motsvarar denna användning. Även denna ansats har visat sig vara svår, mycket på grund av att det ofta tas genvägar i de initiala stegen med att förstå vilka behoven är (Focal point, 1998). Till exempel är ungefär 80% av alla fel i programvaror ett resultat av brister i kravhanteringen (Young, 2001).

I arbetet som redovisas i denna rapport har en studie genomförts avseende föreliggande behov av att genomföra värdering av IT-säkerhet. Dessa behov skall i vidare arbete utgöra en grund för att specificera krav på metodik och verktyg för

värdering av IT-säkerhet i komplexa informationssystem. Denna rapport presenterar resultatet av behovsanalysen i form av en övergripande struktur över identifierade behov och en kort beskrivning av behoven.

Resultaten från studien visar att det finns en relativt stor spännvidd hos de behov som har kommit fram; från behov av att kunna kravställa säkerhet så att värdering kan genomföras, till att kommunicera med ledningen kring resultatet av värderingen för att kunna få mandat för fortsatt utveckling av säkerheten. Det kan tyckas att många av behoven som redovisas är självklara. Till skillnad från rena spekulationer om vilka behoven är, bygger denna studie på ett omfattande datamaterial. Detta material består av dokument som är relevanta för frågeställningen och intervjuer med potentiella användare av metoder och verktyg för värdering av IT-säkerhet. Resultatet av behovsanalysen antyder att metoder och verktyg för värdering av IT-säkerhet måste ge stöd för kravarbete, värdering och riskhantering. Dessa metoder och verktyg bör också ge stöd för att ta fram presentationsmaterial som kan användas dels i vid utbildning av anställda/användare och vid kommunikation med ledningen. Det senare är viktigt för att ledningen skall kunna fatta riktiga beslut gällande informations- och IT-säkerhet.

Det kan invändas att vissa av de presenterade behoven inte är relevanta för utvecklingen av metoder och verktyg för värdering av IT-säkerhet. Det skall dock inte, enligt principer för systemutveckling, hanteras i detta skede, utan under den senare fasen *kravhantering*. Behovsanalysens syfte är enbart att tydliggöra vilka behov som finns relaterade till frågeställningen. Det är bättre att ha en något för omfattade mängd behov som grund för kravarbetet, än för få där vitala behov saknas. Många av behoven är givetvis kända, men de mera okända behoven har potential att resultera i metoder och verktyg med stor effekt för de framtida användarna. Behovsanalysen syftar inte enbart till att påvisa vilka funktioner och egenskaper som skall realiseras, utan det är minst lika viktigt att nyttja behovsspecifikationen för att avgöra vad som **inte** skall realiseras.

Metoden som används för behovsanalys avseende värdering av IT-säkerhet baseras i hög grad på det kvalitetstänkande som sedan årtionden präglat modern utveckling av produkter och tjänster (Bergman & Klefsjö, 1994). Den bygger på att bryta ner allt datamaterial och återskapa en ny helhet som ger en djupare förståelse för fenomenet. På så vis identifieras utsagor ur intervjuer och dokument. Utsagorna omvandlas till behov, vilka struktureras till en ny helhet som bättre förklarar det som eftersöks.

Nästa steg i arbetet blir att specificera de krav som skall ställas på metoder och verktyg avseende värdering av IT-säkerhet.

Referenser

ACSA (2002), *Proc. Workshop on Information Security System Scoring and Ranking*. Applied Computer Security Associates.
http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf

Alves-Foss, J., & Barbosa, S. (1995). Assessing Computer Security Vulnerability. Operating Systems Review, Vol 29, No 3, July 1995, pp. 3–13.

Andersson, R. (2005); A Method for Assessment of System Security, Master's thesis in Information Theory, LiTH-ISY-EX—05/3745—SE, Linköping, Sweden.

Beierholm, M. & Mattsson, P. (2005). *Försvarsmaktens behov av att värdera IT-säkerheten i det nätverksbaserade försvaret*. D-uppsats framlagd vid Linköpings universitet.

Bergman, B. & Klefsjö, B. (1994). *Quality from Customer Needs to Customer Satisfaction*. London: McGraw-Hill.

Blobel, B. & Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems, International Journal of Medical Informatics, Vol. 62, Issue 1, pp. 51-78, June 2001.

CC (1999). *Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements. Version 2.1*, August 1999.

Christiansson, H. (2004). Värdering av IT-säkerhetsanalysmetoder inom samhällsviktig infrastruktur. Användarrapport, FOI-R--1350--SE. Totalförsvarets Forskningsinstitut.

Clark, K., Tyree, S., Dawkins, J., & Hale, J. (2004). Qualitative and Quantitative Analytical Techniques for Network Security Assessment. Proceedings of the 5th IEEE Workshop on Information Assurance. West Point, NY, June 2004.

Cohen, L. (1995). *Quality Function Deployment: How to Make QFD Work for You.* New York, NY: Addison-Wesley.

Engeström, Y. (1990). Learning by Expendning: An Activity – Theoretical Appraoch to Development Research, ISBN: 951-95933-2-2.

Fahs, R. & Wiseman, S. (1999). Re-Floating the Titanic: Multi Level Security in Contemporary Environments.
www.eicar.org/download/titanic.doc

Försvarsmakten (2004). Krav på säkerhetsfunktioner – Grunder. 10 750: 78976. 2004-12-20.

Glaser, B. & Strauss, A. (1967). The discovery of grounded theory: Strategies for qualitative research. New York. Aldine.

Hallberg, N., Andersson, R., & Westerdahl, L. (2005a). Quality-driven process for requirements elicitation: the case of architecture driving requirements. User report FOI-R--1576--SE, Swedish Defence Research Agency.

Hallberg, J., Hallberg, N., Hunstad, A., (2005b), Scenarion för identifiering av behov av värdering gällande IT-säkerhet, FOI Memo 1371, Linköping, Sweden

Hallberg, J., Hallberg, N., Hunstad, A., (2005c), Metod för behovsanalys avseende värdering av IT-säkerhet, FOI Memo 1449, Linköping, Sweden

Hallberg, J., Hunstad, A., Bond, A., Peterson, M., Påhlsson, N. (2004). *System IT Security Assessment*, FOI-R--1468--SE, Linköping, Sweden.

Jonsson, S. & Karlsson, M. (2005). *Behovsanalys, för framtagning av informationssäkerhetsmässiga behov, Bestående av VeRa/IBMB*. D-uppsats framlagd vid Linköpings universitet.

Jungert, E., Derefelt, G., Hallberg, J., Hallberg, N., Hunstad, A., Thurén, R., Albinsson, P.-A., Holmberg, M., Sidenbladh, H., Stenumgaard, P., Worm, A., Ånäs, P. (2004), *Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering,* FOI-rapport FOI-R--1183—SE.

Karlsson, J. (1998). Framgångsrik kravhantering: vid utveckling av programvarusystem, 2(3). Focal point: Linköping.

Oman, P., Krings, A., Conte de Leon, D., & Alves-Foss, J. (2004). Analyzing the Security and Survivability of Real-time Control Systems. Proceedings of the 5th IEEE Workshop on Information Assurance. West Point, NY, June 2004.

OMG. (1999). *OMG Unified Modeling Language Specification*. http://www.omg.org/technology/documents/formal/unified_modeling_language.htm (2001-02-20).

Payne, S. (2001). A Guide to Security Metrics. SANS Security Essentials GSEC Practical Assignment. http://www.sans.org/rr/whitepapers/auditing/55.php

Schudel, G. & Wood, B. (2000). Adversary Work Factor as a Metric for Information Assurance. *Proceedings of the New Security Paradigms Workshop*. Cork, Ireland, Sep. 18-22, 2000.

Shillto, M.L., (2001). Acquiring, Processing, and Deploying Voice Of The Customer. St Luice Press.

Sindre, G. & Opdahl, A.L. (2000). Eliciting security requirements by misuse cases. Proceedings of the 37th International Conference on Technology of Object-Oriented Languages and Systems 2000 (TOOLS-Pacific 2000).

SIS. (2003). Terminologi för informationssäkerhet, SIS HB 550, 2003-08-29.

Swanson, M., Bartol, N., Sabato, J., & Hash, J. (2003). Security metrics guide for information technology systems. Technical Report NIST Special Publication 800-55, NIST, July 2003. http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf.

Wang, C. & Wulf, W. (1997). A Framework for Security Measurement. Proceedings of the National Information Systems Security Conference, Baltimore, MD, pp. 522-533, Oct. 1997.

Witkin, B.R. & Altschuld, J.W. (1995) *Planning and Conducting Needs Assessments: A Practical Guide*, SAGE Publications.

Wood, B. & Bouchard, J. (2001). Red Team Work Factor as a Security Measurement. ACSA Workshop on Information Security System Rating and Ranking, Williamsburg, Virginia, 21-23 May 2001. http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Bouchard.pdf

Young, R. (2001). Effective Requirements Practice. Addison Wesley, Boston, MA, 2001.

Bilaga 1 – Intervjuer och dokument

Följande intervjuer genomfördes:

- Intervju 1: Joakim Stenius, Forskare, Systemutveckling, Totalförsvarets forskningsinstitut, Linköping, 2005-10-04,

- Intervju 2: Magnus Bender, Säkerhetsansvarig LedBat, Markstridsskolan, Skövde, 2005-10-18,

- Intervju 3: Bengt Ackzell, Informationssäkerhet, Generic Systems, Jan Engberg, Informationssäkerhet, Försvarsmakten HKV, och Ingvar Ståhl, Informationssäkerhet, Försvarsmakten HKV, Enköping, 2005-10-19,

- Intervju 4: Daniel Jonsson, Specialist verifiering och validering, TietoEnator, och Peter Nilsson, Specialist verifiering och validering, TietoEnator, Enköping, 2005-10-19,

- Intervju 5: Olle Berglund, IT-säkerhetshandläggare, Totalförsvarets forskningsinstitut, Linköping, 2005-10-26,

- Intervju 6: Peder Blomqvist, Uppdragsledare för FM Arkitekturramverk FM AR, Systemarkitekt LedsystT Arkitektur och Metod, FMV, 2005-10-27,

Följande dokument samlades in för analys:

- Post & Telestyrelsen, Är Internet i Sverige robust?, PTS-ER-2003:1, 19 februari 2003.

- Post & Telestyrelsen, E-handel - fem förutsättningar, PTS-ER-2003:4, 19 februari 2003.

- Kjell Kalmelid & Johan Gustavsson, Inventering av kompetensbehov m.m. inom informationssäkerhet i offentlig sektor, Krisberedskapsmyndigheten, Informationssäkerhets- och analysenheten, Dnr. 0707/2005, 2005-06-16.

- Andreas Malm, Jan Softa, Jan Joel Andersson & Klas Lindström, IT och sårbarhet kritiska beroendeförhållanden i den nationella it-infrastrukturen, Krisberedskapsmyndighetens temaserie 2003:5.

- Gunnar Sjöstedt & Paula Stenström, Vilseledning på Internet, Styrelsen för psykologiskt försvar, Rapport 183, 2002.

- Krisberedskapsmyndigheten, Samhällets informationssäkerhet - Lägesbedömning 2005.

- Krisberedskapsmyndigheten, Basnivå för IT-säkerhet (BITS), dnr: 1123/2003, ISBN: 91-85053-35-X, KBM rekommenderar 2003:2.

- Krisberedskapsmyndigheten, Beredskap mot skadlig kod – en kartläggning av IT- och informationssäkerheten inom större myndigheter och statliga bolag i Sverige med fördjupad analys av skadlig kod, dnr: 0797/2004.

- Post & Telestyrelsen, Tillit till IT vid Internetanvändning, PTS-ER-2002:24, 1 november 2002.

- Försvarsdepartementet, InfoSäkutredningen, Säker information, Statens offentliga utredningar (SOU) SOU 2005:42, 13 maj 2005.

- Christiansson, Henrik (2004), Värdering av IT-säkerhetsanalysmetoder inom samhällsviktig infrastruktur, Stockholm, (FOI-R--1350--SE), Totalförsvarets Forskningsinstitut, 2004.

- Försvarsmakten, Krav på säkerhetsfunktioner – Grunder, 10 750:78976, 2004-12-20.

- Internt arbetsdokument rörande designregler vid utveckling av ledningssystem inom Försvarsmakten.

Bilaga 2 – Intervjuguide

Inledning
Vi arbetar med ett forskningsprojekt inom IT-säkerhetsområdet. Inom detta projekt har vi identifierat svårigheter med att *säkerställa att man har en tillräcklig IT-säkerhet* och om inte hur långt man har kvar för att uppnå detta. Vi vill ha din syn på denna problematik, efter som du …
Inspelning på band, ok?
Ej hemligt!

Bakgrund
Vilken är din nuvarande tjänst?
Vad är din huvudsakliga arbetsuppgift?
Vilken erfarenhet har Du av arbete som inbegriper säkerhetsfrågor?

- *IT-säkerhet*

Syn på säkerhet
Vad är din syn på begreppet IT-säkerhet?

- *Hur definierar du begreppet?*

Vad är din syn på begreppet tillräcklig IT-säkerhet?

- *Varför behövs det?*
- *Varför behöver man känna till om tillräcklig IT-säkerhet erhållits?*

Värdering av IT-säkerhet
Hur säkerställs idag, i er verksamhet, att tillräcklig IT-säkerhet erhållits?

- *Inom er organisation?*
    a. *Hur kvantifierar ni säkerhet?*
- *Vet du hur det fungerar inom någon/några andra organisationer?*
- *Systemlivscykeln: Utveckling, driftsättning, drift och underhåll, avveckling*

Hur väl fungerar de ansatser som syftar till att säkerställa att tillräcklig IT-säkerhet erhållits?

- *Vilka brister har dessa ansatser?*
- *Vilka konsekvenser medför dessa brister?*

Om du fick önska fritt, hur skulle man säkerställa att tillräcklig IT-säkerhet erhållits?
Ser du några praktiska/realistiska förbättringar av hur säkerställandet av tillräcklig IT-säkerhet genomförs idag?

Tack för din medverkan