Hot-, risk- och sårbarhetsanalys

Grunden för IT-säkerhet inom Försvarsmakten

KRISTOFFER LUNDHOLM, JOHAN BENGTSSON,
JONAS HALLBERG

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 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, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

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

www.foi.se

FOI-R--3349--SE
ISSN 1650-1942

Användarrapport
December 2011

Informationssystem

Kristoffer Lundholm, Johan Bengtsson,
Jonas Hallberg

Hot-, risk- och sårbarhetsanalys

Grunden för IT-säkerhet inom Försvarsmakten

Titel	Hot-, risk- och sårbarhetsanalys – Grunden för IT-säkerhet inom Försvarsmakten
Title	Threat, risk and vulnerability analysis – The foundation for IT security within the Swedish Armed Forces
Rapportnr/Report no	FOI-R--3349--SE
Rapporttyp/Report Type	Användarrapport/User Report
Månad/Month	December
Utgivningsår/Year	2011
Antal sidor/Pages	42 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Projektnr/Project no	E53340
Godkänd av/Approved by	Magnus Jändel

FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Informationssystem	Information Systems
Box 1165	Box 1165
581 11 Linköping	SE-581 11 Linköping

Sammanfattning

Hot-, risk- och sårbarhetsanalyser utgör grunden för IT-säkerheten i Försvarsmaktens IT-system. De instruktioner som Försvarsmakten i dagsläget tillhandahåller angående genomförandet av analyserna är knapphändiga. Fokus ligger på vilket underlag som ska tas fram, inte hur det ska gå till. Detta leder till att inriktning och omfattning hos framtagna säkerhetsmålsättningar varierar stort.

Kommunikation kring IT-säkerhet försvåras av att terminologin varierar. Exempelvis anses ofta hotbilden vara slutresultatet av analyserna då det egentligen är de kvarvarande riskerna som avses. Enligt H SÄK IT kan dessa kvarvarande risker också benämnas sårbarheter eller resulterande riskvärden och anses vara brister i systemet.

Avsaknad av tid och resurser för att med egen personal genomföra analyserna är ett tydligt problem. Då sårbarhetsanalysen är avgörande för kravställningen av IT-säkerhet bör den genomföras av Försvarsmaktens personal, inte extern personal. Att den egna personalen inte har tid att genomföra analyserna leder till att deras kompetens inom området blir begränsad, vilket i sin tur skapar ett starkt beroende av externa parter.

Avsaknaden av verksamhetsrepresentanter i analysarbetet leder till generella analysresultat som ofta saknar specifik relevans. Ett syfte med att genomföra analyserna är att avgöra vilka risker som tas vid användning av det tänkta systemet. När kunskapen om den aktuella verksamheten är bristfällig är det inte troligt att analysresultatet ger den efterfrågade förståelsen. Analysernas betydelse för systemets IT-säkerhet kan i dessa fall ifrågasättas.

Utgående från Försvarsmaktens IT-livscykelmodell ska säkerhetsmålsättningen tas fram då IT-systemet fortfarande är i ett konceptstadie, med fokus på verksamhet snarare än teknik. Tanken är god, men verklighetsanknytningen är vag. Analysarbetet genomförs ofta då IT-systemet redan är framtaget, vilket kan vara en bidragande orsak till att ackrediteringen ofta upplevs som tidsödande och som ett hinder på vägen.

Följande rekommendationer ges till Försvarsmakten avseende framtida arbete med hot-, risk- och sårbarhetsanalyser för IT-system.

- Utveckla kunskap om de faktorer som påverkar analyserna
- Ta fram tydliga instruktioner för hur analyserna ska genomföras
- Tillhandahåll relevant utbildning
- Ta fram stöd för nödvändiga bedömningar
- Fokusera analyserna på det specifika snarare än det generella
- Ta fram stöd för att avgöra vilka krav verksamheten ställer på IT-säkerheten

Nyckelord: IT-säkerhet, ackreditering, hot, risk, sårbarhet

Summary

Threat, risk and vulnerability analyses are the basis for IT security in the IT systems of the Swedish Armed Forces. The current documentation of these tasks is scarce in the Swedish armed forces. The focus is on what to deliver, not on how to perform the analyses.

The following recommendations are given to the Swedish Armed Forces for future work on developing the threat, risk and vulnerability analysis of IT systems.

- Develop basic knowledge about the fundamental issues of analysis
- Develop clear instructions on how to implement the assessments
- Provide relevant training
- Develop supporting tools for the analyses
- Focus the analyses on the specific rather than the general aspects
- Develop support to determine demands of the operations on IT security

Keywords: IT security, accreditation, threat, risk, vulnerability

Innehåll

Förord

Många personer har på ett eller annat sätt bidragit till att möjliggöra de studier som ligger till grund för denna rapport. Vi vill tacka följande personer för deras bidrag till arbetet.

Bengt Ackzell

Pierre Anderberg

Kent Andersson

Peter Haglind

Katarina Harcus

Ulrika Lindblom

Johannes Lindgren

Erik Lyttkens

Kristina Malmström

Christer Prinzell

Helene Rantakokko

P-O Sjöberg

Christer Skagert

Ulf Skoglund

1 Inledning

Vilka skyddsåtgärder som ger adekvat IT-säkerhet beror i hög grad på kontexten för aktuellt IT-system. Vid kravställning av IT-säkerhet är det därför väsentligt att identifiera de hot som finns mot IT-systemet i den aktuella kontexten. Utgående från beskrivningar av relevanta hot och IT-säkerhetskrav kan de risker som måste accepteras vid användning av IT-system beskrivas.

Inom Försvarsmakten hanteras behoven av hot- och riskanalyser samt kravställningen av IT-säkerhet inom ramen för auktorisations- och ackrediteringsprocessen. För att det ska vara tillåtet att använda ett IT-system, måste aktuella auktorisations- och ackrediteringsbeslut ha fattats (Försvarsmakten, 2004b).

1.1 Bakgrund till projektet

Denna rapport är producerad inom ramen för projektet Effektivare hot-, risk- och sårbarhetsanalyser. Projektet, som genomförs av Totalförsvarets forskningsinstitut (FOI), löper över 3 år och finansieras inom ramen för Försvarsmaktens Forskning och Teknikutveckling (FoT).

Inom ramen för tidigare arbete har frågeställningar som relaterar till värdering av IT-säkerhet studerats (Bengtsson & Hallberg, 2008a). Slutsatser från det arbetet visar på att det går att effektivisera genomförandet av de hot- och riskanalyser som görs inom ramen för auktorisations- och ackrediteringsprocessen.

Hela auktorisations- och ackrediteringsprocessen är för omfattande för att studera inom ramen för projektet. Fokus för projektet är att effektivisera de hot-, risk- och sårbarhetsanalyser som genomförs inom ramen för arbetet med att ta fram säkerhetsmålsättningar för IT-system. Detta då dessa analyser är grundläggande för att i slutändan erhålla adekvat IT-säkerhet i de framtagna IT-systemen.

1.2 Syfte och målsättning

Det övergripande syftet med denna rapport är att öka kunskapen inom Försvarsmakten och FOI avseende hur hot-, risk- och sårbarhetsanalyser genomförs för IT-system samt vilka behoven av stöd vid genomförandet av dessa analyser är.

Målsättningen för rapporten är att beskriva hur analyserna genomförs såväl som vilka behov av stöd som finns vid genomförandet. Dessa beskrivningar ska baseras på såväl tillgänglig dokumentation som intervjuer med personer som har insikt i relevant verksamhet.

1.3 Bidrag

De huvudsakliga resultaten som beskrivs i denna rapport sammanfattas i följande punkter.

- En sammanställning av det stöd som finns i Försvarsmaktens dokument för genomförande av hot-, risk- och sårbarhetsanalyser för IT-system.
- En sammanställning av hur olika aktörer i verksamheten ser på genomförandet av hot-, risk- och sårbarhetsanalyser.
- En uppsättning med behov avseende stöd vid genomförande av hot-, risk- och sårbarhetsanalyser.
- Rekommendationer till Försvarsmakten avseende hur hot-, risk- och sårbarhetsanalyser kan utvecklas för att resultera i IT-system med ändamålsenlig IT-säkerhet.

1.4 Terminologi

Många begrepp används med olika betydelse i olika sammanhang. Ibland skiftar tyvärr betydelsen även i samma sammanhang. Följande lista beskriver den betydelse som antas för de mest centrala begreppen som används i denna rapport.

- **Analyserna**
  Med analyserna avses i denna rapport de hot-, risk- och sårbarhetsanalyser som ska genomföras under framtagandet av säkerhetsmålsättningen för Försvarsmaktens IT-system. Dessa analyser är i fokus i denna rapport och beskrivs ur olika perspektiv i kapitel 2 och 4.

- **Hot**
  Med hot avses ”möjlig, oönskad händelse med negativa konsekvenser för verksamheten” (SIS, 2007).

- **Hotbild**
  Med hotbild avses ”uppsättning **hot** som bedöms föreligga mot en viss [typ av] verksamhet” (SIS, 2007).

- **IT-system**
  Med IT-system avses system med teknik som hanterar och utbyter information med omgivningen (Försvarsmakten, 2006b). Detta innebär en tydlig koppling till tekniska system.

- **IT-säkerhet**
  Med IT-säkerhet avses säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation (SIS, 2007). Säkerheten i IT-system beror dock inte endast på systemets tekniska lösningar. Därmed behöver beaktande av IT-säkerhet inkludera även andra

aktiviteter och rutiner som påverkar den tekniska utrustningen, såsom hanteringen av lösenord, även om dessa aktiviteter och rutiner i sig inte ingår i IT-systemet.

- **IT-säkerhetskrav**
  Med IT-säkerhetskrav avses de krav som ställs på IT-system för att uppnå adekvat IT-säkerhet. Krav beskriver vad ett system ska uppfylla i form av funktioner, attribut eller principer.

- **Kvarvarande risk**
  Med kvarvarande risker avses de risker som återstår efter att skyddsåtgärder har vidtagits för att minska riskerna behäftade med ett IT-system.

- **Resulterande riskvärden**
  Med resulterande riskvärden avses de bedömda värden som kopplas till kvarvarande risker. Enligt H SÄK IT anger riskvärden nivåer, exempelvis L, M och H, för risker (Försvarsmakten, 2006b, s.75) och utgör ett resultat av sårbarhetsanalyser för IT-system.

- **System**
  Med system avses i denna rapport IT-system.

- **Sårbarhet**
  Med sårbarhet avses i allmänhet den definition som ges i SIS HB 550 (2007) av begreppet svaghet ”brist i skyddet av en tillgång exponerad för hot”. I H SÄK IT används dock begreppet sårbarhet även med betydelserna *resulterande riskvärde* (Försvarsmakten, 2006b, s.75) och *kvarvarande risk* (Försvarsmakten, 2006b, s.168). Sådan användning, relaterad till risk istället för brist, bör undvikas.

- **Säkerhet**
  Med säkerhet avses i denna rapport IT-säkerhet, om inte annat nämns.

- **Säkerhetsmålsättning**
  En säkerhetsmålsättning ska tas fram för alla Försvarsmaktens IT-system redan under det andra steget i IT-livscykelmodellen. Säkerhetsmålsättningen ska innehålla resultaten från aktiviteterna verksamhetsanalys, säkerhetsanalys, författningsanalys, hotanalys, formulera grund för säkerhetskrav, formulera säkerhetskrav, riskanalys och sårbarhetsanalys. Dessa aktiviteter beskrivs i kapitel 2.

1.5 Rapportstruktur

Återstoden av denna rapport består av de kapitel och bilagor vars innehåll beskrivs i följande punkter.

- Kapitel 2 innehåller en beskrivning av en sedan tidigare framtagen sammanställning av de analyser som ska genomföras för att ta fram det underlag som ska ingå i en säkerhetsmålsättning. Denna beskrivning sätter hot-, risk- och sårbarhetsanalysen i ett sammanhang.
- Kapitel 3 beskriver den metod som använts vid framtagandet av de resultat som presenteras i denna rapport.
- Kapitel 4 innehåller de bilder av genomförandet av hot-, risk- och sårbarhetsanalyser som framkommit genom dels studier av dokument, dels de genomförda intervjuerna.
- Kapitel 5 innehåller resultaten från den genomförda behovsanalysen.
- Kapitel 6 består av en diskussion av de presenterade resultaten.
- Kapitel 7 innehåller rekommendationer som baseras på de beskrivna resultaten och diskussionen.
- Bilaga A återger den intervjuguide som nyttjades vid genomförandet av intervjuer.
- Bilaga B innehåller de forskningsfrågor som ligger till grund för intervjuguiden.
- Bilaga C återger de behovsstrukturer som togs fram under behovsanalysen.

2 Bakgrund

Framtagandet av den säkerhetsmålsättning som ska finnas för Försvarsmaktens IT-system inkluderar genomförandet av ett antal aktiviteter. I detta kapitel presenteras dessa aktiviteter kortfattat. Beskrivningarna är baserade på tidigare underlag som tagits fram av FOI (Bengtsson & Hallberg, 2008b, 2008a). Dessa är i sin tur baserade på *H SÄK IT* (Försvarsmakten, 2006b) samt de dokumentmallar som ingår i *Metod och utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten* (*MAACK*) (Försvarsmakten, 2008).

De IT-säkerhetskrav som ska ställas på systemet och de risker som kvarstår även när de ställda kraven uppfylls utgör huvudresultaten av aktiviteterna. Det finns dock ytterligare delresultat som är av betydelse, exempelvis vilken informationssäkerhetsklass som är aktuell för systemet.

I denna rapport ligger fokus på hot-, risk och sårbarhetsanalysen. För att genomföra dessa krävs dock att flera förberedande aktiviteter genomförs. Dessa aktiviteter ingår alla i framtagandet av säkerhetsmålsättningen, vilket ingår i andra steget i Försvarsmaktens IT-livscykelmodell. Nedan beskrivs aktiviteterna i en ordning som de kan genomföras (det finns dock fler alternativ).

Verksamhetsanalysen resulterar i en informationsklassning, som utgör underlag för informationssäkerhetsklassningen, verksamhetens informationssäkerhetsmål och, eventuellt, underlag för den preliminära systembeskrivningen. Huruvida en preliminär systembeskrivning ska tas fram ska framgå av auktorisationsbeslut B1.

Säkerhetsanalysen syftar till att bedöma aktuell informationssäkerhetsklass för de uppgifter IT-systemet ska behandla. Vidare ska en förtida menbedömning genomföras för att visa vilka konsekvenser röjande av information kan leda till.

Författningsanalysen ska klargöra vilka lagar, förordningar, föreskrifter och bestämmelser som ska beaktas vid framtagandet av det berörda IT-systemet och resulterar i en uppsättning författningskrav.

Hotanalysen ska identifiera de hot IT-systemet kommer att exponeras för, vilket resulterar i en specifik hotbild. Avseende genomförande av hotanalyser refereras till *H SÄK Hot* (Försvarsmakten, 2006a) och *H SÄK IT Hot* (Försvarsmakten, 2001).

Aktiviteten *Formulera grund för säkerhetskrav* utgår från de identifierade författningskraven, den specifika hotbilden samt Försvarsmaktens *Beslut om krav på godkända säkerhetsfunktioner, ver. 2.0* (Försvarsmakten, 2004a). De beslutade kraven på säkerhetsfunktioner omnämns ofta som KSF. Aktiviteten syftar till att formulera en grund för säkerhetskrav som är specifikt anpassad för det aktuella systemet. Ur KSF erhålls de krav som formulerats för aktuell

informationssäkerhetsklass. Denna kravmängd kan sedan kompletteras baserat på resultaten av genomförda analyser (H SÄK IT, avsnitt 16.5.3).

Aktiviteten *Formulera säkerhetskrav* utgår från den framtagna grunden för säkerhetskrav samt verksamhetens informationssäkerhetsmål för att formulera en första version av de *säkerhetskrav* som ska ställas på det framtagna IT-systemet med beaktande av såväl IT-system som verksamhet.

Riskanalysen genomförs för att värdera de aktuella riskerna utgående från den framtagna hotbilden. Under riskanalysen skattas de identifierade hotens konsekvens respektive sannolikhet för realisering.

Sårbarhetsanalysen syftar till att bedöma till vilken grad en realisering av de ställda säkerhetskraven kommer att minska de risker som identifierats i riskanalysen. De efter sårbarhetsanalysen resulterande riskvärdena benämns som sårbarheter och anses vara brister i systemet[1].

[1] Detta ger en dubbeltydig användning av begreppet sårbarhet, som brist i systemet eller resulterande riskvärde. Se beskrivningen av begreppet sårbarhet i avsnitt 1.4.

3 Metod

Detta kapitel beskriver tillvägagångssättet för att ta fram de resultat som presenteras i rapporten. För att få en första förståelse för området genomfördes en dokumentstudie där relevanta dokument från Försvarsmakten studerades. Därefter genomfördes en serie med intervjuer för att få insikt i hur hot-, risk- och sårbarhetsanalyser för IT-system genomförs i Försvarsmaktens verksamhet. Baserat på det underlag som erhölls från dokumentstudien och intervjuerna genomfördes en behovsanalys. Dessa aktiviteter beskrivs mer ingående i avsnitt 3.1 till 3.3.

3.1 Dokumentstudie

Dokumentstudien som genomfördes syftade till att skapa en initial översikt av det stöd som finns att hämta i de officiella dokumenten avseende hot-, risk- och sårbarhetsanalyser. Som utgångspunkt för denna översikt användes tidigare publicerade FOI-rapporter (Bengtsson & Hallberg, 2008b, 2008a). De resultat som presenterades i dessa två rapporter sammanfattas i kapitel 2.

För att komplettera dessa tidigare studier studerades ytterligare dokument framtagna av Försvarsmakten med anknytning till hot-, risk- och sårbarhetsanalyser. Första steget i studien bestod i att gå igenom de utvalda dokumenten och identifiera alla avsnitt relaterade till hot-, risk- och sårbarhetsanalyser. Därefter sammanställdes de relevanta avsnitten och figurer som illustrerar beskrivningen av respektive analys skapades.

3.2 Intervjuer

För att få en insikt i hur hot-, risk- och sårbarhetsanalyser i praktiken genomförs i Försvarsmakten intervjuades sju personer (informanter) vars arbetsuppgifter är kopplade till dessa analyser. För att fånga upp så många viktiga aspekter av analyserna som möjligt valdes informanter med olika roller inom processerna för Försvarsmaktens utveckling av IT-system. De personer som intervjuades kommer i kontakt med analyserna genom en eller flera av rollerna projektledare för anskaffning av system, granskare av analyser, materielsystemansvarig, analysexpert, IT-säkerhetsexpert, produktägarrepresentant, systemutvecklare och verksamhetsrepresentant.

Som en grund för intervjufrågorna formulerades en uppsättning om tre grundläggande frågor (forskningsfrågor) som intervjuerna syftade till att besvara. Från dessa togs sedan intervjufrågorna fram. Forskningsfrågorna för intervjustudien var:

- Hur görs hot-, risk- och sårbarhetsanalyser i praktiken?
- Vad är syftet med att göra hot-, risk- och sårbarhetsanalyser?
- Vilka förbättringar kan göras avseende hot-, risk- och sårbarhetsanalyser?

Kopplingen mellan forskningsfrågorna och intervjufrågorna återfinns i Bilaga B.

Den intervjuform som valdes var semistrukturerade intervjuer utgående från en intervjuguide. Syftet med intervjuguiden var att strukturera upp intervjufrågorna på ett logiskt och sammanhängande sätt. Intervjuguiden som användes finns bifogad i Bilaga A

Datainsamlingen från intervjuerna skedde genom att anteckningar fördes av två forskare vid varje intervjutillfälle. Dessa anteckningar sammanställdes sedan gemensamt av forskarna till en sammanfattning av intervjun. Sammanfattningarna skickades ut till respektive informant för att ge tillfälle att korrigera eventuella missförstånd samt komplettera innehållet.

Intervjuerna spelades inte in eftersom ordagrann analys inte var aktuell samtidigt som det var möjligt att kontakta informanterna i efterhand för korrigering och komplettering.

3.3 Behovsanalys

Behovsanalys innebär undersökningar och studier med syfte att identifiera och analysera behov. I denna studie är behovsanalysens syfte att påvisa vilket behov av stöd som finns vid genomförande av de hot-, risk- och sårbarhetsanalyser som krävs för att ta fram det underlag som ska ingå i säkerhetsmålsättningarna för Försvarsmaktens IT-system.

Baserat på resultatet från dokumentstudien (avsnitt 4.1) genomfördes en övergripande behovsanalys. Behov identifierades utifrån de aktiviteter och delaktiviteter som enligt dokumentationen ska genomföras under hot-, risk- och sårbarhetsanalyser. Identifieringen gjordes med hjälp av verktyget hierarkiskt diagram som beskrivs senare i detta avsnitt.

Behovsanalysen som utgår från intervjuerna genomfördes med hjälp av verktygen kundrösttabell, relationsdiagram och hierarkiska diagram. Dessa verktyg beskrivs i följande stycken.

Kundrösttabell (eng. Voice of the Customer Table, VCT) är en notation som utvecklats för att stödja analysen av kunders utsagor (Mazur, 1992). En VCT innehåller åtta kolumner. De utsagor som ska analyseras förs in i första kolumnen. Varje utsaga analyseras därefter i de sex efterföljande kolumnerna med avseende på

- vem som berörs
- vad de anser sig behöva

- när de behöver det
- var det behöver användas
- varför behovet finns
- hur de vill att det ska fungera.

Med stöd av detta kan de bakomliggande verkliga behoven identifieras, vilka noteras i den åttonde, och sista, kolumnen.

Relationsdiagram (eng. Affinity diagrams) används för att analysera de identifierade behovens relationer och struktur (Bossert, 1991). Ofta är de behov som erhålls från kundrösttabeller beskrivna på olika konceptuella nivåer och med olika omfång. I relationsdiagrammen ordnas behoven utifrån en stegvis procedur där liknande behov först inordnas i kategorier. Sammansatta behov kan delas upp och dubbletter tas bort. Därefter grupperas liknande kategorier tills dess att en gemensam toppkategori har erhållits.

Relationsdiagram är ett verktyg för att gruppera behov. Relationsdiagrammens struktur ger dock inte en lika bra översikt av de identifierade behoven och kategorierna som hierarkiska diagram, vilka ibland kallas för träddiagram. Hierarkiska diagram visualiserar på ett tydligare sätt vilka entiteter (behov och kategorier av behov) som ingår i en överordnad entitet. Den förbättrade översikten av strukturen kan användas som ett stöd vid försök att identifiera saknade behov och behovskategorier (Tague, 2005).

4 Genomförande av hot-, risk- och sårbarhetsanalyser

I detta kapitel presenteras bilder av hur hot-, risk- och sårbarhetsanalyser ska genomföras respektive genomförs. I avsnitt 4.1 presenteras den bild av hur analyserna ska genomföras som hämtats ur Försvarsmaktens dokumentation. Avsnitt 4.2 innehåller den bild av hur analyserna genomförs som erhållits från intervjuerna.

4.1 Dokumentationens bild av genomförandet

Försvarsmakten har en uppsättning handböcker och direktiv som bland annat beskriver genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system. Under dokumentationsstudien har följande dokument beaktats.

- **H SÄK IT** (Försvarsmakten, 2006b)
  Handbok för hantering av IT inom Försvarsmakten som bland annat beskriver vilka analyser som ska genomföras samt det förväntade innehållet i en säkerhetsmålsättning.
- **DIT 04** (Försvarsmakten, 2004b)
  Direktivet definierar ansvar och roller för IT-verksamheten inom Försvarsmakten. Dokumentet beskriver Försvarsmaktens IT-livscykelmodell, vilken inte innehåller några detaljer angående genomförandet av hot-, risk- och sårbarhetsanalyser. Således har detta direktiv ej nyttjats vid framtagandet av bilden av genomförandet.
- **H SÄK IT Hot** (Försvarsmakten, 2001)
  Handbok som kompletterar H SÄK IT genom att stödja genomförandet av hotanalyser för IT-system. Handboken innehåller en metodbeskrivning för hotanalyser samt en hotkatalog avseende IT-system.
- **Försvarsmaktens gemensamma riskhanteringsmodell** (Försvarsmakten, 2009)
  Handboken beskriver genomförandet av riskanalyser. Den används i dagsläget inte för IT-system. Således har denna handbok ej nyttjats vid framtagandet av bilden av genomförandet.
- **H SÄK Skydd** (Försvarsmakten, 2007)
  Denna handbok innehåller en beskrivning av riskhantering baserad på en tidigare version av Försvarsmaktens gemensamma riskhanteringsmodell. IT-säkerhet berörs endast övergripande och läsaren refereras till H SÄK IT. Således har denna handbok ej nyttjats vid framtagandet av bilden av genomförandet.

- **H SÄK Hot** (Försvarsmakten, 2006a)
  Denna handbok beskriver hot mot verksamheten på en generell nivå. Kapitel 8 handlar om hot mot tekniska system, men ger kortare beskrivningar av olika typer av hot snarare än en metodbeskrivning för genomförandet av hotanalyser. Således har denna handbok ej nyttjats vid framtagandet av bilden av genomförandet.
- **MAACK** (Försvarsmakten, 2008)
  MAACK innehåller dokumentmallar som utgör ett stöd vid dokumentationen av analysresultaten. De ger dock inget stöd vid själva genomförandet. Således har MAACK ej nyttjats vid framtagandet av bilden av genomförandet.

De följande delavsnittens beskrivningar av hot-, risk- och sårbarhetsanalysen baseras på H SÄK IT och H SÄK IT Hot.

4.1.1 Hotanalys

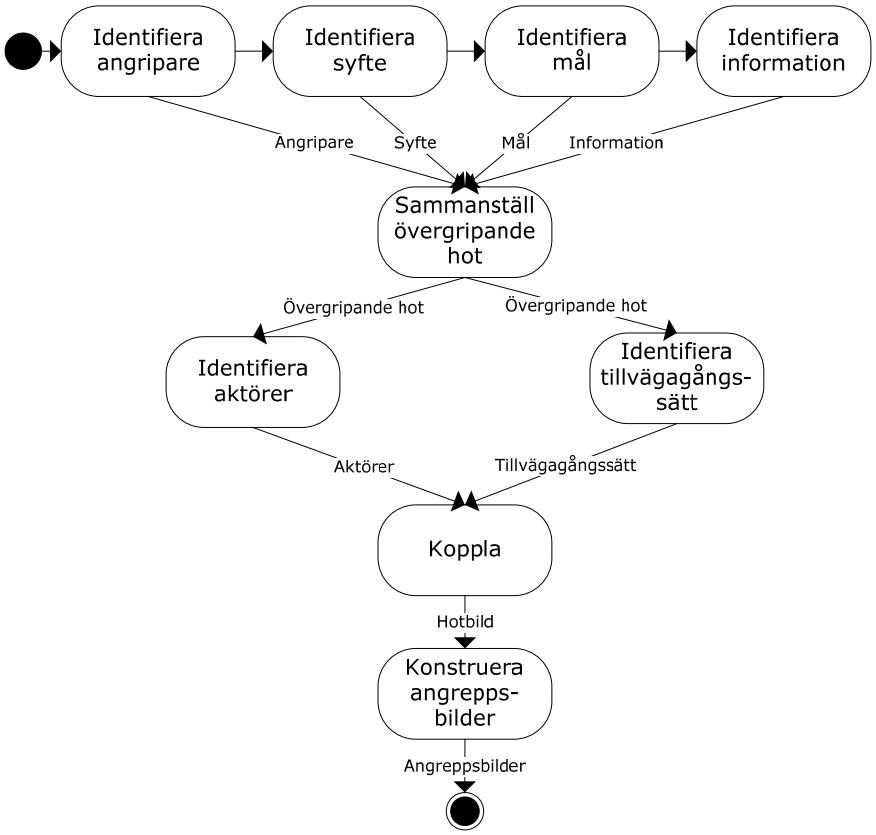
Denna beskrivning av genomförandet av en hotanalys baseras på H SÄK IT Hot (Försvarsmakten, 2001).

Hotanalyser genomförs för att identifiera möjliga hot samt vem eller vad som kan tänkas utlösa dessa hot. Ett hot definieras inom Försvarsmakten som ”en möjlig, oönskad händelse som ger negativa konsekvenser för verksamheten”.

Hoten struktureras efter deras karaktär, som kan vara antingen *fysisk*, *logisk* eller *administrativ*. Fysiska hot omfattar själva IT-utrustningen. Logiska hot omfattar funktioner och tjänster i IT-systemet. Administrativa hot syftar på oönskade händelser som uppstår genom olika typer av brister. Dessa brister omfattar exempelvis

- brister i regelverk
- regelverk som inte följs
- brister i utbildning
- brister i kontrollfunktioner.

Hot kan verkställas av yttre eller inre angripare. Ett hot är antingen oavsiktligt eller avsiktligt. (Försvarsmakten, 2001, s.10)



Figur 1: Genomförande av hotanalys.

Hotanalysen, som illustreras i Figur 1, inleds med att *övergripande hot* identifieras. Ett övergripande hot består av fyra delar där *angripare* först identifieras. *Angripare* avser vem som ligger bakom ett hot, vilket inte nödvändigtvis är den som realiserar hotet (*aktör*). Därefter identifieras angriparens *syfte* och *mål*. Slutligen identifieras vilken *information* som angriparen är intresserad av. De fyra delarna *angripare*, *syfte*, *mål* och *information* sammanställs till en lista av övergripande hot (Tabell 1).

Tabell 1: Exempel på övergripande hot.

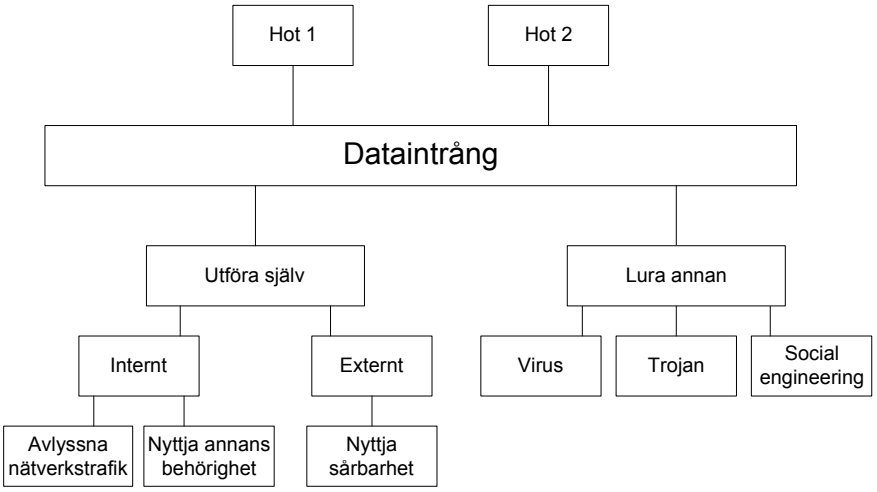
ID	Angripare	Syfte	Mål	Information
1	Främmande makt	Stjäla känslig information	Få kunskap om Försvarsmaktens förmågor	Allt som kan nås
2	Aktivist	Störa verksamheten	Få kontroll över Försvarsmaktens IT-system	

När de övergripande hoten har identifieras ska de konkretiseras. Detta görs genom att identifiera *aktörer* och *tillvägagångssätt*. En aktör är den eller de som konkret skulle kunna realisera ett hot. *Tillvägagångssätt* syftar på hur aktören skulle kunna gå till väga för att realisera ett hot. De övergripande hoten kopplas sedan till de identifierade aktörerna och tillvägagångssätten, vilket resulterar i en uppsättning *konkreta hot* (Tabell 2).

Tabell 2: Exempel på konkreta hot.

Aktör	Tillvägagångssätt	Övergripande hot
Anställd	Manipulera data	1, 2
Anställd	Utpressning	1
Hacker	Dataintrång	1, 2
Hacker	Sabotage	2

Hotanalysen avslutas med att *angreppsbilder* skapas. En angreppsbild skapas för varje tillvägagångssätt som existerar i uppsättningen av konkreta hot (Tabell 2). Exempel på hur en angreppsbild kan se ut återges i Figur 2.



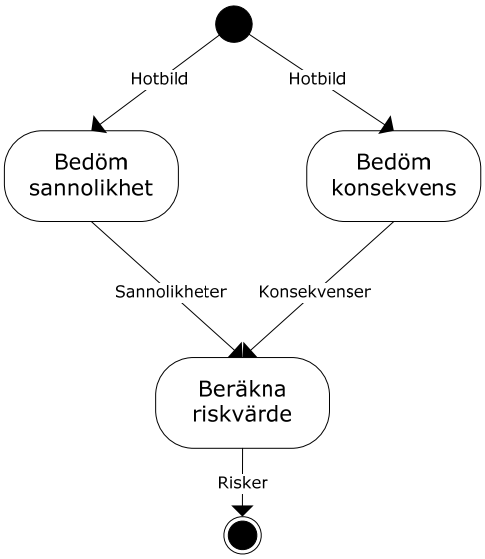
Figur 2: Exempel på angreppsbild för tillvägagångssättet *Dataintrång* som återfinns på rad tre i Tabell 2. I tabellen framgår även de övergripande hoten *hot 1* och *hot 2* som kan nyttja tillvägagångssättet *Dataintrång.*

4.1.2 Riskanalys

Denna beskrivning av genomförandet av en riskanalys baseras på H SÄK IT (Försvarsmakten, 2006b).

En risk är enligt H SÄK IT ett kvantifierat hot. Kvantifieringen avser bedömning av sannolikheten för att hotet ska realiseras samt bedömning av konsekvensen om ett hot realiseras. Utifrån bedömd sannolikhet och konsekvens tas ett riskvärde fram för varje hot. Riskanalysen inkluderar således de tre aktiviteterna bedömning av sannolikhet, bedömning av konsekvens samt framtagande av riskvärde (Figur 3). Dessa aktiviteter ska genomföras för varje hot.

Som stöd vid genomförandet av riskbedömningar rekommenderas användning av SBA Scenario (Försvarsmakten, 2006b, s.74). Bedömningarna av sannolikhet för, samt konsekvens av inträffat hot baseras på erfarenhet och kunskap hos analytikerna. Framtagandet av riskvärden illustreras i H SÄK IT med en figur innehållande två diagram, ett för hot- och riskanalys och ett för sårbarhetsanalys (Försvarsmakten, 2006b, figur 8.2). Diagrammen kopplar låga och höga värden för sannolikhet respektive konsekvens till riskvärdena L, M och H. Det finns dock inga skalor eller värden angivna för axlarna med sannolikhet respektive konsekvens.



Figur 3: Framtagande av risker från identifierade hot.

4.1.3 Sårbarhetsanalys

Denna beskrivning av genomförandet av en sårbarhetsanalys baseras på H SÄK IT (Försvarsmakten, 2006b).

Under sårbarhetsanalysen beaktas riskerna från riskanalysen samt de säkerhetskrav som tagits fram under aktiviteten *Formulera säkerhetskrav* (kapitel 2). Dessa säkerhetskrav kan exempelvis vara krav från KSF (Försvarsmakten, 2004a). Sårbarhetsanalysen syftar till att bedöma huruvida den framtida realiseringen av säkerhetskraven kan reducera eller, i bästa fall, eliminera de identifierade riskerna.

De efter sårbarhetsanalysen kvarvarande riskerna ger upphov till resulterande riskvärden, vars framtagande illustreras i H SÄK IT med en figur (se avsnittet om riskanalys ovan). Dessa riskvärden benämns som sårbarheter och anses vara brister i systemet[2]. Om de kvarvarande riskerna inte kan accepteras eller riskhanteras[3] kan nya säkerhetskrav formuleras och analysen genomföras på nytt (Försvarsmakten, 2006b, avs.8.1). Alternativt kan den funktionalitet som ger

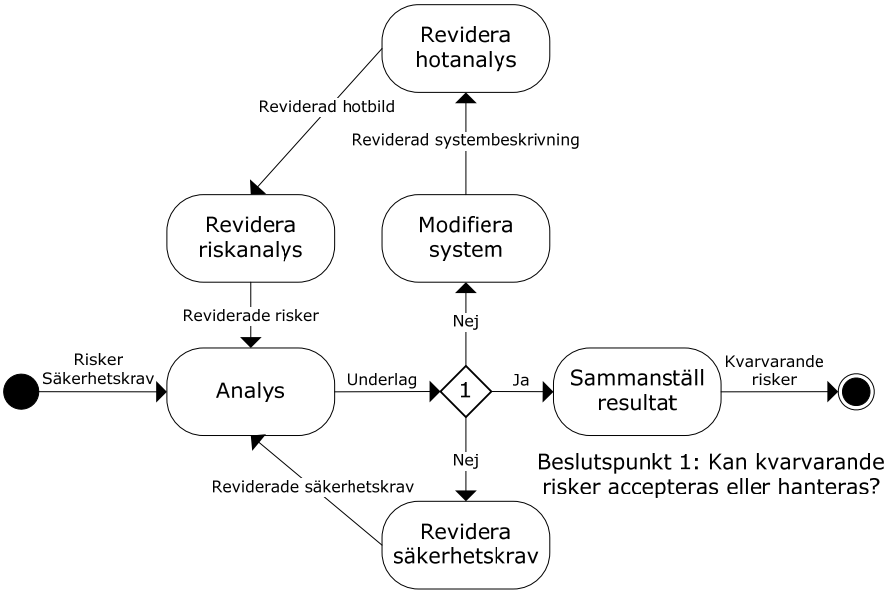
[2] Detta ger en dubbeltydig användning av begreppet sårbarhet, som brist i systemet eller resulterande riskvärde. Se beskrivningen av begreppet sårbarhet i avsnitt 1.4.

[3] Denna användning av termen riskhantering är olycklig då den insinuerar att innebörden av riskhantering är att varken acceptera eller vidta åtgärder mot en risk.

upphov till oacceptabla kvarstående risker tas bort. Därmed utgör sårbarhetsanalysen en iterativ process som pågår tills de kvarvarande riskerna är tillräckligt begränsade för att kunna accepteras eller hanteras. Genomförandet av sårbarhetsanalysen illustreras i Figur 4.

Resultaten från sårbarhetsanalysen utgörs av kvarvarande risker samt en bekräftelse av att framtagna säkerhetskrav är tillräckliga. I praktiken påverkas sårbarhetsanalysen inte bara av identifierade risker och säkerhetskrav, utan även av de krav och behov som verksamheten har på det analyserade systemet.

Den erhållna uppsättningen av säkerhetskrav utgör en viktig aspekt av dokumentet *Säkerhetsmålsättning*[4]. Att avgöra vilka mekanismer som ska nyttjas för att realisera de kravställda säkerhetsfunktionerna utgör dock en senare del av utvecklingsarbetet. (Försvarsmakten, 2006b, avs.8.7)



Figur 4: Framtagande av kvarvarande risker utifrån identifierade risker och framtagna säkerhetskrav.

4.2 Intervjuernas bild av genomförandet

I detta kapitel sammanfattas det som framkom under intervjuerna. Det första avsnittet berör hur analyserna genomförs i praktiken. Det andra avsnittet beskriver den syn på syftet med analyserna som framkom under intervjuerna. Det

[4] Det är därmed säkerhetskrav, inte säkerhetsmål, som ska beskrivas i säkerhetsmålsättningen.

tredje avsnittet innehåller en sammanfattning av identifierade problem och det fjärde avsnittet innehåller framkomna förbättringsförslag relaterade till genomförandet av analyserna.

4.2.1 Hot-, risk- och sårbarhetsanalyser i praktiken

Samtliga dokument som ansågs relevanta i dokumentstudien nämndes av informanterna under intervjuerna. Flertalet av de intervjuade anser att analyserna utgår från de beskrivningar som ges i H SÄK IT och H SÄK IT Hot. Vidare refererar ett flertal av informanterna till MAACK-mallarna som ett stöd vid genomförandet av analyserna.

Gällande indata till analyserna nämner ett fåtal att det finns en uppsättning förutbestämda krav i KSF. Vidare nämner en av de intervjuade att det finns inofficiella listor med hot som används vid genomförande av hotanalyser.

Huvuddelen av de intervjuade anser att det inte finns en etablerad metod för att genomföra analyserna. Hur analyserna genomförs beror till stor del på vem som leder arbetet. Ett fåtal anser dock att det finns en fastställd metod i H SÄK IT, men att denna endast beskriver *vad* som ska tas fram under analyserna, inte *hur*.

På frågan om hur analyserna faktiskt genomförs uttrycker flertalet att det förekommer att underlag från analys av ett annat system modifieras för att passa det nya systemet. Detta är dock ett tillvägagångssätt som de anser vara olämpligt.

I ett fåtal intervjuer framkom att standardlistor över hot är en bra utgångspunkt för hotanalysen. Det finns förvisso risk för att nyttjande av standardlistor över hot leder till att de hot som är specifika för systemet missas. En av de intervjuade påpekade att detta kan kompenseras med erfarenhet hos de som genomför analyserna.

Huvuddelen av de intervjuade anser att det är viktigt att representanter från de verksamheter där systemen ska användas finns med vid analyserna. Så verkar dock inte alltid vara fallet då det framkom att representanterna borde vara mer involverade i analysarbetet.

Ett fåtal av de intervjuade påpekar att det är Försvarsmakten som ska göra analyserna. Flertalet av de intervjuade påpekar dock att analyserna oftast genomförs av FMV, konsulter eller ibland till och med av den tilltänkta leverantören av systemet.

4.2.2 Syftet med hot-, risk- och sårbarhetsanalyser

Huvuddelen av de intervjuade anser att syftet med att göra analyserna är att få system med bättre säkerhet. Den tänkta kopplingen mellan analyserna och system med bättre säkerhet är att resultatet från analyserna ska ligga till grund för de säkerhetskrav som ställs på det tilltänkta systemet. Huruvida detta syfte i

dagsläget är uppfyllt är de intervjuade dock inte helt överens om. Huvuddelen av de intervjuade anser inte att analyserna får den betydelse de borde ha. Detta på grund av att det förekommer att:

- analyser inte genomförs i den omfattning som krävs
- resultatet från analyserna inte beaktas tillräckligt i efterföljande steg i IT-livscykelmodellen
- analyserna genomförs efter att upphandling av systemet redan har påbörjats.

Ett fåtal av de intervjuade anser dock att analyserna har stor inverkan på de krav som ställs på det tilltänkta systemet.

Vidare uttrycker huvuddelen av de intervjuade att analyserna genomförs för att identifiera vilka oönskade händelser som kan inträffa vid användning av systemet. Vissa uttrycker detta som att det är viktigt att alla hot kopplade till systemet är kända medan andra uttrycker det som att det är viktigt att veta vilka risker användare av systemet utsätts för, vilket i dagsläget inte alltid är tydligt.

4.2.3 Problem

Huvuddelen av de tillfrågade anser att analyserna, som de genomförs idag, blir för generella. En anledning till detta är att analyserna ibland genomförs slentrianmässigt genom att ta en gammal analys och återanvända denna. En annan anledning kan vara att underlaget till analyserna såväl som stödet för att genomföra analyserna fokuserar på generella egenskaper som gäller för de flesta system och inte att få med det specifika hos systemen.

Problemet ovan är kopplat till att analyserna ofta genomförs av personal utanför Försvarsmakten samtidigt som representanter från verksamheten inte är delaktiga i analyserna till den grad som behövs.

Ett annat problem som huvuddelen av de intervjuade tar upp är att IT-livscykelmodellen inte är synkroniserad med materielprocessen. Ett fåtal påpekar att detta leder till att arbetet med att göra hot-, risk- och sårbarhetsanalyser inte kommer igång förrän det upptäcks att det krävs ett godkännande enligt IT-livscykelmodellen.

Genomförandet av analyserna upplevs som svårt på ett eller annat sätt av huvuddelen av de intervjuade. Detta tar sig uttryck i att en del av dessa anser att processen är komplex och svår sätta sig in i, medan andra tror att många analyser genomförs endast för att få ett auktorisationsbeslut. I det senare fallet är syftet att utvecklingsprocessen ska kunna fortsätta, snarare än för att få ett system med bra säkerhet.

4.2.4 Förbättringsförslag

Förslagen på förbättringar handlar huvudsakligen om att stödet för att genomföra analyserna skulle kunna förbättras. De förbättringsmöjligheter som de intervjuade förmedlade avseende stöd vid genomförandet av analyserna sammanfattas i listan nedan.

- Ta fram metodbeskrivningar som faktiskt beskriver *hur* analyserna ska genomföras.
- Inför en strukturerad utbildning för hur auktorisationsprocessen fungerar.
- Uppdatera MAACK kontinuerligt.
- Skapa en baslinje för normala system så att analyserna kan fokuseras på det specifika, det vill säga det som skiljer från baslinjen. På så sätt kan tillgängliga resurser fördelas mellan olika systemutvecklingsprojekt på ett sätt som bättre motsvarar systemens omfattning och komplexitet.
- Skapa en katalog över befintliga säkerhetslösningar som kan nyttjas.
- Stöd från gransknings- och beslutsfunktioner för att tydliggöra inriktning för och omfattning av analyserna.
- Samordna analyserna med motsvarande analyser som görs inom ramen för arbetet med systemsäkerhet.

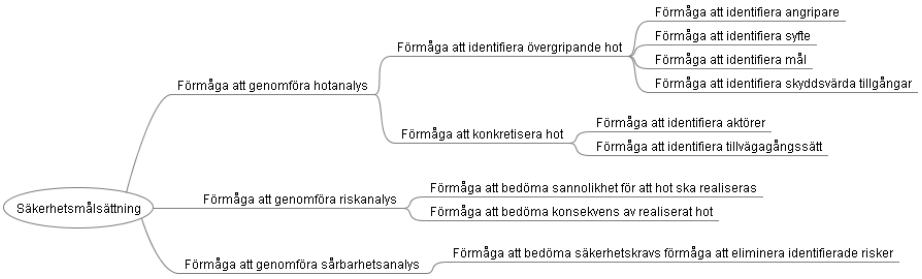
Utöver förslag på hur stödet kan förbättras uppgav en av de intervjuade att ett sätt att få till den specifika relevansen i analyserna är att genomföra dessa i ett senare skede i IT-livscykelmodellen.

5 Behovsanalys

I detta kapitel presenteras de behov som har identifierats under dokumentstudien samt under analysen av de intervjuer som har genomförts.

5.1 Behov från dokumentationen

Utgående från beskrivningen av genomförandet av hot-, risk- och sårbarhetsanalyser som återges i avsnitt 4.1 har ett antal behov identifierats. Att dokumentationen till stor del är fokuserad på *vad* som ska genomföras, snarare än *hur*, återspeglas av den uppsättning behov som presenteras i Figur 5.



Figur 5: Behov som har identifierats utgående från dokumentationen.

Behoven är hierarkiskt strukturerade och utgår från grundbehovet som är att ta fram en *säkerhetsmålsättning*. För att uppfylla grundbehovet måste de tre underliggande behoven *genomföra hotanalys*, *genomföra riskanalys* samt *genomföra sårbarhetsanalys* uppfyllas. Innehållet i en säkerhetsmålsättning omfattar mer än resultatet från de tre analyserna, men övriga delar ligger utanför fokus för denna rapport.

De underliggande behoven för hotanalysen är mer detaljerade än för de två andra analyserna. Anledningen till detta är att det för hotanalysen finns en framtagen handbok (H SÄK IT Hot) som kompletterar H SÄK IT genom att beskriva hur hotanalyser ska genomföras. Motsvarande beskrivningar saknas helt för riskanalys och sårbarhetsanalys.

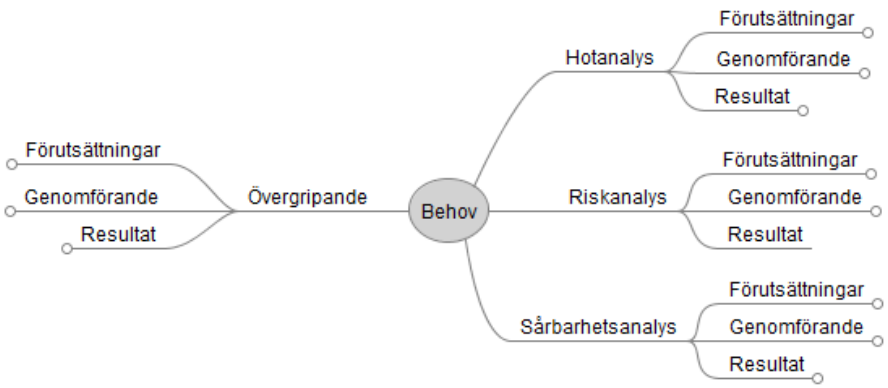
5.2 Behov från intervjuerna

Utgående från de genomförda intervjuerna identifierades behov med hjälp av den metod som beskrivs i avsnitt 3.3. De identifierade behoven grupperades in i de fyra kategorierna *övergripande*, *hotanalys*, *riskanalys* och *sårbarhetsanalys*. Dessa kategorier innehåller totalt 77 behov, varav 42 behov i kategorin

övergripande, 15 i kategorin *hotanalys*, 4 i kategorin *riskanalys* och 16 i kategorin *sårbarhetsanalys*. Samtliga behov återfinns i Bilaga C.

Kategorin *övergripande* omfattar generella behov som anses gälla för alla tre analyserna. De behov som är specifika för en enskild analys sorterades istället in under kategorin för respektive analys. På så sätt uppnåddes en struktur där det specifika för varje analys inte försvann i mängden av generella behov. Behoven i varje kategori är i sin tur indelade i de tre grupperna *förutsättningar*, *genomförande* och *resultat*. Strukturen illustreras i Figur 6.

De generella behoven beskrivs i avsnitt 5.2.1 medan de analysspecifika behoven beskrivs i avsnitt 5.2.2. I dessa avsnitt återges en övergripande beskrivning av den framkomna behovsstrukturen. Vidare lyfts de behov som kan härledas från huvuddelen av intervjuerna fram. Dessa behov listas i detta kapitel och ligger till grund för diskussionen i kapitel 6.



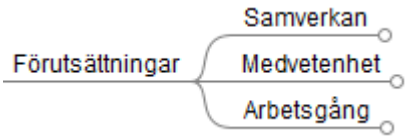
Figur 6: Struktur för gruppering av de behov som identifierades utgående från intervjuerna.

5.2.1 Övergripande behov

Behoven kopplade till gruppen förutsättningar har delats upp i tre undergrupper, *samverkan*, *medvetenhet* och *arbetsgång*, vilket illustreras i Figur 7. Gruppen *samverkan* innehåller behov relaterade till både koordinering av analyser mellan system såväl som samverkan mellan hot-, risk- och sårbarhetsanalyserna och övriga arbetsmoment i IT-livscykelmodellen. Gruppen *medvetenhet* samlar behov relaterade till medvetenhet hos de personer som genomför analyserna samt medvetenhet hos dem som är mottagare av de utvecklade systemen. Behoven i gruppen *arbetsgång* relaterar till egenskaper hos personalen i de grupper som genomför analyserna.

Ett av behoven i gruppen förutsättningar kan härledas från huvuddelen av intervjuerna. Detta behov återfinns i undergruppen *arbetsgång* och återges nedan.

- Egen personal med tid och kompetens att genomföra analyser.

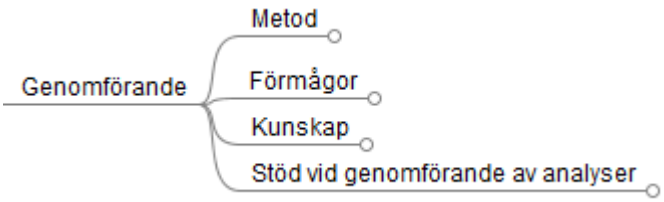


Figur 7: Undergrupper i gruppen förutsättningar

Behoven kopplade till genomförandet av analyserna delades upp i grupperna *metod*, *förmågor*, *kunskap* och *stöd vid genomförande av analyser*, vilket illustreras i Figur 8. Behoven som samlats i gruppen *metod* är kopplade till arbetssätt vid genomförandet av analyserna samt behov avseende egenskaper hos de metoder som används. Gruppen *förmågor* innehåller behov relaterade till kompetenser avseende analysförmåga som krävs vid genomförandet av analyserna. Behoven i gruppen *kunskap* handlar om de kompetenser i form av kunskap om de använda metoderna samt kunskap om hur och när systemet, som analyseras, ska användas. Slutligen innehåller gruppen *stöd vid genomförande av analyser* de behov av stöd som identifierats vid genomförandet av analyserna.

Två av behoven i kategorin genomförande kan härledas från huvuddelen av intervjuerna. Dessa behov återfinns i undergrupperna *kunskap* respektive *stöd vid genomförande av analyser* och återges nedan.

- Kunskap om den verksamhet IT-systemet ska stödja.
- Tydliga instruktioner för hur analyserna ska genomföras.



Figur 8: Undergrupper i gruppen genomförande

De behov som grupperats in under resultat handlar till största delen om vad resultatet ska kunna användas till, men det finns även behov relaterade till egenskaper för resultatet. Två av behoven i kategorin resultat kan kopplas till huvuddelen av intervjuerna.

- Analysresultat som visar att IT-systemet är ackrediterbart.
- Förståelse för vilka risker som tas vid användning av ett tänkt IT-system.

5.2.2 Specifika behov

Behoven kopplade till kategorin hotanalys är spretiga. Dock kan en övergripande röd tråd avseende kompetens identifieras. Behoven i gruppen förutsättningar relaterar i stor utsträckning till kompetenser hos dem som ska genomföra analyserna. Behoven i gruppen genomförande handlar om att använda kompetensen och behoven i gruppen resultat handlar om att resultatet ska vara relevant. Från kategorin hotanalys fanns det ett behov som kunde härledas från huvuddelen av intervjuerna. Detta behov är kopplat till resultatet av hotanalysen och återfinns i gruppen *resultat*.

- Hotbild som är specifik för det aktuella systemet.

Det är relativt få behov som har kopplats specifikt till kategorin riskanalys. De som har identifierats handlar om behov av att kunna bedöma sannolikheten för att ett hot ska realiseras samt konsekvensen om hotet skulle realiseras. Behoven framkommer både i gruppen förutsättningar, det vill säga behov av förmåga, och i gruppen genomförande, det vill säga behov av att göra bedömningarna. Från behovsanalysen framkom inte några behov kopplade till riskanalysens resultat.

Bland de specifika behoven i kategorin sårbarhetsanalys finns i gruppen *förutsättningar* en mängd behov relaterade till att ha personal som har kompetens att genomföra sårbarhetsanalyser. Behoven i gruppen *genomförande* handlar huvudsakligen om framtagandet av IT-säkerhetskrav. Behoven i gruppen *resultat* handlar om kravställning och förståelse för vilka risker användare av systemet utsätts för.

6 Diskussion

Målsättningen med denna rapport är att förmedla hur Försvarsmakten arbetar med hot-, risk- och sårbarhetsanalyser för IT-system, samt vilka behov av stöd som finns under genomförandet av dessa analyser. I detta kapitel förs diskussionen främst utgående från de behov som framträdde extra tydligt under behovsanalysen. De två bilderna av genomförandet av analyserna, som togs fram baserat på tillgänglig dokumentation (avsnitt 4.1) respektive de genomförda intervjuerna (avsnitt 4.2), diskuteras här som en gemensam bild av genomförandet.

Bilden av genomförandet ger en uppfattning om det underlag som utgjort en grund för behovsanalysen. En observation från intervjuerna är att genomförandet är att hot-, risk- och sårbarhetsanalysen ses som *en* analys snarare än som tre separata. Detta illustreras även av figurerna i Bilaga C där större delen av de identifierade behoven är av en övergripande karaktär och inte kan kopplas till någon enskild analys.

Behovsanalysen har varit inriktad på att identifiera direkta behov från dokumentationen och intervjuerna. Detta har fördelen att de behov som återfinns i behovsträden är direkt härledda från de studerade dokumenten och intervjuerna. Däremot finns det tydliga luckor i behovsträdet, vilka behöver fyllas med ytterligare behov för att erhålla en komplett behovsbild.

Tillgång till en hotbild som är specifik för det aktuella systemet är det enda behov som direkt syftar på en av analyserna och som framkom i huvuddelen av intervjuerna. Följande utgör två möjliga orsaker till detta fokus på hotbilden som ett resultat av analyserna.

1. En fastställd hotbild kan ge en erfaren person god insikt i vilka kvarvarande risker som kommer att identifieras i de senare analyserna. Detta gör att hotanalysen kan anses som ett huvudresultat snarare än ett delresultat av analyserna.
2. Det verkar vara vanligt att referera till hotbild som slutresultatet av analyserna, när det egentligen är kvarvarande risker som avses. Enligt H SÄK IT kan dessa kvarvarande risker också benämnas sårbarheter eller resulterande riskvärden och anses vara brister i systemet.

De instruktioner som Försvarsmakten i dagsläget tillhandahåller angående hur genomförandet av analyserna ska gå till är knapphändiga. De utgörs framförallt av beskrivningarna i handböckerna H SÄK IT och H SÄK IT Hot samt dokumentmallarna i MAACK. H SÄK IT beskriver till största del *vad* som ska tas fram till säkerhetsmålsättningen, men det saknas beskrivningar av *hur* det ska göras. H SÄK IT Hot tillhandahåller en beskrivning av hur hot kan identifieras och struktureras. Metodbeskrivningen är dock begränsad till ett fåtal sidor.

Mallarna i MAACK ger framförallt stöd avseende presentationen av analysresultatet. Avsaknaden av *hur*-beskrivningar är en möjlig orsak till variationen avseende säkerhetsmålsättningars inriktning och omfattning. Behovsanalysen påvisar tydligt en avsaknad av enkla och strukturerade instruktioner för hur det efterfrågade underlaget ska tas fram.

Alla IT-system som ska användas inom Försvarsmakten måste vara auktoriserade och ackrediterade. Kraven är desamma på alla IT-system, vilket exempelvis innebär att införandet av en kontorsprogramvara hanteras på samma sätt som införandet av ett ledningssystem. I instruktionerna för analysernas genomförande tas ingen hänsyn till IT-systemets omfattning eller komplexitet.

Avsaknad av tid och resurser för att med egen personal genomföra analyserna är något som lyfts fram som ett tydligt problem. Då sårbarhetsanalysen är avgörande för kravställningen av IT-säkerhet bör den genomföras av Försvarsmaktens personal, inte extern personal. Att den egna personalen inte har tid att genomföra analyserna leder till att deras kompetens inom området blir begränsad, vilket i sin tur skapar ett beroende av externa parter.

Att externa parter i stor utsträckning utför analyserna leder även till att kunskapen om verksamheten som IT-systemen ska stödja är begränsad. Personer med god kännedom om den tänkta verksamheten behöver delta i analysarbetet i större utsträckning för att analyserna ska få någon betydande påverkan på IT-säkerheten i ett IT-system. Avsaknaden av verksamhetsrepresentanter i analysarbetet leder till generella analysresultat som ofta saknar specifik relevans. Ett syfte med att genomföra analyserna är att få förståelse för vilka risker som tas vid användning av ett IT-system. När kunskapen är bristfällig om verksamheten som IT-systemet ska stödja är det inte troligt att analysresultatet ger den efterfrågade förståelsen. Analysernas betydelse för systemets IT-säkerhet kan i dessa fall ifrågasättas. Behov av reell kunskap om den verksamhet som IT-systemen ska stödja, samt vilka risker som tas vid användning av IT-system framträdde tydligt under behovsanalysen.

Utgående från Försvarsmaktens IT-livscykelmodell ska framtagandet av säkerhetsmålsättningen genomföras då IT-systemet fortfarande är i ett konceptstadie, med fokus på verksamhet snarare än teknik. Tanken är god, men verklighetsanknytningen är vag. Analysarbetet genomförs ofta då IT-systemet redan är framtaget, vilket kan vara en bidragande orsak till att auktorisations- och ackrediteringsprocessen av många upplevs som tidsödande och som ett hinder på vägen. Med ett IT-system som redan är framtaget hamnar fokus på snabb och smärtfri ackreditering snarare än att uppnå ett system med adekvat IT-säkerhet.

7 Rekommendationer

Baserat på resultaten av det arbete som presenteras i denna rapport ges följande rekommendationer till Försvarsmakten avseende hot-, risk- och sårbarhetsanalyser för IT-system.

- **Utveckla kunskap om de faktorer som påverkar analyserna**
  Genomförandet av analyserna innehåller många abstrakta uppgifter som kräver att en stor mängd information om olika egenskaper beaktas. Dessa analyser kommer under överskådlig tid att innehålla ett visst mått av subjektiva bedömningar. Grundläggande kunskap om hur de bedömningar som ingår i analyserna påverkas av olika faktorer, såsom tillgång till underlag, metod, metodstöd och deltagare i analysgruppen, är nödvändig för att kunna utveckla ändamålsenliga instruktioner, utbildning och stöd för genomförandet av analyserna.

- **Ta fram tydliga instruktioner för *hur* analyserna ska genomföras**
  En viktig del i detta är att tillhandahålla bra exempel som tydliggör även hur komplexa situationer hanteras. För att instruktionerna ska vara användbara måste hänsyn tas till den situation de ska nyttjas i, dvs. att analysernas omfattning och inriktning kan anpassas efter aktuellt system.

- **Tillhandahåll relevant utbildning**
  Tydlig och strukturerad utbildning av personal är något som efterfrågats och är nödvändigt för att möta flera av de identifierade behoven. Det finns en vilja att öka Försvarsmaktens interna kompetens om analyserna, men tid, resurser och adekvat utbildning saknas. För att kunna ta fram underlag för sådan utbildning är det nödvändigt med tydliga instruktioner, enligt punkten ovan, och en kartläggning av vilken kunskap som är nödvändig för genomförandet av analyserna.

- **Ta fram stöd för nödvändiga bedömningar**
  Under analyserna är det nödvändigt att identifiera aktuell hotbild, bedöma de identifierade hoten samt avgöra hur realiseringen av ställda IT-säkerhetskrav minskar riskerna. Dessa uppgifter kräver kunskap om många olika faktorer och förmåga att sammanställa dessa för att erhålla de efterfrågade resultaten. Ett tydligt stöd för att genomföra dessa bedömningar kan öka validiteten, tillförlitligheten och spårbarheten hos de framtagna resultaten.

- **Fokusera analyserna på det specifika snarare än det generella**
  Det finns flera sätt att uppnå detta. En möjlighet är att definiera någon form av standardsystem som grund för analyserna. Analyserna kan då fokusera på det specifika, det vill säga hur IT-systemet skiljer sig från definierade standardsystem. Det är dock nödvändigt att utreda i vilken omfattning detta är möjligt.

- **Ta fram stöd för att avgöra verksamhetens krav på IT-säkerheten**
  Att avgöra vilka IT-säkerhetskrav som måste ställas för att verksamheter ska kunna bedrivas med adekvat säkerhet är en komplex uppgift. Det är nödvändigt att tydliggöra hur den uppgiften ska lösas inom ramen för såväl instruktioner som utbildning.

8 Referenser

Bengtsson, J. & Hallberg, J. (2008a). Test av relevans och validitet avseende säkerhetsvärdering – En studie av Försvarsmaktens metoder för säkerhetskravställning och sårbarhetsanalys. Användarrapport, FOI-R--2625--SE. Totalförsvarets forskningsinstitut, FOI.

Bengtsson, J. & Hallberg, J. (2008b). Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete. Underlagsrapport, FOI-R--2531--SE. Totalförsvarets forskningsinstitut, FOI.

Bossert, J.L. (1991). Quality Function Deployment: A Practitioner's Approach. I: 1991, Milwaukee, WI, USA: ASQC Quality Press.

Försvarsmakten (2004a). Beslut om krav på godkända säkerhetsfunktioner, ver. 2.0. HKV 10 750:78976.

Försvarsmakten (2004b). Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT 04). HKV 09 626:78369.

Försvarsmakten (2009). Försvarsmaktens gemensamma riskhanteringsmodell. Handbok, M7739-350012. Stockholm: Försvarsmakten.

Försvarsmakten (2006a). Handbok för Försvarsmaktens säkerhetsskyddstjänst, Hotbedömning (H Säk Hot). Handbok, M7745-734022. Stockholm: Försvarsmakten.

Försvarsmakten (2006b). Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik (H SÄK IT). Handbok, M7745-734062. Försvarsmakten.

Försvarsmakten (2001). Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik Hotbeskrivning (H SÄK IT Hot). Handbok, M7745-734051.

Försvarsmakten (2007). Handbok för Försvarsmaktens Säkerhetstjänst, Säkerhetsskyddstjänst (H SÄK Skydd). Handbok, M7739-352005.

Försvarsmakten (2008). MAACK – Metod- & utbildningsstöd för auktorisations- och ackrediteringsprocesserna inom Försvarsmakten.

Mazur, G. (1992). Voice of the Customer Table: A Tutorial. I: 1992, Novi, MI, USA, ss 105-111.

SIS (2007). SIS HB 550: Terminologi för informationssäkerhet, utgåva 3. SIS Förlag.

Tague, N.R. (2005). Quality Toolbox, 2nd edition. ASQ Quality Press.

Bilaga A. Intervjuguide

I denna bilaga återfinns den intervjuguide som låg till grund för de genomförda intervjuerna.

Bakgrundsinformation om informanten

1. Hur kommer du i kontakt med hot- risk- och sårbarhetsanalyser i ditt arbete? (Speciellt avses framtagandet av underlag för auktorisationsbeslut B2)
2. Är hot- risk- och sårbarhetsanalyser något du jobbar med regelbundet?
3. Hur länge har du jobbat med hot- risk- och sårbarhetsanalyser?

Hot-, risk- och sårbarhetsanalyser i praktiken

4. Finns det någon etablerad metod?
   Används den?
5. Hur ser arbetsgången vid en analys ut?
   Är det vanligt att analyser går till på detta sätt? Hur vanligt?
6. Vem eller vilka är det som genomför analysen? (roller)
7. Finns det svårigheter?
8. Finns det saker som fungerar väl?

Hot-, risk- och sårbarhetsanalysens syfte

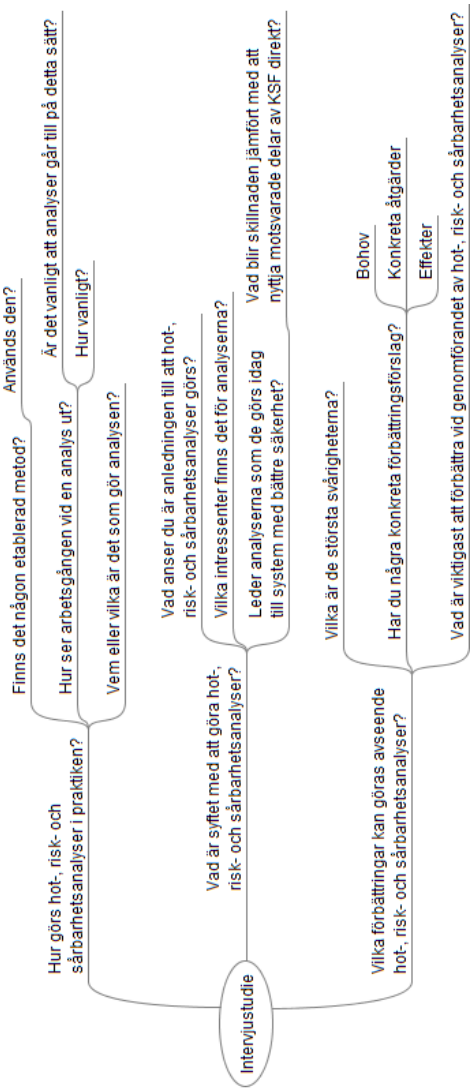
9. Vad anser du är anledningen till att hot-, risk- och sårbarhetsanalyser görs?
10. Vilka intressenter finns det för analyserna?
11. Leder analyserna som de görs idag till system med bättre säkerhet?
    Finns det skillnader jämfört med att nyttja motsvarade delar av KSF direkt?

Förbättringsmöjligheter för hot- risk- och sårbarhetsanalyser

12. Har du några konkreta förbättringsförslag? [Återkoppla till fråga 7]
    (Behov, konkreta åtgärder, effekter)
    Finns det något av dessa som är viktigare än de övriga? Varför?

Bilaga B. Forskningsfrågor

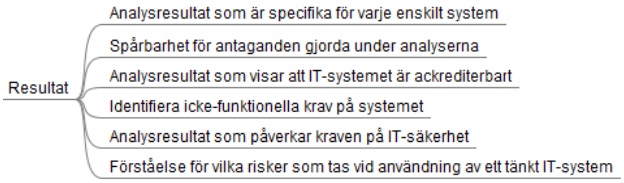
I denna bilaga presenteras de tre forskningsfrågorna och deras koppling till de intervjufrågor som återfinns i intervjuguiden.



Bilaga C. Behovsträd

I denna bilaga presenteras det behovsträd som togs fram under behovsanalysen. Då trädet är mycket omfattande har det delats upp i mindre delar. Först presenteras delträden för de övergripande behoven. Därefter följer delträden för hot-, risk- och sårbarhetsanalysen.

Delträd för de övergripande behoven



Delträd för hot-, risk- och sårbarhetsanalys