Riskhantering för IT-system

Tolv år av forskning och teknikutveckling

Henrik Karlzén och Johan Bengtsson

FOI-R--4835--SE

December 2019

FOI

Henrik Karlzén och Johan Bengtsson

Riskhantering för IT-system

Tolv år av forskning och teknikutveckling

Titel	Riskhantering för IT-system – Tolv år av forskning och teknikutveckling
Title	Risk management for IT systems – Twelve years of research and technological development
Rapportnr/Report no	FOI-R--4835--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	62
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E72778
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: David Teniers d.y., Soldiers playing dice

Sammanfattning

Denna rapport sammanfattar studier inom *riskhantering för IT-system* som bedrivits på FOI de senaste tolv åren (2008–2019). Studierna har finansierats av Försvarsmaktens anslag för forskning och teknikutveckling (FoT) och haft syftet att genom forskning förbättra Försvarsmaktens arbete med att analysera säkerheten i deras IT-system.

Några av de viktigare slutsatserna från studierna är att: det finns behov av att upprätthålla kunskapsnivån om riskbedömningar inom Försvarsmakten; det finns behov av tydligare instruktioner för hur riskhanteringsarbetet ska genomföras; andra vedertagna metoder för riskhantering är av begränsad nytta för Försvarsmakten då stora anpassningar krävs för att de ska kunna användas; IT-säkerhetsexperters bedömningar är mer samstämmiga om jämförelsebaserade metoder används istället för nuvarande tillvägagångssätt.

Det finns flera viktiga frågor som uppstått till följd av studierna och som lämnats obesvarade:

- Hur stor skillnad blir det normalt mellan resultat från riskbedömningar för två olika IT-system?
- Hur beständiga är riskbedömningar över tid och hur ska man hålla sig underrättad om förändringar som sker av system, hot och kontext?
- Hur stor skillnad medför olika riskbedömningsresultat senare i processen i form av rekommenderade skyddsåtgärder?
- Hur ska riskbedömningarna likriktas samtidigt som unika insikter tillvaratas?

Nyckelord: informationssäkerhet, IT-säkerhet, cybersäkerhet, IT-system, risk, konsekvens, sannolikhet, riskhantering, riskbedömning, riskanalys, hot- risk- och sårbarhetsanalys, säkerhetsanalys, säkerhetsmålsättning, säkerhetsvärdering, KSF, riskacceptans, verksamhetsanalys, säkerhetsskyddsanalys, slutrapport

Summary

This report summarises studies in *risk management in IT systems* which have been performed at FOI in the past twelve years (2008–2019). The studies have been financed by the Swedish Armed Forces (SwAF) and had the purpose of, through research, providing support for the SwAF's work on analysing the security of their IT systems.

Some of the most important conclusions from the studies are that: there are needs of maintaining the knowledge level for risk assessments in the SwAF; there are needs for clearer instructions for how the risk management work should be performed; other prevalent methods for risk management are of limited use for the SwAF since large adaptions are necessary; IT security experts' assessments are in more agreement if comparison based methods are used instead of the current approach.

There are several important questions that have arisen in the course of the studies and have been left unanswered:

- How large is typically the difference between results from risk assessments for two different IT systems?
- How persistent are risk assessments over time and how should one stay informed of changes that occur in systems, threats and contexts?
- How large differences do different risk assessment results lead to later in the process in the form of recommended security measures?
- How should different risk assessments be better aligned while capturing unique insights?

Keywords: information security, IT security, cyber security, IT system, risk, severity, probability, risk management, risk assessment, risk analysis, threat risk and vulnerability analysis, security analysis, security objective, security evaluation, KSF, risk acceptance, business process modelling, security protection analysis, final report

Innehåll

1. Inledning 7
2. Bakgrund 8
2.1 Riskhanteringens ursprung 8
2.2 Relaterad forskning 10
2.3 Försvarsmaktens processer och terminologi 12
3. Projektens resultat 15
3.1 Testning av metoder och verktyg för värdering av informationssäkerhet (2008–2010) 16
3.2 Effektivare hot-, risk- och sårbarhetsanalyser (2011–2013) 18
3.3 Bedömning och analys av IT-system (2014–2016) 21
3.4 Metodik för säkerhetsmålsättningsarbete (2017–2019) 24
4. Slutsatser och framtida forskning 27
4.1 Försvarsmaktens behov på området 27
4.2 Utförarnas effekt 27
4.3 Styrkor och svagheter med gängse metoder 28
4.4 Riskbedömning genom jämförelser av risker 28
4.5 Tydligare beskrivningar av risker 29
4.6 Återanvändning av analyser och bedömningar 29
5. Referenser 31
5.1 Riskhanterings ursprung 31
5.2 Relaterad forskning 32
5.3 Försvarsmaktens processer och terminologi 33
5.4 Rapporterna 34
Bilaga A. FOI-rapporter 36
A.1 Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete 36
A.2 The TSAR procedure 37
A.3 Test av relevans och validitet avseende säkerhetsvärdering 38

A.4 Tester av metoder för värdering av informationssäkerhet 39
A.5 The TSAR procedure revision 1 40
A.6 Framtida metoder för värdering av IT-säkerhet 41
A.7 Hot-, risk- och sårbarhetsanalys 42
A.8 Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten 44
A.9 Varför följer inte användarna bestämmelser? 45
A.10 Verktygsstöd för hot-, risk- och sårbarhetsanalyser 46
A.11 Informationsbehov vid säkerhetsanalyser 47
A.12 Effektivare hot-, risk- och sårbarhetsanalyser 48
A.13 IT-säkerhetskrav i Försvarsmakten 49
A.14 Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker 50
A.15 Beskriva och bedöma hot mot IT-system 51
A.16 Riskacceptans 53
A.17 Beskrivning av hot vid säkerhetsanalyser 55
A.18 Verksamhetsanalys 56
Bilaga B. Övriga producerade resultat 58
B.1 FOI-memon 58
B.2 Akademiska forskningsartiklar 59
B.3 Verktygsstödet Sublime 60

1. Inledning

Säkerhet är ett ledord i Försvarsmakten. För IT-system finns dock en stor utmaning att uppnå och upprätthålla säkerheten. Här finns alltså ett stort behov av förbättring. Denna rapport utgör slutrapporten för det treåriga projektet *Metodik för säkerhetsmålsättningsarbete* (2017–2019) och sammanfattar den forskning som utförts i projektet samt i dess tre föregångare[1] under totalt tolv år (2008–2019). Syftet med projekten har varit att genom forskning stödja Försvarsmaktens arbete med att analysera säkerheten i deras IT-system, det vill säga Försvarsmaktens riskhanteringsarbete. Mer specifikt har projekten studerat:

- Försvarsmaktens behov på området.
- De som utför arbetet i riskhanteringsprocessen.
- Styrkor och svagheter med gängse metoder.
- Att bedöma risker genom att jämföra dem med varandra.
- Tydligare beskrivningar av risker.
- Återanvändning av analyser och bedömningar.

Rapporten är därmed primärt avsedd för läsare med fokus på Försvarsmakten och IT-system, men är även relevant för andra med intresse av riskhantering. Rapporten tar sin utgångspunkt i ett bakgrundskapitel som beskriver:

- Ursprunget till riskhantering i allmänhet (avsnitt 2.1).
- En genomgång av vad andra projekt på FOI gjort på det bredare riskhanteringsområdet (avsnitt 2.2).
- En introduktion till Försvarsmaktens processer och terminologi över tid (avsnitt 2.3).

Rapporten beskriver sedan de resultat som forskningen gett i kronologisk ordning (kapitel 3). Därpå ges slutsatser och idéer för framtida forskning (kapitel 4), följt av en förteckning över använda referenser (kapitel 5).

I Bilaga A beskrivs varje rapport mer utförligt och i Bilaga B beskrivs övriga projektresultat i form av FOI-memon[2], akademiska forskningsartiklar[3] och verktygsstödet Sublime.

[1] De tre föregångarna är (med det äldsta först) *Testning av metoder och verktyg för värdering av informationssäkerhet* (2008–2010); *Effektivare hot-, risk- och sårbarhetsanalyser* (2011–2013); samt *Bedömning och analys av IT-system* (2014–2016).

[2] FOI använder så kallade memon för skriftlig dokumentation som av något skäl inte lämpar sig för publicering som FOI-rapport. Typiskt rör det sig om kortare texter som är av mindre intresse för en bredare målgrupp än kunden.

[3] De akademiska forskningsartiklarna presenterar i huvudsak resultaten i FOI-rapporterna, men har forskare som målgrupp.

2. Bakgrund

I detta kapitel beskrivs riskhanteringens ursprung (avsnitt 2.1), vad andra projekt på FOI skrivit om riskhantering (avsnitt 2.2) och Försvarsmaktens processer och terminologi samt förändringar i dessa under åren (avsnitt 2.3).

2.1 Riskhanteringens ursprung

Det första kända fallet av riskbedömning[4] skedde runt år 3200 före vår tideräkning då folkgruppen Asipu i dalen vid Tigris och Eufrat erbjöd stöd vid svåra beslut genom att med gudarnas vägledning bedöma olika utfall (Covello och Mumpower, 1985). År 1693 föreslogs att förväntad livslängd bedöms med hjälp av riskbedömningar och år 1792 användes riskbedömningsmetoder för att bedöma smittkoppsvaccins effektivitet (Covello och Mumpower, 1985). År 1939 infördes det första gränsvärdet för flygplan, vilket specificerade att flygplan måste klara en timme i luften med 99,999 % sannolikhet (Rechard, 1999).

Moderna metoder för riskbedömningar växte till stor del fram i samband med utvecklingen av kärnkraft (Durán m.fl., 2013). Enligt Rechard (1999) infördes år 1941 ett gränsvärde (med en säkerhetsfaktor) för hur mycket strålning människor får utsättas för. Sju år senare (1948) rekommenderade ett amerikanskt nämnd för strålningssäkerhet införandet av principen att minimera strålningsdoserna och därmed risken så långt som möjligt. Denna princip blev 1975 till regel och dessförinnan hade de första så kallade felträden tagits fram 1961. Till följd av Harrisburgolyckan 1979 sattes gränser för maximalt tillåtna sannolikheter för olyckor, dödsfall på grund av strålningsrelaterad cancer samt utsläpp. Dessutom noterade Rechard (1999) att amerikanska rymdstyrelsen Nasa (som tidigare tyckt att riskbedömningar var alltför oprecisa och därför indikerade på alltför stora risker (Feynman, 1986)) införde riskbedömningar efter att risker missats rörande Challenger-olyckan 1986.

Golob och Kožuh (2016) noterade att allvarliga risker fortfarande missas, med exemplet Fukushima-olyckan där riskhanteringen varit otillräcklig för att minimera riskerna i kärnkraftverket. Att bedöma risker är som att sia om framtiden och det görs inte lättare av att riskbedömningar inte har särskilt lång bakgrund akademiskt. Den första akademiska boken publicerades 1963 (Dionne, 2013) och som aktivt forskningsfält har riskhantering bara funnits i tre–fyra decennier (Aven, 2016). För snart trettio år sedan drog Baskerville (1991)

[4] Riskbedömning utgörs av identifiering, analys och värdering av risker. I det vidare begreppet riskhantering ingår också att riskerna hanteras, ofta genom införandet av skydd.

slutsatsen att riskhantering är ett dåligt verktyg för att strukturerat öka informationssäkerheten, men att det inte finns något bättre alternativ. Även om situationen förbättrats något, är konceptuella aspekter som terminologi, processteg, struktur och bedömningsgrunder fortfarande undermåligt klarlagda (Hansson och Hirsch Hadorn, 2017; Aven, 2016).

Att bedöma risker inom områden som flyg och kärnkraft är en utmaning. Å andra sidan fokuserar de i första hand på handhavandefel och olyckor, det vill säga icke-antagonistiska risker. När mänskliga antagonister finns med i bilden – vilket ofta är fallet för Försvarsmakten– blir det ännu svårare. Den ökade svårigheten ligger bland annat i att förstå vad som avskräcker respektive motiverar antagonister och hur ett möjligt offers skydd påverkar sannolikheten att andra blir offer (Durán m.fl., 2013).

Förutom att ha ett antagonistiskt fokus snarare än ett icke-antagonistiskt, har analyser av Försvarsmakten IT-system också andra egenheter. Dels är fokus på informationssäkerhet snarare än personella risker (vilket annars ofta är fallet inom flyg, medicin och kärnkraft), dels görs analyserna inom försvarssektorn. Det är inte uppenbart hur detta påverkar vilken metod som är lämplig för riskbedömningarna, men det kan vara på sin plats att nämna något om vilka vanliga svårigheter och möjliga lösningar som finns.

Courtney (1977) skrev en av de första forskningsartiklarna som föreslog och beskrev en riskbedömningsmetod för informationssäkerhetsområdet samt gav råd som fortfarande är relevanta. Artikeln nämnde att bedömningarna bör inledas med bedömningar av risker som är enklare att kvantifiera eftersom skyddsåtgärder som möter dessa risker kanske även råkar ta hand om mer svårkvantifierade risker som därmed inte måste kvantifieras. Ett relaterat råd var att bedömningarna inte ska göras alltför exakta från början, utan att det är bättre att avvakta ett eventuellt behov av högre precision. Artikeln beskrev också att det är svårt att beskriva hur sannolikhetsbedömningar ska göras, att det är besvärligt att omvandla typiska risker inom försvarssektorn till pengar och att anställda tvingas till avvägningar mellan säkerhet och andra värden som effektivitet. Dessutom beskrevs att det är svårt att övertyga ledningen om att säkerhetsproblem finns och behöver hanteras, förutsatt att data om riskerna inte tagits fram, samtidigt som riskbedömningarna inte kan utföras utan ledningens stöd. En slutsats från artikeln är att det är bra att i grunden använda samma metoder som används inom områden med extrema risker, men att metoderna ofta kan förenklas för att inte kostnaderna att utföra riskhanteringsarbetet ska överstiga vinsterna.

En generell slutsats som kan dras är att riskhanteringsmetoder måste baseras på så korrekta modeller av verkligheten som möjligt samtidigt som metoderna inte

därmed får bli alltför svåranvända (Soo Hoo, 2000). Av detta skäl bör det tydligt framgå vilka förenklingar som ingår i vald riskhanteringsmetod.

2.2 Relaterad forskning

Förutom den forskning som producerats inom ramen för detta projekt och dess föregångare under de tolv åren har det på FOI även producerats ett antal ytterligare publikationer inom området riskhantering, delvis inom andra domäner än IT. Publikationerna omfattar både metodologiska studier och praktisk användning av metoder. Nedan följer en lista med exempel på relaterade publikationer i kronologisk ordning med kort beskrivning av deras primära innehåll.

- **Hotanpassning och krishantering – Erfarenheter av Y2K**
  Tre stora infrastrukturaktörers erfarenheter av riskhantering inför år 2000-problemet[5] (Broberg m.fl., 2000).
- **System IT Security Assessment**
  Befintliga metoder för värdering av IT-säkerhet och förslag på egna metoder och ramverk (Hallberg m.fl., 2004).
- **Crossroads and XMASS: Framework and Method for System IT Security Assessment**
  Ramverk och klassificeringar av metoder för att utvärdera IT-säkerhet och vidareutvecklingen av en värderingsmetod (Hallberg m.fl., 2006).
- **Handbok för IT-säkerhetsvärdering**
  En handbok i att genomföra värdering av IT-systems säkerhet (Hallberg m.fl., 2007a).
- **Refinement and realization of security assessment methods**
  Ett verktyg för värdering av IT-säkerhet (Hallberg m.fl., 2007b).
- **Försvarsmaktens gemensamma riskhanteringsmodell**
  Erfarenheter från utvecklandet av Försvarsmaktens gemensamma riskhanteringsmodell och en översiktlig jämförelse med andra modeller som användes av svenska myndigheter (Palm, 2008).
- **Metodik för riskbedömning**
  Beskriver olika metoder för riskbedömning (Harling m.fl., 2010).
- **Säkerhetsanalys av ett generellt IP-nät**
  En genomförd riskbedömning med teknisk inriktning för generella IP-nätverk (Karlzén och Westerdahl, 2010; Westerdahl, 2010).

[5] Detta dokument producerades av FOI:s föregångare FOA.

- **FOI:s Modell För Risk- Och Sårbarhetsanalys (FORSA)**
  En handbok för en riskhanteringsmodell framtagen på uppdrag av Stockholms stad (Winehav m.fl., 2011).
- **Analytiska verktyg – en översikt av metoder och modeller för underrättelseanalys**
  Presenterar riskanalysmetoder inklusive attackträd (Gustavi m.fl., 2011).
- **Metod- och inventeringsstöd till sektorsövergripande risk- och sårbarhetsanalys**
  En kartläggning av riskanalysmetoder som kan vara lämpliga för Livsmedelsverket (Winehav m.fl., 2012).
- **Underlag till nationell riskbedömning 2012. Resultat från den svenska nationella riskbedömningen 2012**
  Ett underlag för en nationell svensk riskbedömning vad gäller krisberedskap (Winehav m.fl., 2013).
- **Om indirekta, komplexa och oönskade händelser. Att analysera risker med stor osäkerhet**
  En analys och diskussion av vilka karaktärsdrag och begrepp som används för att tala om komplexa risker, som exempelvis de som aldrig tidigare förverkligats. Dessutom beskrevs olika upplevelser av risk, riskkommunikation och råd som att inte försöka undvika komplexitet genom att vara alltför snäv i analysen (Sonnsjö och Mobjörk, 2013).
- **Informationssäkerhet och ekonomi. Ett skannande projekt av aktuell forskning**
  Beskriver forskning inom gränslandet mellan informationssäkerhet och ekonomi med syfte att nå kostnadseffektiv säkerhet. Slutsats drogs att många teoretiska metoder finns, men att de saknar praktisk utvärdering (Hermelin m.fl., 2014). Arbetet togs fram i en avknoppning av projektet *Effektivare hot-, risk- och sårbarhetsanalyser*.
- **Risk- och sårbarhetsanalys för Totalförsvarets forskningsinstitut (FOI) 2014**
  En riskanalys av FOI och skyddsåtgärder för att hantera riskerna. För att inte underlätta för potentiella angripare beskrevs sårbarheter och skyddsåtgärder enbart på en övergripande nivå (Malmberg Andersson m.fl., 2014).
- **Studie: Metodutveckling inom processen för arbetet med risk- och sårbarhetsanalyser**
  En sammanställning och analys av myndigheters metoder för riskanalys (Malmberg Andersson och Denward, 2015).

- **Utmaningar för den kommunala risk- och sårbarhetsanalysen. En studie baserad på intervjuer med säkerhetssamordnare i Västra Götalands län**
  Råd för bättre riskanalysmetoder för kommuner för att i större utsträckning nyttiggöra riskanalyserna och för att stödja hanteringen av risker kopplade till klimatförändringar (Hedtjärn Swaling m.fl., 2016).
- **Oexploderad ammunition, OXA, på övnings- och skjutfält. Beskrivning av några metoder för riskanalys**
  Riskbedömningsmetoder för användning av nedlagda övnings- och skjutfält (Forsén, 2016).
- **Handbok för kommunalt RSA-arbete**
  En handbok för kommunalt riskbedömningsarbete. Handboken vänder sig främst till personer med ansvar för att leda och koordinera riskbedömningsarbetet. Handboken bygger på intervjuer, workshopar och dokumentstudier och är ett resultat av kartläggning och analys av olika arbetssätt samt identifiering av stöd till de aktiviteter som kommunerna ansett svåra (Albinsson m.fl., 2018).

2.3 Försvarsmaktens processer och terminologi

Under tiden för projektens genomförande har det inom Försvarsmakten funnits olika styrande dokument som beskriver arbetsprocesser för hur en grund för adekvata säkerhetsnivåer hos IT-system ska uppnås genom riskbedömningar och övrig riskhantering. Detta avsnitt beskriver dessa processer och dokument samt vilken terminologi som använts. Främst skiljer det sig åt vad gäller terminologi medan de grundläggande aspekterna i processerna bevarats över tid.

År 2004 publicerades *Direktiv för Försvarsmaktens informationsteknikverksamhet* (DIT 04) (Försvarsmakten, 2004a) som presenterade Försvarsmaktens IT-livscykelmodell som beskrev hur det var tänkt att Försvarsmakten skulle arbeta med IT-system från uppstått behov till infört IT-system och slutligen avveckling. För att stödja arbetet med *hot-, risk- och sårbarhetsanalyser* fanns en metod beskriven i *Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik*, H SÄK IT (Försvarsmakten, 2006).

År 2009 utgavs *Försvarsmaktens gemensamma riskhanteringsmodell* (Försvarsmakten, 2009). Tanken var att ha en modell för riskhantering som är gemensam för hela Försvarsmakten. Åren innan den gavs ut hade det uppdagats att "det gjordes olika bedömningar om hot, sårbarheter och risker på olika nivåer i Försvarsmakten. Begreppsfloran var oklar, ansvarsförhållandena otydliga och det saknades en samsyn inom olika områden" (Försvarsmakten, 2009).

Under 2013 kom tre handböcker rörande IT-system som syftade till att bättre beskriva arbetet med att ta fram *säkerhetsmålsättningar*, vilket i Försvarsmakten motsvarar riskhanteringsprocessen. Dessa handböcker, som förändrade Försvarsmaktens sätt att arbeta med säkerhetsmässiga analyser av IT-system, utgörs av:

- **Handbok Säkerhetstjänst Grunder, H SÄK Grunder** (Försvarsmakten, 2013a) som beskriver de delar av Försvarsmaktens riskhanteringsprocess som tillsammans benämns *säkerhetsanalys*. Denna process inleds med att identifiera och prioritera tillgångar och som genom riskbedömning kommer fram till vilka skydd som krävs. *Säkerhetsanalys* är en tillämpning av *Försvarsmaktens gemensamma riskhanteringsmodell.*
- **Handbok Säkerhetstjänst Informationssäkerhet, H SÄK Infosäk** (Försvarsmakten, 2013b) som ersatte H SÄK IT och beskriver säkerhetsanalysen och de steg som kommer före säkerhetsanalysen. Det vill säga *verksamhetsanalys* och *regelverksanalys* samt det steg som kommer efter säkerhetsanalysen, det vill säga *IT-säkerhetsspecifikation* (som beskriver systemet och säkerhetskraven).
- **Processhandbok IT-processen** (Försvarsmakten, 2013c) som beskriver de olika delarna av Försvarsmaktens IT-process och som ersatte DIT 04.

Utöver dessa handböcker har sedan 2004 *KSF 2.0, krav på säkerhetsfunktioner*, (Försvarsmakten, 2004b) varit en viktig del i Försvarsmaktens sätt att arbeta med säkerhetsmässiga analyser genom att tillhandahålla en uppsättning generella säkerhetskrav som styr och vägleder arbetet. Under 2012 ersattes KSF 2.0 med en uppdaterad version kallad *KSF 3.0* (Försvarsmakten, 2012). Den ersattes i sin tur 2014 med KSF 3.1 (Försvarsmakten, 2014).

Med anledning av den nya säkerhetsskyddslagen som trädde i kraft 1 april 2019 (Regeringskansliet, 2018) arbetar Försvarsmakten med att införa nya styrande dokument på området. Lagens nya benämning *säkerhetsskyddsanalys* kommer då att användas, ett begrepp som i lagen förklaras som att ”utreda behovet av säkerhetsskydd”. Med utgångspunkt i analysen är det därefter nödvändigt att ”planera och vidta de säkerhetsskyddsåtgärder som behövs”. Dessutom ska kontroller göras av ens säkerhetsskydd och sådant som är av vikt för säkerhetsskyddet ska anmälas och rapporteras. Lagen har särskilt fokus på konfidentialitet och delar in uppgifter i ”säkerhetsskyddsklasser utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet”. Det bör observeras att det i lagen inte finns något krav på att klassificering görs utifrån riktighet eller tillgänglighet. I propositionen (Regeringen, 2018) inför den nya lagen skrev regeringen att det vore ”mycket svårt för verksamhetsutövare att placera uppgifter i en viss säkerhetsskyddsklass utifrån vilka risker det skulle

innebära för Sveriges säkerhet om uppgifterna förvanskas, förstörs eller görs otillgängliga”. Att se till riktighet och tillgänglighet ingår dock på annat ställe i lagen, nämligen i form av att se till att inte uppgifter obehörigen ”ändras, görs otillgängliga eller förstörs” (Regeringskansliet, 2018).

3. Projektens resultat

Under de senaste tolv åren (2008–2019) har det genomförts fyra forskningsprojekt på FOI med inriktning på att ta fram stöd till Försvarsmaktens arbete med att analysera säkerheten i deras IT-system. Varje projekt har varit treårigt och haft syftet att ta fram stöd till Försvarsmakten med avseende på bättre riskhanteringsmetoder lämpade för deras system. I projekten har det genomförts minst en studie per år vilket resulterat i sammanlagt arton FOI-rapporter som beskriver studiernas resultat.

Studierna har i grova drag gått ut på att ställa identifierade behov i Försvarsmakten mot olika riskhanteringsmetoder. Nedan beskrivs vad varje projekts hade för mer specifikt fokus och detta sammanställs även i Tabell 1.

Tabell 1: De olika projektens specifika forskningsinriktningar från det äldsta projektet (P1) till det senaste (P4).

Forskningsinriktning	P1	P2	P3	P4
Utförarnas effekt.		●	●	●
Styrkor och svagheter med gängse metoder.	●	●	●	●
Riskbedömning genom jämförelser av risker.			●	
Tydligare beskrivningar av risker.			●	●
Återanvändning av analyser och bedömningar.		●	●	●

I det första projektet (2008–2010) var studierna fokuserade på att kartlägga Försvarsmaktens behov och utifrån det beskriva styrkor och svagheter med gängse metoder.

I det andra projektet (2011–2013) fortsatte arbetet med att hitta lämpliga metoder och beskriva deras styrkor och svagheter. Dessutom väcktes frågan om att återanvända analys- och bedömningsresultat samt utförarnas effekt.

I det tredje projektet (2014–2016) fortsatte studierna av återanvändning av analys- och bedömningsresultat samt utförarnas effekt. Dessutom undersöktes en metod där risker jämförs för att bättre kunna prioritera mellan dem samt en metod där risker beskrivs mer strukturerat.

I det fjärde projektet (2017–2019) fortsatte åter studierna av återanvändning av analys- och bedömningsresultat samt utförarnas effekt. Dessutom fortsatte undersökningen av hur hot beskrivs. Vidare studerades allmänna grunder för riskhanteringsprocessen som hur verksamheten kan analyseras och beskrivas, respektive hur risker ska mynna ut i skydd och hanteras över tid.

I avsnitten som följer presenteras resultaten från de fyra projekten i kronologisk ordning med de äldsta först.

3.1 Testning av metoder och verktyg för värdering av informationssäkerhet (2008–2010)

De studier som genomfördes i projektet *Testning av metoder och verktyg för värdering av informationssäkerhet* resulterade i sex FOI-rapporter (Figur 1). Resultaten från var och en av rapporterna beskrivs i Bilaga A.

Figur 1: Collage över de rapporter som producerades år 2008–2010.

När studier ska påbörjas inom ett nytt område är det nödvändigt att först få förståelse för nuläget. För att få förståelse för hur det fungerar när Försvarsmaktens nya IT-system ska godkännas med avseende på IT-säkerhet genomfördes en problemanalys. Under analysen kartlades vilka styrande dokument och vägledningar Försvarsmakten har som beskriver vad som behöver göras för att få ett IT-system godkänt. Fokus låg på att identifiera de arbetsmoment där någon typ av bedömning behöver genomföras samt om det fanns några otydligheter i beskrivningarna. De tidiga stegen av processen med att godkänna IT-system bedömdes vara det område där forskningsprojektet skulle kunna ge bäst bidrag till Försvarsmaktens arbete med att utveckla både metoder och handböcker – framförallt vad gäller hot-, risk- och sårbarhetsanalyserna.

Efter att ha fått en bild av hur Försvarsmakten arbetade med hot-, risk- och sårbarhetsanalyser för IT-system, blev nästa steg att undersöka hur andra gör sina riskbedömningar och om det finns andra analysmetoder som är bättre och som Försvarsmakten skulle kunna använda istället. För att på ett tydligt sätt kunna jämföra olika analysmetoder med den metod Försvarsmakten använde utvecklades proceduren TSAR (Test of Security Assessment Relevance and validity). Proceduren används först för att modellera de aktuella behoven avseende en analysmetod. Därefter jämförs dessa behov med modeller som beskriver varje metods egenskaper. Ett test kan därefter genomföras för att få fram en bedömning av vilken analysmetod som bäst motsvarar de specificerade behoven (relevansen) och hur väl metoden avspeglar verkligheten (validiteten).

Ett test med TSAR för Försvarsmaktens metoder ledde fram till slutsatsen att deras metoder är otydligt beskrivna med avseende på *hur* saker ska göras. Förutom att dessa otydliga beskrivningar försvårar för analytikerna blir det även svårt att utvärdera metodernas relevans och validitet. Ett test av metoder från forskningslitteraturen visade att de metoder som var mer övergripet beskrivna fick bättre resultat i TSAR, men också att ingen metod bedömdes vara tillräckligt relevant för Försvarsmakten. Att de mer övergripande metoderna fick bättre resultat berodde på att vagheten gjorde det svårt att säga att metoderna saknade de egenskaper som krävdes.

Avslutningsvis studerades frågan om vilka analysmetoder som kan vara relevanta för Försvarsmakten. Studien utgick ifrån analysmetoder föreslagna i forskningsartiklar. De flesta analysmetoder som diskuterades i litteraturen visade sig dock vara inriktade på delproblem snarare än problemet som helhet. Analysmetoderna delades därför in i grupper för att istället kunna bedöma hur relevant varje grupp av metoder skulle vara för Försvarsmakten. Resultaten visade att den grupp av metoder som är fokuserade på hantering av ovisshet i värderingsunderlagen är relevant för bedömningar som görs i början av IT-livscykelmodellen då hög ovisshet råder. I de senare stegen av IT-

livscykelmodellen bedömdes istället metodgruppen attackgrafer vara mest relevant.

3.2 Effektivare hot-, risk- och sårbarhetsanalyser (2011–2013)

De studier som genomfördes i projektet *Effektivare hot-, risk- och sårbarhetsanalyser* resulterade i sex FOI-rapporter (Figur 2). Resultaten från var och en av rapporterna beskrivs i Bilaga A.

Figur 2: Collage över de rapporter som producerades år 2011–2013.

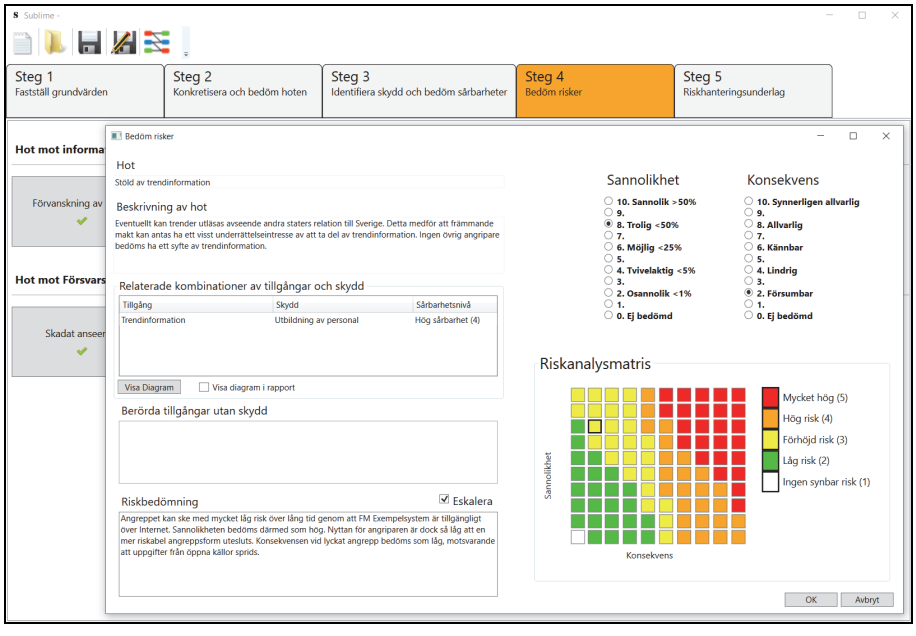
Under det föregående projektet (beskrivet i avsnitt 3.1) identifierades att det är många olika bedömningar som ska göras under en hot-, risk- och sårbarhetsanalys och att det tillgängliga stödet för genomförandet i vissa fall är bristfälligt. För att kunna svara på vilket stöd som behövs för att genomföra analysarbetet genomfördes en behovsanalys. Underlaget till behovsanalysen bestod av två delar: först en litteraturstudie av Försvarsmaktens dokumentation som beskriver hot-, risk- och sårbarhetsanalyser; därefter en intervjustudie. Genom analysen av dokumentationen gavs en bild av hur det var tänkt att analyserna skulle genomföras, medan intervjuerna med personal hos Försvarsmakten, FMV och externa konsulter gav en bild av hur analyserna genomförs i praktiken.

Behovsanalysen bekräftade en av slutsatserna från det föregående projektet att Försvarsmaktens dokumentation kring analyserna till stor del beskriver *vad* som ska göras, snarare än *hur* dessa resultat ska tas fram. En annan slutsats var att användandet av externa konsulter för genomförandet av analyserna påverkar den interna kunskapsnivån angående hur analysarbetet genomförs. När inte den egna personalen själva genomför analyserna missas en viktig poäng med analysarbetet som är att skapa medvetenhet kring vilka risker som finns med det nya IT-systemet. Om de som utför bedömningarna inte är en del av den egna verksamheten kommer verksamheten inte tillgodogöra sig värdefulla erfarenheter och kunskap och riskmedvetenheten kommer att minska. Exempel på andra behov som lyftes fram var bättre verksamhetskunskap och stöd för bedömning av sannolikhet och konsekvens. En möjlighet att minska kraven på personers kunskap skulle kunna vara att definiera standardsystem som bedömningarna kan utgå ifrån. I ett försök att visualisera Försvarsmaktens riskbedömningsmetod och samtidigt försöka möta delar av de behov av analysstöd som hade identifierats i behovsanalysen utvecklades en programvara med namnet *Sublime*[6] (Figur 3).

Med Sublime som utgångspunkt genomfördes en studie för att identifiera hur verktygsstöd skulle utvecklas för att möta de behov som identifierades i behovsanalysen. Studien resulterade i ett lösningsförslag som bedömdes kunna möta merparten av de identifierade behoven. Arbetet med metodstödet resulterade även i nedanstående forskningsfrågor:

- Vilken roll spelar verksamhetsanalysen och hur ska den utformas?
- Hur ska hot identifieras?
- Vilken precision behöver riskbedömningarna ha?
- Hur påverkar analysgruppens sammansättning resultaten?

[6] Sublime beskrivs ytterligare i avsnitt B.3.



Figur 3: Bedömning av risker i Sublime.

En annan typ av stöd vid genomförandet av analyserna är det underlag, i form av information, som ligger till grund för de bedömningar som görs. Genom att sammanställa vilken information som ett antal etablerade analysmetoder beskrev som nödvändig var det möjligt att få en bild av informationsbehovet. Enbart cirka 15 % av den information analysmetoderna använder har specifikt med säkerhet att göra. Mycket av informationen som krävs har istället med verksamheten i stort att göra såsom processer och aktörer. En slutsats var att informationen som behövs generellt sett beskriver verksamheten snarare än informationsobjekt, systembeteenden och tekniska lösningar. Det kunde även konstateras att de etablerade metoderna som studerades inte uttryckligen baseras på vetenskapliga teorier. Vissa metoder bedömdes till och med helt sakna vetenskapligt teoretisk grund.

Som ett sidospår genomfördes även en studie tillsammans med ett projekt finansierat av MSB. Studien resulterade i den första vetenskapliga sammanställningen som gjorts av forskningen om vad som påverkar huruvida användare följer informationssäkerhetsbestämmelser. Dessa teorier kan användas som underlag när exempelvis effekten av administrativa skyddsåtgärder ska bedömas.

3.3 Bedömning och analys av IT-system (2014–2016)

De studier som genomfördes i projektet *Bedömning och analys av IT-system* resulterade i tre FOI-rapporter (Figur 4). Resultaten från var och en av rapporterna beskrivs i Bilaga A.

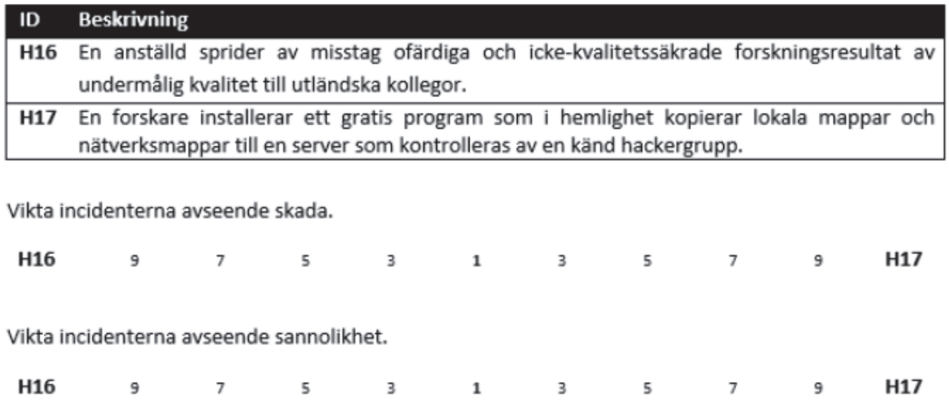
Figur 4: Collage över de rapporter som producerades år 2014–2016.

Riskhanteringsprocessen resulterar i att ett antal skyddsåtgärder identifieras. Dessa skyddsåtgärder omsätts därefter till krav som brukar omnämnas som tillkommande krav. Ett IT-system måste även förhålla sig till de krav som fås från Krav på säkerhetsfunktioner (KSF). En studie genomfördes för att analysera kraven i ett antal genomförda säkerhetsmålsättningar i syfte att se hur stor del av kraven som täcktes in av KSF. Studien visade på att ungefär hälften av kraven i säkerhetsmålsättningarna täcktes in av KSF, medan andra hälften utgjordes av tillkommande krav. Det verkade alltså finnas utrymme att utöka KSF med fler generella krav som bättre täcker in typiska kravmassor. Men att ta fram förslag på nya KSF-krav visade sig svårt eftersom kraven inte får bli alltför specifika och exempelvis peka ut specifika säkerhetslösningar i form av befintliga produkter. Det noterades även att de tillkommande kraven i stor utsträckning var dåligt formulerade och att de krav som rörde tillgänglighet var svåra att hantera.

Studien omfattade även en analys av hur kraven i KSF kan omvandlas till standardlösningar som utgår ifrån vanliga komponenter och procedurer. Den resulterande rekommendationen blev att KSF borde kompletteras med designmönster och information om produkter som möter KSF-kraven. Det

noterades även att det inte är helt rättframt att hantera KSF-kraven i fall med sammansatta system.

Nästa område som studerades var bedömningarna av sannolikhet och konsekvens som i behovsanalysen lyftes fram som något som behövde bättre stöd. Eftersom det kan vara lättare att göra en jämförande bedömning än en absolut sådan gjordes en studie på just jämförelsebaserade bedömningar för att se om det är enklare samt om resultaten blir mer tillförlitliga och precisa. Med en jämförelsebaserad bedömning besvaras frågan *hur sannolikt är hot A jämfört med hot B?* istället för den absoluta bedömningen som besvarar *hur sannolikt är hot A?*. De två metoderna utvärderas i en enkätstudie (Figur 5).



ID	Beskrivning
H16	En anställd sprider av misstag ofärdiga och icke-kvalitetssäkrade forskningsresultat av undermålig kvalitet till utländska kollegor.
H17	En forskare installerar ett gratis program som i hemlighet kopierar lokala mappar och nätverksmappar till en server som kontrolleras av en känd hackergrupp.

Vikta incidenterna avseende skada.

H16 9 7 5 3 1 3 5 7 9 **H17**

Vikta incidenterna avseende sannolikhet.

H16 9 7 5 3 1 3 5 7 9 **H17**

Figur 5: Exempel på enkäten som utvärdera jämförelsebaserade hotbedömningar. Från Hallberg m.fl. (2015).

Den jämförelsebaserade metoden som utvecklades visade sig vara bättre än den traditionella metoden när experter (snarare än lekmän) gjorde bedömningarna. Samtidigt noterades att det med en jämförelsebaserad metod krävs att många bedömningar görs när antalet hot ökar om alla hot ska jämföras med varandra vilket kan krävas för träffsäkerheten. Det observerades även behov av att studera hur de resulterande vikterna för varje hot ska tolkas i det fortsatta analysarbetet.

En annan möjlig faktor som skulle kunna påverka bedömningarna av sannolikhet och konsekvens är hur hotbeskrivningen utformas. Ett experiment genomfördes för att se om utformningen av hotbeskrivningen kan tänkas ha någon påverkan. För att utvärdera olika sorts utformning ställdes hot beskrivna i löpande text mot samma hot presenterade i strukturerad tabellform. Löpande text förutsågs vara enklare att förhålla sig till samtidigt som tolkningsutrymmet skulle bli större. Inga statistiskt signifikanta skillnader mellan metoderna erhölls dock.

Under studien av hotbeskrivningens utformning observerades även att det inte framgår vilka hot som redan hanterats av den generella uppsättningen krav i KSF och vilka som därmed är nödvändiga att bedöma i riskbedömningsarbetet. Detta kan leda till dubbelarbete. Att tillhandahålla kataloger över generella hot skulle kunna underlätta. Men samtidigt skulle sådana kataloger kunna leda till slentrianmässigt analysarbete som missar det specifika med det analyserade IT-systemet.

Det visade sig generellt vara svårt att bedöma antagonistiska risker för IT-system. Detta kan jämföras med liknande typer av bedömningar. Tabell 2 visar hur samstämmiga (eniga) olika områdens experter är vad gäller bedömningar. Om samstämmigheten är ett (1) betyder det *full enighet* och om samstämmigheten är noll (0) betyder det *ingen enighet*. I tabellen är resultat från projekten kursiverade. Det syns att det är betydligt svårare att bedöma hot (riskers) sannolikhet än det är att bedöma deras möjliga konsekvenser.

Tabell 2: Samstämmighet mellan experter inom olika områden. Anpassad från den akademiska forskningsartikeln Hallberg m.fl. (2017) som producerats i projekten och som citerar andras resultat, förutom de kursiverade siffrorna som kommer från en av projektets rapporter Bengtsson m.fl. (2016).

Typ av expert eller bedömning	**Samstämmighet**
Meteorolog	0,95
Revisor	0,76
Riskbedömning av våldsbenägenhet	0,76
Intrångsdetektion	0,64
Godtyckliga kodexekveringsangrepp	0,56
Patologer	0,55
Mjukvarusårbarhetsupptäckt	0,54
Bedömning av konsekvens för IT-säkerhetsrisker	*0,51*
Tillgänglighetsangrepp (DoS)	0,48
Kliniska patologer	0,40
Börsmäklare	0,32
Bedömning av sannolikhet för IT-säkerhetsrisker	*0,20*

3.4 Metodik för säkerhetsmålsättningsarbete (2017–2019)

De studier som genomfördes i projektet *Metodik för säkerhetsmålsättningsarbete* resulterade i tre FOI-rapporter (Figur 6), utöver denna rapport. Resultaten från var och en av rapporterna beskrivs i Bilaga A.

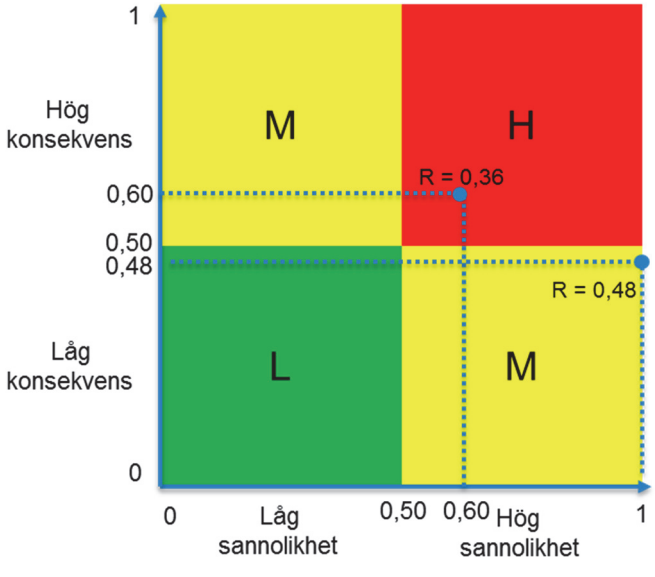
Figur 6: Collage över de rapporter som producerades år 2017–2019.

En studie genomfördes för att undersöka hur organisationers riskacceptans-kriterier formuleras, vilket avgör på vilka grunder risker kan accepteras. Att acceptera de kvarvarande riskerna innebär ett beslut om vilka skyddsåtgärder och övrig hantering av risker som är lämpliga. En farhåga med felaktiga eller obefintliga riskacceptanskriterier är att IT-systemet medför allt för höga risker. Alternativt kan skydd ha införs utan att relationen mellan risk, kostnad och nytta beaktats, troligtvis på grund av svårigheten att översätta mellan de tre enheterna. Dessutom är det svårt att veta hur legitima användare och potentiella angripare anpassar sig efter införda skydd och därmed vilken effekt en skyddsåtgärd faktiskt får. Av denna anledning lyfts det fram ett behov av att regelbundet revidera de bedömningar som gjorts.

I studien noterades också att bedömnings- och analysresultat beror på vem som bedömer eller analyserar. Förutom personernas kunskap lyser också deras värderingar, bias, riskbenägenheter och liknande igenom. Detta ställer krav på kommunikation om gjorda antaganden och ovisshet.

Dessutom noterades det att bedömningarna inte behöver vara mer exakta än vad som krävs för att välja skydden. Vidare lyftes det fram att metoder som baseras

på erfarenhet kan vara ett komplement till de mer strikta riskbedömnings-metoderna anpassade för aktuarier. Angående presentation av resultaten var en slutsats att de populära riskmatriserna är tveksamma att använda. Matriserna kan nämligen ge ett felaktigt intryck av prioriteringsordningen mellan risker när konsekvensen är hög men sannolikheten låg (eller tvärtom). Detta illustreras av Figur 7. Konsekvens från 0 till 1 visas på y-axeln och alla konsekvenser som är mer än 0,5 räknas som höga, medan resterande räknas som låga. På motsvarande sätt fungerar x-axeln som visar sannolikheten. Matrisens fyra färglagda fält visar på en typisk indelning av risken där låga risker hamnar i det gröna fältet (L = låg risk), medelrisker i något av de gula fälten (M = medelrisk) och höga risker i det röda fältet (H = hög risk). För en risk med konsekvens på 0,48 och sannolikhet på 1 blir riskvärdet (produkten) 0,48 vilket ligger i ett gult fält. För en risk med konsekvens på 0,60 och sannolikhet på 0,60 blir riskvärdet 0,36 vilket ligger i det röda fältet. Ett riskvärde på 0,36 visas alltså som en värre (högre) risk än ett riskvärde på 0,48, trots att det omvända vore det korrekta.[7]



Figur 7: Ett exempel på en riskmatris och med indikation på dess begränsningar.

[7] Ett annat exempel kan ges av att en ökning av sannolikhet och konsekvens från 0 jämförs med en ökning av desamma från 0,5. Om ökningen i båda fallen och för både sannolikhet och konsekvens är 0,1 blir skillnaden i riskvärde $0,1^2 = 0,01$ i det första fallet och $(0,5+0,1)^2-0,5^2 = 0,11$ i det andra fallet. En lika stor ökning av vardera konsekvens och sannolikhet leder alltså till en betydligt större skillnad i riskvärde (förflyttning upp mot matrisens övre högra hörn).

I det föregående projektet (beskrivet i avsnitt 3.3) gjordes en inledande studie kring hur hotbeskrivningens utformning påverkar bedömningen av sannolikhet och konsekvens. Detta kompletterades med en ny studie med fokus på hur hot lämpligast beskrivs. En slutsats var att aktören (antagonisten) behöver specificeras med information om exempelvis kapacitet, intention och tillfälle. Människan bakom hotet är ofta det svåraste att modellera och att då ha mer detaljer om aktören kan förbättra möjligheterna till ett fullgott resultat från riskbedömningarna.

Utgångspunkten för allt analysarbete av IT-system är den verksamhets-beskrivning som en genomförd verksamhetsanalys resulterar i. Genom att vara utgångspunkten för arbetet har den stor betydelse för det efterföljande arbetet. En studie genomfördes för att identifiera vad verksamhetsbeskrivningen kan bidra med i ett informationssäkerhetsperspektiv, hur verksamhetsanalysen bör genomföras och vilka informationsmängder som bör ingå i den resulterande verksamhetsbeskrivningen. En slutsats är att Försvarsmakten bör lyfta fram att verksamhetsbeskrivningen inte enbart används som underlag för risk-bedömningar, utan kan påvisa behov av att genomföra förändringar av verksamheten, exempelvis genom införande av nya IT-system.

Studien visade även på att Försvarsmakten har mer säkerhetsfokus och mindre ekonomifokus än litteratur som beskriver verksamhetsanalyser i allmänhet. På samma sätt som i studierna av hot-, risk- och sårbarhetsanalyserna drogs slutsatsen att tillgängliga metodbeskrivningar är otydliga avseende *hur* analysarbetet ska genomföras. En ytterligare slutsats är att vilka analytiker som genomför verksamhetsanalysen har en stor påverkan på den resulterande verksamhetsbeskrivningen. Det identifierades behov av att genomföra en studie för att hitta rätt avvägning mellan att som metodstöd tillhandahålla standardiserade mallar och att tillhandahålla allmänna råd och inspiration.

4. Slutsatser och framtida forskning

I detta kapitel beskrivs slutsatser från de tolv åren av forskning som genomförts i projekten. Kapitlet är indelat i de olika specifika forskningsinriktningar som ingått i projekten och upprepas här från inledningen:

- Försvarsmaktens behov på området (avsnitt 4.1).
- Utförarnas effekt (4.2).
- Styrkor och svagheter med gängse metoder (4.3).
- Riskbedömning genom jämförelse mellan risker (4.4).
- Tydligare beskrivningar av risker (4.5).
- Återanvändning av analyser och bedömningar (4.6).

Den sistnämnda forskningsinriktningen binder ihop de övriga inriktningarna och det bedöms finnas goda möjligheter att studera det vidare. I det avsnittet ges därför ett antal förslag på framtida forskning utöver slutsatser.

4.1 Försvarsmaktens behov på området

I projekten genomfördes behovsanalyser kontinuerligt för att inrikta forskningsstudierna. Ett behov som framkom var att den interna kunskapsnivån inom riskbedömningar behöver upprätthållas, trots eventuell användning av externa konsulter för genomförandet av bedömningar och analyser. Ett annat närliggande behov är att se till att de specifika utförarna påverkar resultatet i mindre mån, det vill säga att personberoendet minskas.

Ett ytterligare behov som framkom var att det behövs bättre instruktioner för genomförandet av riskhanteringsarbetet. Vilken metod som används för riskhanteringsarbetet har betydelse för resultatet. En metod som inte beskriver allt som ska göras, beskriver fel saker eller är otydlig, gör arbetet svårgenomförbart.

De följande avsnitten beskriver närmare hur studierna försökte uppfylla de framkomna behoven.

4.2 Utförarnas effekt

Vem som utför riskhanteringsarbetet har betydelse, exempelvis vad gäller vem som bedömer riskerna. Detta har flera orsaker: olika personer talar olika språk, har olika perspektiv eller olika värderingar. Därtill tar kanske en del personer utgångspunkt i ett brett omfång vad gäller inkluderade tillgångar medan andra tar ett smalare omfång, vilket är särskilt komplicerande med tanke på IT-systems sammansatta natur. Dessutom kan det finnas skillnader i riskbenägenhet, vilket

exempelvis kan få betydelse ifall vissa riskbedömare börjar sin (inre) konsekvensskala vid två (på en skala som går från ett till fem), medan andra börjar den vid ett, vilket i sin tur leder till olika incitament att införa skydd. Ytterligare en skillnad mellan riskbedömare är att de har olika hotkataloger, det vill säga att de bedömer olika uppsättningar av risker. Som helhet gör de individuella skillnaderna att olika personer gör olika bedömningar.

Vem som utför riskhanteringsarbetet har alltså betydelse och skillnaderna i resultat är ganska stora. Detta ställer krav på att det i möjligaste mån framgår vilka resultat som baseras på subjektivitet och i vilken utsträckning. En ansats för att öka spårbarheten är att säkerställa att bedömare tydligare redovisar gjorda antaganden, såsom vilken ovisshet som finns i bedömningarna. Ett första steg är inte nödvändigtvis forskningsmässigt, utan att säkerställa att metoder och handböcker uppmanar bedömarna att inkludera sådan information i resultaten. Kopplat till detta finns också krav på förbättrad kommunikation mellan intressenter och därmed möjligheterna rörande visualisering av resultat och verktygsstöd. Detta relaterar till Sublime, som fortsätter att utvecklas av FOI. De flesta forskningsinsatser på området kan förmodligen ge mer användbara resultat om de utnyttjar möjligheterna med ett verktygsstöd där teori kan testas och utvärderas. Detta relaterar också till att försiktighet bör iakttas vid användning av riskmatriser för kommunikation av risk eftersom sådana matriser kan ge en skev bild i vissa situationer. Närliggande detta är svårigheten att översätta mellan olika typer av risker.

4.3 Styrkor och svagheter med gängse metoder

En ansats är att nyttja metoder från forskningslitteraturen. I projekten togs kvalitetskriterier fram för att utvärdera gängse metoder. Metoderna visade sig vara av begränsad nytta för Försvarsmakten eftersom det krävs stora anpassningar samt att det inte är metoder som tar ett helhetsgrepp. Detta är negativt eftersom det gör det svårare att förbättra Försvarsmaktens riskhanteringsprocess. Samtidigt är det positivt att Försvarsmakten inte har missat någon perfekt metod och detta utgör därför en sorts kvalitetsmärkning. Vidare innebär svårigheten att hitta en färdig metod att det finns gott om utrymme att forska fram en bättre sådan och det är också det återstoden av kapitlet fokuserar på.

4.4 Riskbedömning genom jämförelser av risker

Eftersom inga metoder, som kunde nyttjas direkt, identifierades genomfördes studier som försökte identifiera förbättringar på mer specifika delar av Försvarsmaktens gällande metodik. Ett sådant försök var att undersöka om en

jämförelsebaserad metod för riskbedömning vore bättre än den gällande metoden där risker bedöms i absoluta tal. Med tanke på att resultatet främst ska vara till för att prioritera bland risker vore det rimligt att en jämförelsebaserad metod används. En sådan metod visade sig vara bättre för experter än vad en traditionell (absolutbaserad) metod var. Det finns dock svårigheter med jämförelsebaserade metoder, exempelvis att det måste väljas vilka av alla möjliga jämförelser som ska göras eftersom att göra alla blir alltför tidsödande. Dessutom måste de erhållna resultaten trots allt normalt översättas till absolut risk i slutet av bedömningsarbetet.

4.5 Tydligare beskrivningar av risker

Ett annat försök att ta fram en metodförbättring rörde hur risker och de underliggande hoten ska beskrivas. Att bestämma hotbeskrivningars innehåll är inte lätt. Det rekommenderas ofta att strukturerade hotbeskrivningar (exempelvis tabeller) används istället för löptext. I studierna visade sig detta dock inte ha någon påverkan på resultatet eller på utförarnas belastning. Vad som dock framkom i studierna var att hotaktören (antagonisten) behöver specificeras tydligt för att kunna bedömas. Att bedöma antagonister är dock huvudsakligen en underrättelsefråga snarare än en fråga för forskningen.

4.6 Återanvändning av analyser och bedömningar

För att riskhanteringsarbetet ska leda till bättre resultat som produceras på ett mer kostnadseffektivt sätt är en möjlighet att begränsa mängden bedömningar som behövs och görs. IT-system har normalt en standardmässig utformning och generell hotbild, vilket borde ge upphov till likartade riskbedömningar. Om specifika bedömningar kunde ersättas av redan utförda standardiserade bedömningar skulle personberoendet minska och effektiviseringsvinster möjliggöras. Det vore därför intressant att besvara följande forskningsfråga:

1. Hur stor skillnad blir det normalt mellan resultat från riskbedömningar för två olika IT-system?

Samtidigt förändras verksamheten över tid, tekniska framsteg görs och hotbilden förändras och anpassar sig efter det riskhanteringsarbete som utförts. Det medför att säkerhetsskyddet av ett system aldrig är färdigt utan så länge systemet är i drift måste skydden revideras i takt med förändringarna. Dessutom är frågan om verksamhetsanalyser, riskbedömningar och annat i riskhanteringsprocessen utförs vid rätt tillfälle. När ett IT-system inte än finns kan säkerhetsarbetet i större utsträckning påverka systemet, men å andra sidan är det svårare att veta hur systemet faktiskt kommer att se ut och vilka risker det faktiskt kommer vara

förknippat med. Detta för tankarna till mer *agilt* informationssäkerhetsarbete och en relevant forskningsfråga är därför:

2. Hur beständiga är riskbedömningar över tid och hur ska man hålla sig underrättad om förändringar som sker av system, hot och kontext?

I förlängningen är det också intressant att undersöka hur stor skillnad i effekt olika riskbedömningsresultat normalt ger med tanke på vilka skydd som bedöms behöva införas. Möjligtvis är vissa riskbedömningar inte meningsfulla att göra då det enbart finns en begränsad mängd möjliga skydd, alternativt för att skyddens påverkan på kostnad och nytta är alltför svår att jämföra med risk-minskningen. Utifrån detta kan följande forskningsfrågor formuleras:

3. Hur stor skillnad medför olika riskbedömningsresultat senare i processen i form av rekommenderade skyddsåtgärder?

Om skillnaden i analysresultat blir liten kan det vara mer meningsfullt att för standardmässiga IT-system införa standardmässiga skydd och erfarenhetsbaserade beslut utan några omfattande riskbedömningar. Detta tangerar delvis tanken med KSF:s standardmässiga säkerhetskrav.

En konsekvens av att använda listor över standardhot och standardskydd kan vara att analytikerna slutar att tänka själva, vilket kan leda till att specifika hot och skydd för det specifika IT-systemet missas. På samma tema måste erfarenheter tillvaratas från analyser och bedömningar utförda av personer som kanske inte längre är kvar i verksamheten. Dessutom kan standarduppsättningarna vara så informativa om systemen som helhet att uppsättningarna måste hållas hemliga, vilket minskar nyttan av dessa. Som helhet mynnar detta ut i följande forskningsfråga:

4. Hur ska riskbedömningarna likriktas samtidigt som unika insikter tillvaratas?

5. Referenser

Nedan följer de referenser som används i rapporten, indelade efter vilket avsnitt de primärt används i och uppräknade kronologiskt.

5.1 Riskhanterings ursprung

Courtney, R.H. Jr. 1977. Security risk assessment in electronic data processing systems. Security risk assessment in electronic data processing systems vol. 1:97.

Covello V.T., Mumpower J. 1985. Risk Analysis and Risk Management: An Historical Perspective. Risk Analysis, vol. 5:2.

Feynman, R. 1986. Personal Observations on the Reliability of the Shuttle, Appendix IIF, Report of the Presidential Commission on the Space Shuttle Challenger Accident.

Baskerville, R. 1991. Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, vol. 1:2.

Rechard, R.P. 1999. Historical Relationship Between Performance Assessment for Radioactive Waste Disposal and Other Types of Risk Assessment. Risk Analysis, vol. 19:5.

Soo Hoo, K.J. 2000. How Much Is Enough? A Risk-Management Approach to Computer Security. Consortium for Research on Information Security and Policy (CRISP). Stanford University.

Dionne, G. 2013. Risk Management: History, Definition and Critique. Working Paper 13-02. CIRPEE.

Durán, F.A., Wyss, G.D., Sandoval, J. 2013. Security Risk: A Brief History and New Risk Management Approach. Sandia National Laboratories.

Aven, T. 2016. Risk assessment and risk management: Review of recent advances on their foundation, European Journal of Operational Research, vol. 253:1.

Golob, S., Kožuh, M. 2016. Methodology for determining the risk acceptance criteria for the Seveso establishments, Process Safety and Environmental Protection, vol. 100.

Hansson, S. O., Hirsch Hadorn, G. 2017. Argument-based decision support for risk analysis, Journal of Risk Research. Routledge, vol. 9877.

5.2 Relaterad forskning

Broberg Wulff, M., Knoph, J., Andersson, C., Lewerentz, B. 2000. Hotanpassning och krishantering - Erfarenheter av Y2K. FOA-R–00-01681-240--SE. Försvarets Forskningsanstalt.

Hallberg, J., Hunstad, A., Bond, A., Peterson, M., Åhlsson, N. 2004. System IT Security Assessment. FOI-R--1468--SE. Totalförsvarets forskningsinstitut.

Hallberg, J., Hallberg, N., Hunstad, A. 2006. Crossroads and XMASS: Framework and Method for System IT Security Assessment. FOI-R--2154--SE. Totalförsvarets forskningsinstitut.

Hallberg, J., Hunstad, A., Hallberg, N. 2007a. Handbok för IT-säkerhetsvärdering. FOI Memo 2099. Totalförsvarets forskningsinstitut.

Hallberg, J., Bengtsson, J., Andersson, R. 2007b. Refinement and realization of security assessment methods. FOI-R--2387--SE. Totalförsvarets forskningsinstitut.

Palm, T. 2008. Försvarsmaktens gemensamma riskhanteringsmodell. FOI-R--2591--SE. Totalförsvarets forskningsinstitut.

Harling, S., Berg, A., Karlsson, M., Magnusson, P., Hartmann, M. 2010. Metodik för riskbedömning. FOI-R--3030--SE. Totalförsvarets forskningsinstitut.

Karlzén, H., Westerdahl, L. 2010. Säkerhetsanalys av ett generellt IP-nät, del 1. FOI Memo 3448. Totalförsvarets forskningsinstitut.

Westerdahl, L. 2010. Säkerhetsanalys av ett generellt IP-nät, del 2. FOI Memo 3449. Totalförsvarets forskningsinstitut.

Winehav, M., Nevhage, B., Lusua, J., Mork, J. C., Lindgren, J., Erdeniz, R. 2011. FOI:s Modell För Risk- Och Sårbarhetsanalys (FORSA). FOI-R--3288--SE. Totalförsvarets forskningsinstitut.

Gustavi, T., Johansson, F., Johansson, R., Jändel, M., Kaati, L., Mårtenson, C., Oskarsson, D. 2011. Analytiska verktyg - en översikt av metoder och modeller för underrättelseanalys. FOI-R--3310--SE. Totalförsvarets forskningsinstitut.

Winehav, M., Molin, L., Veibäck, E., Larsson, P. 2012. Metod- och inventeringsstöd till sektorsövergripande risk- och sårbarhetsanalys. FOI-R--3516--SE. Totalförsvarets forskningsinstitut.

Winehav, M., Nevhage, B., Veibäck, E., Stenström, M., Larsson, P., Mobjörk, M. 2013. Underlag till nationell riskbedömning 2012. Resultat från den svenska

nationella riskbedömningen 2012. FOI-R--3612--SE. Totalförsvarets forskningsinstitut.

Sonnsjö, H., Mobjörk, M. 2013. Om indirekta, komplexa och oönskade händelser. Att analysera risker med stor osäkerhet. FOI-R--3649--SE. Totalförsvarets forskningsinstitut.

Hermelin, J., Karlzén, H., Nilsson, P. 2014. Informationssäkerhet och ekonomi. Ett skannande projekt av aktuell forskning. FOI-R--3927--SE. Totalförsvarets forskningsinstitut.

Malmberg Andersson, F., Gozzi, J., Hedtjärn Swaling, V. 2014. Risk- och sårbarhetsanalys för Totalförsvarets forskningsinstitut (FOI) 2014. Enligt förordningen (2006:942) om krisberedskap och höjd beredskap. FOI-R--3959--SE. Totalförsvarets forskningsinstitut.

Malmberg Andersson, F., Denward, C. 2015. Studie: Metodutveckling inom processen för arbetet med risk- och sårbarhetsanalyser. FOI Memo 5294. Totalförsvarets forskningsinstitut.

Hedtjärn Swaling, V., Albinsson, P.-A., Bengtsson, J., Denward, C., Mossberg Sonnek, K., Sparf, A. 2016. Utmaningar för den kommunala risk- och sårbarhetsanalysen. En studie baserad på intervjuer med säkerhetssamordnare i Västra Götalands län. FOI-R--4245--SE. Totalförsvarets forskningsinstitut.

Forsén, R. 2016. Oexploderad ammunition, OXA, på övnings- och skjutfält. Beskrivning av några metoder för riskanalys. FOI-R--4383--SE. Totalförsvarets forskningsinstitut.

Albinsson, P.-A., Bengtsson, J., Denward, C., Sparf, A., Hedtjärn Swaling, V. 2018. Handbok för kommunalt RSA-arbete. FOI-R--4656--SE. Totalförsvarets forskningsinstitut.

5.3 Försvarsmaktens processer och terminologi

Försvarsmakten. 2004a. Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT 04). HKV 09 626:783 69.

Försvarsmakten. 2004b. Beslut om krav på godkända säkerhetsfunktioner, ver. 2.0. 10 750:78976.

Försvarsmakten. 2006. Handbok för Försvarsmaktens säkerhetstjänst, Informationsteknik. H SÄK IT 2006. 10 440:66817.

Försvarsmakten. 2009. Försvarsmaktens gemensamma riskhanteringsmodell. 01 310:900666.

Försvarsmakten. 2012. KSF. Krav på IT-säkerhetsförmågor hos IT-system. v3.0. 10 750:64354.

Försvarsmakten. 2013a. Handbok för Försvarsmaktens säkerhetstjänst, Grunder. H SÄK Grunder. 10 440:55631.

Försvarsmakten. 2013b. Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet. H SÄK Infosäk. 10 440:59810.

Försvarsmakten. 2013c. Processhandbok IT-processen. Bilaga till Fastställande av processhandbok IT-processen. FM2013-4411:1.

Försvarsmakten. 2014. KSF. Krav på IT-säkerhetsförmågor hos IT-system. v3.1. FM2014-5302:1.

Regeringen. 2018. Regeringens proposition 2017/18:89. Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag. Prop. 2017/18:89.

Regeringskansliet. 2018. Säkerhetsskyddslag (2018:585).

5.4 Rapporterna

1. Bengtsson, J., Hallberg, J. 2008. Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete. FOI-R--2531--SE. Totalförsvarets forskningsinstitut.
2. Bengtsson, J., Hallberg, J., Hunstad, A., Löfvenberg, J. 2009a. The TSAR procedure – Test of security assessment relevance and validity. FOI-R--2624--SE. Totalförsvarets forskningsinstitut.
3. Bengtsson, J., Hallberg, J. 2009. Test av relevans och validitet avseende säkerhetsvärdering – En studie av Försvarsmaktens metoder för säkerhetskravställning och sårbarhetsanalys. FOI-R--2625--SE. Totalförsvarets forskningsinstitut.
4. Bengtsson, J., Hallberg, J., Hunstad, A., Lundholm, K. 2009b. Tester av metoder för värdering av informationssäkerhet. FOI-R--2901--SE. Totalförsvarets forskningsinstitut.
5. Bengtsson, J., Lundholm, K., Hallberg, J., Hunstad, A., Löfvenberg, J. 2010a. The TSAR procedure rev. 1 – Test of Security Assessment Relevance. FOI-R--3061--SE. Totalförsvarets forskningsinstitut.
6. Bengtsson, J., Hallberg, J., Lundholm, K. 2010b. Framtida metoder för värdering av IT-säkerhet. FOI-R--3094--SE. Totalförsvarets forskningsinstitut.
7. Lundholm, K., Bengtsson, J., Hallberg, J. 2011. Hot-, risk- och sårbarhetsanalys – Grunden för IT-säkerhet inom Försvarsmakten. FOI-R--3349--SE. Totalförsvarets forskningsinstitut.

8. Bengtsson, J., Hallberg, J., Lundholm, K. 2012a. Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten. FOI-R--3452--SE. Totalförsvarets forskningsinstitut.
9. Sommestad, T., Bengtsson, J., Hallberg, J. 2012. Varför följer inte användarna bestämmelser? – En metaanalys avseende informationssäkerhetsbestämmelser. FOI-R--3524--SE. Totalförsvarets forskningsinstitut.
10. Bengtsson, J., Hallberg, J., Sommestad, T. 2012b. Verktygsstöd för hot-, risk- och sårbarhetsanalyser – realiseringsförslag. FOI-R--3552--SE. Totalförsvarets forskningsinstitut.
11. Sommestad, T., Bengtsson, J., Hallberg, J. 2013. Informationsbehov vid säkerhetsanalyser: En systematisk genomgång av etablerade metoder. FOI-R--3723--SE. Totalförsvarets forskningsinstitut.
12. Hallberg, J., Bengtsson, J., Sommestad, T. 2013. Effektivare hot-, risk- och sårbarhetsanalyser – Vad blev det för resultat?. FOI-R--3785--SE. Totalförsvarets forskningsinstitut.
13. Bengtsson, J., Sommestad, T., Holm, H. 2014. IT-säkerhetskrav i Försvarsmakten – KSF3 och tillkommande säkerhetskrav. FOI-R--4000--SE. Totalförsvarets forskningsinstitut.
14. Hallberg, J., Bengtsson, J., Karlzén, H. 2015. Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker - En studie av vikt. FOI-R--4152--SE. Totalförsvarets forskningsinstitut.
15. Bengtsson, J., Hallberg, J., Karlzén, H. 2016. Beskriva och bedöma hot mot IT-system – Varför är det svårt?. FOI-R--4330--SE. Totalförsvarets forskningsinstitut.
16. Karlzén, H., Bengtsson, J., Hallberg, J. 2018a. Riskacceptans – Kostnadseffektiv riskhantering för IT-system. FOI-R--4521--SE. Totalförsvarets forskningsinstitut.
17. Hallberg, J., Bengtsson, J., Karlzén, H. 2018. Beskrivning av hot vid säkerhetsanalyser. Innehåll och utformning. FOI-R--4676--SE. Totalförsvarets forskningsinstitut.
18. Karlzén, H., Jansson, O., Bengtsson, J., Bildsten, C., Valassi, C. 2019. Verksamhetsanalys – Genomförande och betydelse för säkra IT-system. FOI-R--4857--SE. Totalförsvarets forskningsinstitut.

Bilaga A. FOI-rapporter

För vart och ett av de följande avsnitten ges en sammanfattning av en rapport tillsammans med en bild av rapportens framsida. Dessa sammanfattningar är utförligare beskrivningar av rapporterna än vad som ges i sammanfattningen av projektens resultat i kapitel 3.

Rapporterna kommer i kronologisk ordning med den äldsta först. En referenslista för rapporterna finns i avsnitt 5.4. För vidare läsning går samtliga rapporter att ladda ner på foi.se.

A.1 Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete

Rapporten *Värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete* (Bengtsson och Hallberg, 2008) beskriver den första studien som genomfördes inom projektet *Testning av metoder och verktyg för värdering av informationssäkerhet*. Det primära syftet med studien var att bygga upp kunskap inom FOI om hur det går till när en tillräcklig IT-säkerhetsnivå ska säkerställas för nya IT-system som tas fram inom Försvarsmakten.

Studien utgick från Försvarsmaktens IT- livscykelmodell i DIT 04 som beskriver arbetsgången från ett identifierat verksamhetsbehov till att uppnå ett godkänt IT-system i drift (Försvarsmakten, 2004a). Dessutom utgick studien från då gällande H SÄK IT som innehöll beskrivningar för vad olika analysaktiviteter förväntades omfatta eller resultera i (Försvarsmakten, 2006).

I rapporten presenteras modeller över de olika analysaktiviteterna och hur dessa förhåller sig till varandra. I dessa analysaktiviteter identifierades totalt 49 värderingsaspekter. Med *värderingsaspekter* avsågs situationer där det krävdes någon typ av värdering (bedömning) för att kunna genomföra uppgiften, fatta välgrundade beslut eller producera efterfrågade resultat. Ett exempel är att systemägaren ska anmäla ”otillräcklig säkerhetsnivå till militärdistriktet/MUST

ITSA och produktägaren", där värderingsaspekten utgörs av att bedöma huruvida systemet har en otillräcklig säkerhetsnivå.

Till de 49 värderingsaspekterna identifierades även 150 tillhörande frågeställningar. Frågeställningarna beskrev saker som var otydligt beskrivna i instruktionerna, eller som i alla fall lämnade ett stort tolkningsutrymme. Exempel på identifierade otydligheter i exemplet på värderingsaspekt är hur säkerhetsnivån i ett IT-system ska mätas och var gränsen går för när nivån ska anses vara tillräcklig.

Resultatet av studien utgjorde en start på kunskapsuppbyggnaden inom FOI för hur Försvarsmaktens arbetar med att bedöma IT-säkerheten i IT-system.

A.2 The TSAR procedure

Rapporten *The TSAR procedure* (Bengtsson m.fl., 2009a) beskriver en studie som genomfördes för att först identifiera vad som karaktäriserar analysmetoder för bedömning av IT-säkerhetsnivå och därefter skapa en procedur som kan ge stöd i att välja vilken analysmetod som bäst motsvarar aktuella behov. Proceduren skulle möjliggöra bedömning av analysmetodens *relevans* (hur väl den motsvarar behoven) och *validitet* (hur väl den avspeglar verkligheten).

I rapporten presenteras TSAR, en procedur för att karaktärisera analysmetoder genom att bedöma i vilken utsträckning de uppfyller en uppsättning med föreslagna kvaliteter. TSAR inkluderar två uppsättningar med kvaliteter som beskriver metodens relevans respektive validitet. Kvaliteterna är indelade i kategorier som täcker in allt från analysmetodens analysomfång till stödda systemmodelleringstekniker och huruvida metoden ger underlag för relaterade processer såsom kravformulering, systemutveckling och riskhantering.

Genom att bedöma tillgängliga analysmetoder med hjälp av TSAR byggs en databas upp över de olika metodernas kvaliteter. Med en databas på plats finns förutsättningarna för att vid nästa analystillfälle kunna identifiera vilken

analysmetod som bäst motsvarar behoven. Detta görs genom att behoven beskrivs i form av samma kvaliteter som användes för att beskriva metoderna. Denna önskelista över kvaliteter jämförs sedan med analysmetoderna i databasen. Jämförelsen resulterar i ett rankingvärde för hur väl varje metod motsvarar önskemålen.

A.3 Test av relevans och validitet avseende säkerhetsvärdering

Rapporten *Test av relevans och validitet avseende säkerhetsvärdering* (Bengtsson och Hallberg, 2009) beskriver en studie där relevansen och validiteten testades för Försvarsmaktens metoder för säkerhetskravställning och riskbedömningar. Studien byggde vidare på den tidigare kartläggningen av värderingsaspekter inom Försvarsmaktens IT-säkerhetsarbete (avsnitt A.1) och använde den föreslagna proceduren TSAR (avsnitt A.2) som stöd för valet av analysmetod.

Studien fokuserade på de processteg där de säkerhetsrelaterade kraven formuleras för det planerade systemet. Detta avgör till stor del vilket underlag som kommer att behöva tas fram och vilket IT-säkerhetsrelaterat arbete som kommer att behöva utföras.

Två delaktiviteter identifierades som lämpliga att testa med hjälp av TSAR för att bedöma relevans och validitet. De två aktiviteterna var *sårbarhetsanalys* och *framtagande av säkerhetskrav*. En inledande genomgång av de två delaktiviteterna resulterade i flera figurer över de arbetsmoment som skulle genomföras för varje delaktivitet samt flera frågor kring oklarheter i metodbeskrivningarna. Figurerna och oklarheterna stämdes av med personer på Försvarsmakten, antingen via intervjuer eller via e-post.

Ett tydligt resultat från användningen av TSAR var att Försvarsmaktens tillgängliga metodbeskrivningar inte hade den detaljrikedom som var nödvändig för att det skulle vara möjligt att genomföra rättvisande tester. Det framkom

även motstridiga svar i de frågeformulär som skickades ut. Det genomförda testet resulterade således i låga värden för både relevans och validitet för båda delaktiviteterna. Även om testet inte kunde ge någon rättvisande bild av huruvida rätt analysmetoder används för momenten så gav det insikt i att Försvarsmaktens tillgängliga dokumentation beskriver *vad* som ska göras, men sällan *hur* det ska genomföras.

A.4 Tester av metoder för värdering av informationssäkerhet

Rapporten *Tester av metoder för värdering av informationssäkerhet* (Bengtsson m.fl., 2009b) beskriver en studie där relevans och validitet testades för i forskningslitteraturen beskrivna metoder för värdering av informationssäkerhet. En inledande litteraturstudie resulterade i 25 identifierade metoder för värdering av informationssäkerhet där metoderna uppfyllde uppsatta urvalskriterier. Av de 25 identifierade metoderna valdes sju ut som lämpliga kandidater att testa med hjälp av proceduren TSAR (avsnitt A.3). Inför testningen gjordes en bedömning av vilka värderingsbehov som förelåg för varje steg i Försvarsmaktens IT-livscykelmodell. Behoven återspeglade vilka egenskaper en värderingsmetod behöver ha för att anses vara relevant för stegen i Försvarsmaktens IT-livscykelmodell. Syftet med testningen var både att utvärdera TSAR och att utvärdera vilka värderingsmetoder som lämpar sig bäst för respektive steg i Försvarsmaktens IT-livscykelmodell.

Resultaten från testningen visade på att ingen av de testade metoderna bedömdes ha nödvändiga egenskaper för att anses relevanta för Försvarsmakten. Under testningen blev det tydligt att det var svårt att bedöma om metoder som bara beskrevs på en övergripande nivå eller var vagt definierade hade de nödvändiga egenskaperna. En slutsats var att TSAR behöver kompletteras med fler egenskaper som behöver beskrivas ännu tydligare och indelas i fler delegenskaper.

A.5 The TSAR procedure revision 1

Rapporten *The TSAR procedure revision 1* (Bengtsson m.fl., 2010a) beskriver en uppdaterad version av proceduren TSAR som introducerades i avsnitt A.2 och testades i avsnitt A.3 och A.4. Den största skillnaden i denna uppdaterade version av TSAR var att momentet att bedöma en analysmetods validitet (hur väl metoden avspeglar verkligheten) togs bort. Den initiala tanken med TSAR var att den skulle vara ett stöd genom att ge en grovfiltrering av analysmetoder som kan tänkas motsvara analysbehoven. Att bedöma kvaliteterna som relaterar till en metods relevans kräver inte mer än en övergripande genomgång av metodbeskrivningen. Att bedöma kriterierna som relaterar till en metods validitet kräver däremot en mer djupgående studie av analysmetoden, vilket skulle motverka den initiala tanken med TSAR. Förändringen att inte bedöma validitet innebar även behov av att uppdatera de kvaliteter som definierats.

Revisionen av TSAR innebar att hela metoden kunde presenteras i en mer kortfattad rapport som helt fokuserade på att presentera proceduren och hur den används.

A.6 Framtida metoder för värdering av IT-säkerhet

Rapporten *Framtida metoder för värdering av IT-säkerhet* (Bengtsson m.fl., 2010b) beskriver en studie som syftade till att identifiera vilka typer av metoder som kan vara relevanta för Försvarsmakten att använda för att värdera IT-säkerhet. Studien utgick från de senaste årens publicerade forskningsartiklar, snarare än redan etablerade metoder, för att på så sätt identifiera de senaste tillvägagångssätten som diskuteras i forskningsvärlden. De forskningsartiklar som utgjorde underlaget var oftast inriktade på att lösa mindre delproblem snarare än att ta fram en helhetslösning för hur värdering av IT-säkerhet ska gå till. För att ge en bild av vilka inriktningar som var aktuella inom forskningen så grupperades de olika forskningsartiklarna i metodgrupper. Metodgruppernas relevans för Försvarsmakten testades sedan med hjälp av testproceduren TSAR (avsnitt A.5) för att få en uppfattning vilka inriktningar som kan vara relevanta för Försvarsmakten att använda i framtiden under respektive steg i IT-livscykelmodellen som beskrivs i DIT 04 (Försvarsmakten, 2004a).

Grupperingen av forskningsartiklar resulterade i följande fyra metodgrupper:

1. **Attackgrafer**
   Metoder som utgår från systemstruktur och kända sårbarheter för att skapa en graf över hur motståndare kan ta sig mellan olika noder i systemet.
2. **Hantering av ovisshet i värderingsunderlagen**
   Metoder som är inriktade på att hantera oklara indata. Huvudsakligen fokuserar metoderna på användandet av icke fullständiga indata.
3. **Tillståndsmodeller och simulering**
   Metoder som använder formella modelleringstekniker för att beskriva de olika tillstånd det analyserade systemet kan befinna sig i.
4. **Aggregering av värden**
   Metoder som fokuserar på problemet med att slå samman olika

säkerhetsrelaterade värden till en uppsättning sammansatta säkerhetsvärden.

I de tidiga stegen i IT-livscykelmodellen har något system oftast ännu inte realiserats, vilket innebär analysunderlag som inte är kompletta eller som innehåller ovisshet. Under dessa steg bedöms metoderna som fokuserar på hantering av inkompletta värderingsunderlag ha högst relevans.

Under de senare stegen i IT-livscykelmodellen när realiseringen av ett IT-system har påbörjats bedöms istället attackgrafsmetoderna ha störst relevans. Denna typ av metoder utgår mestadels från underlag som kan samlas in från olika typer av systemloggar eller genom att skanna av IT-systemet för att identifiera nätverkstopologi och de ingående nodernas egenskaper. För att insamlingen av underlag ska vara möjlig förutsätts att realiseringen av IT-systemet inletts.

A.7 Hot-, risk- och sårbarhetsanalys

Rapporten *Hot-, risk- och sårbarhetsanalys* (Lundholm m.fl., 2011) beskriver en studie som syftade till att skapa bättre förståelse för hur hot-, risk- och sårbarhetsanalyser genomförs inom Försvarsmakten. Studien inleddes med en litteraturstudie som fokuserade på Försvarsmaktens dokumentation för hur dessa analyser ska genomföras. Därefter genomfördes intervjuer med personer som jobbar med att genomföra dessa analyser för att få en förståelse för hur arbetet går till i praktiken. Med litteraturstudien och intervjuerna som underlag genomfördes en behovsanalys som syftade till att identifiera behovet av stöd vid genomförandet av hot-, risk- och sårbarhetsanalyserna. Behovsanalysen resulterade i 77 identifierade behov av stöd under genomförandet av analyserna.

En av de slutsatser som presenteras i rapporten är att nyttjandet av extern personal för genomförandet av analyserna påverkar den interna kunskapsnivån angående hur analysarbetet genomförs. En viktig poäng med att genomföra analyserna är att bland analysdeltagarna skapa en medvetenhet kring vilka risker

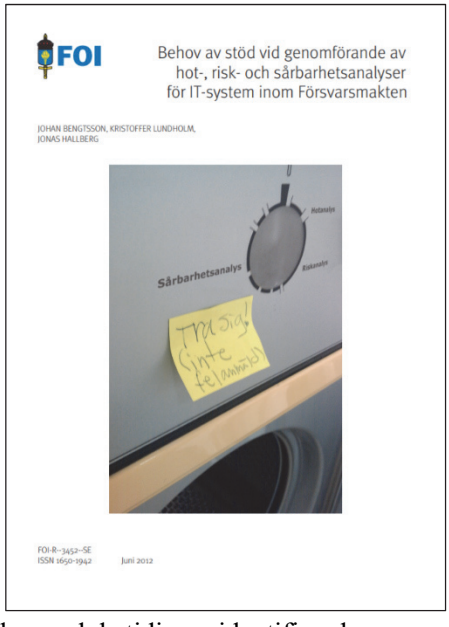
som finns med det tänkta systemet. Denna riskmedvetenhet är något som missas när den egna personalen inte genomför analysarbetet själva. Deltagande från verksamhetsrepresentanter var även något som identifierades som bristfälligt.

En annan slutsats var att det finns behov av bättre stöd vid genomförandet av hot-, risk- och sårbarhetsanalyser. Med stöd avsågs bland annat dokumentation som beskriver *hur* efterfrågade analysresultat ska tas fram samt vad resultatet på en mer detaljerad nivå egentligen förväntas vara. Den dokumentation som finns tillgänglig från Försvarsmakten beskriver till stor del *vad* som ska göras, men inte speciellt mycket om *hur* resultaten ska uppnås.

I rapporten ges följande rekommendationer till Försvarsmakten.

- **Utveckla kunskap om de faktorer som påverkar analyserna**
  Det behövs mer kunskap om hur analysarbetets subjektiva bedömningar påverkas av exempelvis tillgängligt analysunderlag, vald analysmetod, analysstöd samt vilka personer som deltar i analysarbetet.
- **Ta fram tydliga instruktioner för *hur* analyserna ska genomföras**
  Instruktionerna behöver inkludera exempel som inte bara visar enklast möjliga fall utan även visar hur mer komplexa situationer kan hanteras.
- **Tillhandahåll relevant utbildning**
  Tydlig och strukturerad utbildning av personal efterfrågas 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.
- **Ta fram stöd för nödvändiga bedömningar**
  Under analysarbetet krävs kunskap om många olika faktorer samtidigt som det krävs en förmåga att kunna sammanställa dessa faktorer till de efterfrågade analysresultaten. Ett tydligt stöd för hur bedömningarna ska genomföras kan öka analysresultatens validitet, tillförlitlighet och spårbarhet.
- **Fokusera analyserna på det specifika snarare än det generella**
  Definiera ett antal standardsystem som analyserna kan utgå ifrån. På så sätt kan analysarbetet fokuseras på det specifika, det vill säga hur aktuellt IT-system skiljer sig från standardsystemet.
- **Ta fram stöd för att avgöra verksamhetens krav på IT-säkerheten**
  Det är en komplex uppgift att avgöra vilka IT-säkerhetskrav som måste ställas för att en verksamhet ska kunna bedrivas med adekvat säkerhet. Det är nödvändigt att tydliggöra hur den uppgiften ska lösas inom ramen för såväl instruktioner som utbildning.

A.8 Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten



Rapporten *Behov av stöd vid genomförande av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten* (Bengtsson m.fl., 2012a) beskriver resultaten från en behovsanalys avseende behovet av stöd vid genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system inom Försvarsmakten. Behovsanalysen var en komplettering och revidering av den behovsanalys som presenterades i avsnitt A.7. Kompletteringen bestod av att ytterligare intervjuer genomfördes med personer som, inom ramen för sin tjänst, deltog i hot-, risk- och sårbarhetsanalyser för Försvarsmaktens IT-system. De nya behov som identifierades genom de kompletterande intervjuerna sammanfördes med de tidigare identifierade behoven för att genomföra en reviderad analys.

Den reviderade versionen av behovsanalysen innebar en tydligare gruppering av de resulterande behoven som även innebar att flertalet behov kunde kombineras. Den reviderade listan av behov omfattar 32 behov indelat i de fem kategorierna organisatoriska förutsättningar, tillvägagångssätt, kunskap, stöd vid bedömningar samt analysresultat. De fem mest uttalade behoven återges i listan nedan.

1. Behov av instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram.
2. Behov av kunskap om den verksamhet som IT-systemet ska stödja.
3. Behov av egen personal inom Försvarsmakten som har tid och kompetens att genomföra analyserna.
4. Behov av stöd för att bedöma sannolikhet för realisering av hot.
5. Behov av stöd för att bedöma konsekvens vid realisering av hot.

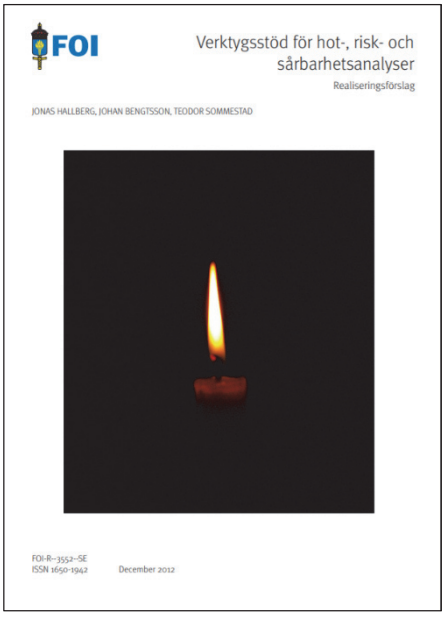
A.9 Varför följer inte användarna bestämmelser?

Rapporten *Varför följer inte användarna bestämmelser?* (Sommestad m.fl., 2012) beskriver den första vetenskapliga sammanställningen[8] som gjorts av forskningen om vad som påverkar huruvida användare följer informationssäkerhetsbestämmelser. Det verkar som att viktiga faktorer är användarnas attityd, hur användarna upplever rådande normer, vilka konkurrerande behov till att följa bestämmelserna användarna ser, huruvida användarna upplever att de har rätt att bryta mot bestämmelserna (eftersom de är så bra på annat) och om användarna tycker att det är bra för säkerheten att följa bestämmelserna. Mindre viktiga faktorer verkar vara användarnas upplevelser av sanktioner, belöningar och hot. Rapporten noterar samtidigt att dessa resultat är ganska preliminära och att det behövs mer forskning på området.

Att mäta hur användare faktiskt beter sig när påverkansfaktorerna ändras är svårt och de flesta utvärderingar baseras istället på enkätundersökningar där användarna svarar om de har för avsikt att följa bestämmelserna (som de kanske inte ens känner till). Vilka faktorer som påverkar och hur starkt de påverkar kan också vara olika exempelvis från person till person, eller i olika kontexter. Upplever till exempel användarna att de inte känner till varandras normer kan de ju inte agera på dessa normer utan andra påverkansfaktorer får rimligen spela en större roll.

[8] Rapporten baserades på en akademisk forskningsartikel (Sommestad m.fl., 2014) som togs fram i projektet.

A.10 Verktygsstöd för hot-, risk- och sårbarhetsanalyser

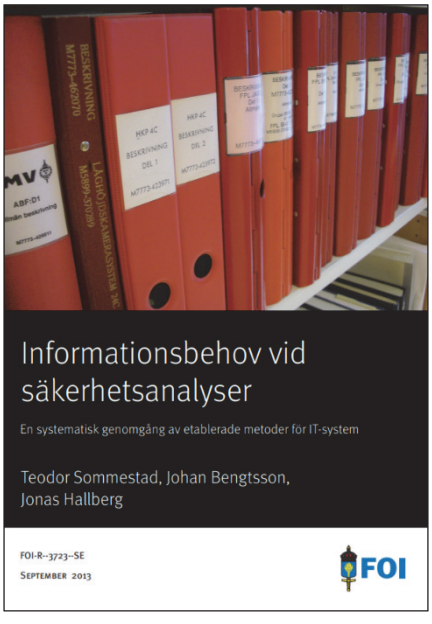


Rapporten *Verktygsstöd för hot-, risk- och sårbarhetsanalyser* (Bengtsson m.fl., 2012b) beskriver en studie vars syfte var att ge Försvarsmakten konkreta förslag på hur de 32 behov av stöd vid genomförandet av hot-, risk- och sårbarhetsanalyser som identifierades i avsnitt A.8 skulle kunna mötas med hjälp av ett mjukvaruverktyg. Studien resulterade i mer än 20 realiseringsförslag som tillsammans bedömdes kunna möta de flesta av de 32 identifierade behoven av stöd. Realiseringsförslagen kategoriserades utifrån vilket arbetsmoment de berörde.

Utöver realiseringsförslagen identifierades även några forskningsfrågor. Forskningsfrågorna lyfte bland annat fram att det för verksamhetsanalysen behöver undersökas i vilken utsträckning den resulterande verksamhetsbeskrivningen i dagsläget påverkar hot-, risk- och sårbarhetsanalysen samt efterföljande aktiviteter. Det behöver även undersökas vad verksamhetsbeskrivningen behöver innehålla för att kunna få önskad inriktning av efterföljande aktiviteter, samt vilka underlag som krävs för att genomföra en sådan verksamhetsanalys. Dessutom behöver det undersökas vilket underlag som krävs för att möjliggöra identifiering av relevanta hot och vilken precision riskvärdena behöver ha för att de ska vara meningsfulla. Slutligen behöver det även undersökas vilket underlag som krävs för att kunna genomföra analysen med önskvärd precision.

På en övergripande nivå lyftes det fram att det för verksamhetsanalys så väl som för hot-, risk- och sårbarhetsanalys behöver undersökas i vilken utsträckning analysgruppens sammansättning påverkar analysresultaten. Det behöver även undersökas hur nyttan med ett planerat IT-system kan kvantifieras för att tillhandahålla mer utav en helhetsbedömning.

A.11 Informationsbehov vid säkerhetsanalyser



Rapporten *Informationsbehov vid säkerhetsanalyser* (Sommestad m.fl., 2013) beskriver en studie av hur säkerhetsanalyser (riskbedömning och identifiering av lämpliga skydd) ska genomföras. Ett antal etablerade metoder i forskningslitteraturen gås igenom med slutsatsen att dessa metoder inte uttryckligen baseras på teorier och ibland baseras de inte ens implicit på teorier. Detta innebär en svårighet att välja mellan metoderna. Dessutom observeras att metoderna förmodligen kräver anpassning för varje organisation som ämnar använda dem.

Rapporten observerar också att en central svårighet i analyserna är vilken information som ska ligga till grund för dem. Det kan lätt bli dyrt att samla in information och normalt måste prioriteringar göras angående vilken information som ska samlas in. Exempelvis går det kanske inte alls att få kunskap om vissa saker såsom antagonisters avsikter. En svårighet kopplat till detta är att det finns många olika intressenter och roller. Rapporten ställer också frågan hur man ska gå tillväga när det enligt de gängse metoderna finns flera systemägare och besvarar denna fråga med att man bör försöka få ner antalet ägare till en per tillgång och i övrigt använda modulering och prioritering. Ytterligare en slutsats är att bara ungefär en sjundedel av den nödvändiga informationen är säkerhetsspecifik (exempelvis om hot, sårbarheter och skyddsåtgärder). Vidare efterfrågar metoderna generellt information om verksamheten hellre än informationen systemet ska behandla, vilka beteenden som är tänkbara rörande systemet och vilka tekniska lösningar som ska finnas.

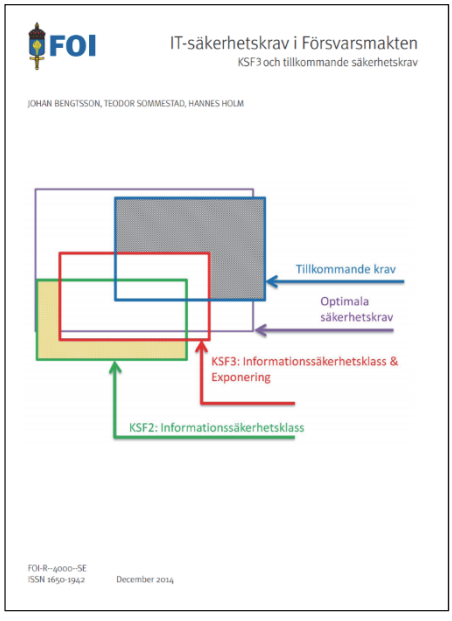
En slutsats är att Försvarsmakten bör fundera på hur detaljerade analyserna behöver vara jämfört med att mer standardiserade analyser utförs. Kopplat till detta är också vilka lärdomar man tänker sig att utföraren ska kunna dra, eftersom mer standardiserade analyser leder till färre möjliga lärdomar än mer anpassade analyser.

A.12 Effektivare hot-, risk- och sårbarhetsanalyser

Rapporten *Effektivare hot-, risk- och sårbarhetsanalyser* (Hallberg m.fl., 2013) ger en sammanställning och diskussion av de resultat som framkommit under åren 2011–2013 (A.7–A.11). Följande resultat lyfts särskilt fram:

- Det finns en stor uppsättning behov kopplade till stöd vid genomförandet av hot-, risk- och sårbarhetsanalyser, exempelvis avseende instruktioner som tydligt beskriver vad analysresultaten ska innehålla samt hur dessa resultat ska tas fram.
- Det finns inga befintliga ramverk framtagna av andra aktörer som direkt kan nyttjas för att effektivisera Försvarsmaktens analyser. Om ett befintligt ramverk ska nyttjas måste det anpassas.
- Inom Försvarsmakten finns intresse för IT-baserade verktyg som stödjer ett strukturerat genomförande. Det finns även intresse av att medverka i framtagande av behovs- och kravbilder för ett sådant verktyg.
- Det finns flera möjligheter att realisera funktioner i ett IT-baserat verktyg som kan stödja och effektivisera genomförandet.
- Det finns behov av att vetenskapligt testa och undersöka antaganden och teorier som ligger till grund för nuvarande praxis som omger hot-, risk- och sårbarhetsanalyser.

A.13 IT-säkerhetskrav i Försvarsmakten



Rapporten *IT-säkerhetskrav i Försvarsmakten* (Bengtsson m.fl., 2014) beskriver en studie som analyserade ett antal genomförda säkerhetsmålsättningar (riskhanteringsprocesser) för att undersöka hur väl version 3.0[9] av KSF, Krav på IT-säkerhetsförmågor hos IT-system (Försvarsmakten, 2012) täcker in de resulterande säkerhetskraven. KSF utgör en uppsättning generella säkerhetskrav som styr och vägleder. Det visade sig att de krav som framgick av de genomförda säkerhetsmålsättningarna bara till hälften utgjordes av sådana generella KSF-krav. Studien försökte därför bidra med nya generella säkerhetskrav som skulle kunna utgöra en del av en ny version av KSF. Det visade sig dock vara komplicerat på grund av svårigheten att hitta en balans mellan en generell (högre) nivå som ändå vägleder och en mer specifik (lägre) nivå som snarare pekar ut produkter. En annan utmaning med detta var att medan KSF-kraven var välformulerade, var de tillkommande kraven mindre välformulerade. Särskilt komplicerade att hantera var de tillkommande kraven rörande tillgänglighet. En tredjedel av dessa rörde icke-antagonistiska hot och mer än hälften handlade om fysiska skydd.

Förutom att undersöka genomförda säkerhetsmålsättningar studerades också den akademiska forskningslitteraturens modeller. Dessa hade dock en mer specifik (lägre) abstraktionsnivå för tillgänglighetsaspekter och hade samtidigt mindre fokus på antagonister. Vidare var abstraktionsnivån också annorlunda rörande spårbarhet. För riktighet däremot observerades en tillräcklig matchning redan idag mellan forskningslitteraturs modell och KSF.

Rapporten beskriver också en undersökning av hur kraven i KSF kan omvandlas till standardlösningar som utgår ifrån vanliga komponenter och procedurer. Rekommendationen blev att KSF borde kompletteras med designmönster och produkter som möter kraven, även om en sådan komplettering inte kan vara fullständig. Rapporten noterar också att det inte är rättframt att hantera

[9] Nu gällande version är 3.1 (Försvarsmakten, 2014).

sammansatta system utifrån KSF. Användning av andra aktörers system gör att kravmassan ökar, exempelvis på grund av avtalskrav.

A.14 Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker

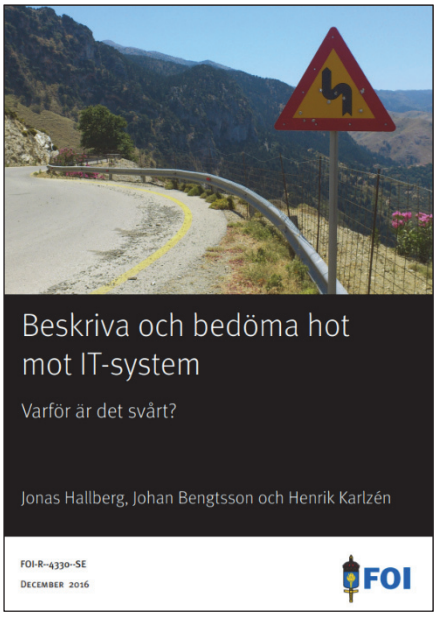
Rapporten *Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker* (Hallberg m.fl., 2015) beskriver en studie av hur bedömningar av hots sannolikhet och konsekvens varierade inom Försvarsmakten. En behovsanalys genomfördes för att hitta metodförbättringar. Behovsanalysen visade bland annat på att det fanns flera metoder att utgå ifrån och att det var otydligt vilken som skulle väljas. Dessutom visade analysen ett behov av att kunna jämföra olika hot för att bättre kunna prioritera vilka hot som främst behövde skyddas mot.

Utifrån behovsanalysen togs en jämförbarhetsbaserad metod fram där relativa bedömningar först görs, före konvertering till det absoluta. Den jämförelsebaserade metoden (baserad på Analytical Hierarchy Process, AHP) jämfördes med den klassiska i ett experiment. Eftersom det saknades ett rätt svar, fick mer samstämmighet mellan bedömare (tillsammans med mindre kognitiv belastning, det vill säga svårighet, möda och behövd tid) vara måttet på vilken metod som fungerade bäst. Den använda jämförelsebaserade metoden visade sig inte vara bättre än den klassiska, men förslag på en bättre jämförelsebaserad metod gavs. Exempelvis kan en annan skala användas som väger detaljeringsgraden mot att det mer detaljerade är svårare att hantera. Vidare är det oklart hur översättning från relativa till absoluta vikter bör göras.

Rapporten nämner också att behovsanalysen visade på att analysen behöver vara spårbar och att analysens resultat behöver kunna visualiseras. Som ett svar till detta implementerades den valda jämförelsebaserade metoden i verktygsstödet Sublime (avsnitt B.3), vilken ger fördelar vad gäller visualisering och anpassningsbarhet. Rapporten drar till sist en slutsats om att skyddsåtgärdernas

effekt på riskerna behöver kunna bedömas för att avgöra om föreslagna skydd minskar riskerna tillräckligt mycket.

A.15 Beskriva och bedöma hot mot IT-system



Rapporten *Beskriva och bedöma hot mot IT-system* (Bengtsson m.fl., 2016) beskriver en studie som konstaterar att det finns ett behov av att undvika personberoende när det gäller hot-bedömningar för IT-system. För att undvika beroendet av en enskild bedömare, måste samstämmigheten mellan olika bedömare ökas. Att förbättra metoden för riskbedömning ligger då nära till hands. Två olika tester för att öka samstämmigheten gjordes.

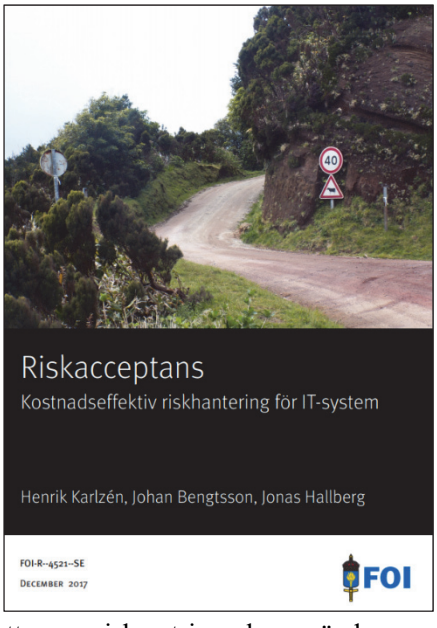
Det ena testet ställde en traditionell metod mot en jämförelsebaserad hotbedömning och utvärderade detta i ett experiment. Den jämförelsebaserade visade sig vara bättre än den traditionella när experter (snarare än lekmän) gjorde bedömningarna. Samtidigt noterades att det med en jämförelsebaserad metod kan bli ett stort antal bedömningar som ska göras om alla hot ska jämföras med varandra. Samtidigt blir metoden inte tillförlitlig nog om det minimala förhållningssättet används där varje hot enbart bedöms mot ett annat hot. En annan observation var att det finns ett behov av att jämförda (relativa) prioritetsvärden översätts till absoluta sådana, även om det inte är uttryckligen nödvändigt enligt Försvarsmaktens process (metod) där absoluta bedömningar visserligen ska tas fram, men utan att användas. Vidare observerades att det är en utmaning att välja antal steg i bedömningsskalan. Rapporten beskriver försök att hitta den bästa skalan med resultatet att det beror på hur exakt bedömning som behövs. För niogradiga skalor verkar en skala baserad på geometrisk progression (där varje nästa steg i skalan utgör en viss multipel, större än ett, av nuvarande steg) bäst.

Ingen relevant tidigare forskning kunde hittas om hur hotbeskrivningar bör utformas och vad de bör innehålla. Det gjordes därför ett test rörande utformningen av hotbeskrivningar. Testet jämförde strukturerade tabeller (enligt den gängse metoden) med löpande text för hotbeskrivningars utformning.

Löpande text antogs vara enklare att förhålla sig till, samtidigt som det troligen skulle lämna större tolkningsutrymme. Inga statistiskt signifikanta skillnader mellan metoderna erhölls dock. Några möjliga störvariabler undersöktes. Kanske skillnad i respondenters upplevda ovisshet rörande deras bedömningar spelade roll. Respondenter som var mer ovissa på sina bedömningar verkar via sparbenägenhet också sätta lägre siffror för konsekvenserna (vilket leder till att färre skydd behöver köpas). Alternativt leder ovissheten till mer försiktiga bedömningar nära snittet. En annan möjlighet är att en del respondenter är mindre bekväma med att ta risker och att de därför väljer högre siffror för riskerna. Det är också möjligt att hotbeskrivningarna varit alltför otydliga, kanske på grund av att fiktiva scenarier använts. Ett förslag var att utöka Försvarsmaktens analysmetod med informationselementet *tillvägagångssätt* för att förtydliga.

Rapporten gör några ytterligare observationer. En är att det är svårt att avgöra vilket omfång/vilka systemgränser och vems perspektiv som ska användas vid analys av ett IT-system, särskilt som dagens IT-system tenderar att vara sammankopplade. En annan observation är att det inte framgår vilka hot som redan hanterats av den generella uppsättningen krav i KSF v3.1 (Försvarsmakten, 2014), vilket försvårar identifierandet av hot alternativt skapar dubbelarbete. Kopplat till detta noteras det att hotkataloger kan snabba på processen, även om de kan leda till slentrian. Och om inte alla har samma katalog blir förutsättningarna för olika bedömare olika och personberoendet ökar.

A.16 Riskacceptans



Rapporten *Riskacceptans* (Karlzén m.fl., 2018a) beskriver en studie som fortsatte på flera saker tidigare studier tagit upp. Exempelvis nämns problemet med att bedömningar (exempelvis av risk) är personberoende. Även när enbart experter anlitas kan personberoende finnas, bland annat genom att experter faller tillbaka på sina värderingar när de inte kan förlita sig på sin expertis. Rörande personberoende finns också aspekten riskbenägenhet, vilket är en faktor som behöver utredas vidare. För att minska personberoendet krävs dialog med olika intressenter. För att uppnå god dialog mellan exempelvis beslutsfattare och säkerhetsexperter kan det vara fördelaktigt med en visualisering av analysresultaten. Försiktighet måste då iakttas om riskmatriser ska användas eftersom de fungerar dåligt när det råder negativ korrelation mellan konsekvens och sannolikhet. Angående redovisningen är en trend i forskningen att tillförlitligheten bedömaren har till sina bedömningar, liksom underliggande antaganden, ska framgå. Rapporten tar också upp svårigheten med att avgöra var systemgränsen ska gå, det vill säga vad som ingår i systemet som en risk-bedömning ska beakta.

Rapportens huvudfokus är riskacceptans och det noteras att forskningen om riskacceptans är omogen. Detta innebär att mer fokus bör läggas på att klarlägga det konceptuella med exempelvis terminologi och bedömningsgrunder, snarare än på mer kvantitativa frågor. Det noteras även att riskhantering är ett dåligt verktyg för att öka informationssäkerheten (men att det inte finns något bättre alternativ). I vissa fall verkar det vara bättre att gå ifrån en strikt strukturerad (aktuarisk) metod och istället använda en mer ostrukturerad men situationsanpassad metod. En möjlighet är också att lägga fokus på generella erfarenheter om vilka säkerhetsskydd och vilket säkerhetstänk som krävs (traditionella säkerhetsprinciper).

Vidare framgår att alltför mycket fokus lagts på att minska risker, utan att väga in kostnaden för att minska risken, såsom hur nyttan minskas på grund av skydden, eller att skydden inte minskar risken utan istället möjliggör ökad nytta

för samma risknivå som tidigare, eller hur mycket skydden kostar att köpa. Riskacceptans måste väga in risker, kostnader och nyttor. För att väga dessa aspekter mot varandra krävs att organisationens övergripande behov lyser igenom i riskacceptanskriterier som präglar hela riskhanteringsprocessen. Dessutom behövs en översättning mellan olika enheter, som exempelvis kronor och människoliv.

Eftersom det är svårt att utföra riskbedömningar kan det vara lämpligt att genomföra bedömningarna igen efter en viss tid. Detta är också viktigt med tanke på att IT-system utvecklas i rask takt och omvärlden förändras. En möjlig förenkling till att göra fullständiga riskbedömningar är att säkerställa att ett nytt system i alla fall inte är sämre än ett befintligt. Det är då viktigt att inte kraven på nya system är alltför höga samtidigt som befintliga system kommer undan den förändrade kravställningen. En annan möjlig förenkling är att inte göra analyserna mer exakta än de behöver vara. Eftersom analyserna ofta ligger till grund för att välja skydd, är det relevant att undersöka hur specifika skydden är och i vilken mån en mer exakt riskbedömning gör det lättare att välja skydd. Mer generella riskbedömningar skulle också göra bedömningarna enklare att genomföra och kommunicera.

Rapporten lyfter också fram det speciella med antagonister inom IT-säkerhet. IT-systemen gör det möjligt att verka på avstånd, anonymt, utan att det märks så mycket och med automatisering. Hotet är alltså svårhanterligt och det görs inte enklare av att antagonisterna är svåra att modellera, exempelvis på grund av att deras upplevelser av exempelvis möjliga vinster och straffande skydd spelar roll. Om den möjliga vinsten ökar, ökar förmodligen också intentionen att angripa, vilket gör att det finns ett samband mellan sannolikheten för att drabbas av ett visst angrepp och de möjliga konsekvenserna av angreppet. Ett sätt som föreslagits för att modellera förhållandet mellan antagonister och försvarare är spelteori.

A.17 Beskrivning av hot vid säkerhetsanalyser

Rapporten *Beskrivning av hot vid säkerhetsanalyser* (Hallberg m.fl., 2018) beskriver en studie av vad en hotbeskrivning bör innehålla och hur den bör presenteras. Från den närliggande kravformulerings-forskningen identifierades principer som kan vägleda utformningen av hotbeskrivningar. Dessa principer säger bland annat att krav ska formuleras på enhetlig form, inte innehålla vaga ord, och vara spårbara tillbaka till källan till kravet. Vidare beskrivs vilka informationselement som olika typer av standarder anser att hotbeskrivningar bör bestå av.

Rapporten lyfter också fram att en verksamhet och dess tillgångar kan kategoriseras på olika sätt och därmed identifiera möjliga hot mot verksamheten och tillgångarna. Två möjliga uppsättningar informationselement för hotbeskrivningar (med skillnaden om aktören var specificerad eller ej) valdes ut och utvärderades med en enkät för att se vilken som gav mer samstämmighet mellan bedömare. En slutsats var att aktören behöver specificeras mer detaljerat, exempelvis avseende kapacitet, intention och tillfälle. Det är dock svårt att avgöra hur väl resultatet motsvarar verkligheten eftersom studien enbart baserades på fiktiva scenarier. Dessutom noterades att det är enklare att bedöma konsekvens än sannolikhet.

A.18 Verksamhetsanalys

Rapporten *Verksamhetsanalys* (Karlzén m.fl., 2019) beskriver en studie av verksamhetsanalyser och hur de kan förbättras. Verksamhetsanalyser utgör grunden för riskbedömning. I verksamhetsanalyser analyseras befintlig eller planerad verksamhet och analysen resulterar i en verksamhetsbeskrivning. Denna rapport syftar till att skapa bättre förutsättningar att utföra och redovisa de verksamhetsanalyser som görs i Försvarsmakten vid framtagandet av nya IT-system. Närmare bestämt undersöktes vad verksamhetsanalyser kan bidra med i ett informations-säkerhetsperspektiv, hur analyserna bör genomföras och vilka informationsmängder som bör ingå. Rapporten baseras på dokument från Försvarsmakten och civila myndigheter, akademiska forskningsartiklar samt intervjuer med personer som utför verksamhetsanalyser.

Likheter och skillnader mellan Försvarsmaktens dokument och de övriga informationsskällorna extraherades och analyserades. I Försvarsmaktens dokument nämns inte ekonomiska aspekter i samband med verksamhetsanalys. Det är möjligt att ekonomiska aspekter aktualiseras först senare i processen när kostnaderna för skydd ska tas hänsyn till eller att säkerheten alltid går före, varför ekonomin är närmast irrelevant. Det är möjligt att det är av samma skäl som Försvarsmaktens texter om verksamhetsanalys inte inkluderar aspekter som avtal, kontrakt, leverantörer och kunder. En annan skillnad mellan Försvarsmaktens dokument och forskningslitteraturen är att Försvarsmakten har mer säkerhetsfokus och framförallt mer informationssäkerhetsfokus. I intervjuerna framkom i kontrast med litteraturen en farhåga om att förlitandet på färdiga mallar och checklistor kan ge slentrianmässiga analyser som missar viktiga specifika delar.

En slutsats är att Försvarsmakten bör lyfta fram att verksamhetsanalyser inte bara används inför riskbedömningar utan även kan vara upphovet till att förändringar av verksamheten inleds såsom satsningar på nya IT-system. Med andra ord borde analysen åtminstone till del göras före IT-systemet ens är påtänkt. En annan slutsats är att de som utför analyserna bör ha gedigen

erfarenhet om verksamheten och att vikten av kommunikation och olika sorters granskning betonas. Kopplat till detta bör också analysernas göras om när relevanta förändringar skett av verksamhet eller omvärld. En sista slutsats är att det saknas stöd i Försvarsmaktens dokument för hur analyserna ska genomföras och särskilt för faktorer som verksamhetens vision, ekonomi och kultur. För att undvika problem med slentrian och konfidentialitet behövs en utvärdering som hittar rätt avvägning mellan att tillhandahålla standardiserade beskrivningar eller mallar och att ge allmänna råd och inspiration.

Bilaga B. Övriga producerade resultat

I denna bilaga listas de dokument som utöver FOI-rapporter producerats i projekten. Dessa innefattar FOI-memon (B.1) och vetenskapliga bidrag (B.2) som publicerats i en akademisk tidskrift eller presenterats vid akademisk konferens. Dessutom beskrivs verktygsstödet Sublime (B.3) som delvis har utvecklats inom ramen för projekten.

B.1 FOI-memon

Bengtsson, J. 2009. Sammanfattning av Workshop avseende samverkan gällande lägesförståelse informationsarenan. FOI MEMO 2829. Totalförsvarets forskningsinstitut.

Bengtsson, J. 2009. Avrapportering milstolpe Q3. FOI MEMO 2930. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J., Hunstad, A., Lundholm, K. 2010. Transfer av resultat till Försvarsmakten. FOI MEMO 3201. Totalförsvarets forskningsinstitut.

Sundmark, T., Lundholm, K., Bengtsson, J., Hallberg, J. 2010. Test of Security assessment relevance – demonstrator. FOI MEMO 3262. Totalförsvarets forskningsinstitut.

Bengtsson, J. 2010. Workshop IT-säkerhetsforskning Enköping 2010. FOI MEMO 3324. Totalförsvarets forskningsinstitut.

Hallberg, J., Hallberg, N. 2011. Reserapport—IEEE International Systems Conference 2011. FOI MEMO 3567. Totalförsvarets forskningsinstitut.

Lundholm, K., Bengtsson, J., Hunstad, A., Sundmark, T, Hallberg, J. 2011. Litteraturstudie – Riskhanteringsmetoder. FOI MEMO 3608. Totalförsvarets forskningsinstitut.

Lundholm, K., Bengtsson, J., Hallberg, J. 2011. Studie av ett IT-säkerhetsproblem. FOI MEMO 3788. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J. 2012. Seminariedag 2011 – Diskussion angående genomförandet av hot-, risk- och sårbarhetsanalyser för IT-system. FOI MEMO 3885. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J. 2013. Workshop: Nytt säkerhetsanalysverktyg. FOI MEMO 4484. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J. 2013. Workshop om säkerhetsanalysverktyg. FOI MEMO 4485. Totalförsvarets forskningsinstitut.

Bengtsson, J., Gustafsson, T., Hallberg, J., Jacob Löfvenberg, Lars Westerdahl. 2013. Seminariedag 2013. FOI MEMO 4656. Totalförsvarets forskningsinstitut.

Bengtsson, J. 2014. Infoblad för Effektivare hot-, risk- och sårbarhetsanalyser. FOI MEMO 4817. Totalförsvarets forskningsinstitut.

Bengtsson, J. 2014. Bedömning och analys av IT-system – Q1 och Q2 2014. FOI MEMO 4984. Totalförsvarets forskningsinstitut.

Bengtsson, J. 2014. Infoblad för projektet Bedömning och analys av IT-system. FOI MEMO 5208. Totalförsvarets forskningsinstitut.

Lindahl, B., Bengtsson, J. 2014. Visualisering av risker i Sublime. FOI MEMO 5218. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J. 2017. Experter är mer samstämmiga när en jämförelsebaserad metod används. FOI MEMO 6011. Totalförsvarets forskningsinstitut.

Bengtsson, J., Hallberg, J. 2019. Jämförelsebaserad riskbedömning. FOI MEMO 5683. Totalförsvarets forskningsinstitut.

B.2 Akademiska forskningsartiklar

Nedan anges de akademiska forskningsartiklar projekten producerat. För varje artikel finns också det S-nummer som används för att referera till artikeln i FOI:s system.

Hallberg, J., Bengtsson, J., Hallberg, N. 2008. Modeling and assessment of systems security. MODSEC@ MoDELS. (FOI-S--2969--SE).

Bengtsson, J., Hallberg, J., Sundmark, T., Hallberg, N. 2009c. Assessment of IT security in emergency management information systems. Fifteenth International Conference on Distributed Multimedia Systems. (FOI-S--3172--SE).

Löf, F., Stomberg, J., Sommestad, T., Ekstedt, M., Hallberg, J., Bengtsson, J. 2010. An approach to network security assessment based on probalistic relational models. First Workshop on Secure Control Systems (SCS-1). (FOI-S--3388--SE).

Sommestad, T., Hallberg, J. 2012. Cyber security exercises and competitions as a platform for cyber security experiments. NordSec. (FOI-S--4218--SE).

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J. 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security vol. 22:1. (FOI-S--4675--SE).

Korman, M., Ekstedt, M., Sommestad, T., Hallberg, J., Bengtsson, J. 2014. Overview of Enterprise Information Needs in Information Security Risk Assessment. IEEE EDOC – Enterprise Computing Conference. (FOI-S--4984--SE).

Holm, H., Sommestad, T., Bengtsson, J. 2015. Requirements Engineering: The quest for the dependent variable. IEEE International Requirements Engineering Conference. (FOI-S--5168--SE).

Karlzén, H., Bengtsson, J., Hallberg, J. 2017. Assessing Information Security Risks Using Pairwise Weighting. International Conference on Information Systems Security and Privacy. (FOI-S--5663--SE).

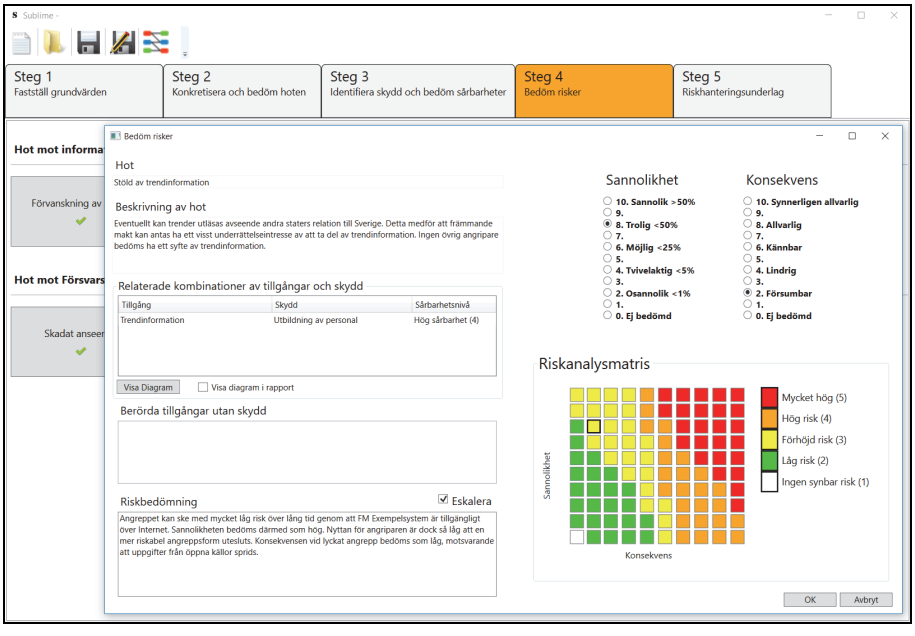
Hallberg, J., Bengtsson, J., Hallberg, N., Karlzén, H., Sommestad, T. 2017. The Significance of Information Security Risk Assessments Exploring the Consensus of Raters' Perceptions of Probability and Severity. International conference on Security and Management. (FOI-S--5782--SE).

Karlzén, H., Bengtsson, J., Hallberg, J. 2018b. A Test of Structured Threat Descriptions for Information Security Risk Assessments. International Conference on Information Systems Security and Privacy. (FOI-S--5827--SE).

B.3 Verktygsstödet Sublime

En programvara utvecklades som en del i arbetet med att studera vilket verktygsstöd som behövs för genomförandet av riskbedömningar. Verktygsstödet går under namnet Sublime och är en implementation av Försvarsmaktens gemensamma riskhanteringsmodell (Försvarsmakten, 2009).[10] Syftet med att utveckla Sublime var först och främst att visa på hur en programvara av detta slag kan komplettera befintliga metodhandböcker och stödja både de personer som genomför analysarbetet och de personer som därefter ska granska analysresultaten eller fatta beslut baserat på dessa. Det finns således en tydlig koppling till de behov av stöd vid genomförandet av analyserna som identifierades i rapporten som beskrivs i Bilaga A, avsnitt A.8.

[10] Anledningen till att Försvarsmaktens gemensamma riskhanteringsmodell valdes var att Sublime togs fram tillsammans med ett annat projekt som genomfördes åt *Försvarsmaktens arbetsgrupp för säker och rationell informationshantering* (FM AgSäkRatIH) där Försvarsmaktens gemensamma riskhanteringsmodells applicerbarhet för analys av IT-system skulle undersökas.



Figur 8: Bedömning av risker i Sublime.

Sublime är uppbyggt utifrån metodens fem steg där olika deluppgifter ska genomföras. Första steget syftar till att fastställa grundvärden för analysarbetet genom att exempelvis beskriva verksamheten, skyddsvärda tillgångar samt vilka skalor som ska användas vid bedömningarna. I steg två definieras de konkreta hoten mot de skyddsvärda tillgångarna för att därefter i steg tre definiera skydden. I steg fyra, görs bedömningen av sannolikhet och konsekvens för det aktuella hotet (Figur 8). I steg fem visualiseras analysresultaten.

Sublime stödjer den som ska genomföra analysen genom att arbetet struktureras enligt den givna metoden och att den information som är relevant att ta del av vid varje bedömning finns tillgänglig. Ett exempel återges i Figur 8 där risken ska bedömas. För att stödja bedömningen av sannolikheten och konsekvensen visas informationen från tidigare steg i metoden som har koppling till aktuellt hot, som exempelvis en beskrivning av hotet och de skydd som anges påverka hotet. Den som genomför analysen får även en överblick av arbetet genom att det i översiktsvyn går att se hur långt arbetet har kommit med varje uppgift.

När analysarbetet väl genomförts och befintliga risker bedömts vara på en acceptabel nivå behöver någon typ av rapport eller beslutsunderlag skapas. I Sublime kan rapporten automatiskt genereras i Word-format utifrån den information som matats in i programmet under analysarbetets gång. Denna funktionalitet underlättar inte enbart för den som genomföra analysarbetet utan

även för den som ska granska analysresultaten. Om analysresultaten presenteras på ett gemensamt format underlättas granskningen då granskaren känner igen strukturen och då lättare kan hitta de delar som är av intresse att granska. Vid en fortsatt utveckling av Sublime skulle det vara möjligt att i programmet generera resultaten i enlighet olika mallar för att anpassa representationen till målgruppen. Exempelvis skulle en beslutsfattare kunna vara mer intresserad av att se de övergripande analysresultaten, medan en granskare har större intresse av att få ta del av alla underliggande detaljer.

Utöver att visa på hur ett verktygsstöd som stödjer analysarbetet skulle kunna utformas har Sublime även använts för att testa olika forskningsresultat som framkommit. Ett exempel är det jämförelsebaserade bedömningssätt som beskrivs i Bilaga A, avsnitt A.14. Utöver att i en rapport beskriva ett alternativt sätt att genomföra bedömningar, implementerades tillvägagångssättet i Sublime så att den praktiska nyttan gick att utvärdera. Genom att praktiskt kunna utvärdera jämförelsebaserade bedömningar gick det lättare att identifiera för- och nackdelar med tillvägagångssättet. Det blev även lättare att på ett tydligt sätt presentera resultaten med en visuell representation.

I dagsläget sker ingen utveckling av Sublime inom ramen för projektet, men inom ett internfinansierat projekt på FOI utvecklas en ny version av Sublime som baseras på Försvarsmaktens metod för säkerhetsanalys.

Denna rapport sammanfattar studier inom *riskhantering för IT-system* som bedrivits på FOI de senaste tolv åren (2008–2019). Studierna har finansierats av Försvarsmaktens anslag för forskning och teknikutveckling (FoT) och haft syftet att genom forskning förbättra Försvarsmaktens arbete med att analysera säkerheten i deras IT-system.

Några av de viktigare slutsatserna från studierna är att: det finns behov av att upprätthålla kunskapsnivån om riskbedömningar inom Försvarsmakten; det finns behov av tydligare instruktioner för hur riskhanteringsarbetet ska genomföras; andra vedertagna metoder för riskhantering är av begränsad nytta för Försvarsmakten då stora anpassningar krävs för att de ska kunna användas; IT-säkerhetsexperters bedömningar är mer samstämmiga om jämförelsebaserade metoder används istället för nuvarande tillvägagångssätt.

Det finns flera viktiga frågor som uppstått till följd av studierna och som lämnats obesvarade:

- Hur stor skillnad blir det normalt mellan resultat från riskbedömningar för två olika IT-system?
- Hur beständiga är riskbedömningar över tid och hur ska man hålla sig underrättad om förändringar som sker av system, hot och kontext?
- Hur stor skillnad medför olika riskbedömningsresultat senare i processen i form av rekommenderade skyddsåtgärder?
- Hur ska riskbedömningarna likriktas samtidigt som unika insikter tillvaratas?

FOI

ISSN 1650-1942

www.foi.se